```
./build/output/kernel.exe: file format elf32-i386

Disassembly of section .text:

c0101000 <bswap_16>:
c0101000: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c0101004: 86 e0                         xchg ah, al
c0101006: c3                            ret

c0101007 <bswap_32>:
c0101007: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c010100b: 86 e0                         xchg ah, al
c010100d: c1 c0 10                      rol eax, 16
c0101010: 86 e0                         xchg ah, al
c0101012: c3                            ret

c0101013 <bswap_64>:
c0101013: 8b 54 24 04                   mov edx, dword ptr [esp + 4]
c0101017: 86 f2                         xchg dh, dl
c0101019: c1 c2 10                      rol edx, 16
c010101c: 86 f2                         xchg dh, dl
c010101e: 8b 44 24 08                   mov eax, dword ptr [esp + 8]
c0101022: 86 e0                         xchg ah, al
c0101024: c1 c0 10                      rol eax, 16
c0101027: 86 e0                         xchg ah, al
c0101029: c3                            ret

c010102a <toupper>:
c010102a: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c010102e: 8d 50 9f                      lea edx, [eax - 97]
c0101031: 83 fa 19                      cmp edx, 25
c0101034: 77 03                         ja 0xc0101039 <toupper+0xf>
c0101036: 83 e8 20                      sub eax, 32
c0101039: c3                            ret

c010103a <tolower>:
c010103a: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c010103e: 8d 50 bf                      lea edx, [eax - 65]
c0101041: 83 fa 19                      cmp edx, 25
c0101044: 77 03                         ja 0xc0101049 <tolower+0xf>
c0101046: 83 c0 20                      add eax, 32
c0101049: c3                            ret

c010104a <isalpha>:
c010104a: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c010104e: 83 e0 df                      and eax, -33
c0101051: 83 e8 41                      sub eax, 65
c0101054: 83 f8 19                      cmp eax, 25
c0101057: 0f 96 c0                      setbe al
c010105a: 0f b6 c0                      movzx eax, al
c010105d: c3                            ret

c010105e <isalnum>:
c010105e: 8b 54 24 04                   mov edx, dword ptr [esp + 4]
c0101062: 52                            push edx
c0101063: e8 e2 ff ff ff                call 0xc010104a <isalpha>
c0101068: 59                            pop ecx
c0101069: 89 c1                         mov ecx, eax
c010106b: b8 01 00 00 00                mov eax, 1
c0101070: 85 c9                         test ecx, ecx
c0101072: 75 0b                         jne 0xc010107f <isalnum+0x21>
c0101074: 83 ea 30                      sub edx, 48
c0101077: 31 c0                         xor eax, eax
c0101079: 83 fa 09                      cmp edx, 9
c010107c: 0f 96 c0                      setbe al
c010107f: c3                            ret

c0101080 <iscntrl>:
c0101080: 8b 54 24 04                   mov edx, dword ptr [esp + 4]
c0101084: 83 fa 7f                      cmp edx, 127
```

```
c01010c7: 0f 96 c0                  setbe al
c01010ca: 0f b6 c0                  movzx eax, al
c01010cd: c3                        ret

c01010ce <isprint>:
c01010ce: ff 74 24 04               push dword ptr [esp + 4]
c01010d2: e8 a9 ff ff ff            call 0xc0101080 <iscntrl>
c01010d7: 5a                        pop edx
c01010d8: 85 c0                     test eax, eax
c01010da: 0f 94 c0                  sete al
c01010dd: 0f b6 c0                  movzx eax, al
c01010e0: c3                        ret

c01010e1 <isgraph>:
c01010e1: 8b 4c 24 04               mov ecx, dword ptr [esp + 4]
c01010e5: 51                        push ecx
c01010e6: e8 e3 ff ff ff            call 0xc01010ce <isprint>
c01010eb: 5a                        pop edx
c01010ec: 83 f9 20                  cmp ecx, 32
c01010ef: 0f 95 c2                  setne dl
c01010f2: 85 c0                     test eax, eax
c01010f4: 0f 95 c0                  setne al
c01010f7: 0f b6 c0                  movzx eax, al
c01010fa: 21 d0                     and eax, edx
c01010fc: c3                        ret

c01010fd <isspace>:
c01010fd: 8b 54 24 04               mov edx, dword ptr [esp + 4]
c0101101: 8d 42 f7                  lea eax, [edx - 9]
c0101104: 83 f8 04                  cmp eax, 4
c0101107: 0f 96 c0                  setbe al
c010110a: 83 fa 20                  cmp edx, 32
c010110d: 0f 94 c2                  sete dl
c0101110: 09 d0                     or eax, edx
c0101112: 0f b6 c0                  movzx eax, al
c0101115: c3                        ret

c0101116 <ispunct>:
c0101116: 8b 4c 24 04               mov ecx, dword ptr [esp + 4]
c010111a: 51                        push ecx
c010111b: e8 ae ff ff ff            call 0xc01010ce <isprint>
c0101120: 5a                        pop edx
c0101121: 85 c0                     test eax, eax
c0101123: 74 1e                     je 0xc0101143 <ispunct+0x2d>
c0101125: 51                        push ecx
c0101126: e8 d2 ff ff ff            call 0xc01010fd <isspace>
c010112b: 5a                        pop edx
c010112c: 89 c2                     mov edx, eax
c010112e: 31 c0                     xor eax, eax
c0101130: 85 d2                     test edx, edx
c0101132: 75 0f                     jne 0xc0101143 <ispunct+0x2d>
c0101134: 51                        push ecx
c0101135: e8 24 ff ff ff            call 0xc010105e <isalnum>
c010113a: 5a                        pop edx
c010113b: 85 c0                     test eax, eax
c010113d: 0f 94 c0                  sete al
c0101140: 0f b6 c0                  movzx eax, al
c0101143: c3                        ret

c0101144 <isupper>:
c0101144: 8b 44 24 04               mov eax, dword ptr [esp + 4]
c0101148: 83 e8 41                  sub eax, 65
c010114b: 83 f8 19                  cmp eax, 25
c010114e: 0f 96 c0                  setbe al
c0101151: 0f b6 c0                  movzx eax, al
c0101154: c3                        ret

c0101155 <isxdigit>:
c0101155: 8b 44 24 04               mov eax, dword ptr [esp + 4]
c0101159: 8d 48 d0                  lea ecx, [eax - 48]
c010115c: ba 01 00 00 00            mov edx, 1
```

```
c010119f: 5f                            pop edi
c01011a0: c3                            ret

c01011a1 <strcmp>:
c01011a1: 31 c9                         xor ecx, ecx
c01011a3: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c01011a7: 0f b6 04 08                   movzx eax, byte ptr [eax + ecx]
c01011ab: 8b 54 24 08                   mov edx, dword ptr [esp + 8]
c01011af: 0f b6 14 0a                   movzx edx, byte ptr [edx + ecx]
c01011b3: 84 c0                         test al, al
c01011b5: 74 05                         je 0xc01011bc <strcmp+0x1b>
c01011b7: 41                            inc ecx
c01011b8: 38 d0                         cmp al, dl
c01011ba: 74 e7                         je 0xc01011a3 <strcmp+0x2>
c01011bc: 29 d0                         sub eax, edx
c01011be: c3                            ret

c01011bf <strcpy>:
c01011bf: 8b 54 24 04                   mov edx, dword ptr [esp + 4]
c01011c3: 31 c0                         xor eax, eax
c01011c5: 8b 4c 24 08                   mov ecx, dword ptr [esp + 8]
c01011c9: 8a 0c 01                      mov cl, byte ptr [ecx + eax]
c01011cc: 88 0c 02                      mov byte ptr [edx + eax], cl
c01011cf: 40                            inc eax
c01011d0: 84 c9                         test cl, cl
c01011d2: 75 f1                         jne 0xc01011c5 <strcpy+0x6>
c01011d4: 89 d0                         mov eax, edx
c01011d6: c3                            ret

c01011d7 <strlen>:
c01011d7: 8b 54 24 04                   mov edx, dword ptr [esp + 4]
c01011db: 31 c0                         xor eax, eax
c01011dd: 80 3c 02 00                   cmp byte ptr [edx + eax], 0
c01011e1: 74 03                         je 0xc01011e6 <strlen+0xf>
c01011e3: 40                            inc eax
c01011e4: eb f7                         jmp 0xc01011dd <strlen+0x6>
c01011e6: c3                            ret

c01011e7 <memchr>:
c01011e7: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c01011eb: 8b 4c 24 08                   mov ecx, dword ptr [esp + 8]
c01011ef: 8b 54 24 0c                   mov edx, dword ptr [esp + 12]
c01011f3: 01 c2                         add edx, eax
c01011f5: 39 d0                         cmp eax, edx
c01011f7: 74 07                         je 0xc0101200 <memchr+0x19>
c01011f9: 38 08                         cmp byte ptr [eax], cl
c01011fb: 74 05                         je 0xc0101202 <memchr+0x1b>
c01011fd: 40                            inc eax
c01011fe: eb f5                         jmp 0xc01011f5 <memchr+0xe>
c0101200: 31 c0                         xor eax, eax
c0101202: c3                            ret

c0101203 <memcmp>:
c0101203: 56                            push esi
c0101204: 53                            push ebx
c0101205: 8b 44 24 0c                   mov eax, dword ptr [esp + 12]
c0101209: 8b 54 24 10                   mov edx, dword ptr [esp + 16]
c010120d: 8b 74 24 14                   mov esi, dword ptr [esp + 20]
c0101211: 01 c6                         add esi, eax
c0101213: 39 f0                         cmp eax, esi
c0101215: 74 15                         je 0xc010122c <memcmp+0x29>
c0101217: 8a 08                         mov cl, byte ptr [eax]
c0101219: 8a 1a                         mov bl, byte ptr [edx]
c010121b: 38 d9                         cmp cl, bl
c010121d: 72 11                         jb 0xc0101230 <memcmp+0x2d>
c010121f: 40                            inc eax
c0101220: 42                            inc edx
c0101221: 38 cb                         cmp bl, cl
c0101223: 73 ee                         jae 0xc0101213 <memcmp+0x10>
c0101225: b8 01 00 00 00                mov eax, 1
c010122a: eb 07                         jmp 0xc0101233 <memcmp+0x30>
```

```
c0101263: c3                            ret

c0101264 <memmove>:
c0101264: 57                            push edi
c0101265: 56                            push esi
c0101266: 8b 54 24 0c                   mov edx, dword ptr [esp + 12]
c010126a: 8b 74 24 10                   mov esi, dword ptr [esp + 16]
c010126e: 8b 44 24 14                   mov eax, dword ptr [esp + 20]
c0101272: 39 d6                         cmp esi, edx
c0101274: 72 0b                         jb 0xc0101281 <memmove+0x1d>
c0101276: 01 d0                         add eax, edx
c0101278: 89 d7                         mov edi, edx
c010127a: 39 c7                         cmp edi, eax
c010127c: 74 10                         je 0xc010128e <memmove+0x2a>
c010127e: a4                            movsb byte ptr es:[edi], byte ptr [esi]
c010127f: eb f9                         jmp 0xc010127a <memmove+0x16>
c0101281: 83 e8 01                      sub eax, 1
c0101284: 72 08                         jb 0xc010128e <memmove+0x2a>
c0101286: 8a 0c 06                      mov cl, byte ptr [esi + eax]
c0101289: 88 0c 02                      mov byte ptr [edx + eax], cl
c010128c: eb f3                         jmp 0xc0101281 <memmove+0x1d>
c010128e: 89 d0                         mov eax, edx
c0101290: 5e                            pop esi
c0101291: 5f                            pop edi
c0101292: c3                            ret

c0101293 <strcat>:
c0101293: 53                            push ebx
c0101294: 8b 44 24 08                   mov eax, dword ptr [esp + 8]
c0101298: 89 c2                         mov edx, eax
c010129a: 8a 0a                         mov cl, byte ptr [edx]
c010129c: 89 d3                         mov ebx, edx
c010129e: 8d 52 01                      lea edx, [edx + 1]
c01012a1: 84 c9                         test cl, cl
c01012a3: 75 f5                         jne 0xc010129a <strcat+0x7>
c01012a5: 31 d2                         xor edx, edx
c01012a7: 8b 4c 24 0c                   mov ecx, dword ptr [esp + 12]
c01012ab: 8a 0c 11                      mov cl, byte ptr [ecx + edx]
c01012ae: 88 0c 13                      mov byte ptr [ebx + edx], cl
c01012b1: 42                            inc edx
c01012b2: 84 c9                         test cl, cl
c01012b4: 75 f1                         jne 0xc01012a7 <strcat+0x14>
c01012b6: 5b                            pop ebx
c01012b7: c3                            ret

c01012b8 <strncpy>:
c01012b8: 56                            push esi
c01012b9: 53                            push ebx
c01012ba: 8b 54 24 0c                   mov edx, dword ptr [esp + 12]
c01012be: 8b 4c 24 10                   mov ecx, dword ptr [esp + 16]
c01012c2: 8b 74 24 14                   mov esi, dword ptr [esp + 20]
c01012c6: 01 d6                         add esi, edx
c01012c8: 89 d0                         mov eax, edx
c01012ca: 39 f0                         cmp eax, esi
c01012cc: 74 0e                         je 0xc01012dc <strncpy+0x24>
c01012ce: 8a 19                         mov bl, byte ptr [ecx]
c01012d0: 40                            inc eax
c01012d1: 80 fb 01                      cmp bl, 1
c01012d4: 83 d9 ff                      sbb ecx, -1
c01012d7: 88 58 ff                      mov byte ptr [eax - 1], bl
c01012da: eb ee                         jmp 0xc01012ca <strncpy+0x12>
c01012dc: 89 d0                         mov eax, edx
c01012de: 5b                            pop ebx
c01012df: 5e                            pop esi
c01012e0: c3                            ret

c01012e1 <strchr>:
c01012e1: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c01012e5: 8a 10                         mov dl, byte ptr [eax]
c01012e7: 3a 54 24 08                   cmp dl, byte ptr [esp + 8]
c01012eb: 74 07                         je 0xc01012f4 <strchr+0x13>
```

```
c010131e <IsLeapYear>:
c010131e: a8 03                         test al, 3
c0101320: 75 27                         jne 0xc0101349 <IsLeapYear+0x2b>
c0101322: 53                            push ebx
c0101323: 89 c1                         mov ecx, eax
c0101325: bb 64 00 00 00                mov ebx, 100
c010132a: 99                            cdq
c010132b: f7 fb                         idiv ebx
c010132d: b8 01 00 00 00                mov eax, 1
c0101332: 85 d2                         test edx, edx
c0101334: 75 19                         jne 0xc010134f <IsLeapYear+0x31>
c0101336: bb 90 01 00 00                mov ebx, 400
c010133b: 89 c8                         mov eax, ecx
c010133d: 99                            cdq
c010133e: f7 fb                         idiv ebx
c0101340: 31 c0                         xor eax, eax
c0101342: 85 d2                         test edx, edx
c0101344: 0f 94 c0                      sete al
c0101347: eb 06                         jmp 0xc010134f <IsLeapYear+0x31>
c0101349: 31 c0                         xor eax, eax
c010134b: 83 e0 01                      and eax, 1
c010134e: c3                            ret
c010134f: 83 e0 01                      and eax, 1
c0101352: 5b                            pop ebx
c0101353: c3                            ret

c0101354 <TimeStructToValue>:
c0101354: 55                            push ebp
c0101355: 57                            push edi
c0101356: 56                            push esi
c0101357: 53                            push ebx
c0101358: 83 ec 14                      sub esp, 20
c010135b: 8b 7c 24 30                   mov edi, dword ptr [esp + 48]
c010135f: 8d 87 bf f9 ff ff             lea eax, [edi - 1601]
c0101365: 31 c9                         xor ecx, ecx
c0101367: 31 db                         xor ebx, ebx
c0101369: 3d 1f 03 00 00                cmp eax, 799
c010136e: 0f 87 f6 00 00 00             ja 0xc010146a <TimeStructToValue+0x116>
c0101374: 8a 44 24 2c                   mov al, byte ptr [esp + 44]
c0101378: 89 c5                         mov ebp, eax
c010137a: 48                            dec eax
c010137b: 3c 0b                         cmp al, 11
c010137d: 0f 87 e7 00 00 00             ja 0xc010146a <TimeStructToValue+0x116>
c0101383: 8a 54 24 2b                   mov dl, byte ptr [esp + 43]
c0101387: 8d 42 ff                      lea eax, [edx - 1]
c010138a: 3c 1e                         cmp al, 30
c010138c: 0f 87 d8 00 00 00             ja 0xc010146a <TimeStructToValue+0x116>
c0101392: 0f b6 74 24 28                movzx esi, byte ptr [esp + 40]
c0101397: 0f b6 44 24 29                movzx eax, byte ptr [esp + 41]
c010139c: 6b c0 3c                      imul eax, eax, 60
c010139f: 0f b6 4c 24 2a                movzx ecx, byte ptr [esp + 42]
c01013a4: 69 c9 10 0e 00 00             imul ecx, ecx, 3600
c01013aa: 89 cb                         mov ebx, ecx
c01013ac: c1 fb 1f                      sar ebx, 31
c01013af: 01 c1                         add ecx, eax
c01013b1: 83 d3 00                      adc ebx, 0
c01013b4: 01 f1                         add ecx, esi
c01013b6: 83 d3 00                      adc ebx, 0
c01013b9: 89 0c 24                      mov dword ptr [esp], ecx
c01013bc: 89 5c 24 04                   mov dword ptr [esp + 4], ebx
c01013c0: 0f b6 c2                      movzx eax, dl
c01013c3: 48                            dec eax
c01013c4: 99                            cdq
c01013c5: 89 eb                         mov ebx, ebp
c01013c7: 0f b6 cb                      movzx ecx, bl
c01013ca: 8b 0c 8d fc 2f 11 c0          mov ecx, dword ptr [4*ecx - 1072615428]
c01013d1: 89 cb                         mov ebx, ecx
c01013d3: c1 fb 1f                      sar ebx, 31
c01013d6: 89 de                         mov esi, ebx
c01013d8: 89 cb                         mov ebx, ecx
```

```
c010142d: 99                            cdq
c010142e: 01 d8                         add eax, ebx
c0101430: 11 f2                         adc edx, esi
c0101432: 69 da 80 51 01 00             imul ebx, edx, 86400
c0101438: b9 80 51 01 00                mov ecx, 86400
c010143d: f7 e1                         mul ecx
c010143f: 01 da                         add edx, ebx
c0101441: 8b 34 24                      mov esi, dword ptr [esp]
c0101444: 8b 7c 24 04                   mov edi, dword ptr [esp + 4]
c0101448: 01 c6                         add esi, eax
c010144a: 11 d7                         adc edi, edx
c010144c: 69 cf 40 42 0f 00             imul ecx, edi, 1000000
c0101452: bb 40 42 0f 00                mov ebx, 1000000
c0101457: 89 f0                         mov eax, esi
c0101459: f7 e3                         mul ebx
c010145b: 01 ca                         add edx, ecx
c010145d: 8b 4c 24 34                   mov ecx, dword ptr [esp + 52]
c0101461: 89 cb                         mov ebx, ecx
c0101463: c1 fb 1f                      sar ebx, 31
c0101466: 01 c1                         add ecx, eax
c0101468: 11 d3                         adc ebx, edx
c010146a: 89 c8                         mov eax, ecx
c010146c: 89 da                         mov edx, ebx
c010146e: 83 c4 14                      add esp, 20
c0101471: 5b                            pop ebx
c0101472: 5e                            pop esi
c0101473: 5f                            pop edi
c0101474: 5d                            pop ebp
c0101475: c3                            ret

c0101476 <TimeValueToStruct>:
c0101476: 55                            push ebp
c0101477: 57                            push edi
c0101478: 56                            push esi
c0101479: 53                            push ebx
c010147a: 83 ec 3c                      sub esp, 60
c010147d: 8b 74 24 50                   mov esi, dword ptr [esp + 80]
c0101481: 8b 7c 24 54                   mov edi, dword ptr [esp + 84]
c0101485: 8b 6c 24 58                   mov ebp, dword ptr [esp + 88]
c0101489: 8d 5c 24 28                   lea ebx, [esp + 40]
c010148d: 83 ec 0c                      sub esp, 12
c0101490: 53                            push ebx
c0101491: 6a 00                         push 0
c0101493: 68 40 42 0f 00                push 1000000
c0101498: 55                            push ebp
c0101499: 57                            push edi
c010149a: e8 d9 db 00 00                call 0xc010f078 <__udivmoddi4>
c010149f: 83 c4 14                      add esp, 20
c01014a2: 8b 4c 24 34                   mov ecx, dword ptr [esp + 52]
c01014a6: 89 4c 24 20                   mov dword ptr [esp + 32], ecx
c01014aa: 53                            push ebx
c01014ab: 6a 00                         push 0
c01014ad: 6a 3c                         push 60
c01014af: 52                            push edx
c01014b0: 50                            push eax
c01014b1: e8 c2 db 00 00                call 0xc010f078 <__udivmoddi4>
c01014b6: 83 c4 20                      add esp, 32
c01014b9: 8b 4c 24 28                   mov ecx, dword ptr [esp + 40]
c01014bd: 89 4c 24 18                   mov dword ptr [esp + 24], ecx
c01014c1: 6a 00                         push 0
c01014c3: 6a 3c                         push 60
c01014c5: 52                            push edx
c01014c6: 50                            push eax
c01014c7: e8 90 da 00 00                call 0xc010ef5c <__umoddi3>
c01014cc: 83 c4 10                      add esp, 16
c01014cf: 89 44 24 1c                   mov dword ptr [esp + 28], eax
c01014d3: 6a 00                         push 0
c01014d5: 68 00 a4 93 d6                push 3600000000
c01014da: 55                            push ebp
c01014db: 57                            push edi
c01014dc: e8 6f d9 00 00                call 0xc010ee50 <__udivdi3>
```

```
c010153e: 89 54 24 24                   mov dword ptr [esp + 36], edx
c0101542: 8b 44 24 0c                   mov eax, dword ptr [esp + 12]
c0101546: e8 d3 fd ff ff                call 0xc010131e <IsLeapYear>
c010154b: 0f b6 c0                      movzx eax, al
c010154e: 8b 54 24 24                   mov edx, dword ptr [esp + 36]
c0101552: eb d3                         jmp 0xc0101527 <TimeValueToStruct+0xb1>
c0101554: 8b 2c 95 fc 2f 11 c0          mov ebp, dword ptr [4*edx - 1072615428]
c010155b: 31 c0                         xor eax, eax
c010155d: 83 fa 02                      cmp edx, 2
c0101560: 7e 0c                         jle 0xc010156e <TimeValueToStruct+0xf8>
c0101562: 8b 44 24 0c                   mov eax, dword ptr [esp + 12]
c0101566: e8 b3 fd ff ff                call 0xc010131e <IsLeapYear>
c010156b: 0f b6 c0                      movzx eax, al
c010156e: 01 c5                         add ebp, eax
c0101570: 29 eb                         sub ebx, ebp
c0101572: eb 35                         jmp 0xc01015a9 <TimeValueToStruct+0x133>
c0101574: fe 44 24 13                   inc byte ptr [esp + 19]
c0101578: 80 7c 24 13 0d                cmp byte ptr [esp + 19], 13
c010157d: 75 2a                         jne 0xc01015a9 <TimeValueToStruct+0x133>
c010157f: 8b 44 24 0c                   mov eax, dword ptr [esp + 12]
c0101583: e8 96 fd ff ff                call 0xc010131e <IsLeapYear>
c0101588: 0f b6 c0                      movzx eax, al
c010158b: 05 6d 01 00 00                add eax, 365
c0101590: 29 c3                         sub ebx, eax
c0101592: ff 44 24 0c                   inc dword ptr [esp + 12]
c0101596: 81 7c 24 0c 61 09 00 00       cmp dword ptr [esp + 12], 2401
c010159e: 0f 85 6d ff ff ff             jne 0xc0101511 <TimeValueToStruct+0x9b>
c01015a4: bf 61 09 00 00                mov edi, 2401
c01015a9: 8a 44 24 18                   mov al, byte ptr [esp + 24]
c01015ad: 88 06                         mov byte ptr [esi], al
c01015af: 8a 44 24 1c                   mov al, byte ptr [esp + 28]
c01015b3: 88 46 01                      mov byte ptr [esi + 1], al
c01015b6: 8a 44 24 20                   mov al, byte ptr [esp + 32]
c01015ba: 88 46 02                      mov byte ptr [esi + 2], al
c01015bd: 43                            inc ebx
c01015be: 88 5e 03                      mov byte ptr [esi + 3], bl
c01015c1: 8a 44 24 13                   mov al, byte ptr [esp + 19]
c01015c5: 88 46 04                      mov byte ptr [esi + 4], al
c01015c8: 89 7e 08                      mov dword ptr [esi + 8], edi
c01015cb: 8b 44 24 14                   mov eax, dword ptr [esp + 20]
c01015cf: 89 46 0c                      mov dword ptr [esi + 12], eax
c01015d2: 89 f0                         mov eax, esi
c01015d4: 83 c4 3c                      add esp, 60
c01015d7: 5b                            pop ebx
c01015d8: 5e                            pop esi
c01015d9: 5f                            pop edi
c01015da: 5d                            pop ebp
c01015db: c2 04 00                      ret 4

c01015de <GetWeekday>:
c01015de: 83 ec 0c                      sub esp, 12
c01015e1: 6a 14                         push 20
c01015e3: 68 00 60 d7 1d                push 500654080
c01015e8: ff 74 24 1c                   push dword ptr [esp + 28]
c01015ec: ff 74 24 1c                   push dword ptr [esp + 28]
c01015f0: e8 5b d8 00 00                call 0xc010ee50 <__udivdi3>
c01015f5: 40                            inc eax
c01015f6: b9 07 00 00 00                mov ecx, 7
c01015fb: 99                            cdq
c01015fc: f7 f9                         idiv ecx
c01015fe: 8d 42 01                      lea eax, [edx + 1]
c0101601: 83 c4 1c                      add esp, 28
c0101604: c3                            ret

c0101605 <TimeValueToUnixTime>:
c0101605: 83 ec 0c                      sub esp, 12
c0101608: 6a 00                         push 0
c010160a: 68 40 42 0f 00                push 1000000
c010160f: ff 74 24 1c                   push dword ptr [esp + 28]
c0101613: ff 74 24 1c                   push dword ptr [esp + 28]
c0101617: e8 34 d8 00 00                call 0xc010ee50 <__udivdi3>
```

```
c0101662: 31 d2                         xor edx, edx
c0101664: f7 71 04                      div dword ptr [ecx + 4]
c0101667: 8b 01                         mov eax, dword ptr [ecx]
c0101669: 8b 04 90                      mov eax, dword ptr [eax + 4*edx]
c010166c: 85 c0                         test eax, eax
c010166e: 75 04                         jne 0xc0101674 <GetInternalNode+0x2d>
c0101670: 31 ff                         xor edi, edi
c0101672: eb 39                         jmp 0xc01016ad <GetInternalNode+0x66>
c0101674: 83 ec 0c                      sub esp, 12
c0101677: 50                            push eax
c0101678: e8 5c 05 00 00                call 0xc0101bd9 <ListGetNextNode>
c010167d: 89 c3                         mov ebx, eax
c010167f: 83 c4 10                      add esp, 16
c0101682: 85 c0                         test eax, eax
c0101684: 74 ea                         je 0xc0101670 <GetInternalNode+0x29>
c0101686: 83 ec 0c                      sub esp, 12
c0101689: 53                            push ebx
c010168a: e8 66 05 00 00                call 0xc0101bf5 <ListGetDataFromNode>
c010168f: 89 c7                         mov edi, eax
c0101691: 58                            pop eax
c0101692: 5a                            pop edx
c0101693: 56                            push esi
c0101694: ff 37                         push dword ptr [edi]
c0101696: e8 06 fb ff ff                call 0xc01011a1 <strcmp>
c010169b: 83 c4 10                      add esp, 16
c010169e: 85 c0                         test eax, eax
c01016a0: 74 0b                         je 0xc01016ad <GetInternalNode+0x66>
c01016a2: 83 ec 0c                      sub esp, 12
c01016a5: 53                            push ebx
c01016a6: e8 2e 05 00 00                call 0xc0101bd9 <ListGetNextNode>
c01016ab: eb d0                         jmp 0xc010167d <GetInternalNode+0x36>
c01016ad: 89 f8                         mov eax, edi
c01016af: 5b                            pop ebx
c01016b0: 5e                            pop esi
c01016b1: 5f                            pop edi
c01016b2: c3                            ret

c01016b3 <HashmapCreate>:
c01016b3: 56                            push esi
c01016b4: 53                            push ebx
c01016b5: 83 ec 10                      sub esp, 16
c01016b8: 8b 74 24 1c                   mov esi, dword ptr [esp + 28]
c01016bc: 6a 08                         push 8
c01016be: e8 8c 22 00 00                call 0xc010394f <AllocHeap>
c01016c3: 89 c3                         mov ebx, eax
c01016c5: 89 70 04                      mov dword ptr [eax + 4], esi
c01016c8: c1 e6 02                      shl esi, 2
c01016cb: 89 34 24                      mov dword ptr [esp], esi
c01016ce: e8 8e 22 00 00                call 0xc0103961 <AllocHeapZero>
c01016d3: 89 03                         mov dword ptr [ebx], eax
c01016d5: 89 d8                         mov eax, ebx
c01016d7: 83 c4 14                      add esp, 20
c01016da: 5b                            pop ebx
c01016db: 5e                            pop esi
c01016dc: c3                            ret

c01016dd <HashmapContains>:
c01016dd: 83 ec 0c                      sub esp, 12
c01016e0: 8b 54 24 14                   mov edx, dword ptr [esp + 20]
c01016e4: 8b 44 24 10                   mov eax, dword ptr [esp + 16]
c01016e8: e8 5a ff ff ff                call 0xc0101647 <GetInternalNode>
c01016ed: 85 c0                         test eax, eax
c01016ef: 0f 95 c0                      setne al
c01016f2: 83 c4 0c                      add esp, 12
c01016f5: c3                            ret

c01016f6 <HashmapGet>:
c01016f6: 83 ec 0c                      sub esp, 12
c01016f9: 8b 54 24 14                   mov edx, dword ptr [esp + 20]
c01016fd: 8b 44 24 10                   mov eax, dword ptr [esp + 16]
c0101701: e8 41 ff ff ff                call 0xc0101647 <GetInternalNode>
```

```
c010174d: 31 c0                   xor eax, eax
c010174f: 47                      inc edi
c0101750: 0f be 57 ff             movsx edx, byte ptr [edi - 1]
c0101754: 84 d2                   test dl, dl
c0101756: 74 07                   je 0xc010175f <HashmapSet+0x4e>
c0101758: 6b c0 1f                imul eax, eax, 31
c010175b: 01 d0                   add eax, edx
c010175d: eb f0                   jmp 0xc010174f <HashmapSet+0x3e>
c010175f: 31 d2                   xor edx, edx
c0101761: f7 73 04                div dword ptr [ebx + 4]
c0101764: 89 d7                   mov edi, edx
c0101766: 8b 03                   mov eax, dword ptr [ebx]
c0101768: 8d 2c 90                lea ebp, [eax + 4*edx]
c010176b: 83 7d 00 00             cmp dword ptr [ebp], 0
c010176f: 75 08                   jne 0xc0101779 <HashmapSet+0x68>
c0101771: e8 c2 02 00 00          call 0xc0101a38 <ListCreate>
c0101776: 89 45 00                mov dword ptr [ebp], eax
c0101779: 89 74 24 24             mov dword ptr [esp + 36], esi
c010177d: 8b 03                   mov eax, dword ptr [ebx]
c010177f: 8b 04 b8                mov eax, dword ptr [eax + 4*edi]
c0101782: 89 44 24 20             mov dword ptr [esp + 32], eax
c0101786: 83 c4 0c                add esp, 12
c0101789: 5b                      pop ebx
c010178a: 5e                      pop esi
c010178b: 5f                      pop edi
c010178c: 5d                      pop ebp
c010178d: e9 e5 02 00 00          jmp 0xc0101a77 <ListInsertEnd>
c0101792: 89 68 04                mov dword ptr [eax + 4], ebp
c0101795: 83 c4 0c                add esp, 12
c0101798: 5b                      pop ebx
c0101799: 5e                      pop esi
c010179a: 5f                      pop edi
c010179b: 5d                      pop ebp
c010179c: c3                      ret

c010179d <SwapElements>:
c010179d: 55                      push ebp
c010179e: 57                      push edi
c010179f: 56                      push esi
c01017a0: 53                      push ebx
c01017a1: 83 ec 0c                sub esp, 12
c01017a4: 89 c3                   mov ebx, eax
c01017a6: 8b 40 0c                mov eax, dword ptr [eax + 12]
c01017a9: 0f af d0                imul edx, eax
c01017ac: c1 e2 03                shl edx, 3
c01017af: 0f af c1                imul eax, ecx
c01017b2: c1 e0 03                shl eax, 3
c01017b5: 31 c9                   xor ecx, ecx
c01017b7: 39 4b 0c                cmp dword ptr [ebx + 12], ecx
c01017ba: 7e 3a                   jle 0xc01017f6 <SwapElements+0x59>
c01017bc: 8b 73 14                mov esi, dword ptr [ebx + 20]
c01017bf: 01 d6                   add esi, edx
c01017c1: 8b 3e                   mov edi, dword ptr [esi]
c01017c3: 8b 6e 04                mov ebp, dword ptr [esi + 4]
c01017c6: 89 3c 24                mov dword ptr [esp], edi
c01017c9: 89 6c 24 04             mov dword ptr [esp + 4], ebp
c01017cd: 8b 7b 14                mov edi, dword ptr [ebx + 20]
c01017d0: 8b 6c 07 04             mov ebp, dword ptr [edi + eax + 4]
c01017d4: 8b 3c 07                mov edi, dword ptr [edi + eax]
c01017d7: 89 3e                   mov dword ptr [esi], edi
c01017d9: 89 6e 04                mov dword ptr [esi + 4], ebp
c01017dc: 8b 73 14                mov esi, dword ptr [ebx + 20]
c01017df: 8b 3c 24                mov edi, dword ptr [esp]
c01017e2: 8b 6c 24 04             mov ebp, dword ptr [esp + 4]
c01017e6: 89 3c 06                mov dword ptr [esi + eax], edi
c01017e9: 89 6c 06 04             mov dword ptr [esi + eax + 4], ebp
c01017ed: 41                      inc ecx
c01017ee: 83 c2 08                add edx, 8
c01017f1: 83 c0 08                add eax, 8
c01017f4: eb c1                   jmp 0xc01017b7 <SwapElements+0x1a>
c01017f6: 83 c4 0c                add esp, 12
```

```
c0101830: 8b 2c ce                      mov ebp, dword ptr [esi + 8*ecx]
c0101833: 39 2c fe                      cmp dword ptr [esi + 8*edi], ebp
c0101836: 8b 7c 24 04                   mov edi, dword ptr [esp + 4]
c010183a: 1b 7c ce 04                   sbb edi, dword ptr [esi + 8*ecx + 4]
c010183e: 0f 92 c1                      setb cl
c0101841: 3a 4b 10                      cmp cl, byte ptr [ebx + 16]
c0101844: 74 02                         je 0xc0101848 <GetMinOrMaxIndex+0x4a>
c0101846: 89 d0                         mov eax, edx
c0101848: 83 c4 0c                      add esp, 12
c010184b: 5b                            pop ebx
c010184c: 5e                            pop esi
c010184d: 5f                            pop edi
c010184e: 5d                            pop ebp
c010184f: c3                            ret

c0101850 <HeapAdtCreate>:
c0101850: 55                            push ebp
c0101851: 57                            push edi
c0101852: 56                            push esi
c0101853: 53                            push ebx
c0101854: 83 ec 18                      sub esp, 24
c0101857: 8b 7c 24 2c                   mov edi, dword ptr [esp + 44]
c010185b: 8b 6c 24 30                   mov ebp, dword ptr [esp + 48]
c010185f: 8b 74 24 34                   mov esi, dword ptr [esp + 52]
c0101863: 6a 18                         push 24
c0101865: e8 e5 20 00 00                call 0xc010394f <AllocHeap>
c010186a: 89 c3                         mov ebx, eax
c010186c: 89 38                         mov dword ptr [eax], edi
c010186e: 31 c0                         xor eax, eax
c0101870: 89 43 04                      mov dword ptr [ebx + 4], eax
c0101873: 89 73 08                      mov dword ptr [ebx + 8], esi
c0101876: 83 c6 07                      add esi, 7
c0101879: c1 ee 03                      shr esi, 3
c010187c: 46                            inc esi
c010187d: 89 73 0c                      mov dword ptr [ebx + 12], esi
c0101880: 89 e8                         mov eax, ebp
c0101882: 88 43 10                      mov byte ptr [ebx + 16], al
c0101885: 0f af fe                      imul edi, esi
c0101888: c1 e7 03                      shl edi, 3
c010188b: 89 3c 24                      mov dword ptr [esp], edi
c010188e: e8 bc 20 00 00                call 0xc010394f <AllocHeap>
c0101893: 89 43 14                      mov dword ptr [ebx + 20], eax
c0101896: 89 d8                         mov eax, ebx
c0101898: 83 c4 1c                      add esp, 28
c010189b: 5b                            pop ebx
c010189c: 5e                            pop esi
c010189d: 5f                            pop edi
c010189e: 5d                            pop ebp
c010189f: c3                            ret

c01018a0 <HeapAdtDestroy>:
c01018a0: 53                            push ebx
c01018a1: 83 ec 14                      sub esp, 20
c01018a4: 8b 5c 24 1c                   mov ebx, dword ptr [esp + 28]
c01018a8: ff 73 14                      push dword ptr [ebx + 20]
c01018ab: e8 c3 20 00 00                call 0xc0103973 <FreeHeap>
c01018b0: 89 5c 24 20                   mov dword ptr [esp + 32], ebx
c01018b4: 83 c4 18                      add esp, 24
c01018b7: 5b                            pop ebx
c01018b8: e9 b6 20 00 00                jmp 0xc0103973 <FreeHeap>

c01018bd <HeapAdtInsert>:
c01018bd: 55                            push ebp
c01018be: 57                            push edi
c01018bf: 56                            push esi
c01018c0: 53                            push ebx
c01018c1: 83 ec 1c                      sub esp, 28
c01018c4: 8b 74 24 38                   mov esi, dword ptr [esp + 56]
c01018c8: 8b 7c 24 3c                   mov edi, dword ptr [esp + 60]
c01018cc: 8b 44 24 30                   mov eax, dword ptr [esp + 48]
c01018d0: 8b 58 04                      mov ebx, dword ptr [eax + 4]
```

```
c010192b: 89 c6                  mov esi, eax
c010192d: 89 c2                  mov edx, eax
c010192f: 0f af d7               imul edx, edi
c0101932: 89 d9                  mov ecx, ebx
c0101934: 0f af cf               imul ecx, edi
c0101937: 8b 44 15 04            mov eax, dword ptr [ebp + edx + 4]
c010193b: 89 44 24 0c            mov dword ptr [esp + 12], eax
c010193f: 8b 44 0d 04            mov eax, dword ptr [ebp + ecx + 4]
c0101943: 8b 54 15 00            mov edx, dword ptr [ebp + edx]
c0101947: 39 54 0d 00            cmp dword ptr [ebp + ecx], edx
c010194b: 1b 44 24 0c            sbb eax, dword ptr [esp + 12]
c010194f: 0f 92 c0               setb al
c0101952: 8b 4c 24 30            mov ecx, dword ptr [esp + 48]
c0101956: 38 41 10               cmp byte ptr [ecx + 16], al
c0101959: 74 11                  je 0xc010196c <HeapAdtInsert+0xaf>
c010195b: 89 d9                  mov ecx, ebx
c010195d: 89 f2                  mov edx, esi
c010195f: 8b 44 24 30            mov eax, dword ptr [esp + 48]
c0101963: e8 35 fe ff ff         call 0xc010179d <SwapElements>
c0101968: 89 f3                  mov ebx, esi
c010196a: eb b0                  jmp 0xc010191c <HeapAdtInsert+0x5f>
c010196c: 83 c4 1c               add esp, 28
c010196f: 5b                     pop ebx
c0101970: 5e                     pop esi
c0101971: 5f                     pop edi
c0101972: 5d                     pop ebp
c0101973: c3                     ret

c0101974 <HeapAdtPeek>:
c0101974: 53                     push ebx
c0101975: 83 ec 08               sub esp, 8
c0101978: 8b 54 24 10            mov edx, dword ptr [esp + 16]
c010197c: 8b 44 24 14            mov eax, dword ptr [esp + 20]
c0101980: 83 78 04 00            cmp dword ptr [eax + 4], 0
c0101984: 75 0e                  jne 0xc0101994 <HeapAdtPeek+0x20>
c0101986: 53                     push ebx
c0101987: 53                     push ebx
c0101988: 68 20 04 11 c0         push 3222340640
c010198d: 6a 0f                  push 15
c010198f: e8 ba 71 00 00         call 0xc0108b4e <PanicEx>
c0101994: 8b 40 14               mov eax, dword ptr [eax + 20]
c0101997: 8b 08                  mov ecx, dword ptr [eax]
c0101999: 8b 58 04               mov ebx, dword ptr [eax + 4]
c010199c: 89 0a                  mov dword ptr [edx], ecx
c010199e: 89 5a 04               mov dword ptr [edx + 4], ebx
c01019a1: 83 c0 08               add eax, 8
c01019a4: 89 42 08               mov dword ptr [edx + 8], eax
c01019a7: 89 d0                  mov eax, edx
c01019a9: 83 c4 08               add esp, 8
c01019ac: 5b                     pop ebx
c01019ad: c2 04 00               ret 4

c01019b0 <HeapAdtPop>:
c01019b0: 57                     push edi
c01019b1: 56                     push esi
c01019b2: 53                     push ebx
c01019b3: 8b 5c 24 10            mov ebx, dword ptr [esp + 16]
c01019b7: 8b 43 04               mov eax, dword ptr [ebx + 4]
c01019ba: 85 c0                  test eax, eax
c01019bc: 75 0e                  jne 0xc01019cc <HeapAdtPop+0x1c>
c01019be: 50                     push eax
c01019bf: 50                     push eax
c01019c0: 68 35 04 11 c0         push 3222340661
c01019c5: 6a 0f                  push 15
c01019c7: e8 82 71 00 00         call 0xc0108b4e <PanicEx>
c01019cc: 48                     dec eax
c01019cd: 89 43 04               mov dword ptr [ebx + 4], eax
c01019d0: 31 d2                  xor edx, edx
c01019d2: 8b 43 0c               mov eax, dword ptr [ebx + 12]
c01019d5: 39 d0                  cmp eax, edx
c01019d7: 7e 1a                  jle 0xc01019f3 <HeapAdtPop+0x43>
```

```
c0101a26: 5e                            pop esi
c0101a27: 5f                            pop edi
c0101a28: c3                            ret

c0101a29 <TreeSize>:
c0101a29: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c0101a2d: 8b 00                         mov eax, dword ptr [eax]
c0101a2f: c3                            ret

c0101a30 <HeapAdtGetUsedSize>:
c0101a30: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c0101a34: 8b 40 04                      mov eax, dword ptr [eax + 4]
c0101a37: c3                            ret

c0101a38 <ListCreate>:
c0101a38: 83 ec 18                      sub esp, 24
c0101a3b: 6a 0c                         push 12
c0101a3d: e8 1f 1f 00 00                call 0xc0103961 <AllocHeapZero>
c0101a42: 83 c4 1c                      add esp, 28
c0101a45: c3                            ret

c0101a46 <ListInsertStart>:
c0101a46: 53                            push ebx
c0101a47: 83 ec 14                      sub esp, 20
c0101a4a: 8b 5c 24 1c                   mov ebx, dword ptr [esp + 28]
c0101a4e: 6a 08                         push 8
c0101a50: e8 fa 1e 00 00                call 0xc010394f <AllocHeap>
c0101a55: 8b 54 24 24                   mov edx, dword ptr [esp + 36]
c0101a59: 89 10                         mov dword ptr [eax], edx
c0101a5b: 8b 53 08                      mov edx, dword ptr [ebx + 8]
c0101a5e: 89 50 04                      mov dword ptr [eax + 4], edx
c0101a61: 83 c4 10                      add esp, 16
c0101a64: 83 7b 04 00                   cmp dword ptr [ebx + 4], 0
c0101a68: 75 03                         jne 0xc0101a6d <ListInsertStart+0x27>
c0101a6a: 89 43 08                      mov dword ptr [ebx + 8], eax
c0101a6d: 89 43 04                      mov dword ptr [ebx + 4], eax
c0101a70: ff 03                         inc dword ptr [ebx]
c0101a72: 83 c4 08                      add esp, 8
c0101a75: 5b                            pop ebx
c0101a76: c3                            ret

c0101a77 <ListInsertEnd>:
c0101a77: 56                            push esi
c0101a78: 53                            push ebx
c0101a79: 53                            push ebx
c0101a7a: 8b 5c 24 10                   mov ebx, dword ptr [esp + 16]
c0101a7e: 8b 73 08                      mov esi, dword ptr [ebx + 8]
c0101a81: 85 f6                         test esi, esi
c0101a83: 75 12                         jne 0xc0101a97 <ListInsertEnd+0x20>
c0101a85: 83 ec 0c                      sub esp, 12
c0101a88: 6a 08                         push 8
c0101a8a: e8 c0 1e 00 00                call 0xc010394f <AllocHeap>
c0101a8f: 89 43 08                      mov dword ptr [ebx + 8], eax
c0101a92: 89 43 04                      mov dword ptr [ebx + 4], eax
c0101a95: eb 16                         jmp 0xc0101aad <ListInsertEnd+0x36>
c0101a97: 83 ec 0c                      sub esp, 12
c0101a9a: 6a 08                         push 8
c0101a9c: e8 ae 1e 00 00                call 0xc010394f <AllocHeap>
c0101aa1: 89 46 04                      mov dword ptr [esi + 4], eax
c0101aa4: 8b 43 08                      mov eax, dword ptr [ebx + 8]
c0101aa7: 8b 40 04                      mov eax, dword ptr [eax + 4]
c0101aaa: 89 43 08                      mov dword ptr [ebx + 8], eax
c0101aad: 83 c4 10                      add esp, 16
c0101ab0: 8b 43 08                      mov eax, dword ptr [ebx + 8]
c0101ab3: 8b 54 24 14                   mov edx, dword ptr [esp + 20]
c0101ab7: 89 10                         mov dword ptr [eax], edx
c0101ab9: 8b 43 08                      mov eax, dword ptr [ebx + 8]
c0101abc: 31 d2                         xor edx, edx
c0101abe: 89 50 04                      mov dword ptr [eax + 4], edx
c0101ac1: ff 03                         inc dword ptr [ebx]
c0101ac3: 59                            pop ecx
```

```
c0101afa <ListGetData>:
c0101afa: 83 ec 0c                      sub esp, 12
c0101afd: 8b 4c 24 14                   mov ecx, dword ptr [esp + 20]
c0101b01: 8b 44 24 10                   mov eax, dword ptr [esp + 16]
c0101b05: 8b 40 04                      mov eax, dword ptr [eax + 4]
c0101b08: 31 d2                         xor edx, edx
c0101b0a: 85 c0                         test eax, eax
c0101b0c: 74 0a                         je 0xc0101b18 <ListGetData+0x1e>
c0101b0e: 39 ca                         cmp edx, ecx
c0101b10: 74 10                         je 0xc0101b22 <ListGetData+0x28>
c0101b12: 42                            inc edx
c0101b13: 8b 40 04                      mov eax, dword ptr [eax + 4]
c0101b16: eb f2                         jmp 0xc0101b0a <ListGetData+0x10>
c0101b18: 83 ec 0c                      sub esp, 12
c0101b1b: 6a 10                         push 16
c0101b1d: e8 7d 70 00 00                call 0xc0108b9f <Panic>
c0101b22: 8b 00                         mov eax, dword ptr [eax]
c0101b24: 83 c4 0c                      add esp, 12
c0101b27: c3                            ret

c0101b28 <ListDeleteIndex>:
c0101b28: 55                            push ebp
c0101b29: 57                            push edi
c0101b2a: 56                            push esi
c0101b2b: 53                            push ebx
c0101b2c: 83 ec 0c                      sub esp, 12
c0101b2f: 8b 5c 24 20                   mov ebx, dword ptr [esp + 32]
c0101b33: 8b 44 24 24                   mov eax, dword ptr [esp + 36]
c0101b37: 39 03                         cmp dword ptr [ebx], eax
c0101b39: 0f 9e c0                      setle al
c0101b3c: 8b 54 24 24                   mov edx, dword ptr [esp + 36]
c0101b40: c1 ea 1f                      shr edx, 31
c0101b43: 08 d0                         or al, dl
c0101b45: 75 43                         jne 0xc0101b8a <ListDeleteIndex+0x62>
c0101b47: 8b 6b 04                      mov ebp, dword ptr [ebx + 4]
c0101b4a: 89 ea                         mov edx, ebp
c0101b4c: 31 c9                         xor ecx, ecx
c0101b4e: 31 f6                         xor esi, esi
c0101b50: 85 d2                         test edx, edx
c0101b52: 74 38                         je 0xc0101b8c <ListDeleteIndex+0x64>
c0101b54: 8b 7a 04                      mov edi, dword ptr [edx + 4]
c0101b57: 39 4c 24 24                   cmp dword ptr [esp + 36], ecx
c0101b5b: 75 26                         jne 0xc0101b83 <ListDeleteIndex+0x5b>
c0101b5d: 39 d5                         cmp ebp, edx
c0101b5f: 75 05                         jne 0xc0101b66 <ListDeleteIndex+0x3e>
c0101b61: 89 7b 04                      mov dword ptr [ebx + 4], edi
c0101b64: eb 03                         jmp 0xc0101b69 <ListDeleteIndex+0x41>
c0101b66: 89 7e 04                      mov dword ptr [esi + 4], edi
c0101b69: 3b 53 08                      cmp edx, dword ptr [ebx + 8]
c0101b6c: 75 03                         jne 0xc0101b71 <ListDeleteIndex+0x49>
c0101b6e: 89 73 08                      mov dword ptr [ebx + 8], esi
c0101b71: 83 ec 0c                      sub esp, 12
c0101b74: 52                            push edx
c0101b75: e8 f9 1d 00 00                call 0xc0103973 <FreeHeap>
c0101b7a: ff 0b                         dec dword ptr [ebx]
c0101b7c: 83 c4 10                      add esp, 16
c0101b7f: b0 01                         mov al, 1
c0101b81: eb 09                         jmp 0xc0101b8c <ListDeleteIndex+0x64>
c0101b83: 41                            inc ecx
c0101b84: 89 d6                         mov esi, edx
c0101b86: 89 fa                         mov edx, edi
c0101b88: eb c6                         jmp 0xc0101b50 <ListDeleteIndex+0x28>
c0101b8a: 31 c0                         xor eax, eax
c0101b8c: 83 c4 0c                      add esp, 12
c0101b8f: 5b                            pop ebx
c0101b90: 5e                            pop esi
c0101b91: 5f                            pop edi
c0101b92: 5d                            pop ebp
c0101b93: c3                            ret

c0101b94 <ListDeleteData>:
```

```
c0101be0: 85 c0                         test eax, eax
c0101be2: 75 0a                         jne 0xc0101bee <ListGetNextNode+0x15>
c0101be4: 83 ec 0c                      sub esp, 12
c0101be7: 6a 10                         push 16
c0101be9: e8 b1 6f 00 00                call 0xc0108b9f <Panic>
c0101bee: 8b 40 04                      mov eax, dword ptr [eax + 4]
c0101bf1: 83 c4 0c                      add esp, 12
c0101bf4: c3                            ret

c0101bf5 <ListGetDataFromNode>:
c0101bf5: 83 ec 0c                      sub esp, 12
c0101bf8: 8b 44 24 10                   mov eax, dword ptr [esp + 16]
c0101bfc: 85 c0                         test eax, eax
c0101bfe: 75 0a                         jne 0xc0101c0a <ListGetDataFromNode+0x15>
c0101c00: 83 ec 0c                      sub esp, 12
c0101c03: 6a 10                         push 16
c0101c05: e8 95 6f 00 00                call 0xc0108b9f <Panic>
c0101c0a: 8b 00                         mov eax, dword ptr [eax]
c0101c0c: 83 c4 0c                      add esp, 12
c0101c0f: c3                            ret

c0101c10 <ListGetDataAtIndex>:
c0101c10: 8b 54 24 08                   mov edx, dword ptr [esp + 8]
c0101c14: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c0101c18: 8b 40 04                      mov eax, dword ptr [eax + 4]
c0101c1b: 85 d2                         test edx, edx
c0101c1d: 7e 06                         jle 0xc0101c25 <ListGetDataAtIndex+0x15>
c0101c1f: 4a                            dec edx
c0101c20: 85 c0                         test eax, eax
c0101c22: 75 f4                         jne 0xc0101c18 <ListGetDataAtIndex+0x8>
c0101c24: c3                            ret
c0101c25: 85 c0                         test eax, eax
c0101c27: 74 02                         je 0xc0101c2b <ListGetDataAtIndex+0x1b>
c0101c29: 8b 00                         mov eax, dword ptr [eax]
c0101c2b: c3                            ret

c0101c2c <StackAdtCreate>:
c0101c2c: 53                            push ebx
c0101c2d: 83 ec 14                      sub esp, 20
c0101c30: 6a 04                         push 4
c0101c32: e8 18 1d 00 00                call 0xc010394f <AllocHeap>
c0101c37: 89 c3                         mov ebx, eax
c0101c39: e8 fa fd ff ff                call 0xc0101a38 <ListCreate>
c0101c3e: 89 03                         mov dword ptr [ebx], eax
c0101c40: 89 d8                         mov eax, ebx
c0101c42: 83 c4 18                      add esp, 24
c0101c45: 5b                            pop ebx
c0101c46: c3                            ret

c0101c47 <StackAdtDestroy>:
c0101c47: 53                            push ebx
c0101c48: 83 ec 14                      sub esp, 20
c0101c4b: 8b 5c 24 1c                   mov ebx, dword ptr [esp + 28]
c0101c4f: ff 33                         push dword ptr [ebx]
c0101c51: e8 5a ff ff ff                call 0xc0101bb0 <ListDestroy>
c0101c56: 89 5c 24 20                   mov dword ptr [esp + 32], ebx
c0101c5a: 83 c4 18                      add esp, 24
c0101c5d: 5b                            pop ebx
c0101c5e: e9 10 1d 00 00                jmp 0xc0103973 <FreeHeap>

c0101c63 <StackAdtPush>:
c0101c63: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c0101c67: 8b 00                         mov eax, dword ptr [eax]
c0101c69: 89 44 24 04                   mov dword ptr [esp + 4], eax
c0101c6d: e9 d4 fd ff ff                jmp 0xc0101a46 <ListInsertStart>

c0101c72 <StackAdtPeek>:
c0101c72: 83 ec 18                      sub esp, 24
c0101c75: 8b 44 24 1c                   mov eax, dword ptr [esp + 28]
c0101c79: ff 30                         push dword ptr [eax]
c0101c7b: e8 59 ff ff ff                call 0xc0101bd9 <ListGetNextNode>
```

```
c0101cbf <AvlGet>:
c0101cbf: 57                            push edi
c0101cc0: 56                            push esi
c0101cc1: 53                            push ebx
c0101cc2: 89 d6                         mov esi, edx
c0101cc4: 89 cf                         mov edi, ecx
c0101cc6: 89 c3                         mov ebx, eax
c0101cc8: 85 db                         test ebx, ebx
c0101cca: 74 2a                         je 0xc0101cf6 <AvlGet+0x37>
c0101ccc: 50                            push eax
c0101ccd: 50                            push eax
c0101cce: 56                            push esi
c0101ccf: ff 73 08                      push dword ptr [ebx + 8]
c0101cd2: ff d7                         call edi
c0101cd4: 83 c4 10                      add esp, 16
c0101cd7: 85 c0                         test eax, eax
c0101cd9: 75 05                         jne 0xc0101ce0 <AvlGet+0x21>
c0101cdb: 8b 5b 08                      mov ebx, dword ptr [ebx + 8]
c0101cde: eb 16                         jmp 0xc0101cf6 <AvlGet+0x37>
c0101ce0: 89 f9                         mov ecx, edi
c0101ce2: 89 f2                         mov edx, esi
c0101ce4: 8b 03                         mov eax, dword ptr [ebx]
c0101ce6: e8 d4 ff ff ff                call 0xc0101cbf <AvlGet>
c0101ceb: 85 c0                         test eax, eax
c0101ced: 75 05                         jne 0xc0101cf4 <AvlGet+0x35>
c0101cef: 8b 5b 04                      mov ebx, dword ptr [ebx + 4]
c0101cf2: eb d4                         jmp 0xc0101cc8 <AvlGet+0x9>
c0101cf4: 89 c3                         mov ebx, eax
c0101cf6: 89 d8                         mov eax, ebx
c0101cf8: 5b                            pop ebx
c0101cf9: 5e                            pop esi
c0101cfa: 5f                            pop edi
c0101cfb: c3                            ret

c0101cfc <AvlContains>:
c0101cfc: 85 c0                         test eax, eax
c0101cfe: 74 46                         je 0xc0101d46 <AvlContains+0x4a>
c0101d00: 57                            push edi
c0101d01: 56                            push esi
c0101d02: 53                            push ebx
c0101d03: 89 c3                         mov ebx, eax
c0101d05: 89 d6                         mov esi, edx
c0101d07: 89 cf                         mov edi, ecx
c0101d09: 50                            push eax
c0101d0a: 50                            push eax
c0101d0b: 52                            push edx
c0101d0c: ff 73 08                      push dword ptr [ebx + 8]
c0101d0f: ff d1                         call ecx
c0101d11: 89 c2                         mov edx, eax
c0101d13: 83 c4 10                      add esp, 16
c0101d16: b0 01                         mov al, 1
c0101d18: 85 d2                         test edx, edx
c0101d1a: 74 2d                         je 0xc0101d49 <AvlContains+0x4d>
c0101d1c: 89 f9                         mov ecx, edi
c0101d1e: 89 f2                         mov edx, esi
c0101d20: 8b 03                         mov eax, dword ptr [ebx]
c0101d22: e8 d5 ff ff ff                call 0xc0101cfc <AvlContains>
c0101d27: 88 c2                         mov dl, al
c0101d29: b8 01 00 00 00                mov eax, 1
c0101d2e: 84 d2                         test dl, dl
c0101d30: 75 0f                         jne 0xc0101d41 <AvlContains+0x45>
c0101d32: 8b 43 04                      mov eax, dword ptr [ebx + 4]
c0101d35: 89 f9                         mov ecx, edi
c0101d37: 89 f2                         mov edx, esi
c0101d39: e8 be ff ff ff                call 0xc0101cfc <AvlContains>
c0101d3e: 0f b6 c0                      movzx eax, al
c0101d41: 83 e0 01                      and eax, 1
c0101d44: eb 03                         jmp 0xc0101d49 <AvlContains+0x4d>
c0101d46: 31 c0                         xor eax, eax
c0101d48: c3                            ret
c0101d49: 5b                            pop ebx
```

```
c0101d82: ff 73 08                  push dword ptr [ebx + 8]
c0101d85: ff d6                     call esi
c0101d87: 83 c4 10                  add esp, 16
c0101d8a: 83 ec 0c                  sub esp, 12
c0101d8d: 53                        push ebx
c0101d8e: e8 e0 1b 00 00            call 0xc0103973 <FreeHeap>
c0101d93: 83 c4 14                  add esp, 20
c0101d96: 5b                        pop ebx
c0101d97: 5e                        pop esi
c0101d98: c3                        ret
c0101d99: c3                        ret

c0101d9a <AvlPrint>:
c0101d9a: 56                        push esi
c0101d9b: 53                        push ebx
c0101d9c: 51                        push ecx
c0101d9d: 89 c3                     mov ebx, eax
c0101d9f: 89 d6                     mov esi, edx
c0101da1: 85 db                     test ebx, ebx
c0101da3: 74 2e                     je 0xc0101dd3 <AvlPrint+0x39>
c0101da5: 89 f2                     mov edx, esi
c0101da7: 8b 03                     mov eax, dword ptr [ebx]
c0101da9: e8 ec ff ff ff            call 0xc0101d9a <AvlPrint>
c0101dae: 85 f6                     test esi, esi
c0101db0: 75 11                     jne 0xc0101dc3 <AvlPrint+0x29>
c0101db2: 52                        push edx
c0101db3: 52                        push edx
c0101db4: ff 73 08                  push dword ptr [ebx + 8]
c0101db7: 68 49 04 11 c0            push 3222340681
c0101dbc: e8 04 6d 00 00            call 0xc0108ac5 <LogWriteSerial>
c0101dc1: eb 08                     jmp 0xc0101dcb <AvlPrint+0x31>
c0101dc3: 83 ec 0c                  sub esp, 12
c0101dc6: ff 73 08                  push dword ptr [ebx + 8]
c0101dc9: ff d6                     call esi
c0101dcb: 83 c4 10                  add esp, 16
c0101dce: 8b 5b 04                  mov ebx, dword ptr [ebx + 4]
c0101dd1: eb ce                     jmp 0xc0101da1 <AvlPrint+0x7>
c0101dd3: 58                        pop eax
c0101dd4: 5b                        pop ebx
c0101dd5: 5e                        pop esi
c0101dd6: c3                        ret

c0101dd7 <AvlGetHeight>:
c0101dd7: 55                        push ebp
c0101dd8: 57                        push edi
c0101dd9: 56                        push esi
c0101dda: 53                        push ebx
c0101ddb: 83 ec 0c                  sub esp, 12
c0101dde: 89 c3                     mov ebx, eax
c0101de0: 31 f6                     xor esi, esi
c0101de2: 85 db                     test ebx, ebx
c0101de4: 74 75                     je 0xc0101e5b <AvlGetHeight+0x84>
c0101de6: 81 fb ff ff ff 0e         cmp ebx, 251658239
c0101dec: 77 10                     ja 0xc0101dfe <AvlGetHeight+0x27>
c0101dee: 50                        push eax
c0101def: 50                        push eax
c0101df0: 53                        push ebx
c0101df1: 68 55 04 11 c0            push 3222340693
c0101df6: e8 ca 6c 00 00            call 0xc0108ac5 <LogWriteSerial>
c0101dfb: 83 c4 10                  add esp, 16
c0101dfe: 8b 03                     mov eax, dword ptr [ebx]
c0101e00: 31 ed                     xor ebp, ebp
c0101e02: 85 c0                     test eax, eax
c0101e04: 74 0c                     je 0xc0101e12 <AvlGetHeight+0x3b>
c0101e06: 31 c9                     xor ecx, ecx
c0101e08: 3d ff ff ff 0e            cmp eax, 251658239
c0101e0d: 0f 96 c1                  setbe cl
c0101e10: 89 cd                     mov ebp, ecx
c0101e12: 8b 53 04                  mov edx, dword ptr [ebx + 4]
c0101e15: 31 ff                     xor edi, edi
c0101e17: 85 d2                     test edx, edx
```

```
c0101e62: 5f                            pop edi
c0101e63: 5d                            pop ebp
c0101e64: c3                            ret

c0101e65 <AvlGetBalance>:
c0101e65: 85 c0                         test eax, eax
c0101e67: 74 20                         je 0xc0101e89 <AvlGetBalance+0x24>
c0101e69: 56                            push esi
c0101e6a: 53                            push ebx
c0101e6b: 52                            push edx
c0101e6c: 89 c6                         mov esi, eax
c0101e6e: 8b 00                         mov eax, dword ptr [eax]
c0101e70: e8 62 ff ff ff                call 0xc0101dd7 <AvlGetHeight>
c0101e75: 89 c3                         mov ebx, eax
c0101e77: 8b 46 04                      mov eax, dword ptr [esi + 4]
c0101e7a: e8 58 ff ff ff                call 0xc0101dd7 <AvlGetHeight>
c0101e7f: 89 c2                         mov edx, eax
c0101e81: 89 d8                         mov eax, ebx
c0101e83: 29 d0                         sub eax, edx
c0101e85: 59                            pop ecx
c0101e86: 5b                            pop ebx
c0101e87: 5e                            pop esi
c0101e88: c3                            ret
c0101e89: 31 c0                         xor eax, eax
c0101e8b: c3                            ret

c0101e8c <AvlBalance>:
c0101e8c: 53                            push ebx
c0101e8d: 83 ec 08                      sub esp, 8
c0101e90: 89 c3                         mov ebx, eax
c0101e92: 85 c0                         test eax, eax
c0101e94: 74 5a                         je 0xc0101ef0 <AvlBalance+0x64>
c0101e96: e8 ca ff ff ff                call 0xc0101e65 <AvlGetBalance>
c0101e9b: 83 f8 fe                      cmp eax, -2
c0101e9e: 75 27                         jne 0xc0101ec7 <AvlBalance+0x3b>
c0101ea0: 8b 43 04                      mov eax, dword ptr [ebx + 4]
c0101ea3: e8 bd ff ff ff                call 0xc0101e65 <AvlGetBalance>
c0101ea8: 48                            dec eax
c0101ea9: 75 10                         jne 0xc0101ebb <AvlBalance+0x2f>
c0101eab: 8b 53 04                      mov edx, dword ptr [ebx + 4]
c0101eae: 8b 02                         mov eax, dword ptr [edx]
c0101eb0: 8b 48 04                      mov ecx, dword ptr [eax + 4]
c0101eb3: 89 50 04                      mov dword ptr [eax + 4], edx
c0101eb6: 89 0a                         mov dword ptr [edx], ecx
c0101eb8: 89 43 04                      mov dword ptr [ebx + 4], eax
c0101ebb: 8b 43 04                      mov eax, dword ptr [ebx + 4]
c0101ebe: 8b 10                         mov edx, dword ptr [eax]
c0101ec0: 89 18                         mov dword ptr [eax], ebx
c0101ec2: 89 53 04                      mov dword ptr [ebx + 4], edx
c0101ec5: eb 27                         jmp 0xc0101eee <AvlBalance+0x62>
c0101ec7: 83 f8 02                      cmp eax, 2
c0101eca: 75 24                         jne 0xc0101ef0 <AvlBalance+0x64>
c0101ecc: 8b 03                         mov eax, dword ptr [ebx]
c0101ece: e8 92 ff ff ff                call 0xc0101e65 <AvlGetBalance>
c0101ed3: 40                            inc eax
c0101ed4: 75 0e                         jne 0xc0101ee4 <AvlBalance+0x58>
c0101ed6: 8b 13                         mov edx, dword ptr [ebx]
c0101ed8: 8b 42 04                      mov eax, dword ptr [edx + 4]
c0101edb: 8b 08                         mov ecx, dword ptr [eax]
c0101edd: 89 10                         mov dword ptr [eax], edx
c0101edf: 89 4a 04                      mov dword ptr [edx + 4], ecx
c0101ee2: 89 03                         mov dword ptr [ebx], eax
c0101ee4: 8b 03                         mov eax, dword ptr [ebx]
c0101ee6: 8b 50 04                      mov edx, dword ptr [eax + 4]
c0101ee9: 89 58 04                      mov dword ptr [eax + 4], ebx
c0101eec: 89 13                         mov dword ptr [ebx], edx
c0101eee: 89 c3                         mov ebx, eax
c0101ef0: 89 d8                         mov eax, ebx
c0101ef2: 83 c4 08                      add esp, 8
c0101ef5: 5b                            pop ebx
c0101ef6: c3                            ret
```

```
c0101f39: 85 c0                   test eax, eax
c0101f3b: 8b 43 04                mov eax, dword ptr [ebx + 4]
c0101f3e: 8b 4c 24 0c             mov ecx, dword ptr [esp + 12]
c0101f42: 7e 10                   jle 0xc0101f54 <AvlDelete+0x5d>
c0101f44: 89 f2                   mov edx, esi
c0101f46: e8 ac ff ff ff          call 0xc0101ef7 <AvlDelete>
c0101f4b: 89 43 04                mov dword ptr [ebx + 4], eax
c0101f4e: 89 de                   mov esi, ebx
c0101f50: 31 db                   xor ebx, ebx
c0101f52: eb 1e                   jmp 0xc0101f72 <AvlDelete+0x7b>
c0101f54: 8b 33                   mov esi, dword ptr [ebx]
c0101f56: 85 f6                   test esi, esi
c0101f58: 74 16                   je 0xc0101f70 <AvlDelete+0x79>
c0101f5a: 85 c0                   test eax, eax
c0101f5c: 74 14                   je 0xc0101f72 <AvlDelete+0x7b>
c0101f5e: 89 c2                   mov edx, eax
c0101f60: 89 d6                   mov esi, edx
c0101f62: 8b 12                   mov edx, dword ptr [edx]
c0101f64: 85 d2                   test edx, edx
c0101f66: 75 f8                   jne 0xc0101f60 <AvlDelete+0x69>
c0101f68: 8b 56 08                mov edx, dword ptr [esi + 8]
c0101f6b: 89 53 08                mov dword ptr [ebx + 8], edx
c0101f6e: eb d6                   jmp 0xc0101f46 <AvlDelete+0x4f>
c0101f70: 89 c6                   mov esi, eax
c0101f72: 83 ec 0c                sub esp, 12
c0101f75: 53                      push ebx
c0101f76: e8 f8 19 00 00          call 0xc0103973 <FreeHeap>
c0101f7b: 89 f0                   mov eax, esi
c0101f7d: 83 c4 24                add esp, 36
c0101f80: 5b                      pop ebx
c0101f81: 5e                      pop esi
c0101f82: e9 05 ff ff ff          jmp 0xc0101e8c <AvlBalance>
c0101f87: 31 c0                   xor eax, eax
c0101f89: c3                      ret

c0101f8a <AvlInsert>:
c0101f8a: 55                      push ebp
c0101f8b: 57                      push edi
c0101f8c: 56                      push esi
c0101f8d: 53                      push ebx
c0101f8e: 83 ec 24                sub esp, 36
c0101f91: 89 c3                   mov ebx, eax
c0101f93: 89 d7                   mov edi, edx
c0101f95: ff 70 08                push dword ptr [eax + 8]
c0101f98: 52                      push edx
c0101f99: 89 4c 24 1c             mov dword ptr [esp + 28], ecx
c0101f9d: ff d1                   call ecx
c0101f9f: 83 c4 10                add esp, 16
c0101fa2: 85 c0                   test eax, eax
c0101fa4: 8b 4c 24 0c             mov ecx, dword ptr [esp + 12]
c0101fa8: 79 41                   jns 0xc0101feb <AvlInsert+0x61>
c0101faa: 8b 03                   mov eax, dword ptr [ebx]
c0101fac: 85 c0                   test eax, eax
c0101fae: 75 1b                   jne 0xc0101fcb <AvlInsert+0x41>
c0101fb0: 83 ec 0c                sub esp, 12
c0101fb3: 6a 0c                   push 12
c0101fb5: e8 95 19 00 00          call 0xc010394f <AllocHeap>
c0101fba: 89 c6                   mov esi, eax
c0101fbc: 31 d2                   xor edx, edx
c0101fbe: 89 10                   mov dword ptr [eax], edx
c0101fc0: 89 50 04                mov dword ptr [eax + 4], edx
c0101fc3: 89 78 08                mov dword ptr [eax + 8], edi
c0101fc6: 83 c4 10                add esp, 16
c0101fc9: eb 09                   jmp 0xc0101fd4 <AvlInsert+0x4a>
c0101fcb: 89 fa                   mov edx, edi
c0101fcd: e8 b8 ff ff ff          call 0xc0101f8a <AvlInsert>
c0101fd2: 89 c6                   mov esi, eax
c0101fd4: 8b 6b 04                mov ebp, dword ptr [ebx + 4]
c0101fd7: 8b 7b 08                mov edi, dword ptr [ebx + 8]
c0101fda: 83 ec 0c                sub esp, 12
c0101fdd: 6a 0c                   push 12
```

```
c0102030: 89 44 24 0c                   mov dword ptr [esp + 12], eax
c0102034: 83 ec 0c                      sub esp, 12
c0102037: 53                            push ebx
c0102038: e8 36 19 00 00                call 0xc0103973 <FreeHeap>
c010203d: 8b 44 24 1c                   mov eax, dword ptr [esp + 28]
c0102041: 83 c4 2c                      add esp, 44
c0102044: 5b                            pop ebx
c0102045: 5e                            pop esi
c0102046: 5f                            pop edi
c0102047: 5d                            pop ebp
c0102048: e9 3f fe ff ff                jmp 0xc0101e8c <AvlBalance>

c010204d <TreeCreate>:
c010204d: 83 ec 18                      sub esp, 24
c0102050: 6a 10                         push 16
c0102052: e8 f8 18 00 00                call 0xc010394f <AllocHeap>
c0102057: 31 d2                         xor edx, edx
c0102059: 89 10                         mov dword ptr [eax], edx
c010205b: 89 50 04                      mov dword ptr [eax + 4], edx
c010205e: 89 50 08                      mov dword ptr [eax + 8], edx
c0102061: c7 40 0c 4d 1d 10 c0          mov dword ptr [eax + 12], 3222281549
c0102068: 83 c4 1c                      add esp, 28
c010206b: c3                            ret

c010206c <TreeSetDeletionHandler>:
c010206c: 8b 54 24 04                   mov edx, dword ptr [esp + 4]
c0102070: 8b 42 08                      mov eax, dword ptr [edx + 8]
c0102073: 8b 4c 24 08                   mov ecx, dword ptr [esp + 8]
c0102077: 89 4a 08                      mov dword ptr [edx + 8], ecx
c010207a: c3                            ret

c010207b <TreeSetComparator>:
c010207b: 8b 54 24 04                   mov edx, dword ptr [esp + 4]
c010207f: 8b 42 0c                      mov eax, dword ptr [edx + 12]
c0102082: 8b 4c 24 08                   mov ecx, dword ptr [esp + 8]
c0102086: 89 4a 0c                      mov dword ptr [edx + 12], ecx
c0102089: c3                            ret

c010208a <TreeInsert>:
c010208a: 53                            push ebx
c010208b: 83 ec 08                      sub esp, 8
c010208e: 8b 5c 24 10                   mov ebx, dword ptr [esp + 16]
c0102092: 8b 43 04                      mov eax, dword ptr [ebx + 4]
c0102095: 85 c0                         test eax, eax
c0102097: 75 1d                         jne 0xc01020b6 <TreeInsert+0x2c>
c0102099: 83 ec 0c                      sub esp, 12
c010209c: 6a 0c                         push 12
c010209e: e8 ac 18 00 00                call 0xc010394f <AllocHeap>
c01020a3: 31 c9                         xor ecx, ecx
c01020a5: 89 08                         mov dword ptr [eax], ecx
c01020a7: 89 48 04                      mov dword ptr [eax + 4], ecx
c01020aa: 8b 54 24 24                   mov edx, dword ptr [esp + 36]
c01020ae: 89 50 08                      mov dword ptr [eax + 8], edx
c01020b1: 83 c4 10                      add esp, 16
c01020b4: eb 0c                         jmp 0xc01020c2 <TreeInsert+0x38>
c01020b6: 8b 4b 0c                      mov ecx, dword ptr [ebx + 12]
c01020b9: 8b 54 24 14                   mov edx, dword ptr [esp + 20]
c01020bd: e8 c8 fe ff ff                call 0xc0101f8a <AvlInsert>
c01020c2: 89 43 04                      mov dword ptr [ebx + 4], eax
c01020c5: ff 03                         inc dword ptr [ebx]
c01020c7: 83 c4 08                      add esp, 8
c01020ca: 5b                            pop ebx
c01020cb: c3                            ret

c01020cc <TreeDelete>:
c01020cc: 53                            push ebx
c01020cd: 83 ec 08                      sub esp, 8
c01020d0: 8b 5c 24 10                   mov ebx, dword ptr [esp + 16]
c01020d4: 8b 4b 0c                      mov ecx, dword ptr [ebx + 12]
c01020d7: 8b 43 04                      mov eax, dword ptr [ebx + 4]
c01020da: 8b 54 24 14                   mov edx, dword ptr [esp + 20]
```

```
c010212a: 83 c4 08                  add esp, 8
c010212d: 5b                        pop ebx
c010212e: e9 40 18 00 00            jmp 0xc0103973 <FreeHeap>

c0102133 <TreePrint>:
c0102133: 8b 44 24 04               mov eax, dword ptr [esp + 4]
c0102137: 8b 40 04                  mov eax, dword ptr [eax + 4]
c010213a: 8b 54 24 08               mov edx, dword ptr [esp + 8]
c010213e: e9 57 fc ff ff            jmp 0xc0101d9a <AvlPrint>

c0102143 <ReduceCache>:
c0102143: 53                        push ebx
c0102144: 83 ec 10                  sub esp, 16
c0102147: 8b 5c 24 18               mov ebx, dword ptr [esp + 24]
c010214b: 6a ff                     push -1
c010214d: ff 73 0c                  push dword ptr [ebx + 12]
c0102150: e8 e4 45 00 00            call 0xc0106739 <AcquireSemaphore>
c0102155: 8b 43 0c                  mov eax, dword ptr [ebx + 12]
c0102158: 89 44 24 20               mov dword ptr [esp + 32], eax
c010215c: 83 c4 18                  add esp, 24
c010215f: 5b                        pop ebx
c0102160: e9 4e 47 00 00            jmp 0xc01068b3 <ReleaseSemaphore>

c0102165 <ReduceCacheAmounts>:
c0102165: 57                        push edi
c0102166: 56                        push esi
c0102167: 53                        push ebx
c0102168: 89 c6                     mov esi, eax
c010216a: 83 ec 0c                  sub esp, 12
c010216d: ff 35 04 40 11 c0         push dword ptr [-1072611324]
c0102173: e8 61 fa ff ff            call 0xc0101bd9 <ListGetNextNode>
c0102178: 89 c3                     mov ebx, eax
c010217a: 83 c4 10                  add esp, 16
c010217d: bf 43 21 10 c0            mov edi, 3222282563
c0102182: 89 f0                     mov eax, esi
c0102184: 84 c0                     test al, al
c0102186: 74 05                     je 0xc010218d <ReduceCacheAmounts+0x28>
c0102188: bf b6 21 10 c0            mov edi, 3222282678
c010218d: 85 db                     test ebx, ebx
c010218f: 74 21                     je 0xc01021b2 <ReduceCacheAmounts+0x4d>
c0102191: 83 ec 0c                  sub esp, 12
c0102194: 53                        push ebx
c0102195: e8 5b fa ff ff            call 0xc0101bf5 <ListGetDataFromNode>
c010219a: 5a                        pop edx
c010219b: 8b 40 30                  mov eax, dword ptr [eax + 48]
c010219e: ff 70 28                  push dword ptr [eax + 40]
c01021a1: ff d7                     call edi
c01021a3: 89 1c 24                  mov dword ptr [esp], ebx
c01021a6: e8 2e fa ff ff            call 0xc0101bd9 <ListGetNextNode>
c01021ab: 89 c3                     mov ebx, eax
c01021ad: 83 c4 10                  add esp, 16
c01021b0: eb db                     jmp 0xc010218d <ReduceCacheAmounts+0x28>
c01021b2: 5b                        pop ebx
c01021b3: 5e                        pop esi
c01021b4: 5f                        pop edi
c01021b5: c3                        ret

c01021b6 <TossCache>:
c01021b6: 53                        push ebx
c01021b7: 83 ec 10                  sub esp, 16
c01021ba: 8b 5c 24 18               mov ebx, dword ptr [esp + 24]
c01021be: 6a ff                     push -1
c01021c0: ff 73 0c                  push dword ptr [ebx + 12]
c01021c3: e8 71 45 00 00            call 0xc0106739 <AcquireSemaphore>
c01021c8: 58                        pop eax
c01021c9: ff 73 08                  push dword ptr [ebx + 8]
c01021cc: e8 42 ff ff ff            call 0xc0102113 <TreeDestroy>
c01021d1: e8 77 fe ff ff            call 0xc010204d <TreeCreate>
c01021d6: 89 43 08                  mov dword ptr [ebx + 8], eax
c01021d9: 8b 43 0c                  mov eax, dword ptr [ebx + 12]
c01021dc: 89 44 24 20               mov dword ptr [esp + 32], eax
```

```
c0102229: b9 00 00 00 00                mov ecx, 0
c010222e: 72 4a                         jb 0xc010227a <Comparator+0x91>
c0102230: 39 54 24 04                   cmp dword ptr [esp + 4], edx
c0102234: 75 3f                         jne 0xc0102275 <Comparator+0x8c>
c0102236: 39 04 24                      cmp dword ptr [esp], eax
c0102239: 75 3a                         jne 0xc0102275 <Comparator+0x8c>
c010223b: 8b 34 24                      mov esi, dword ptr [esp]
c010223e: 8b 7c 24 04                   mov edi, dword ptr [esp + 4]
c0102242: 03 75 04                      add esi, dword ptr [ebp + 4]
c0102245: 83 d7 00                      adc edi, 0
c0102248: 89 fb                         mov ebx, edi
c010224a: 39 f0                         cmp eax, esi
c010224c: 89 d7                         mov edi, edx
c010224e: 19 df                         sbb edi, ebx
c0102250: b9 00 00 00 00                mov ecx, 0
c0102255: 72 23                         jb 0xc010227a <Comparator+0x91>
c0102257: 8b 1c 24                      mov ebx, dword ptr [esp]
c010225a: 39 d8                         cmp eax, ebx
c010225c: 89 d7                         mov edi, edx
c010225e: 1b 7c 24 04                   sbb edi, dword ptr [esp + 4]
c0102262: b9 01 00 00 00                mov ecx, 1
c0102267: 72 11                         jb 0xc010227a <Comparator+0x91>
c0102269: 39 c3                         cmp ebx, eax
c010226b: 8b 7c 24 04                   mov edi, dword ptr [esp + 4]
c010226f: 19 d7                         sbb edi, edx
c0102271: 19 c9                         sbb ecx, ecx
c0102273: eb 05                         jmp 0xc010227a <Comparator+0x91>
c0102275: b9 01 00 00 00                mov ecx, 1
c010227a: 89 c8                         mov eax, ecx
c010227c: 83 c4 0c                      add esp, 12
c010227f: 5b                            pop ebx
c0102280: 5e                            pop esi
c0102281: 5f                            pop edi
c0102282: 5d                            pop ebp
c0102283: c3                            ret

c0102284 <IsCacheCreationAllowed>:
c0102284: 83 ec 24                      sub esp, 36
c0102287: 6a ff                         push -1
c0102289: ff 35 00 40 11 c0             push dword ptr [-1072611328]
c010228f: e8 a5 44 00 00                call 0xc0106739 <AcquireSemaphore>
c0102294: 58                            pop eax
c0102295: 83 3d 08 40 11 c0 00          cmp dword ptr [-1072611320], 0
c010229c: 0f 94 44 24 1b                sete byte ptr [esp + 27]
c01022a1: ff 35 00 40 11 c0             push dword ptr [-1072611328]
c01022a7: e8 07 46 00 00                call 0xc01068b3 <ReleaseSemaphore>
c01022ac: 8a 44 24 1f                   mov al, byte ptr [esp + 31]
c01022b0: 83 c4 2c                      add esp, 44
c01022b3: c3                            ret

c01022b4 <RemoveCacheEntryHandler>:
c01022b4: 83 ec 18                      sub esp, 24
c01022b7: 68 a1 04 11 c0                push 3222340769
c01022bc: e8 1c 68 00 00                call 0xc0108add <LogDeveloperWarning>
c01022c1: c7 44 24 20 c7 04 11 c0       mov dword ptr [esp + 32], 3222340807
c01022c9: 83 c4 1c                      add esp, 28
c01022cc: e9 0c 68 00 00                jmp 0xc0108add <LogDeveloperWarning>

c01022d1 <CreateDiskCache>:
c01022d1: 83 ec 18                      sub esp, 24
c01022d4: 8b 44 24 1c                   mov eax, dword ptr [esp + 28]
c01022d8: ff 70 30                      push dword ptr [eax + 48]
c01022db: e8 10 83 00 00                call 0xc010a5f0 <VnodeOpDirentType>
c01022e0: 8b 44 24 20                   mov eax, dword ptr [esp + 32]
c01022e4: 83 c4 1c                      add esp, 28
c01022e7: c3                            ret

c01022e8 <SetDiskCaches>:
c01022e8: 53                            push ebx
c01022e9: 83 ec 08                      sub esp, 8
c01022ec: 8b 5c 24 10                   mov ebx, dword ptr [esp + 16]
```

```
c010234d: e9 61 45 00 00                jmp 0xc01068b3 <ReleaseSemaphore>
c0102352: 83 c4 08                      add esp, 8
c0102355: 5b                            pop ebx
c0102356: c3                            ret

c0102357 <InitDiskCaches>:
c0102357: 83 ec 0c                      sub esp, 12
c010235a: e8 d9 f6 ff ff                call 0xc0101a38 <ListCreate>
c010235f: a3 04 40 11 c0                mov dword ptr [3222355972], eax
c0102364: 50                            push eax
c0102365: 6a 00                         push 0
c0102367: 6a 01                         push 1
c0102369: 68 e6 04 11 c0                push 3222340838
c010236e: e8 66 43 00 00                call 0xc01066d9 <CreateSemaphore>
c0102373: a3 00 40 11 c0                mov dword ptr [3222355968], eax
c0102378: 83 c4 1c                      add esp, 28
c010237b: c3                            ret

c010237c <ReadWrite>:
c010237c: 31 c0                         xor eax, eax
c010237e: c3                            ret

c010237f <InitNullDevice>:
c010237f: 57                            push edi
c0102380: 56                            push esi
c0102381: 83 ec 54                      sub esp, 84
c0102384: 8d 7c 24 10                   lea edi, [esp + 16]
c0102388: b9 10 00 00 00                mov ecx, 16
c010238d: 31 c0                         xor eax, eax
c010238f: f3 ab                         rep  stosd dword ptr es:[edi], eax
c0102391: e8 36 77 00 00                call 0xc0109acc <NextDevId>
c0102396: 89 44 24 08                   mov dword ptr [esp + 8], eax
c010239a: 99                            cdq
c010239b: 89 54 24 0c                   mov dword ptr [esp + 12], edx
c010239f: c7 44 24 14 ff 01 01 00       mov dword ptr [esp + 20], 66047
c01023a7: c7 44 24 18 01 00 00 00       mov dword ptr [esp + 24], 1
c01023af: 83 ec 48                      sub esp, 72
c01023b2: 8d 74 24 50                   lea esi, [esp + 80]
c01023b6: b9 12 00 00 00                mov ecx, 18
c01023bb: 89 e7                         mov edi, esp
c01023bd: f3 a5                         rep  movsd dword ptr es:[edi], dword ptr [esi
c01023bf: 83 ec 28                      sub esp, 40
c01023c2: be 00 00 11 c0                mov esi, 3222339584
c01023c7: b9 0a 00 00 00                mov ecx, 10
c01023cc: 89 e7                         mov edi, esp
c01023ce: f3 a5                         rep  movsd dword ptr es:[edi], dword ptr [esi
c01023d0: e8 de 7f 00 00                call 0xc010a3b3 <CreateVnode>
c01023d5: 83 c4 68                      add esp, 104
c01023d8: 68 ed 04 11 c0                push 3222340845
c01023dd: 50                            push eax
c01023de: e8 e6 79 00 00                call 0xc0109dc9 <AddVfsMount>
c01023e3: 83 c4 64                      add esp, 100
c01023e6: 5e                            pop esi
c01023e7: 5f                            pop edi
c01023e8: c3                            ret

c01023e9 <Create>:
c01023e9: 53                            push ebx
c01023ea: 83 ec 08                      sub esp, 8
c01023ed: 8b 44 24 10                   mov eax, dword ptr [esp + 16]
c01023f1: 8b 58 28                      mov ebx, dword ptr [eax + 40]
c01023f4: b8 04 00 00 00                mov eax, 4
c01023f9: 83 3b 00                      cmp dword ptr [ebx], 0
c01023fc: 75 21                         jne 0xc010241f <Create+0x36>
c01023fe: 83 ec 0c                      sub esp, 12
c0102401: 6a 01                         push 1
c0102403: 6a 01                         push 1
c0102405: ff 74 24 34                   push dword ptr [esp + 52]
c0102409: ff 74 24 34                   push dword ptr [esp + 52]
c010240d: 8b 44 24 30                   mov eax, dword ptr [esp + 48]
c0102411: ff 30                         push dword ptr [eax]
```

```
c010245e: c3                            ret

c010245f <Access.isra.0>:
c010245f: 55                            push ebp
c0102460: 57                            push edi
c0102461: 56                            push esi
c0102462: 53                            push ebx
c0102463: 83 ec 4c                      sub esp, 76
c0102466: 89 d3                         mov ebx, edx
c0102468: 89 cd                         mov ebp, ecx
c010246a: 8b 52 0c                      mov edx, dword ptr [edx + 12]
c010246d: 8b 4b 10                      mov ecx, dword ptr [ebx + 16]
c0102470: 89 d6                         mov esi, edx
c0102472: 89 cf                         mov edi, ecx
c0102474: 03 70 0c                      add esi, dword ptr [eax + 12]
c0102477: 13 78 10                      adc edi, dword ptr [eax + 16]
c010247a: 89 74 24 18                   mov dword ptr [esp + 24], esi
c010247e: 89 7c 24 1c                   mov dword ptr [esp + 28], edi
c0102482: 8b 73 04                      mov esi, dword ptr [ebx + 4]
c0102485: 8b 7b 08                      mov edi, dword ptr [ebx + 8]
c0102488: 89 74 24 08                   mov dword ptr [esp + 8], esi
c010248c: 89 7c 24 0c                   mov dword ptr [esp + 12], edi
c0102490: 8b 70 14                      mov esi, dword ptr [eax + 20]
c0102493: 8b 78 18                      mov edi, dword ptr [eax + 24]
c0102496: 89 34 24                      mov dword ptr [esp], esi
c0102499: 89 7c 24 04                   mov dword ptr [esp + 4], edi
c010249d: 8b 74 24 08                   mov esi, dword ptr [esp + 8]
c01024a1: 8b 7c 24 0c                   mov edi, dword ptr [esp + 12]
c01024a5: 01 d6                         add esi, edx
c01024a7: 11 cf                         adc edi, ecx
c01024a9: 89 74 24 10                   mov dword ptr [esp + 16], esi
c01024ad: 89 7c 24 14                   mov dword ptr [esp + 20], edi
c01024b1: 8b 7c 24 10                   mov edi, dword ptr [esp + 16]
c01024b5: 39 3c 24                      cmp dword ptr [esp], edi
c01024b8: 8b 7c 24 04                   mov edi, dword ptr [esp + 4]
c01024bc: 1b 7c 24 14                   sbb edi, dword ptr [esp + 20]
c01024c0: 72 11                         jb 0xc01024d3 <Access.isra.0+0x74>
c01024c2: 8b 54 24 08                   mov edx, dword ptr [esp + 8]
c01024c6: 8b 4c 24 0c                   mov ecx, dword ptr [esp + 12]
c01024ca: 89 14 24                      mov dword ptr [esp], edx
c01024cd: 89 4c 24 04                   mov dword ptr [esp + 4], ecx
c01024d1: eb 12                         jmp 0xc01024e5 <Access.isra.0+0x86>
c01024d3: 8b 34 24                      mov esi, dword ptr [esp]
c01024d6: 8b 7c 24 04                   mov edi, dword ptr [esp + 4]
c01024da: 29 d6                         sub esi, edx
c01024dc: 19 cf                         sbb edi, ecx
c01024de: 89 34 24                      mov dword ptr [esp], esi
c01024e1: 89 7c 24 04                   mov dword ptr [esp + 4], edi
c01024e5: 8d 7c 24 20                   lea edi, [esp + 32]
c01024e9: b9 08 00 00 00                mov ecx, 8
c01024ee: 89 de                         mov esi, ebx
c01024f0: f3 a5                         rep  movsd dword ptr es:[edi], dword ptr [esi
c01024f2: 8b 14 24                      mov edx, dword ptr [esp]
c01024f5: 8b 4c 24 04                   mov ecx, dword ptr [esp + 4]
c01024f9: 89 54 24 24                   mov dword ptr [esp + 36], edx
c01024fd: 89 4c 24 28                   mov dword ptr [esp + 40], ecx
c0102501: 8b 54 24 18                   mov edx, dword ptr [esp + 24]
c0102505: 8b 4c 24 1c                   mov ecx, dword ptr [esp + 28]
c0102509: 89 54 24 2c                   mov dword ptr [esp + 44], edx
c010250d: 89 4c 24 30                   mov dword ptr [esp + 48], ecx
c0102511: ba cb a2 10 c0                mov edx, 3222315723
c0102516: 89 e9                         mov ecx, ebp
c0102518: 84 c9                         test cl, cl
c010251a: 74 05                         je 0xc0102521 <Access.isra.0+0xc2>
c010251c: ba da a2 10 c0                mov edx, 3222315738
c0102521: 51                            push ecx
c0102522: 51                            push ecx
c0102523: 8d 4c 24 28                   lea ecx, [esp + 40]
c0102527: 51                            push ecx
c0102528: ff 70 04                      push dword ptr [eax + 4]
c010252b: ff d2                         call edx
```

```
c0102578 <Read>:
c0102578: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c010257c: 8b 40 28                      mov eax, dword ptr [eax + 40]
c010257f: 31 c9                         xor ecx, ecx
c0102581: 8b 54 24 08                   mov edx, dword ptr [esp + 8]
c0102585: e9 d5 fe ff ff                jmp 0xc010245f <Access.isra.0>

c010258a <CreatePartition>:
c010258a: 55                            push ebp
c010258b: 57                            push edi
c010258c: 56                            push esi
c010258d: 53                            push ebx
c010258e: 83 ec 78                      sub esp, 120
c0102591: 8b bc 24 90 00 00 00          mov edi, dword ptr [esp + 144]
c0102598: 8b ac 24 94 00 00 00          mov ebp, dword ptr [esp + 148]
c010259f: 8b 84 24 98 00 00 00          mov eax, dword ptr [esp + 152]
c01025a6: 8b 94 24 9c 00 00 00          mov edx, dword ptr [esp + 156]
c01025ad: 89 44 24 0c                   mov dword ptr [esp + 12], eax
c01025b1: 89 54 24 10                   mov dword ptr [esp + 16], edx
c01025b5: 8b b4 24 a4 00 00 00          mov esi, dword ptr [esp + 164]
c01025bc: 8b 94 24 ac 00 00 00          mov edx, dword ptr [esp + 172]
c01025c3: 89 54 24 18                   mov dword ptr [esp + 24], edx
c01025c7: 6a 28                         push 40
c01025c9: e8 81 13 00 00                call 0xc010394f <AllocHeap>
c01025ce: 89 c3                         mov ebx, eax
c01025d0: 8b 84 24 90 00 00 00          mov eax, dword ptr [esp + 144]
c01025d7: 89 43 04                      mov dword ptr [ebx + 4], eax
c01025da: 89 73 1c                      mov dword ptr [ebx + 28], esi
c01025dd: 8b 84 24 a4 00 00 00          mov eax, dword ptr [esp + 164]
c01025e4: 89 43 08                      mov dword ptr [ebx + 8], eax
c01025e7: 8b 44 24 10                   mov eax, dword ptr [esp + 16]
c01025eb: 8b 54 24 14                   mov edx, dword ptr [esp + 20]
c01025ef: 89 43 14                      mov dword ptr [ebx + 20], eax
c01025f2: 89 53 18                      mov dword ptr [ebx + 24], edx
c01025f5: 89 7b 0c                      mov dword ptr [ebx + 12], edi
c01025f8: 89 6b 10                      mov dword ptr [ebx + 16], ebp
c01025fb: 8b 84 24 ac 00 00 00          mov eax, dword ptr [esp + 172]
c0102602: 89 43 20                      mov dword ptr [ebx + 32], eax
c0102605: 8b 54 24 1c                   mov edx, dword ptr [esp + 28]
c0102609: 88 53 24                      mov byte ptr [ebx + 36], dl
c010260c: 31 c0                         xor eax, eax
c010260e: 89 03                         mov dword ptr [ebx], eax
c0102610: 8d 7c 24 30                   lea edi, [esp + 48]
c0102614: b9 0e 00 00 00                mov ecx, 14
c0102619: 31 c0                         xor eax, eax
c010261b: f3 ab                         rep  stosd dword ptr es:[edi], eax
c010261d: e8 aa 74 00 00                call 0xc0109acc <NextDevId>
c0102622: 89 44 24 28                   mov dword ptr [esp + 40], eax
c0102626: c1 f8 1f                      sar eax, 31
c0102629: 89 44 24 2c                   mov dword ptr [esp + 44], eax
c010262d: c7 44 24 34 ff 81 00 00       mov dword ptr [esp + 52], 33279
c0102635: c7 44 24 38 01 00 00 00       mov dword ptr [esp + 56], 1
c010263d: 8b 44 24 10                   mov eax, dword ptr [esp + 16]
c0102641: 89 44 24 4c                   mov dword ptr [esp + 76], eax
c0102645: 89 f0                         mov eax, esi
c0102647: 99                            cdq
c0102648: 52                            push edx
c0102649: 56                            push esi
c010264a: ff 74 24 1c                   push dword ptr [esp + 28]
c010264e: ff 74 24 1c                   push dword ptr [esp + 28]
c0102652: e8 f9 c7 00 00                call 0xc010ee50 <__udivdi3>
c0102657: 83 ec 38                      sub esp, 56
c010265a: 89 84 24 b0 00 00 00          mov dword ptr [esp + 176], eax
c0102661: 89 b4 24 b4 00 00 00          mov dword ptr [esp + 180], esi
c0102668: 8d 74 24 70                   lea esi, [esp + 112]
c010266c: b9 12 00 00 00                mov ecx, 18
c0102671: 89 e7                         mov edi, esp
c0102673: f3 a5                         rep  movsd dword ptr es:[edi], dword ptr [esi
c0102675: 83 ec 28                      sub esp, 40
c0102678: be 40 00 11 c0                mov esi, 3222339648
c010267d: b9 0a 00 00 00                mov ecx, 10
```

```
c01026bb: 8b 7c 24 38                mov edi, dword ptr [esp + 56]
c01026bf: 8b 5c 24 3c                mov ebx, dword ptr [esp + 60]
c01026c3: c1 e3 04                   shl ebx, 4
c01026c6: 8d 83 be 01 00 00          lea eax, [ebx + 446]
c01026cc: 50                         push eax
c01026cd: ff 74 24 40                push dword ptr [esp + 64]
c01026d1: 68 f5 04 11 c0             push 3222340853
c01026d6: e8 ea 63 00 00             call 0xc0108ac5 <LogWriteSerial>
c01026db: 8a 84 1f be 01 00 00       mov al, byte ptr [edi + ebx + 446]
c01026e2: 88 44 24 1f                mov byte ptr [esp + 31], al
c01026e6: 83 c4 10                   add esp, 16
c01026e9: a8 7f                      test al, 127
c01026eb: 74 07                      je 0xc01026f4 <TryCreateMbrPartition+0x40>
c01026ed: 31 c0                      xor eax, eax
c01026ef: e9 d6 00 00 00             jmp 0xc01027ca <TryCreateMbrPartition+0x116>
c01026f4: 0f b6 ac 1f c2 01 00 00    movzx ebp, byte ptr [edi + ebx + 450]
c01026fc: 0f b6 94 1f c9 01 00 00    movzx edx, byte ptr [edi + ebx + 457]
c0102704: c1 e2 08                   shl edx, 8
c0102707: 0f b6 84 1f c8 01 00 00    movzx eax, byte ptr [edi + ebx + 456]
c010270f: 09 d0                      or eax, edx
c0102711: c1 e0 08                   shl eax, 8
c0102714: 0f b6 94 1f c7 01 00 00    movzx edx, byte ptr [edi + ebx + 455]
c010271c: 09 c2                      or edx, eax
c010271e: c1 e2 08                   shl edx, 8
c0102721: 0f b6 b4 1f c6 01 00 00    movzx esi, byte ptr [edi + ebx + 454]
c0102729: 09 d6                      or esi, edx
c010272b: 0f b6 84 1f cd 01 00 00    movzx eax, byte ptr [edi + ebx + 461]
c0102733: c1 e0 08                   shl eax, 8
c0102736: 0f b6 94 1f cc 01 00 00    movzx edx, byte ptr [edi + ebx + 460]
c010273e: 09 c2                      or edx, eax
c0102740: c1 e2 08                   shl edx, 8
c0102743: 0f b6 84 1f cb 01 00 00    movzx eax, byte ptr [edi + ebx + 459]
c010274b: 09 d0                      or eax, edx
c010274d: c1 e0 08                   shl eax, 8
c0102750: 0f b6 bc 1f ca 01 00 00    movzx edi, byte ptr [edi + ebx + 458]
c0102758: 09 c7                      or edi, eax
c010275a: ff 74 24 30                push dword ptr [esp + 48]
c010275e: 57                         push edi
c010275f: 56                         push esi
c0102760: 68 17 05 11 c0             push 3222340887
c0102765: e8 5b 63 00 00             call 0xc0108ac5 <LogWriteSerial>
c010276a: 83 c4 10                   add esp, 16
c010276d: 89 f0                      mov eax, esi
c010276f: 09 f8                      or eax, edi
c0102771: 0f 84 76 ff ff ff          je 0xc01026ed <TryCreateMbrPartition+0x39>
c0102777: 8b 4c 24 3c                mov ecx, dword ptr [esp + 60]
c010277b: 89 cb                      mov ebx, ecx
c010277d: c1 fb 1f                   sar ebx, 31
c0102780: 89 0c 24                   mov dword ptr [esp], ecx
c0102783: 89 5c 24 04                mov dword ptr [esp + 4], ebx
c0102787: 83 ec 0c                   sub esp, 12
c010278a: 0f be 44 24 1b             movsx eax, byte ptr [esp + 27]
c010278f: c1 e8 1f                   shr eax, 31
c0102792: 50                         push eax
c0102793: 55                         push ebp
c0102794: ff 74 24 50                push dword ptr [esp + 80]
c0102798: ff 74 24 50                push dword ptr [esp + 80]
c010279c: 8b 4c 24 20                mov ecx, dword ptr [esp + 32]
c01027a0: 0f af cf                   imul ecx, edi
c01027a3: 89 f8                      mov eax, edi
c01027a5: f7 64 24 58                mul dword ptr [esp + 88]
c01027a9: 01 ca                      add edx, ecx
c01027ab: 52                         push edx
c01027ac: 50                         push eax
c01027ad: 8b 4c 24 28                mov ecx, dword ptr [esp + 40]
c01027b1: 0f af ce                   imul ecx, esi
c01027b4: 89 f0                      mov eax, esi
c01027b6: f7 64 24 60                mul dword ptr [esp + 96]
c01027ba: 01 ca                      add edx, ecx
c01027bc: 52                         push edx
c01027bd: 50                         push eax
```

```
c01027ff: 74 64                         je 0xc0102865 <GetMbrPartitions+0x93>
c0102801: 89 c5                         mov ebp, eax
c0102803: 80 b8 fe 01 00 00 55          cmp byte ptr [eax + 510], 85
c010280a: 75 59                         jne 0xc0102865 <GetMbrPartitions+0x93>
c010280c: 80 b8 ff 01 00 00 aa          cmp byte ptr [eax + 511], -86
c0102813: 75 50                         jne 0xc0102865 <GetMbrPartitions+0x93>
c0102815: 83 ec 0c                      sub esp, 12
c0102818: 68 04 01 00 00                push 260
c010281d: e8 2d 11 00 00                call 0xc010394f <AllocHeap>
c0102822: 89 c3                         mov ebx, eax
c0102824: b9 41 00 00 00                mov ecx, 65
c0102829: 31 c0                         xor eax, eax
c010282b: 89 df                         mov edi, ebx
c010282d: f3 ab                         rep  stosd dword ptr es:[edi], eax
c010282f: 83 c4 10                      add esp, 16
c0102832: 31 ff                         xor edi, edi
c0102834: 89 4c 24 0c                   mov dword ptr [esp + 12], ecx
c0102838: 56                            push esi
c0102839: 57                            push edi
c010283a: 55                            push ebp
c010283b: ff 74 24 3c                   push dword ptr [esp + 60]
c010283f: e8 70 fe ff ff                call 0xc01026b4 <TryCreateMbrPartition>
c0102844: 83 c4 10                      add esp, 16
c0102847: 85 c0                         test eax, eax
c0102849: 8b 4c 24 0c                   mov ecx, dword ptr [esp + 12]
c010284d: 74 04                         je 0xc0102853 <GetMbrPartitions+0x81>
c010284f: 89 04 8b                      mov dword ptr [ebx + 4*ecx], eax
c0102852: 41                            inc ecx
c0102853: 47                            inc edi
c0102854: 83 ff 04                      cmp edi, 4
c0102857: 75 db                         jne 0xc0102834 <GetMbrPartitions+0x62>
c0102859: 50                            push eax
c010285a: 50                            push eax
c010285b: 56                            push esi
c010285c: 55                            push ebp
c010285d: e8 96 2c 00 00                call 0xc01054f8 <UnmapVirt>
c0102862: 83 c4 10                      add esp, 16
c0102865: 89 d8                         mov eax, ebx
c0102867: 83 c4 1c                      add esp, 28
c010286a: 5b                            pop ebx
c010286b: 5e                            pop esi
c010286c: 5f                            pop edi
c010286d: 5d                            pop ebp
c010286e: c3                            ret

c010286f <GetPartitionsForDisk>:
c010286f: e9 5e ff ff ff                jmp 0xc01027d2 <GetMbrPartitions>

c0102874 <ReadWrite>:
c0102874: 8b 54 24 08                   mov edx, dword ptr [esp + 8]
c0102878: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c010287c: 8b 40 28                      mov eax, dword ptr [eax + 40]
c010287f: 80 78 0c 00                   cmp byte ptr [eax + 12], 0
c0102883: 75 0c                         jne 0xc0102891 <ReadWrite+0x1d>
c0102885: 8b 40 08                      mov eax, dword ptr [eax + 8]
c0102888: 89 44 24 04                   mov dword ptr [esp + 4], eax
c010288c: e9 55 3b 00 00                jmp 0xc01063e6 <MailboxAccess>
c0102891: 8b 42 14                      mov eax, dword ptr [edx + 20]
c0102894: f7 d8                         neg eax
c0102896: 19 c0                         sbb eax, eax
c0102898: 83 e0 1a                      and eax, 26
c010289b: c3                            ret

c010289c <BreakPipe>:
c010289c: 83 ec 0c                      sub esp, 12
c010289f: 8b 44 24 10                   mov eax, dword ptr [esp + 16]
c01028a3: 8b 40 28                      mov eax, dword ptr [eax + 40]
c01028a6: 81 78 04 b9 a9 06 a3          cmp dword ptr [eax + 4], 2735122873
c01028ad: 75 10                         jne 0xc01028bf <BreakPipe+0x23>
c01028af: 81 38 94 d7 f6 39             cmp dword ptr [eax], 972478356
c01028b5: 75 08                         jne 0xc01028bf <BreakPipe+0x23>
```

```
c010290e: 83 ec 28                  sub esp, 40
c0102911: be 80 00 11 c0            mov esi, 3222339712
c0102916: b9 0a 00 00 00            mov ecx, 10
c010291b: 89 e7                     mov edi, esp
c010291d: f3 a5                     rep  movsd dword ptr es:[edi], dword ptr [esi
c010291f: e8 8f 7a 00 00            call 0xc010a3b3 <CreateVnode>
c0102924: 89 c6                     mov esi, eax
c0102926: 83 c4 64                  add esp, 100
c0102929: 6a 10                     push 16
c010292b: e8 1f 10 00 00            call 0xc010394f <AllocHeap>
c0102930: 89 c3                     mov ebx, eax
c0102932: c7 04 24 00 08 00 00      mov dword ptr [esp], 2048
c0102939: e8 e0 36 00 00            call 0xc010601e <MailboxCreate>
c010293e: 89 43 08                  mov dword ptr [ebx + 8], eax
c0102941: c6 43 0c 00               mov byte ptr [ebx + 12], 0
c0102945: c7 03 94 d7 f6 39         mov dword ptr [ebx], 972478356
c010294b: c7 43 04 b9 a9 06 a3      mov dword ptr [ebx + 4], 2735122873
c0102952: 89 5e 28                  mov dword ptr [esi + 40], ebx
c0102955: 89 f0                     mov eax, esi
c0102957: 83 c4 60                  add esp, 96
c010295a: 5b                        pop ebx
c010295b: 5e                        pop esi
c010295c: 5f                        pop edi
c010295d: c3                        ret

c010295e <LineProcessor>:
c010295e: 55                        push ebp
c010295f: 57                        push edi
c0102960: 56                        push esi
c0102961: 53                        push ebx
c0102962: 83 ec 2c                  sub esp, 44
c0102965: 8b 44 24 40               mov eax, dword ptr [esp + 64]
c0102969: 8b 78 28                  mov edi, dword ptr [eax + 40]
c010296c: 8b 07                     mov eax, dword ptr [edi]
c010296e: 8b 70 28                  mov esi, dword ptr [eax + 40]
c0102971: 8b 57 10                  mov edx, dword ptr [edi + 16]
c0102974: 89 d5                     mov ebp, edx
c0102976: 89 54 24 0c               mov dword ptr [esp + 12], edx
c010297a: 83 e5 02                  and ebp, 2
c010297d: 53                        push ebx
c010297e: 8d 44 24 23               lea eax, [esp + 35]
c0102982: 50                        push eax
c0102983: 6a ff                     push -1
c0102985: ff 76 08                  push dword ptr [esi + 8]
c0102988: e8 fa 38 00 00            call 0xc0106287 <MailboxGet>
c010298d: 83 c4 10                  add esp, 16
c0102990: 85 ed                     test ebp, ebp
c0102992: 0f 95 c3                  setne bl
c0102995: 8b 54 24 0c               mov edx, dword ptr [esp + 12]
c0102999: 80 e2 01                  and dl, 1
c010299c: 74 48                     je 0xc01029e6 <LineProcessor+0x88>
c010299e: 0f b6 44 24 1f            movzx eax, byte ptr [esp + 31]
c01029a3: 3c 08                     cmp al, 8
c01029a5: 75 30                     jne 0xc01029d7 <LineProcessor+0x79>
c01029a7: 84 db                     test bl, bl
c01029a9: 74 2c                     je 0xc01029d7 <LineProcessor+0x79>
c01029ab: 83 bf ac 02 00 00 00      cmp dword ptr [edi + 684], 0
c01029b2: 7e 32                     jle 0xc01029e6 <LineProcessor+0x88>
c01029b4: 51                        push ecx
c01029b5: 6a 08                     push 8
c01029b7: 6a ff                     push -1
c01029b9: ff 76 04                  push dword ptr [esi + 4]
c01029bc: e8 62 38 00 00            call 0xc0106223 <MailboxAdd>
c01029c1: 83 c4 0c                  add esp, 12
c01029c4: 6a 20                     push 32
c01029c6: 6a ff                     push -1
c01029c8: ff 76 04                  push dword ptr [esi + 4]
c01029cb: e8 53 38 00 00            call 0xc0106223 <MailboxAdd>
c01029d0: 83 c4 0c                  add esp, 12
c01029d3: 6a 08                     push 8
c01029d5: eb 02                     jmp 0xc01029d9 <LineProcessor+0x7b>
```

```
c0102a3b: 74 08                         je 0xc0102a45 <LineProcessor+0xe7>
c0102a3d: 85 ed                         test ebp, ebp
c0102a3f: 0f 85 2c ff ff ff             jne 0xc0102971 <LineProcessor+0x13>
c0102a45: 8b 44 24 40                   mov eax, dword ptr [esp + 64]
c0102a49: 8b 58 28                      mov ebx, dword ptr [eax + 40]
c0102a4c: 8b 03                         mov eax, dword ptr [ebx]
c0102a4e: 8b 50 28                      mov edx, dword ptr [eax + 40]
c0102a51: 31 ed                         xor ebp, ebp
c0102a53: 3b ab ac 02 00 00             cmp ebp, dword ptr [ebx + 684]
c0102a59: 7d 1f                         jge 0xc0102a7a <LineProcessor+0x11c>
c0102a5b: 51                            push ecx
c0102a5c: 0f b6 44 2b 54                movzx eax, byte ptr [ebx + ebp + 84]
c0102a61: 50                            push eax
c0102a62: 6a ff                         push -1
c0102a64: ff 72 0c                      push dword ptr [edx + 12]
c0102a67: 89 54 24 1c                   mov dword ptr [esp + 28], edx
c0102a6b: e8 b3 37 00 00                call 0xc0106223 <MailboxAdd>
c0102a70: 45                            inc ebp
c0102a71: 83 c4 10                      add esp, 16
c0102a74: 8b 54 24 0c                   mov edx, dword ptr [esp + 12]
c0102a78: eb d9                         jmp 0xc0102a53 <LineProcessor+0xf5>
c0102a7a: 31 c0                         xor eax, eax
c0102a7c: 89 83 ac 02 00 00             mov dword ptr [ebx + 684], eax
c0102a82: e9 ea fe ff ff                jmp 0xc0102971 <LineProcessor+0x13>

c0102a87 <SubordinateIoctl>:
c0102a87: 57                            push edi
c0102a88: 56                            push esi
c0102a89: 83 ec 74                      sub esp, 116
c0102a8c: 8b 94 24 84 00 00 00          mov edx, dword ptr [esp + 132]
c0102a93: 8b 8c 24 88 00 00 00          mov ecx, dword ptr [esp + 136]
c0102a9a: 8b 84 24 80 00 00 00          mov eax, dword ptr [esp + 128]
c0102aa1: 8b 78 28                      mov edi, dword ptr [eax + 40]
c0102aa4: 8d 42 ff                      lea eax, [edx - 1]
c0102aa7: 83 f8 02                      cmp eax, 2
c0102aaa: 77 3f                         ja 0xc0102aeb <SubordinateIoctl+0x64>
c0102aac: b8 01 00 00 00                mov eax, 1
c0102ab1: 4a                            dec edx
c0102ab2: 75 69                         jne 0xc0102b1d <SubordinateIoctl+0x96>
c0102ab4: 89 e6                         mov esi, esp
c0102ab6: 52                            push edx
c0102ab7: 52                            push edx
c0102ab8: 6a 00                         push 0
c0102aba: 6a 00                         push 0
c0102abc: 6a 00                         push 0
c0102abe: 6a 50                         push 80
c0102ac0: 51                            push ecx
c0102ac1: 56                            push esi
c0102ac2: e8 5b 6d 00 00                call 0xc0109822 <CreateTransferReadingFromUse
c0102ac7: 89 f4                         mov esp, esi
c0102ac9: 6a 00                         push 0
c0102acb: 6a 50                         push 80
c0102acd: 56                            push esi
c0102ace: 8d 74 24 2c                   lea esi, [esp + 44]
c0102ad2: 56                            push esi
c0102ad3: e8 1b 6a 00 00                call 0xc01094f3 <PerformTransfer>
c0102ad8: 83 c4 10                      add esp, 16
c0102adb: 85 c0                         test eax, eax
c0102add: 75 3e                         jne 0xc0102b1d <SubordinateIoctl+0x96>
c0102adf: 83 c7 04                      add edi, 4
c0102ae2: b9 14 00 00 00                mov ecx, 20
c0102ae7: f3 a5                         rep  movsd dword ptr es:[edi], dword ptr [esi
c0102ae9: eb 32                         jmp 0xc0102b1d <SubordinateIoctl+0x96>
c0102aeb: b8 07 00 00 00                mov eax, 7
c0102af0: 85 d2                         test edx, edx
c0102af2: 75 29                         jne 0xc0102b1d <SubordinateIoctl+0x96>
c0102af4: 8d 74 24 20                   lea esi, [esp + 32]
c0102af8: 50                            push eax
c0102af9: 50                            push eax
c0102afa: 6a 00                         push 0
c0102afc: 6a 00                         push 0
```

```
c0102b3c: 75 06                         jne 0xc0102b44 <SubordinateWrite+0x21>
c0102b3e: 83 7b 04 00                   cmp dword ptr [ebx + 4], 0
c0102b42: 74 19                         je 0xc0102b5d <SubordinateWrite+0x3a>
c0102b44: 83 f8 21                      cmp eax, 33
c0102b47: 75 10                         jne 0xc0102b59 <SubordinateWrite+0x36>
c0102b49: 51                            push ecx
c0102b4a: 51                            push ecx
c0102b4b: 53                            push ebx
c0102b4c: ff 76 04                      push dword ptr [esi + 4]
c0102b4f: e8 92 38 00 00                call 0xc01063e6 <MailboxAccess>
c0102b54: 83 c4 10                      add esp, 16
c0102b57: eb df                         jmp 0xc0102b38 <SubordinateWrite+0x15>
c0102b59: 85 c0                         test eax, eax
c0102b5b: 74 ec                         je 0xc0102b49 <SubordinateWrite+0x26>
c0102b5d: 5a                            pop edx
c0102b5e: 5b                            pop ebx
c0102b5f: 5e                            pop esi
c0102b60: c3                            ret

c0102b61 <SubordinateRead>:
c0102b61: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c0102b65: 8b 40 28                      mov eax, dword ptr [eax + 40]
c0102b68: 8b 00                         mov eax, dword ptr [eax]
c0102b6a: 8b 40 28                      mov eax, dword ptr [eax + 40]
c0102b6d: 8b 40 0c                      mov eax, dword ptr [eax + 12]
c0102b70: 89 44 24 04                   mov dword ptr [esp + 4], eax
c0102b74: e9 6d 38 00 00                jmp 0xc01063e6 <MailboxAccess>

c0102b79 <MasterWrite>:
c0102b79: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c0102b7d: 8b 40 28                      mov eax, dword ptr [eax + 40]
c0102b80: 8b 40 08                      mov eax, dword ptr [eax + 8]
c0102b83: 89 44 24 04                   mov dword ptr [esp + 4], eax
c0102b87: e9 5a 38 00 00                jmp 0xc01063e6 <MailboxAccess>

c0102b8c <MasterRead>:
c0102b8c: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c0102b90: 8b 40 28                      mov eax, dword ptr [eax + 40]
c0102b93: 8b 40 04                      mov eax, dword ptr [eax + 4]
c0102b96: 89 44 24 04                   mov dword ptr [esp + 4], eax
c0102b9a: e9 47 38 00 00                jmp 0xc01063e6 <MailboxAccess>

c0102b9f <MasterClose>:
c0102b9f: 53                            push ebx
c0102ba0: 83 ec 14                      sub esp, 20
c0102ba3: 8b 44 24 1c                   mov eax, dword ptr [esp + 28]
c0102ba7: 8b 58 28                      mov ebx, dword ptr [eax + 40]
c0102baa: ff 73 04                      push dword ptr [ebx + 4]
c0102bad: e8 1f 35 00 00                call 0xc01060d1 <MailboxDestroy>
c0102bb2: 58                            pop eax
c0102bb3: ff 73 0c                      push dword ptr [ebx + 12]
c0102bb6: e8 16 35 00 00                call 0xc01060d1 <MailboxDestroy>
c0102bbb: 5a                            pop edx
c0102bbc: ff 73 08                      push dword ptr [ebx + 8]
c0102bbf: e8 0d 35 00 00                call 0xc01060d1 <MailboxDestroy>
c0102bc4: 59                            pop ecx
c0102bc5: ff 73 10                      push dword ptr [ebx + 16]
c0102bc8: e8 a9 3e 00 00                call 0xc0106a76 <TerminateThread>
c0102bcd: 89 1c 24                      mov dword ptr [esp], ebx
c0102bd0: e8 9e 0d 00 00                call 0xc0103973 <FreeHeap>
c0102bd5: 31 c0                         xor eax, eax
c0102bd7: 83 c4 18                      add esp, 24
c0102bda: 5b                            pop ebx
c0102bdb: c3                            ret

c0102bdc <CreatePseudoTerminal>:
c0102bdc: 55                            push ebp
c0102bdd: 57                            push edi
c0102bde: 56                            push esi
c0102bdf: 53                            push ebx
c0102be0: 83 ec 5c                      sub esp, 92
```

```
c0102c4e: b9 0a 00 00 00              mov ecx, 10
c0102c53: 89 e7                       mov edi, esp
c0102c55: f3 a5                       rep  movsd dword ptr es:[edi], dword ptr [esi
c0102c57: e8 57 77 00 00              call 0xc010a3b3 <CreateVnode>
c0102c5c: 89 c6                       mov esi, eax
c0102c5e: 83 c4 64                    add esp, 100
c0102c61: 6a 14                       push 20
c0102c63: e8 e7 0c 00 00              call 0xc010394f <AllocHeap>
c0102c68: 89 c3                       mov ebx, eax
c0102c6a: c7 04 24 b0 02 00 00        mov dword ptr [esp], 688
c0102c71: e8 d9 0c 00 00              call 0xc010394f <AllocHeap>
c0102c76: 89 c7                       mov edi, eax
c0102c78: 89 33                       mov dword ptr [ebx], esi
c0102c7a: c7 04 24 00 10 00 00        mov dword ptr [esp], 4096
c0102c81: e8 98 33 00 00              call 0xc010601e <MailboxCreate>
c0102c86: 89 43 04                    mov dword ptr [ebx + 4], eax
c0102c89: c7 04 24 00 10 00 00        mov dword ptr [esp], 4096
c0102c90: e8 89 33 00 00              call 0xc010601e <MailboxCreate>
c0102c95: 89 43 08                    mov dword ptr [ebx + 8], eax
c0102c98: c7 04 24 2c 01 00 00        mov dword ptr [esp], 300
c0102c9f: e8 7a 33 00 00              call 0xc010601e <MailboxCreate>
c0102ca4: 89 43 0c                    mov dword ptr [ebx + 12], eax
c0102ca7: e8 cd 19 00 00              call 0xc0104679 <GetVas>
c0102cac: 68 a5 05 11 c0              push 3222341029
c0102cb1: 50                          push eax
c0102cb2: 56                          push esi
c0102cb3: 68 5e 29 10 c0              push 3222284638
c0102cb8: e8 8b 4c 00 00              call 0xc0107948 <CreateThread>
c0102cbd: 89 43 10                    mov dword ptr [ebx + 16], eax
c0102cc0: 89 2f                       mov dword ptr [edi], ebp
c0102cc2: c7 47 10 03 00 00 00        mov dword ptr [edi + 16], 3
c0102cc9: 89 5d 28                    mov dword ptr [ebp + 40], ebx
c0102ccc: 89 7e 28                    mov dword ptr [esi + 40], edi
c0102ccf: 8b 84 24 90 00 00 00        mov eax, dword ptr [esp + 144]
c0102cd6: 89 28                       mov dword ptr [eax], ebp
c0102cd8: 8b 84 24 94 00 00 00        mov eax, dword ptr [esp + 148]
c0102cdf: 89 30                       mov dword ptr [eax], esi
c0102ce1: 83 c4 7c                    add esp, 124
c0102ce4: 5b                          pop ebx
c0102ce5: 5e                          pop esi
c0102ce6: 5f                          pop edi
c0102ce7: 5d                          pop ebp
c0102ce8: c3                          ret

c0102ce9 <Read>:
c0102ce9: 53                          push ebx
c0102cea: 83 ec 18                    sub esp, 24
c0102ced: 8b 5c 24 24                 mov ebx, dword ptr [esp + 36]
c0102cf1: 83 7b 08 00                 cmp dword ptr [ebx + 8], 0
c0102cf5: 74 21                       je 0xc0102d18 <Read+0x2f>
c0102cf7: e8 60 2e 00 00              call 0xc0105b5c <rand>
c0102cfc: 88 44 24 0f                 mov byte ptr [esp + 15], al
c0102d00: 6a 00                       push 0
c0102d02: 6a 01                       push 1
c0102d04: 53                          push ebx
c0102d05: 8d 44 24 1b                 lea eax, [esp + 27]
c0102d09: 50                          push eax
c0102d0a: e8 e4 67 00 00              call 0xc01094f3 <PerformTransfer>
c0102d0f: 83 c4 10                    add esp, 16
c0102d12: 85 c0                       test eax, eax
c0102d14: 74 db                       je 0xc0102cf1 <Read+0x8>
c0102d16: eb 08                       jmp 0xc0102d20 <Read+0x37>
c0102d18: 83 7b 04 00                 cmp dword ptr [ebx + 4], 0
c0102d1c: 75 d9                       jne 0xc0102cf7 <Read+0xe>
c0102d1e: 31 c0                       xor eax, eax
c0102d20: 83 c4 18                    add esp, 24
c0102d23: 5b                          pop ebx
c0102d24: c3                          ret

c0102d25 <InitRandomDevice>:
c0102d25: 57                          push edi
```

```
c0102d8d: 5f                            pop edi
c0102d8e: c3                            ret

c0102d8f <RegisterFilesystem>:
c0102d8f: 57                            push edi
c0102d90: 56                            push esi
c0102d91: 53                            push ebx
c0102d92: 8b 44 24 10                   mov eax, dword ptr [esp + 16]
c0102d96: 8b 7c 24 14                   mov edi, dword ptr [esp + 20]
c0102d9a: 85 ff                         test edi, edi
c0102d9c: 0f 84 91 00 00 00             je 0xc0102e33 <RegisterFilesystem+0xa4>
c0102da2: 85 c0                         test eax, eax
c0102da4: 0f 84 89 00 00 00             je 0xc0102e33 <RegisterFilesystem+0xa4>
c0102daa: 83 ec 0c                      sub esp, 12
c0102dad: 50                            push eax
c0102dae: e8 42 e5 ff ff                call 0xc01012f5 <strdup>
c0102db3: 89 c6                         mov esi, eax
c0102db5: 58                            pop eax
c0102db6: 5a                            pop edx
c0102db7: 6a ff                         push -1
c0102db9: ff 35 20 40 11 c0             push dword ptr [-1072611296]
c0102dbf: e8 75 39 00 00                call 0xc0106739 <AcquireSemaphore>
c0102dc4: a1 24 40 11 c0                mov eax, dword ptr [3222356004]
c0102dc9: 83 c4 10                      add esp, 16
c0102dcc: bb 04 00 00 00                mov ebx, 4
c0102dd1: 83 f8 07                      cmp eax, 7
c0102dd4: 7f 19                         jg 0xc0102def <RegisterFilesystem+0x60>
c0102dd6: 8d 50 01                      lea edx, [eax + 1]
c0102dd9: 89 15 24 40 11 c0             mov dword ptr [-1072611292], edx
c0102ddf: 89 34 c5 40 40 11 c0          mov dword ptr [8*eax - 1072611264], esi
c0102de6: 89 3c c5 44 40 11 c0          mov dword ptr [8*eax - 1072611260], edi
c0102ded: 31 db                         xor ebx, ebx
c0102def: a1 24 40 11 c0                mov eax, dword ptr [3222356004]
c0102df4: 8d 50 01                      lea edx, [eax + 1]
c0102df7: 89 15 24 40 11 c0             mov dword ptr [-1072611292], edx
c0102dfd: 89 34 c5 40 40 11 c0          mov dword ptr [8*eax - 1072611264], esi
c0102e04: 89 3c c5 44 40 11 c0          mov dword ptr [8*eax - 1072611260], edi
c0102e0b: 83 ec 0c                      sub esp, 12
c0102e0e: ff 35 20 40 11 c0             push dword ptr [-1072611296]
c0102e14: e8 9a 3a 00 00                call 0xc01068b3 <ReleaseSemaphore>
c0102e19: 83 c4 10                      add esp, 16
c0102e1c: 85 db                         test ebx, ebx
c0102e1e: 74 18                         je 0xc0102e38 <RegisterFilesystem+0xa9>
c0102e20: 83 ec 0c                      sub esp, 12
c0102e23: 56                            push esi
c0102e24: e8 4a 0b 00 00                call 0xc0103973 <FreeHeap>
c0102e29: 83 c4 10                      add esp, 16
c0102e2c: bb 04 00 00 00                mov ebx, 4
c0102e31: eb 05                         jmp 0xc0102e38 <RegisterFilesystem+0xa9>
c0102e33: bb 07 00 00 00                mov ebx, 7
c0102e38: 89 d8                         mov eax, ebx
c0102e3a: 5b                            pop ebx
c0102e3b: 5e                            pop esi
c0102e3c: 5f                            pop edi
c0102e3d: c3                            ret

c0102e3e <InitFilesystemTable>:
c0102e3e: 83 ec 10                      sub esp, 16
c0102e41: 31 c0                         xor eax, eax
c0102e43: a3 24 40 11 c0                mov dword ptr [3222356004], eax
c0102e48: 6a 00                         push 0
c0102e4a: 6a 01                         push 1
c0102e4c: 68 af 05 11 c0                push 3222341039
c0102e51: e8 83 38 00 00                call 0xc01066d9 <CreateSemaphore>
c0102e56: a3 20 40 11 c0                mov dword ptr [3222356000], eax
c0102e5b: 5a                            pop edx
c0102e5c: 59                            pop ecx
c0102e5d: 68 db ad 10 c0                push 3222318555
c0102e62: 68 b8 05 11 c0                push 3222341048
c0102e67: e8 23 ff ff ff                call 0xc0102d8f <RegisterFilesystem>
c0102e6c: 83 c4 1c                      add esp, 28
```

```
c0102ec1: 83 ec 0c                  sub esp, 12
c0102ec4: ff 35 20 40 11 c0         push dword ptr [-1072611296]
c0102eca: e8 e4 39 00 00            call 0xc01068b3 <ReleaseSemaphore>
c0102ecf: 8b 44 24 1c               mov eax, dword ptr [esp + 28]
c0102ed3: 83 c4 10                  add esp, 16
c0102ed6: bb 03 00 00 00            mov ebx, 3
c0102edb: 85 c0                     test eax, eax
c0102edd: 75 05                     jne 0xc0102ee4 <MountFilesystemForDisk+0x74>
c0102edf: eb 3b                     jmp 0xc0102f1c <MountFilesystemForDisk+0xac>
c0102ee1: 43                        inc ebx
c0102ee2: eb b9                     jmp 0xc0102e9d <MountFilesystemForDisk+0x2d>
c0102ee4: 83 ec 0c                  sub esp, 12
c0102ee7: 6a 00                     push 0
c0102ee9: 6a 00                     push 0
c0102eeb: 68 f2 04 11 c0            push 3222340850
c0102ef0: 83 c0 30                  add eax, 48
c0102ef3: 50                        push eax
c0102ef4: ff 76 30                  push dword ptr [esi + 48]
c0102ef7: e8 33 76 00 00            call 0xc010a52f <VnodeOpCreate>
c0102efc: 89 c3                     mov ebx, eax
c0102efe: 83 c4 20                  add esp, 32
c0102f01: 85 c0                     test eax, eax
c0102f03: 75 17                     jne 0xc0102f1c <MountFilesystemForDisk+0xac>
c0102f05: e8 22 5e 00 00            call 0xc0108d2c <GenerateNewMountedDiskName>
c0102f0a: 52                        push edx
c0102f0b: 52                        push edx
c0102f0c: 50                        push eax
c0102f0d: 8b 44 24 18               mov eax, dword ptr [esp + 24]
c0102f11: ff 70 30                  push dword ptr [eax + 48]
c0102f14: e8 b0 6e 00 00            call 0xc0109dc9 <AddVfsMount>
c0102f19: 83 c4 10                  add esp, 16
c0102f1c: 89 d8                     mov eax, ebx
c0102f1e: 83 c4 14                  add esp, 20
c0102f21: 5b                        pop ebx
c0102f22: 5e                        pop esi
c0102f23: c3                        ret

c0102f24 <InitUserspace>:
c0102f24: 83 ec 14                  sub esp, 20
c0102f27: 68 da 05 11 c0            push 3222341082
c0102f2c: 6a 00                     push 0
c0102f2e: e8 ac 46 00 00            call 0xc01075df <CreateUsermodeProcess>
c0102f33: 83 c4 1c                  add esp, 28
c0102f36: c3                        ret

c0102f37 <InitSystemMounts>:
c0102f37: 83 ec 1c                  sub esp, 28
c0102f3a: 8d 44 24 08               lea eax, [esp + 8]
c0102f3e: 50                        push eax
c0102f3f: 6a 00                     push 0
c0102f41: 6a 00                     push 0
c0102f43: 68 e8 05 11 c0            push 3222341096
c0102f48: e8 00 71 00 00            call 0xc010a04d <OpenFile>
c0102f4d: 83 c4 10                  add esp, 16
c0102f50: 85 c0                     test eax, eax
c0102f52: 74 09                     je 0xc0102f5d <InitSystemMounts+0x26>
c0102f54: 50                        push eax
c0102f55: 50                        push eax
c0102f56: 68 f5 05 11 c0            push 3222341109
c0102f5b: eb 21                     jmp 0xc0102f7e <InitSystemMounts+0x47>
c0102f5d: 50                        push eax
c0102f5e: 50                        push eax
c0102f5f: 68 fb 05 11 c0            push 3222341115
c0102f64: 8b 44 24 14               mov eax, dword ptr [esp + 20]
c0102f68: ff 70 30                  push dword ptr [eax + 48]
c0102f6b: e8 59 6e 00 00            call 0xc0109dc9 <AddVfsMount>
c0102f70: 83 c4 10                  add esp, 16
c0102f73: 85 c0                     test eax, eax
c0102f75: 74 0e                     je 0xc0102f85 <InitSystemMounts+0x4e>
c0102f77: 50                        push eax
c0102f78: 50                        push eax
```

```
c0102fcb: 83 c4 1c                      add esp, 28
c0102fce: c3                            ret

c0102fcf <InitThread>:
c0102fcf: 83 ec 0c                      sub esp, 12
c0102fd2: e8 4e fd ff ff                call 0xc0102d25 <InitRandomDevice>
c0102fd7: e8 a3 f3 ff ff                call 0xc010237f <InitNullDevice>
c0102fdc: e8 52 52 00 00                call 0xc0108233 <InitConsole>
c0102fe1: e8 e8 3b 00 00                call 0xc0106bce <InitProcess>
c0102fe6: e8 6c f3 ff ff                call 0xc0102357 <InitDiskCaches>
c0102feb: e8 4e fe ff ff                call 0xc0102e3e <InitFilesystemTable>
c0102ff0: 83 ec 0c                      sub esp, 12
c0102ff3: 6a 00                         push 0
c0102ff5: e8 16 94 00 00                call 0xc010c410 <ArchInitDev>
c0102ffa: e8 38 ff ff ff                call 0xc0102f37 <InitSystemMounts>
c0102fff: e8 9e 0e 00 00                call 0xc0103ea2 <InitSwapfile>
c0103004: e8 c9 53 00 00                call 0xc01083d2 <InitSymbolTable>
c0103009: c7 04 24 01 00 00 00          mov dword ptr [esp], 1
c0103010: e8 fb 93 00 00                call 0xc010c410 <ArchInitDev>
c0103015: e8 94 6e 00 00                call 0xc0109eae <InitRootsFilesystem>
c010301a: e8 37 42 00 00                call 0xc0107256 <InitProgramLoader>
c010301f: e8 00 ff ff ff                call 0xc0102f24 <InitUserspace>
c0103024: e8 a1 7e 00 00                call 0xc010aeca <ArchCallGlobalConstructors>
c0103029: 83 c4 10                      add esp, 16
c010302c: 83 ec 0c                      sub esp, 12
c010302f: 68 a0 86 01 00                push 100000
c0103034: e8 57 4e 00 00                call 0xc0107e90 <SleepMilli>
c0103039: eb ee                         jmp 0xc0103029 <InitThread+0x5a>

c010303b <GetBootInformation>:
c010303b: 57                            push edi
c010303c: 56                            push esi
c010303d: 8b 44 24 0c                   mov eax, dword ptr [esp + 12]
c0103041: be 80 40 11 c0                mov esi, 3222356096
c0103046: b9 31 00 00 00                mov ecx, 49
c010304b: 89 c7                         mov edi, eax
c010304d: f3 a4                         rep  movsb byte ptr es:[edi], byte ptr [esi]
c010304f: 5e                            pop esi
c0103050: 5f                            pop edi
c0103051: c2 04 00                      ret 4

c0103054 <KernelMain>:
c0103054: 55                            push ebp
c0103055: 57                            push edi
c0103056: 56                            push esi
c0103057: 53                            push ebx
c0103058: 83 ec 0c                      sub esp, 12
c010305b: 8b 6c 24 20                   mov ebp, dword ptr [esp + 32]
c010305f: bf 80 40 11 c0                mov edi, 3222356096
c0103064: b9 31 00 00 00                mov ecx, 49
c0103069: 89 ee                         mov esi, ebp
c010306b: f3 a4                         rep  movsb byte ptr es:[edi], byte ptr [esi]
c010306d: 31 ff                         xor edi, edi
c010306f: 89 f8                         mov eax, edi
c0103071: ba f9 03 00 00                mov edx, 1017
c0103076: ee                            out dx, al
c0103077: be fb 03 00 00                mov esi, 1019
c010307c: b0 80                         mov al, -128
c010307e: 89 f2                         mov edx, esi
c0103080: ee                            out dx, al
c0103081: b3 03                         mov bl, 3
c0103083: b9 f8 03 00 00                mov ecx, 1016
c0103088: 88 d8                         mov al, bl
c010308a: 89 ca                         mov edx, ecx
c010308c: ee                            out dx, al
c010308d: 89 f8                         mov eax, edi
c010308f: ba f9 03 00 00                mov edx, 1017
c0103094: ee                            out dx, al
c0103095: 88 d8                         mov al, bl
c0103097: 89 f2                         mov edx, esi
c0103099: ee                            out dx, al
```

```
c01030f1: e8 bb 08 00 00                call 0xc01039b1 <InitHeap>
c01030f6: e8 a1 00 00 00                call 0xc010319c <InitBootstrapCpu>
c01030fb: e8 97 28 00 00                call 0xc0105997 <InitVirt>
c0103100: e8 be 0c 00 00                call 0xc0103dc3 <ReinitPhys>
c0103105: e8 a3 00 00 00                call 0xc01031ad <InitOtherCpu>
c010310a: e8 6a 15 00 00                call 0xc0104679 <GetVas>
c010310f: 6a 00                         push 0
c0103111: 6a 1e                         push 30
c0103113: 6a 00                         push 0
c0103115: 6a 00                         push 0
c0103117: 68 56 06 11 c0                push 3222341206
c010311c: 50                            push eax
c010311d: 6a 00                         push 0
c010311f: 68 cf 2f 10 c0                push 3222286287
c0103124: e8 c5 46 00 00                call 0xc01077ee <CreateThreadEx>
c0103129: 83 c4 3c                      add esp, 60
c010312c: 5b                            pop ebx
c010312d: 5e                            pop esi
c010312e: 5f                            pop edi
c010312f: 5d                            pop ebp
c0103130: e9 5b 49 00 00                jmp 0xc0107a90 <StartMultitasking>

c0103135 <InitCpuTableEntry>:
c0103135: 56                            push esi
c0103136: 53                            push ebx
c0103137: 52                            push edx
c0103138: 89 c2                         mov edx, eax
c010313a: 89 c6                         mov esi, eax
c010313c: c1 e6 06                      shl esi, 6
c010313f: 8d 9e c0 40 11 c0             lea ebx, [esi - 1072611136]
c0103145: 89 43 0c                      mov dword ptr [ebx + 12], eax
c0103148: 31 c9                         xor ecx, ecx
c010314a: 89 4b 10                      mov dword ptr [ebx + 16], ecx
c010314d: 89 4b 20                      mov dword ptr [ebx + 32], ecx
c0103150: 89 8e c0 40 11 c0             mov dword ptr [esi - 1072611136], ecx
c0103156: 89 4b 04                      mov dword ptr [ebx + 4], ecx
c0103159: 66 c7 43 1c 00 00             mov word ptr [ebx + 28], 0
c010315f: b8 c0 44 11 c0                mov eax, 3222357184
c0103164: 85 d2                         test edx, edx
c0103166: 74 10                         je 0xc0103178 <InitCpuTableEntry+0x43>
c0103168: 83 ec 0c                      sub esp, 12
c010316b: 68 90 08 00 00                push 2192
c0103170: e8 ec 07 00 00                call 0xc0103961 <AllocHeapZero>
c0103175: 83 c4 10                      add esp, 16
c0103178: 89 43 08                      mov dword ptr [ebx + 8], eax
c010317b: 50                            push eax
c010317c: 6a 03                         push 3
c010317e: 68 5b 06 11 c0                push 3222341211
c0103183: 81 c6 e4 40 11 c0             add esi, 3222356196
c0103189: 56                            push esi
c010318a: e8 b0 37 00 00                call 0xc010693f <InitSpinlock>
c010318f: 83 c4 14                      add esp, 20
c0103192: 5b                            pop ebx
c0103193: 5e                            pop esi
c0103194: c3                            ret

c0103195 <InitCpuTable>:
c0103195: 31 c0                         xor eax, eax
c0103197: e9 99 ff ff ff                jmp 0xc0103135 <InitCpuTableEntry>

c010319c <InitBootstrapCpu>:
c010319c: 83 ec 18                      sub esp, 24
c010319f: 68 c0 40 11 c0                push 3222356160
c01031a4: e8 69 7d 00 00                call 0xc010af12 <ArchInitBootstrapCpu>
c01031a9: 83 c4 1c                      add esp, 28
c01031ac: c3                            ret

c01031ad <InitOtherCpu>:
c01031ad: 83 ec 0c                      sub esp, 12
c01031b0: b8 01 00 00 00                mov eax, 1
c01031b5: e8 7b ff ff ff                call 0xc0103135 <InitCpuTableEntry>
```

```
c0103201: 05 c0 40 11 c0                add eax, 3222356160
c0103206: c3                            ret

c0103207 <RegisterIrqHandler>:
c0103207: 56                            push esi
c0103208: 53                            push ebx
c0103209: 53                            push ebx
c010320a: 8b 5c 24 10                   mov ebx, dword ptr [esp + 16]
c010320e: 8b 74 24 14                   mov esi, dword ptr [esp + 20]
c0103212: 85 f6                         test esi, esi
c0103214: 74 34                         je 0xc010324a <RegisterIrqHandler+0x43>
c0103216: 81 fb ff 00 00 00             cmp ebx, 255
c010321c: 77 2c                         ja 0xc010324a <RegisterIrqHandler+0x43>
c010321e: 83 3c 9d 60 4d 11 c0 00       cmp dword ptr [4*ebx - 1072607904], 0
c0103226: 75 0c                         jne 0xc0103234 <RegisterIrqHandler+0x2d>
c0103228: e8 0b e8 ff ff                call 0xc0101a38 <ListCreate>
c010322d: 89 04 9d 60 4d 11 c0          mov dword ptr [4*ebx - 1072607904], eax
c0103234: 51                            push ecx
c0103235: 51                            push ecx
c0103236: 56                            push esi
c0103237: ff 34 9d 60 4d 11 c0          push dword ptr [4*ebx - 1072607904]
c010323e: e8 34 e8 ff ff                call 0xc0101a77 <ListInsertEnd>
c0103243: 83 c4 10                      add esp, 16
c0103246: 31 c0                         xor eax, eax
c0103248: eb 05                         jmp 0xc010324f <RegisterIrqHandler+0x48>
c010324a: b8 07 00 00 00                mov eax, 7
c010324f: 5a                            pop edx
c0103250: 5b                            pop ebx
c0103251: 5e                            pop esi
c0103252: c3                            ret

c0103253 <RespondToIrq>:
c0103253: 57                            push edi
c0103254: 56                            push esi
c0103255: 53                            push ebx
c0103256: 8b 5c 24 10                   mov ebx, dword ptr [esp + 16]
c010325a: 8b 7c 24 18                   mov edi, dword ptr [esp + 24]
c010325e: 83 ec 0c                      sub esp, 12
c0103261: ff 74 24 20                   push dword ptr [esp + 32]
c0103265: e8 12 01 00 00                call 0xc010337c <RaiseIrql>
c010326a: 89 c6                         mov esi, eax
c010326c: 89 1c 24                      mov dword ptr [esp], ebx
c010326f: e8 5b 7f 00 00                call 0xc010b1cf <ArchSendEoi>
c0103274: 8b 04 9d 60 4d 11 c0          mov eax, dword ptr [4*ebx - 1072607904]
c010327b: 83 c4 10                      add esp, 16
c010327e: 85 c0                         test eax, eax
c0103280: 75 0c                         jne 0xc010328e <RespondToIrq+0x3b>
c0103282: 89 74 24 10                   mov dword ptr [esp + 16], esi
c0103286: 5b                            pop ebx
c0103287: 5e                            pop esi
c0103288: 5f                            pop edi
c0103289: e9 2a 01 00 00                jmp 0xc01033b8 <LowerIrql>
c010328e: 83 ec 0c                      sub esp, 12
c0103291: 50                            push eax
c0103292: e8 42 e9 ff ff                call 0xc0101bd9 <ListGetNextNode>
c0103297: 89 c3                         mov ebx, eax
c0103299: 83 c4 10                      add esp, 16
c010329c: 85 c0                         test eax, eax
c010329e: 74 e2                         je 0xc0103282 <RespondToIrq+0x2f>
c01032a0: 83 ec 0c                      sub esp, 12
c01032a3: 53                            push ebx
c01032a4: e8 4c e9 ff ff                call 0xc0101bf5 <ListGetDataFromNode>
c01032a9: 89 3c 24                      mov dword ptr [esp], edi
c01032ac: ff d0                         call eax
c01032ae: 83 c4 10                      add esp, 16
c01032b1: 85 c0                         test eax, eax
c01032b3: 74 cd                         je 0xc0103282 <RespondToIrq+0x2f>
c01032b5: 83 ec 0c                      sub esp, 12
c01032b8: 53                            push ebx
c01032b9: e8 1b e9 ff ff                call 0xc0101bd9 <ListGetNextNode>
c01032be: eb d7                         jmp 0xc0103297 <RespondToIrq+0x44>
```

```
c0103310: 05 c0 40 11 c0                add eax, 3222356160
c0103315: 8b 50 10                      mov edx, dword ptr [eax + 16]
c0103318: 39 ca                         cmp edx, ecx
c010331a: 74 09                         je 0xc0103325 <DeferUntilIrql+0x2c>
c010331c: 85 d2                         test edx, edx
c010331e: 75 12                         jne 0xc0103332 <DeferUntilIrql+0x39>
c0103320: 83 f9 01                      cmp ecx, 1
c0103323: 75 0d                         jne 0xc0103332 <DeferUntilIrql+0x39>
c0103325: 89 5c 24 20                   mov dword ptr [esp + 32], ebx
c0103329: 89 f0                         mov eax, esi
c010332b: 83 c4 14                      add esp, 20
c010332e: 5b                            pop ebx
c010332f: 5e                            pop esi
c0103330: ff e0                         jmp eax
c0103332: 39 ca                         cmp edx, ecx
c0103334: 7d 0e                         jge 0xc0103344 <DeferUntilIrql+0x4b>
c0103336: 50                            push eax
c0103337: 50                            push eax
c0103338: 68 73 06 11 c0                push 3222341235
c010333d: 6a 0c                         push 12
c010333f: e8 0a 58 00 00                call 0xc0108b4e <PanicEx>
c0103344: 80 78 1c 00                   cmp byte ptr [eax + 28], 0
c0103348: 74 1f                         je 0xc0103369 <DeferUntilIrql+0x70>
c010334a: 89 74 24 08                   mov dword ptr [esp + 8], esi
c010334e: 89 5c 24 0c                   mov dword ptr [esp + 12], ebx
c0103352: 89 cb                         mov ebx, ecx
c0103354: c1 fb 1f                      sar ebx, 31
c0103357: 53                            push ebx
c0103358: 51                            push ecx
c0103359: 8d 54 24 10                   lea edx, [esp + 16]
c010335d: 52                            push edx
c010335e: ff 70 14                      push dword ptr [eax + 20]
c0103361: e8 57 e5 ff ff                call 0xc01018bd <HeapAdtInsert>
c0103366: 83 c4 10                      add esp, 16
c0103369: 83 c4 14                      add esp, 20
c010336c: 5b                            pop ebx
c010336d: 5e                            pop esi
c010336e: c3                            ret

c010336f <GetIrql>:
c010336f: 0f 21 d8                      mov eax, dr3
c0103372: c1 e0 06                      shl eax, 6
c0103375: 8b 80 d0 40 11 c0             mov eax, dword ptr [eax - 1072611120]
c010337b: c3                            ret

c010337c <RaiseIrql>:
c010337c: 53                            push ebx
c010337d: 83 ec 08                      sub esp, 8
c0103380: 8b 54 24 10                   mov edx, dword ptr [esp + 16]
c0103384: fa                            cli
c0103385: 0f 21 d8                      mov eax, dr3
c0103388: c1 e0 06                      shl eax, 6
c010338b: 05 c0 40 11 c0                add eax, 3222356160
c0103390: 8b 58 10                      mov ebx, dword ptr [eax + 16]
c0103393: 39 d3                         cmp ebx, edx
c0103395: 7e 0e                         jle 0xc01033a5 <RaiseIrql+0x29>
c0103397: 50                            push eax
c0103398: 50                            push eax
c0103399: 68 92 06 11 c0                push 3222341266
c010339e: 6a 0c                         push 12
c01033a0: e8 a9 57 00 00                call 0xc0108b4e <PanicEx>
c01033a5: 89 50 10                      mov dword ptr [eax + 16], edx
c01033a8: 83 ec 0c                      sub esp, 12
c01033ab: 52                            push edx
c01033ac: e8 23 7e 00 00                call 0xc010b1d4 <ArchSetIrql>
c01033b1: 89 d8                         mov eax, ebx
c01033b3: 83 c4 18                      add esp, 24
c01033b6: 5b                            pop ebx
c01033b7: c3                            ret

c01033b8 <LowerIrql>:
```

```
c0103402: 8b 74 24 20                   mov esi, dword ptr [esp + 32]
c0103406: 83 c4 0c                      add esp, 12
c0103409: 39 fe                         cmp esi, edi
c010340b: 7c 53                         jl 0xc0103460 <LowerIrql+0xa8>
c010340d: 83 fe 01                      cmp esi, 1
c0103410: 75 02                         jne 0xc0103414 <LowerIrql+0x5c>
c0103412: 31 f6                         xor esi, esi
c0103414: 8b 44 24 1c                   mov eax, dword ptr [esp + 28]
c0103418: 8b 50 04                      mov edx, dword ptr [eax + 4]
c010341b: 8b 00                         mov eax, dword ptr [eax]
c010341d: 85 c0                         test eax, eax
c010341f: 75 14                         jne 0xc0103435 <LowerIrql+0x7d>
c0103421: 83 ec 0c                      sub esp, 12
c0103424: 56                            push esi
c0103425: e8 aa 7d 00 00                call 0xc010b1d4 <ArchSetIrql>
c010342a: 83 c4 10                      add esp, 16
c010342d: 80 7b 1c 00                   cmp byte ptr [ebx + 28], 0
c0103431: 75 b2                         jne 0xc01033e5 <LowerIrql+0x2d>
c0103433: eb 2b                         jmp 0xc0103460 <LowerIrql+0xa8>
c0103435: 89 44 24 0c                   mov dword ptr [esp + 12], eax
c0103439: 89 54 24 08                   mov dword ptr [esp + 8], edx
c010343d: 83 ec 0c                      sub esp, 12
c0103440: 55                            push ebp
c0103441: e8 6a e5 ff ff                call 0xc01019b0 <HeapAdtPop>
c0103446: 89 73 10                      mov dword ptr [ebx + 16], esi
c0103449: 89 34 24                      mov dword ptr [esp], esi
c010344c: e8 83 7d 00 00                call 0xc010b1d4 <ArchSetIrql>
c0103451: 8b 54 24 18                   mov edx, dword ptr [esp + 24]
c0103455: 89 14 24                      mov dword ptr [esp], edx
c0103458: 8b 44 24 1c                   mov eax, dword ptr [esp + 28]
c010345c: ff d0                         call eax
c010345e: eb ca                         jmp 0xc010342a <LowerIrql+0x72>
c0103460: 83 ff 01                      cmp edi, 1
c0103463: 75 02                         jne 0xc0103467 <LowerIrql+0xaf>
c0103465: 31 ff                         xor edi, edi
c0103467: 89 7b 10                      mov dword ptr [ebx + 16], edi
c010346a: 83 ec 0c                      sub esp, 12
c010346d: 57                            push edi
c010346e: e8 61 7d 00 00                call 0xc010b1d4 <ArchSetIrql>
c0103473: 83 c4 10                      add esp, 16
c0103476: 85 ff                         test edi, edi
c0103478: 75 16                         jne 0xc0103490 <LowerIrql+0xd8>
c010347a: 80 7b 1d 00                   cmp byte ptr [ebx + 29], 0
c010347e: 74 10                         je 0xc0103490 <LowerIrql+0xd8>
c0103480: c6 43 1d 00                   mov byte ptr [ebx + 29], 0
c0103484: 83 c4 2c                      add esp, 44
c0103487: 5b                            pop ebx
c0103488: 5e                            pop esi
c0103489: 5f                            pop edi
c010348a: 5d                            pop ebp
c010348b: e9 4e 45 00 00                jmp 0xc01079de <Schedule>
c0103490: 83 c4 2c                      add esp, 44
c0103493: 5b                            pop ebx
c0103494: 5e                            pop esi
c0103495: 5f                            pop edi
c0103496: 5d                            pop ebp
c0103497: c3                            ret

c0103498 <PostponeScheduleUntilStandardIrql>:
c0103498: 0f 21 d8                      mov eax, dr3
c010349b: c1 e0 06                      shl eax, 6
c010349e: c6 80 dd 40 11 c0 01          mov byte ptr [eax - 1072611107], 1
c01034a5: c3                            ret

c01034a6 <InitIrql>:
c01034a6: 53                            push ebx
c01034a7: 83 ec 0c                      sub esp, 12
c01034aa: 0f 21 db                      mov ebx, dr3
c01034ad: 6a 08                         push 8
c01034af: 6a 01                         push 1
c01034b1: 6a 20                         push 32
```

```
c01034fe <RemoveBlock>:
c01034fe: 53                            push ebx
c01034ff: 8b 5a 08                      mov ebx, dword ptr [edx + 8]
c0103502: 8b 4a 04                      mov ecx, dword ptr [edx + 4]
c0103505: 85 db                         test ebx, ebx
c0103507: 75 1d                         jne 0xc0103526 <RemoveBlock+0x28>
c0103509: 85 c9                         test ecx, ecx
c010350b: 75 0b                         jne 0xc0103518 <RemoveBlock+0x1a>
c010350d: 31 c9                         xor ecx, ecx
c010350f: 89 0c 85 00 60 11 c0          mov dword ptr [4*eax - 1072603136], ecx
c0103516: eb 22                         jmp 0xc010353a <RemoveBlock+0x3c>
c0103518: 89 0c 85 00 60 11 c0          mov dword ptr [4*eax - 1072603136], ecx
c010351f: 31 d2                         xor edx, edx
c0103521: 89 51 08                      mov dword ptr [ecx + 8], edx
c0103524: eb 14                         jmp 0xc010353a <RemoveBlock+0x3c>
c0103526: 85 c9                         test ecx, ecx
c0103528: 75 07                         jne 0xc0103531 <RemoveBlock+0x33>
c010352a: 31 c0                         xor eax, eax
c010352c: 89 43 04                      mov dword ptr [ebx + 4], eax
c010352f: eb 09                         jmp 0xc010353a <RemoveBlock+0x3c>
c0103531: 89 4b 04                      mov dword ptr [ebx + 4], ecx
c0103534: 8b 42 08                      mov eax, dword ptr [edx + 8]
c0103537: 89 41 08                      mov dword ptr [ecx + 8], eax
c010353a: 5b                            pop ebx
c010353b: c3                            ret

c010353c <GetInsertionIndex>:
c010353c: 83 f8 08                      cmp eax, 8
c010353f: 74 1f                         je 0xc0103560 <GetInsertionIndex+0x24>
c0103541: 31 d2                         xor edx, edx
c0103543: 39 04 95 80 01 11 c0          cmp dword ptr [4*edx - 1072627328], eax
c010354a: 72 04                         jb 0xc0103550 <GetInsertionIndex+0x14>
c010354c: 8d 42 ff                      lea eax, [edx - 1]
c010354f: c3                            ret
c0103550: 42                            inc edx
c0103551: 83 fa 22                      cmp edx, 34
c0103554: 75 ed                         jne 0xc0103543 <GetInsertionIndex+0x7>
c0103556: 83 ec 18                      sub esp, 24
c0103559: 6a 07                         push 7
c010355b: e8 3f 56 00 00                call 0xc0108b9f <Panic>
c0103560: 31 c0                         xor eax, eax
c0103562: c3                            ret

c0103563 <RefillReservePages>:
c0103563: 53                            push ebx
c0103564: 83 ec 14                      sub esp, 20
c0103567: 68 8c 60 11 c0                push 3222364300
c010356c: e8 e9 33 00 00                call 0xc010695a <AcquireSpinlock>
c0103571: 83 c4 10                      add esp, 16
c0103574: 31 c0                         xor eax, eax
c0103576: 31 d2                         xor edx, edx
c0103578: 80 b8 48 30 11 c0 00          cmp byte ptr [eax - 1072615352], 0
c010357f: 74 0c                         je 0xc010358d <RefillReservePages+0x2a>
c0103581: 8b 88 44 30 11 c0             mov ecx, dword ptr [eax - 1072615356]
c0103587: 39 ca                         cmp edx, ecx
c0103589: 73 02                         jae 0xc010358d <RefillReservePages+0x2a>
c010358b: 89 ca                         mov edx, ecx
c010358d: 83 c0 0c                      add eax, 12
c0103590: 3d c0 00 00 00                cmp eax, 192
c0103595: 75 e1                         jne 0xc0103578 <RefillReservePages+0x15>
c0103597: 81 fa ff 3f 00 00             cmp edx, 16383
c010359d: 0f 87 8b 00 00 00             ja 0xc010362e <RefillReservePages+0xcb>
c01035a3: 83 ec 0c                      sub esp, 12
c01035a6: 68 8c 60 11 c0                push 3222364300
c01035ab: e8 fa 33 00 00                call 0xc01069aa <ReleaseSpinlock>
c01035b0: 58                            pop eax
c01035b1: 5a                            pop edx
c01035b2: 6a 00                         push 0
c01035b4: 6a 00                         push 0
c01035b6: 6a 13                         push 19
c01035b8: 68 00 40 00 00                push 16384
```

```
c010362b: 83 c4 10                      add esp, 16
c010362e: c7 44 24 10 8c 60 11 c0       mov dword ptr [esp + 16], 3222364300
c0103636: 83 c4 08                      add esp, 8
c0103639: 5b                            pop ebx
c010363a: e9 6b 33 00 00                jmp 0xc01069aa <ReleaseSpinlock>

c010363f <AddBlock.isra.0>:
c010363f: 55                            push ebp
c0103640: 57                            push edi
c0103641: 56                            push esi
c0103642: 53                            push ebx
c0103643: 83 ec 0c                      sub esp, 12
c0103646: 89 c3                         mov ebx, eax
c0103648: 8b 3b                         mov edi, dword ptr [ebx]
c010364a: 83 e7 fc                      and edi, -4
c010364d: 8d 47 f8                      lea eax, [edi - 8]
c0103650: e8 e7 fe ff ff                call 0xc010353c <GetInsertionIndex>
c0103655: 89 c1                         mov ecx, eax
c0103657: 8b 43 fc                      mov eax, dword ptr [ebx - 4]
c010365a: 83 e0 fc                      and eax, -4
c010365d: 89 de                         mov esi, ebx
c010365f: 29 c6                         sub esi, eax
c0103661: 8d 2c 3b                      lea ebp, [ebx + edi]
c0103664: 8b 06                         mov eax, dword ptr [esi]
c0103666: a8 01                         test al, 1
c0103668: 8b 55 00                      mov edx, dword ptr [ebp]
c010366b: 74 62                         je 0xc01036cf <AddBlock.isra.0+0x90>
c010366d: f6 c2 01                      test dl, 1
c0103670: 74 28                         je 0xc010369a <AddBlock.isra.0+0x5b>
c0103672: 31 f6                         xor esi, esi
c0103674: 89 73 08                      mov dword ptr [ebx + 8], esi
c0103677: 8b 04 8d 00 60 11 c0          mov eax, dword ptr [4*ecx - 1072603136]
c010367e: 89 43 04                      mov dword ptr [ebx + 4], eax
c0103681: 85 c0                         test eax, eax
c0103683: 74 03                         je 0xc0103688 <AddBlock.isra.0+0x49>
c0103685: 89 58 08                      mov dword ptr [eax + 8], ebx
c0103688: 89 1c 8d 00 60 11 c0          mov dword ptr [4*ecx - 1072603136], ebx
c010368f: 83 23 fe                      and dword ptr [ebx], -2
c0103692: 83 c4 0c                      add esp, 12
c0103695: 5b                            pop ebx
c0103696: 5e                            pop esi
c0103697: 5f                            pop edi
c0103698: 5d                            pop ebp
c0103699: c3                            ret
c010369a: 83 e2 fc                      and edx, -4
c010369d: 8d 42 f8                      lea eax, [edx - 8]
c01036a0: e8 97 fe ff ff                call 0xc010353c <GetInsertionIndex>
c01036a5: 89 ea                         mov edx, ebp
c01036a7: e8 52 fe ff ff                call 0xc01034fe <RemoveBlock>
c01036ac: 8b 55 00                      mov edx, dword ptr [ebp]
c01036af: 83 e2 fc                      and edx, -4
c01036b2: 01 fa                         add edx, edi
c01036b4: 89 d8                         mov eax, ebx
c01036b6: e8 30 fe ff ff                call 0xc01034eb <SetSizeTags>
c01036bb: 31 d2                         xor edx, edx
c01036bd: 89 53 08                      mov dword ptr [ebx + 8], edx
c01036c0: 89 53 04                      mov dword ptr [ebx + 4], edx
c01036c3: 83 23 fe                      and dword ptr [ebx], -2
c01036c6: 89 de                         mov esi, ebx
c01036c8: 89 f3                         mov ebx, esi
c01036ca: e9 79 ff ff ff                jmp 0xc0103648 <AddBlock.isra.0+0x9>
c01036cf: 83 e0 fc                      and eax, -4
c01036d2: 83 e8 08                      sub eax, 8
c01036d5: 80 e2 01                      and dl, 1
c01036d8: 74 15                         je 0xc01036ef <AddBlock.isra.0+0xb0>
c01036da: e8 5d fe ff ff                call 0xc010353c <GetInsertionIndex>
c01036df: 89 f2                         mov edx, esi
c01036e1: e8 18 fe ff ff                call 0xc01034fe <RemoveBlock>
c01036e6: 8b 16                         mov edx, dword ptr [esi]
c01036e8: 83 e2 fc                      and edx, -4
c01036eb: 01 fa                         add edx, edi
```

```
c0103739: 56                            push esi
c010373a: 53                            push ebx
c010373b: 83 ec 0c                      sub esp, 12
c010373e: 89 c3                         mov ebx, eax
c0103740: 89 d0                         mov eax, edx
c0103742: 8d 79 08                      lea edi, [ecx + 8]
c0103745: 8b 2b                         mov ebp, dword ptr [ebx]
c0103747: 83 e5 fc                      and ebp, -4
c010374a: 89 ee                         mov esi, ebp
c010374c: 29 fe                         sub esi, edi
c010374e: 89 da                         mov edx, ebx
c0103750: 83 fe 0f                      cmp esi, 15
c0103753: 77 15                         ja 0xc010376a <AllocateBlock+0x33>
c0103755: e8 a4 fd ff ff                call 0xc01034fe <RemoveBlock>
c010375a: 89 ea                         mov edx, ebp
c010375c: 89 d8                         mov eax, ebx
c010375e: e8 88 fd ff ff                call 0xc01034eb <SetSizeTags>
c0103763: 83 0b 01                      or dword ptr [ebx], 1
c0103766: 89 de                         mov esi, ebx
c0103768: eb 26                         jmp 0xc0103790 <AllocateBlock+0x59>
c010376a: e8 8f fd ff ff                call 0xc01034fe <RemoveBlock>
c010376f: 89 f2                         mov edx, esi
c0103771: 89 d8                         mov eax, ebx
c0103773: e8 73 fd ff ff                call 0xc01034eb <SetSizeTags>
c0103778: 01 de                         add esi, ebx
c010377a: 89 fa                         mov edx, edi
c010377c: 89 f0                         mov eax, esi
c010377e: e8 68 fd ff ff                call 0xc01034eb <SetSizeTags>
c0103783: 83 0e 01                      or dword ptr [esi], 1
c0103786: 83 23 fe                      and dword ptr [ebx], -2
c0103789: 89 d8                         mov eax, ebx
c010378b: e8 af fe ff ff                call 0xc010363f <AddBlock.isra.0>
c0103790: 89 f0                         mov eax, esi
c0103792: 83 c4 0c                      add esp, 12
c0103795: 5b                            pop ebx
c0103796: 5e                            pop esi
c0103797: 5f                            pop edi
c0103798: 5d                            pop ebp
c0103799: c3                            ret

c010379a <AllocHeapEx>:
c010379a: 55                            push ebp
c010379b: 57                            push edi
c010379c: 56                            push esi
c010379d: 53                            push ebx
c010379e: 83 ec 1c                      sub esp, 28
c01037a1: 8b 5c 24 30                   mov ebx, dword ptr [esp + 48]
c01037a5: 85 db                         test ebx, ebx
c01037a7: 0f 84 96 01 00 00             je 0xc0103943 <AllocHeapEx+0x1a9>
c01037ad: 81 fb ff 0d 00 00             cmp ebx, 3583
c01037b3: 76 10                         jbe 0xc01037c5 <AllocHeapEx+0x2b>
c01037b5: 51                            push ecx
c01037b6: 51                            push ecx
c01037b7: 53                            push ebx
c01037b8: 68 c6 06 11 c0                push 3222341318
c01037bd: e8 1b 53 00 00                call 0xc0108add <LogDeveloperWarning>
c01037c2: 83 c4 10                      add esp, 16
c01037c5: 83 ec 0c                      sub esp, 12
c01037c8: 68 8c 60 11 c0                push 3222364300
c01037cd: e8 88 31 00 00                call 0xc010695a <AcquireSpinlock>
c01037d2: 83 c4 10                      add esp, 16
c01037d5: 83 fb 08                      cmp ebx, 8
c01037d8: 73 05                         jae 0xc01037df <AllocHeapEx+0x45>
c01037da: bb 08 00 00 00                mov ebx, 8
c01037df: 83 c3 07                      add ebx, 7
c01037e2: 83 e3 f8                      and ebx, -8
c01037e5: 31 c0                         xor eax, eax
c01037e7: 39 1c 85 80 01 11 c0          cmp dword ptr [4*eax - 1072627328], ebx
c01037ee: 73 03                         jae 0xc01037f3 <AllocHeapEx+0x59>
c01037f0: 40                            inc eax
c01037f1: eb f4                         jmp 0xc01037e7 <AllocHeapEx+0x4d>
```

```
c0103856: 72 12                   jb 0xc010386a <AllocHeapEx+0xd0>
c0103858: 83 f8 ff                cmp eax, -1
c010385b: 74 0b                   je 0xc0103868 <AllocHeapEx+0xce>
c010385d: 6b f8 0c                imul edi, eax, 12
c0103860: 3b 8f 44 30 11 c0       cmp ecx, dword ptr [edi - 1072615356]
c0103866: 73 02                   jae 0xc010386a <AllocHeapEx+0xd0>
c0103868: 89 d0                   mov eax, edx
c010386a: 42                      inc edx
c010386b: 83 fa 10                cmp edx, 16
c010386e: 75 d2                   jne 0xc0103842 <AllocHeapEx+0xa8>
c0103870: 83 f8 ff                cmp eax, -1
c0103873: 75 07                   jne 0xc010387c <AllocHeapEx+0xe2>
c0103875: 83 ec 0c                sub esp, 12
c0103878: 6a 16                   push 22
c010387a: eb 34                   jmp 0xc01038b0 <AllocHeapEx+0x116>
c010387c: 6b c0 0c                imul eax, eax, 12
c010387f: 8d 90 40 30 11 c0       lea edx, [eax - 1072615360]
c0103885: 8b 88 40 30 11 c0       mov ecx, dword ptr [eax - 1072615360]
c010388b: 8d 3c 31                lea edi, [ecx + esi]
c010388e: 89 b8 40 30 11 c0       mov dword ptr [eax - 1072615360], edi
c0103894: 8b 42 04                mov eax, dword ptr [edx + 4]
c0103897: 29 f0                   sub eax, esi
c0103899: 89 42 04                mov dword ptr [edx + 4], eax
c010389c: 3d ff 0f 00 00          cmp eax, 4095
c01038a1: 77 04                   ja 0xc01038a7 <AllocHeapEx+0x10d>
c01038a3: c6 42 08 00             mov byte ptr [edx + 8], 0
c01038a7: 85 c9                   test ecx, ecx
c01038a9: 75 0a                   jne 0xc01038b5 <AllocHeapEx+0x11b>
c01038ab: 83 ec 0c                sub esp, 12
c01038ae: 6a 05                   push 5
c01038b0: e8 ea 52 00 00          call 0xc0108b9f <Panic>
c01038b5: 8d 79 08                lea edi, [ecx + 8]
c01038b8: 8d 6c 31 f8             lea ebp, [ecx + esi - 8]
c01038bc: ba 08 00 00 00          mov edx, 8
c01038c1: 89 c8                   mov eax, ecx
c01038c3: 89 4c 24 0c             mov dword ptr [esp + 12], ecx
c01038c7: e8 1f fc ff ff          call 0xc01034eb <SetSizeTags>
c01038cc: 8d 56 f0                lea edx, [esi - 16]
c01038cf: 89 f8                   mov eax, edi
c01038d1: e8 15 fc ff ff          call 0xc01034eb <SetSizeTags>
c01038d6: ba 08 00 00 00          mov edx, 8
c01038db: 89 e8                   mov eax, ebp
c01038dd: e8 09 fc ff ff          call 0xc01034eb <SetSizeTags>
c01038e2: 8b 4c 24 0c             mov ecx, dword ptr [esp + 12]
c01038e6: 31 c0                   xor eax, eax
c01038e8: 89 41 10                mov dword ptr [ecx + 16], eax
c01038eb: 89 41 0c                mov dword ptr [ecx + 12], eax
c01038ee: 83 09 01                or dword ptr [ecx], 1
c01038f1: 83 4d 00 01             or dword ptr [ebp], 1
c01038f5: 8b 41 08                mov eax, dword ptr [ecx + 8]
c01038f8: 89 c2                   mov edx, eax
c01038fa: 83 e2 fe                and edx, -2
c01038fd: 89 51 08                mov dword ptr [ecx + 8], edx
c0103900: 83 e0 fc                and eax, -4
c0103903: 83 e8 08                sub eax, 8
c0103906: e8 31 fc ff ff          call 0xc010353c <GetInsertionIndex>
c010390b: 89 c2                   mov edx, eax
c010390d: 89 3c 85 00 60 11 c0    mov dword ptr [4*eax - 1072603136], edi
c0103914: 89 d9                   mov ecx, ebx
c0103916: 89 f8                   mov eax, edi
c0103918: e8 1a fe ff ff          call 0xc0103737 <AllocateBlock>
c010391d: 89 c6                   mov esi, eax
c010391f: 83 ec 0c                sub esp, 12
c0103922: 68 8c 60 11 c0          push 3222364300
c0103927: e8 7e 30 00 00          call 0xc01069aa <ReleaseSpinlock>
c010392c: 83 c6 04                add esi, 4
c010392f: 83 c4 10                add esp, 16
c0103932: f6 44 24 34 01          test byte ptr [esp + 52], 1
c0103937: 74 0c                   je 0xc0103945 <AllocHeapEx+0x1ab>
c0103939: 31 c0                   xor eax, eax
c010393b: 89 f7                   mov edi, esi
```

```
c0103973: 53                            push ebx
c0103974: 83 ec 08                      sub esp, 8
c0103977: 8b 5c 24 10                   mov ebx, dword ptr [esp + 16]
c010397b: 85 db                         test ebx, ebx
c010397d: 74 2d                         je 0xc01039ac <FreeHeap+0x39>
c010397f: 31 c9                         xor ecx, ecx
c0103981: 89 4b 04                      mov dword ptr [ebx + 4], ecx
c0103984: 89 0b                         mov dword ptr [ebx], ecx
c0103986: 83 ec 0c                      sub esp, 12
c0103989: 68 8c 60 11 c0                push 3222364300
c010398e: e8 c7 2f 00 00                call 0xc010695a <AcquireSpinlock>
c0103993: 8d 43 fc                      lea eax, [ebx - 4]
c0103996: e8 a4 fc ff ff                call 0xc010363f <AddBlock.isra.0>
c010399b: c7 44 24 20 8c 60 11 c0       mov dword ptr [esp + 32], 3222364300
c01039a3: 83 c4 18                      add esp, 24
c01039a6: 5b                            pop ebx
c01039a7: e9 fe 2f 00 00                jmp 0xc01069aa <ReleaseSpinlock>
c01039ac: 83 c4 08                      add esp, 8
c01039af: 5b                            pop ebx
c01039b0: c3                            ret

c01039b1 <InitHeap>:
c01039b1: 83 ec 10                      sub esp, 16
c01039b4: 6a 03                         push 3
c01039b6: 68 0f 07 11 c0                push 3222341391
c01039bb: 68 8c 60 11 c0                push 3222364300
c01039c0: e8 7a 2f 00 00                call 0xc010693f <InitSpinlock>
c01039c5: 83 c4 1c                      add esp, 28
c01039c8: c3                            ret

c01039c9 <ReallocHeap>:
c01039c9: 55                            push ebp
c01039ca: 57                            push edi
c01039cb: 56                            push esi
c01039cc: 53                            push ebx
c01039cd: 83 ec 1c                      sub esp, 28
c01039d0: 8b 6c 24 30                   mov ebp, dword ptr [esp + 48]
c01039d4: 8b 44 24 34                   mov eax, dword ptr [esp + 52]
c01039d8: 8b 5d fc                      mov ebx, dword ptr [ebp - 4]
c01039db: 83 e3 fc                      and ebx, -4
c01039de: 39 c3                         cmp ebx, eax
c01039e0: 73 32                         jae 0xc0103a14 <ReallocHeap+0x4b>
c01039e2: 83 ec 0c                      sub esp, 12
c01039e5: 50                            push eax
c01039e6: e8 64 ff ff ff                call 0xc010394f <AllocHeap>
c01039eb: 83 c4 10                      add esp, 16
c01039ee: 85 c0                         test eax, eax
c01039f0: 75 04                         jne 0xc01039f6 <ReallocHeap+0x2d>
c01039f2: 89 c5                         mov ebp, eax
c01039f4: eb 1e                         jmp 0xc0103a14 <ReallocHeap+0x4b>
c01039f6: 89 c7                         mov edi, eax
c01039f8: 89 44 24 0c                   mov dword ptr [esp + 12], eax
c01039fc: 89 ee                         mov esi, ebp
c01039fe: 89 d9                         mov ecx, ebx
c0103a00: f3 a4                         rep  movsb byte ptr es:[edi], byte ptr [esi]
c0103a02: 83 ec 0c                      sub esp, 12
c0103a05: 55                            push ebp
c0103a06: e8 68 ff ff ff                call 0xc0103973 <FreeHeap>
c0103a0b: 83 c4 10                      add esp, 16
c0103a0e: 8b 44 24 0c                   mov eax, dword ptr [esp + 12]
c0103a12: eb de                         jmp 0xc01039f2 <ReallocHeap+0x29>
c0103a14: 89 e8                         mov eax, ebp
c0103a16: 83 c4 1c                      add esp, 28
c0103a19: 5b                            pop ebx
c0103a1a: 5e                            pop esi
c0103a1b: 5f                            pop edi
c0103a1c: 5d                            pop ebp
c0103a1d: c3                            ret

c0103a1e <IsBitmapEntryFree>:
c0103a1e: 89 c1                         mov ecx, eax
```

```
c0103a6b: 83 ec 08                  sub esp, 8
c0103a6e: a1 08 b0 11 c0            mov eax, dword ptr [3222384648]
c0103a73: 83 f8 1f                  cmp eax, 31
c0103a76: 77 11                     ja 0xc0103a89 <EvictPagesIfNeeded+0x28>
c0103a78: 83 ec 0c                  sub esp, 12
c0103a7b: 6a 02                     push 2
c0103a7d: e8 66 e8 ff ff            call 0xc01022e8 <SetDiskCaches>
c0103a82: 83 c4 10                  add esp, 16
c0103a85: 31 db                     xor ebx, ebx
c0103a87: eb 23                     jmp 0xc0103aac <EvictPagesIfNeeded+0x4b>
c0103a89: 83 f8 2f                  cmp eax, 47
c0103a8c: 77 27                     ja 0xc0103ab5 <EvictPagesIfNeeded+0x54>
c0103a8e: 83 ec 0c                  sub esp, 12
c0103a91: 6a 01                     push 1
c0103a93: eb e8                     jmp 0xc0103a7d <EvictPagesIfNeeded+0x1c>
c0103a95: 83 fb 05                  cmp ebx, 5
c0103a98: 74 1b                     je 0xc0103ab5 <EvictPagesIfNeeded+0x54>
c0103a9a: ff 05 80 b0 13 c0         inc dword ptr [-1072451456]
c0103aa0: e8 22 1c 00 00            call 0xc01056c7 <EvictVirt>
c0103aa5: ff 0d 80 b0 13 c0         dec dword ptr [-1072451456]
c0103aab: 43                        inc ebx
c0103aac: 83 3d 08 b0 11 c0 1f      cmp dword ptr [-1072582648], 31
c0103ab3: 76 e0                     jbe 0xc0103a95 <EvictPagesIfNeeded+0x34>
c0103ab5: c7 44 24 10 18 07 11 c0   mov dword ptr [esp + 16], 3222341400
c0103abd: 83 c4 08                  add esp, 8
c0103ac0: 5b                        pop ebx
c0103ac1: e9 ff 4f 00 00            jmp 0xc0108ac5 <LogWriteSerial>
c0103ac6: c3                        ret

c0103ac7 <DeallocPhys>:
c0103ac7: 53                        push ebx
c0103ac8: 83 ec 14                  sub esp, 20
c0103acb: 8b 5c 24 1c               mov ebx, dword ptr [esp + 28]
c0103acf: c1 eb 0c                  shr ebx, 12
c0103ad2: 68 20 b0 13 c0            push 3222515744
c0103ad7: e8 7e 2e 00 00            call 0xc010695a <AcquireSpinlock>
c0103adc: ff 05 08 b0 11 c0         inc dword ptr [-1072582648]
c0103ae2: 89 d8                     mov eax, ebx
c0103ae4: e8 62 ff ff ff            call 0xc0103a4b <DeallocateBitmapEntry>
c0103ae9: a1 10 b0 11 c0            mov eax, dword ptr [3222384656]
c0103aee: 83 c4 10                  add esp, 16
c0103af1: 85 c0                     test eax, eax
c0103af3: 74 12                     je 0xc0103b07 <DeallocPhys+0x40>
c0103af5: 8b 15 0c b0 11 c0         mov edx, dword ptr [-1072582644]
c0103afb: 8d 4a 01                  lea ecx, [edx + 1]
c0103afe: 89 0d 0c b0 11 c0         mov dword ptr [-1072582644], ecx
c0103b04: 89 1c 90                  mov dword ptr [eax + 4*edx], ebx
c0103b07: 83 ec 0c                  sub esp, 12
c0103b0a: 68 20 b0 13 c0            push 3222515744
c0103b0f: e8 96 2e 00 00            call 0xc01069aa <ReleaseSpinlock>
c0103b14: 83 c4 10                  add esp, 16
c0103b17: 83 3d 08 b0 11 c0 40      cmp dword ptr [-1072582648], 64
c0103b1e: 76 0f                     jbe 0xc0103b2f <DeallocPhys+0x68>
c0103b20: 31 c9                     xor ecx, ecx
c0103b22: 89 4c 24 10               mov dword ptr [esp + 16], ecx
c0103b26: 83 c4 08                  add esp, 8
c0103b29: 5b                        pop ebx
c0103b2a: e9 b9 e7 ff ff            jmp 0xc01022e8 <SetDiskCaches>
c0103b2f: 83 c4 08                  add esp, 8
c0103b32: 5b                        pop ebx
c0103b33: c3                        ret

c0103b34 <DeallocPhysContiguous>:
c0103b34: 56                        push esi
c0103b35: 53                        push ebx
c0103b36: 52                        push edx
c0103b37: 8b 74 24 10               mov esi, dword ptr [esp + 16]
c0103b3b: 31 db                     xor ebx, ebx
c0103b3d: 83 ec 0c                  sub esp, 12
c0103b40: ff 74 24 20               push dword ptr [esp + 32]
c0103b44: e8 76 1f 00 00            call 0xc0105abf <BytesToPages>
```

```
c0103b92: 50                            push eax
c0103b93: 6a 00                         push 0
c0103b95: 68 61 3a 10 c0                push 3222288993
c0103b9a: 6a 00                         push 0
c0103b9c: e8 58 f7 ff ff                call 0xc01032f9 <DeferUntilIrql>
c0103ba1: 83 c4 10                      add esp, 16
c0103ba4: 8b 15 10 b0 11 c0             mov edx, dword ptr [-1072582640]
c0103baa: 85 d2                         test edx, edx
c0103bac: 75 1b                         jne 0xc0103bc9 <AllocPhys+0x60>
c0103bae: 31 db                         xor ebx, ebx
c0103bb0: 89 d8                         mov eax, ebx
c0103bb2: e8 67 fe ff ff                call 0xc0103a1e <IsBitmapEntryFree>
c0103bb7: 84 c0                         test al, al
c0103bb9: 75 1c                         jne 0xc0103bd7 <AllocPhys+0x6e>
c0103bbb: 81 c3 ff ff 0f 00             add ebx, 1048575
c0103bc1: 81 e3 ff ff 0f 00             and ebx, 1048575
c0103bc7: eb e7                         jmp 0xc0103bb0 <AllocPhys+0x47>
c0103bc9: a1 0c b0 11 c0                mov eax, dword ptr [3222384652]
c0103bce: 48                            dec eax
c0103bcf: a3 0c b0 11 c0                mov dword ptr [3222384652], eax
c0103bd4: 8b 1c 82                      mov ebx, dword ptr [edx + 4*eax]
c0103bd7: 89 d8                         mov eax, ebx
c0103bd9: e8 57 fe ff ff                call 0xc0103a35 <AllocateBitmapEntry>
c0103bde: ff 0d 08 b0 11 c0             dec dword ptr [-1072582648]
c0103be4: 83 ec 0c                      sub esp, 12
c0103be7: 68 20 b0 13 c0                push 3222515744
c0103bec: e8 b9 2d 00 00                call 0xc01069aa <ReleaseSpinlock>
c0103bf1: 89 d8                         mov eax, ebx
c0103bf3: c1 e0 0c                      shl eax, 12
c0103bf6: 83 c4 18                      add esp, 24
c0103bf9: 5b                            pop ebx
c0103bfa: c3                            ret

c0103bfb <AllocPhysContiguous>:
c0103bfb: 55                            push ebp
c0103bfc: 57                            push edi
c0103bfd: 56                            push esi
c0103bfe: 53                            push ebx
c0103bff: 83 ec 1c                      sub esp, 28
c0103c02: 8b 7c 24 38                   mov edi, dword ptr [esp + 56]
c0103c06: 83 3d 10 b0 11 c0 00          cmp dword ptr [-1072582640], 0
c0103c0d: 0f 84 a0 00 00 00             je 0xc0103cb3 <AllocPhysContiguous+0xb8>
c0103c13: 83 ec 0c                      sub esp, 12
c0103c16: ff 74 24 3c                   push dword ptr [esp + 60]
c0103c1a: e8 a0 1e 00 00                call 0xc0105abf <BytesToPages>
c0103c1f: 89 c6                         mov esi, eax
c0103c21: 8b 44 24 44                   mov eax, dword ptr [esp + 68]
c0103c25: 05 ff 0f 00 00                add eax, 4095
c0103c2a: c1 e8 0c                      shr eax, 12
c0103c2d: 89 44 24 18                   mov dword ptr [esp + 24], eax
c0103c31: 83 c4 10                      add esp, 16
c0103c34: 89 fb                         mov ebx, edi
c0103c36: c1 eb 0c                      shr ebx, 12
c0103c39: 85 ff                         test edi, edi
c0103c3b: 75 08                         jne 0xc0103c45 <AllocPhysContiguous+0x4a>
c0103c3d: a1 00 b0 11 c0                mov eax, dword ptr [3222384640]
c0103c42: 8d 58 01                      lea ebx, [eax + 1]
c0103c45: 83 ec 0c                      sub esp, 12
c0103c48: 68 20 b0 13 c0                push 3222515744
c0103c4d: e8 08 2d 00 00                call 0xc010695a <AcquireSpinlock>
c0103c52: 8d 46 20                      lea eax, [esi + 32]
c0103c55: 83 c4 10                      add esp, 16
c0103c58: 3b 05 08 b0 11 c0             cmp eax, dword ptr [-1072582648]
c0103c5e: 73 43                         jae 0xc0103ca3 <AllocPhysContiguous+0xa8>
c0103c60: 8b 7c 24 3c                   mov edi, dword ptr [esp + 60]
c0103c64: c1 ef 0c                      shr edi, 12
c0103c67: 31 ed                         xor ebp, ebp
c0103c69: eb 32                         jmp 0xc0103c9d <AllocPhysContiguous+0xa2>
c0103c6b: 31 d2                         xor edx, edx
c0103c6d: 83 7c 24 3c 00                cmp dword ptr [esp + 60], 0
c0103c72: 74 10                         je 0xc0103c84 <AllocPhysContiguous+0x89>
```

```
c0103cca: 29 eb                   sub ebx, ebp
c0103ccc: 39 5c 24 08             cmp dword ptr [esp + 8], ebx
c0103cd0: 72 4a                   jb 0xc0103d1c <AllocPhysContiguous+0x121>
c0103cd2: 89 d8                   mov eax, ebx
c0103cd4: e8 5c fd ff ff          call 0xc0103a35 <AllocateBitmapEntry>
c0103cd9: a1 0c b0 11 c0          mov eax, dword ptr [3222384652]
c0103cde: 8b 35 10 b0 11 c0       mov esi, dword ptr [-1072582640]
c0103ce4: 89 f1                   mov ecx, esi
c0103ce6: 31 d2                   xor edx, edx
c0103ce8: 39 c2                   cmp edx, eax
c0103cea: 74 2d                   je 0xc0103d19 <AllocPhysContiguous+0x11e>
c0103cec: 89 cd                   mov ebp, ecx
c0103cee: 8d 7a 01                lea edi, [edx + 1]
c0103cf1: 83 c1 04                add ecx, 4
c0103cf4: 3b 5d 00                cmp ebx, dword ptr [ebp]
c0103cf7: 75 1c                   jne 0xc0103d15 <AllocPhysContiguous+0x11a>
c0103cf9: 48                      dec eax
c0103cfa: a3 0c b0 11 c0          mov dword ptr [3222384652], eax
c0103cff: 51                      push ecx
c0103d00: 29 d0                   sub eax, edx
c0103d02: c1 e0 02                shl eax, 2
c0103d05: 50                      push eax
c0103d06: 8d 04 be                lea eax, [esi + 4*edi]
c0103d09: 50                      push eax
c0103d0a: 55                      push ebp
c0103d0b: e8 54 d5 ff ff          call 0xc0101264 <memmove>
c0103d10: 83 c4 10                add esp, 16
c0103d13: eb 04                   jmp 0xc0103d19 <AllocPhysContiguous+0x11e>
c0103d15: 89 fa                   mov edx, edi
c0103d17: eb cf                   jmp 0xc0103ce8 <AllocPhysContiguous+0xed>
c0103d19: 43                      inc ebx
c0103d1a: eb b0                   jmp 0xc0103ccc <AllocPhysContiguous+0xd1>
c0103d1c: 83 ec 0c                sub esp, 12
c0103d1f: 68 20 b0 13 c0          push 3222515744
c0103d24: e8 81 2c 00 00          call 0xc01069aa <ReleaseSpinlock>
c0103d29: 89 d8                   mov eax, ebx
c0103d2b: c1 e0 0c                shl eax, 12
c0103d2e: 83 c4 10                add esp, 16
c0103d31: 83 c4 1c                add esp, 28
c0103d34: 5b                      pop ebx
c0103d35: 5e                      pop esi
c0103d36: 5f                      pop edi
c0103d37: 5d                      pop ebp
c0103d38: c3                      ret

c0103d39 <InitPhys>:
c0103d39: 57                      push edi
c0103d3a: 56                      push esi
c0103d3b: 53                      push ebx
c0103d3c: 50                      push eax
c0103d3d: 6a 03                   push 3
c0103d3f: 68 31 07 11 c0          push 3222341425
c0103d44: 68 20 b0 13 c0          push 3222515744
c0103d49: e8 f1 2b 00 00          call 0xc010693f <InitSpinlock>
c0103d4e: 83 c4 10                add esp, 16
c0103d51: 83 ec 0c                sub esp, 12
c0103d54: ff 74 24 1c             push dword ptr [esp + 28]
c0103d58: e8 72 96 00 00          call 0xc010d3cf <ArchGetMemory>
c0103d5d: 89 c6                   mov esi, eax
c0103d5f: 83 c4 10                add esp, 16
c0103d62: 85 c0                   test eax, eax
c0103d64: 74 59                   je 0xc0103dbf <InitPhys+0x86>
c0103d66: 8b 08                   mov ecx, dword ptr [eax]
c0103d68: 8b 58 04                mov ebx, dword ptr [eax + 4]
c0103d6b: 89 c8                   mov eax, ecx
c0103d6d: 89 da                   mov edx, ebx
c0103d6f: 05 ff 0f 00 00          add eax, 4095
c0103d74: 83 d2 00                adc edx, 0
c0103d77: 0f ac d0 0c             shrd eax, edx, 12
c0103d7b: c1 ea 0c                shr edx, 12
c0103d7e: 89 c7                   mov edi, eax
```

```
c0103dcc: 6a 13                         push 19
c0103dce: a1 00 b0 11 c0                mov eax, dword ptr [3222384640]
c0103dd3: 8d 04 85 04 00 00 00          lea eax, [4*eax + 4]
c0103dda: 50                            push eax
c0103ddb: 6a 00                         push 0
c0103ddd: 6a 00                         push 0
c0103ddf: e8 64 15 00 00                call 0xc0105348 <MapVirt>
c0103de4: 89 c6                         mov esi, eax
c0103de6: a3 10 b0 11 c0                mov dword ptr [3222384656], eax
c0103deb: 83 c4 20                      add esp, 32
c0103dee: 31 db                         xor ebx, ebx
c0103df0: 89 d8                         mov eax, ebx
c0103df2: e8 27 fc ff ff                call 0xc0103a1e <IsBitmapEntryFree>
c0103df7: 84 c0                         test al, al
c0103df9: 74 11                         je 0xc0103e0c <ReinitPhys+0x49>
c0103dfb: a1 0c b0 11 c0                mov eax, dword ptr [3222384652]
c0103e00: 8d 50 01                      lea edx, [eax + 1]
c0103e03: 89 15 0c b0 11 c0             mov dword ptr [-1072582644], edx
c0103e09: 89 1c 86                      mov dword ptr [esi + 4*eax], ebx
c0103e0c: 43                            inc ebx
c0103e0d: 81 fb 00 00 10 00             cmp ebx, 1048576
c0103e13: 75 db                         jne 0xc0103df0 <ReinitPhys+0x2d>
c0103e15: bb ff ff 0f 00                mov ebx, 1048575
c0103e1a: 2b 1d 00 b0 11 c0             sub ebx, dword ptr [-1072582656]
c0103e20: c1 eb 11                      shr ebx, 17
c0103e23: 89 d8                         mov eax, ebx
c0103e25: c1 e0 0c                      shl eax, 12
c0103e28: be 20 b0 13 c0                mov esi, 3222515744
c0103e2d: 29 c6                         sub esi, eax
c0103e2f: 81 e6 00 f0 ff ff             and esi, 4294963200
c0103e35: 83 eb 01                      sub ebx, 1
c0103e38: 72 22                         jb 0xc0103e5c <ReinitPhys+0x99>
c0103e3a: 83 ec 0c                      sub esp, 12
c0103e3d: 56                            push esi
c0103e3e: e8 e0 96 00 00                call 0xc010d523 <ArchVirtualToPhysical>
c0103e43: 89 04 24                      mov dword ptr [esp], eax
c0103e46: e8 7c fc ff ff                call 0xc0103ac7 <DeallocPhys>
c0103e4b: 81 c6 00 10 00 00             add esi, 4096
c0103e51: ff 05 04 b0 11 c0             inc dword ptr [-1072582652]
c0103e57: 83 c4 10                      add esp, 16
c0103e5a: eb d9                         jmp 0xc0103e35 <ReinitPhys+0x72>
c0103e5c: 58                            pop eax
c0103e5d: 5b                            pop ebx
c0103e5e: 5e                            pop esi
c0103e5f: c3                            ret

c0103e60 <GetTotalPhysKilobytes>:
c0103e60: a1 04 b0 11 c0                mov eax, dword ptr [3222384644]
c0103e65: c1 e0 02                      shl eax, 2
c0103e68: c3                            ret

c0103e69 <GetFreePhysKilobytes>:
c0103e69: a1 08 b0 11 c0                mov eax, dword ptr [3222384648]
c0103e6e: c1 e0 02                      shl eax, 2
c0103e71: c3                            ret

c0103e72 <SetBitmapEntry>:
c0103e72: 56                            push esi
c0103e73: 53                            push ebx
c0103e74: 89 c1                         mov ecx, eax
c0103e76: 89 d6                         mov esi, edx
c0103e78: 89 c3                         mov ebx, eax
c0103e7a: c1 eb 03                      shr ebx, 3
c0103e7d: 03 1d 44 b0 13 c0             add ebx, dword ptr [-1072451516]
c0103e83: 8a 13                         mov dl, byte ptr [ebx]
c0103e85: 83 e1 07                      and ecx, 7
c0103e88: b8 01 00 00 00                mov eax, 1
c0103e8d: d3 e0                         shl eax, cl
c0103e8f: 89 f1                         mov ecx, esi
c0103e91: 84 c9                         test cl, cl
c0103e93: 74 04                         je 0xc0103e99 <SetBitmapEntry+0x27>
```

```
c0103ee5: c1 e0 0c                  shl eax, 12
c0103ee8: 31 d2                     xor edx, edx
c0103eea: 05 ff ff ff 07            add eax, 134217727
c0103eef: 83 d2 00                  adc edx, 0
c0103ef2: 0f ac d0 1b               shrd eax, edx, 27
c0103ef6: c1 ea 1b                  shr edx, 27
c0103ef9: 89 c2                     mov edx, eax
c0103efb: c1 e2 0f                  shl edx, 15
c0103efe: 89 15 3c b0 13 c0         mov dword ptr [-1072451524], edx
c0103f04: 5a                        pop edx
c0103f05: 59                        pop ecx
c0103f06: 6a 00                     push 0
c0103f08: 6a 00                     push 0
c0103f0a: 6a 13                     push 19
c0103f0c: c1 e0 0c                  shl eax, 12
c0103f0f: 50                        push eax
c0103f10: 6a 00                     push 0
c0103f12: 6a 00                     push 0
c0103f14: e8 2f 14 00 00            call 0xc0105348 <MapVirt>
c0103f19: a3 44 b0 13 c0            mov dword ptr [3222515780], eax
c0103f1e: 83 c4 2c                  add esp, 44
c0103f21: c3                        ret

c0103f22 <GetSwapfile>:
c0103f22: a1 64 b0 13 c0            mov eax, dword ptr [3222515812]
c0103f27: c3                        ret

c0103f28 <AllocSwap>:
c0103f28: 55                        push ebp
c0103f29: 57                        push edi
c0103f2a: 56                        push esi
c0103f2b: 53                        push ebx
c0103f2c: 83 ec 18                  sub esp, 24
c0103f2f: 68 48 b0 13 c0            push 3222515784
c0103f34: e8 21 2a 00 00            call 0xc010695a <AcquireSpinlock>
c0103f39: ff 05 40 b0 13 c0         inc dword ptr [-1072451520]
c0103f3f: a1 3c b0 13 c0            mov eax, dword ptr [3222515772]
c0103f44: 8b 15 44 b0 13 c0         mov edx, dword ptr [-1072451516]
c0103f4a: 83 c4 10                  add esp, 16
c0103f4d: 31 db                     xor ebx, ebx
c0103f4f: be 01 00 00 00            mov esi, 1
c0103f54: 39 d8                     cmp eax, ebx
c0103f56: 74 19                     je 0xc0103f71 <AllocSwap+0x49>
c0103f58: 89 d9                     mov ecx, ebx
c0103f5a: c1 e9 03                  shr ecx, 3
c0103f5d: 0f b6 3c 0a               movzx edi, byte ptr [edx + ecx]
c0103f61: 89 d9                     mov ecx, ebx
c0103f63: 83 e1 07                  and ecx, 7
c0103f66: 89 f5                     mov ebp, esi
c0103f68: d3 e5                     shl ebp, cl
c0103f6a: 85 ef                     test edi, ebp
c0103f6c: 74 0d                     je 0xc0103f7b <AllocSwap+0x53>
c0103f6e: 43                        inc ebx
c0103f6f: eb e3                     jmp 0xc0103f54 <AllocSwap+0x2c>
c0103f71: 83 ec 0c                  sub esp, 12
c0103f74: 6a 20                     push 32
c0103f76: e8 24 4c 00 00            call 0xc0108b9f <Panic>
c0103f7b: ba 01 00 00 00            mov edx, 1
c0103f80: 89 d8                     mov eax, ebx
c0103f82: e8 eb fe ff ff            call 0xc0103e72 <SetBitmapEntry>
c0103f87: 83 ec 0c                  sub esp, 12
c0103f8a: 68 48 b0 13 c0            push 3222515784
c0103f8f: e8 16 2a 00 00            call 0xc01069aa <ReleaseSpinlock>
c0103f94: 89 d8                     mov eax, ebx
c0103f96: 31 d2                     xor edx, edx
c0103f98: 83 c4 1c                  add esp, 28
c0103f9b: 5b                        pop ebx
c0103f9c: 5e                        pop esi
c0103f9d: 5f                        pop edi
c0103f9e: 5d                        pop ebp
c0103f9f: c3                        ret
```

```
c0103ff9 <VirtAvlComparator>:
c0103ff9: 55                            push ebp
c0103ffa: 57                            push edi
c0103ffb: 56                            push esi
c0103ffc: 53                            push ebx
c0103ffd: 8b 7c 24 14                   mov edi, dword ptr [esp + 20]
c0104001: 8b 54 24 18                   mov edx, dword ptr [esp + 24]
c0104005: 8b 37                         mov esi, dword ptr [edi]
c0104007: 89 f0                         mov eax, esi
c0104009: c1 e8 0c                      shr eax, 12
c010400c: 8b 1a                         mov ebx, dword ptr [edx]
c010400e: 89 d9                         mov ecx, ebx
c0104010: c1 e9 0c                      shr ecx, 12
c0104013: 39 c8                         cmp eax, ecx
c0104015: 72 0f                         jb 0xc0104026 <VirtAvlComparator+0x2d>
c0104017: 8b 6a 0c                      mov ebp, dword ptr [edx + 12]
c010401a: 01 cd                         add ebp, ecx
c010401c: 31 d2                         xor edx, edx
c010401e: 39 e8                         cmp eax, ebp
c0104020: 72 1a                         jb 0xc010403c <VirtAvlComparator+0x43>
c0104022: 39 c8                         cmp eax, ecx
c0104024: 75 09                         jne 0xc010402f <VirtAvlComparator+0x36>
c0104026: 03 47 0c                      add eax, dword ptr [edi + 12]
c0104029: 31 d2                         xor edx, edx
c010402b: 39 c1                         cmp ecx, eax
c010402d: 72 0d                         jb 0xc010403c <VirtAvlComparator+0x43>
c010402f: ba 01 00 00 00                mov edx, 1
c0104034: 39 f3                         cmp ebx, esi
c0104036: 72 04                         jb 0xc010403c <VirtAvlComparator+0x43>
c0104038: 39 de                         cmp esi, ebx
c010403a: 19 d2                         sbb edx, edx
c010403c: 89 d0                         mov eax, edx
c010403e: 5b                            pop ebx
c010403f: 5e                            pop esi
c0104040: 5f                            pop edi
c0104041: 5d                            pop ebp
c0104042: c3                            ret

c0104043 <InsertIntoAvl>:
c0104043: 53                            push ebx
c0104044: 83 ec 08                      sub esp, 8
c0104047: 89 d3                         mov ebx, edx
c0104049: f6 42 05 04                   test byte ptr [edx + 5], 4
c010404d: 74 3d                         je 0xc010408c <InsertIntoAvl+0x49>
c010404f: 0f 21 d8                      mov eax, dr3
c0104052: 83 ec 0c                      sub esp, 12
c0104055: c1 e0 06                      shl eax, 6
c0104058: 05 e4 40 11 c0                add eax, 3222356196
c010405d: 50                            push eax
c010405e: e8 f7 28 00 00                call 0xc010695a <AcquireSpinlock>
c0104063: 0f 21 d8                      mov eax, dr3
c0104066: 5a                            pop edx
c0104067: 59                            pop ecx
c0104068: 53                            push ebx
c0104069: c1 e0 06                      shl eax, 6
c010406c: ff b0 e0 40 11 c0             push dword ptr [eax - 1072611104]
c0104072: e8 13 e0 ff ff                call 0xc010208a <TreeInsert>
c0104077: 0f 21 d8                      mov eax, dr3
c010407a: c1 e0 06                      shl eax, 6
c010407d: 05 e4 40 11 c0                add eax, 3222356196
c0104082: 89 04 24                      mov dword ptr [esp], eax
c0104085: e8 20 29 00 00                call 0xc01069aa <ReleaseSpinlock>
c010408a: eb 0a                         jmp 0xc0104096 <InsertIntoAvl+0x53>
c010408c: 51                            push ecx
c010408d: 51                            push ecx
c010408e: 52                            push edx
c010408f: ff 30                         push dword ptr [eax]
c0104091: e8 f4 df ff ff                call 0xc010208a <TreeInsert>
c0104096: 83 c4 10                      add esp, 16
c0104099: 83 c4 08                      add esp, 8
c010409c: 5b                            pop ebx
```

```
c01040e9: 52                            push edx
c01040ea: ff 30                         push dword ptr [eax]
c01040ec: e8 db df ff ff                call 0xc01020cc <TreeDelete>
c01040f1: 83 c4 10                      add esp, 16
c01040f4: 83 c4 08                      add esp, 8
c01040f7: 5b                            pop ebx
c01040f8: c3                            ret

c01040f9 <SplitLargePageEntryIntoMultiple.constprop.0.isra.0>:
c01040f9: 55                            push ebp
c01040fa: 57                            push edi
c01040fb: 56                            push esi
c01040fc: 53                            push ebx
c01040fd: 83 ec 1c                      sub esp, 28
c0104100: 89 44 24 0c                   mov dword ptr [esp + 12], eax
c0104104: 83 79 0c 01                   cmp dword ptr [ecx + 12], 1
c0104108: 0f 84 ff 00 00 00             je 0xc010420d <SplitLargePageEntryIntoMultipl
c010410e: 89 d5                         mov ebp, edx
c0104110: 89 cb                         mov ebx, ecx
c0104112: 83 79 20 01                   cmp dword ptr [ecx + 32], 1
c0104116: 74 10                         je 0xc0104128 <SplitLargePageEntryIntoMultipl
c0104118: 83 ec 0c                      sub esp, 12
c010411b: 68 46 07 11 c0                push 3222341446
c0104120: e8 b8 49 00 00                call 0xc0108add <LogDeveloperWarning>
c0104125: 83 c4 10                      add esp, 16
c0104128: 8b 03                         mov eax, dword ptr [ebx]
c010412a: c1 e8 0c                      shr eax, 12
c010412d: 89 44 24 04                   mov dword ptr [esp + 4], eax
c0104131: c1 ed 0c                      shr ebp, 12
c0104134: 39 e8                         cmp eax, ebp
c0104136: 73 6c                         jae 0xc01041a4 <SplitLargePageEntryIntoMultip
c0104138: 83 ec 0c                      sub esp, 12
c010413b: 68 8d 07 11 c0                push 3222341517
c0104140: e8 80 49 00 00                call 0xc0108ac5 <LogWriteSerial>
c0104145: 89 e8                         mov eax, ebp
c0104147: 8b 74 24 14                   mov esi, dword ptr [esp + 20]
c010414b: 29 f0                         sub eax, esi
c010414d: 89 44 24 18                   mov dword ptr [esp + 24], eax
c0104151: c7 04 24 24 00 00 00          mov dword ptr [esp], 36
c0104158: e8 f2 f7 ff ff                call 0xc010394f <AllocHeap>
c010415d: 89 c2                         mov edx, eax
c010415f: b9 09 00 00 00                mov ecx, 9
c0104164: 89 c7                         mov edi, eax
c0104166: 89 de                         mov esi, ebx
c0104168: f3 a5                         rep  movsd dword ptr es:[edi], dword ptr [esi
c010416a: 8b 44 24 18                   mov eax, dword ptr [esp + 24]
c010416e: 89 42 0c                      mov dword ptr [edx + 12], eax
c0104171: 8b 44 24 14                   mov eax, dword ptr [esp + 20]
c0104175: 29 e8                         sub eax, ebp
c0104177: 01 43 0c                      add dword ptr [ebx + 12], eax
c010417a: 8b 44 24 18                   mov eax, dword ptr [esp + 24]
c010417e: c1 e0 0c                      shl eax, 12
c0104181: 01 03                         add dword ptr [ebx], eax
c0104183: 8b 4b 18                      mov ecx, dword ptr [ebx + 24]
c0104186: 83 c4 10                      add esp, 16
c0104189: 85 c9                         test ecx, ecx
c010418b: 74 05                         je 0xc0104192 <SplitLargePageEntryIntoMultipl
c010418d: 01 c1                         add ecx, eax
c010418f: 89 4b 18                      mov dword ptr [ebx + 24], ecx
c0104192: f6 43 04 04                   test byte ptr [ebx + 4], 4
c0104196: 74 03                         je 0xc010419b <SplitLargePageEntryIntoMultipl
c0104198: 01 43 10                      add dword ptr [ebx + 16], eax
c010419b: 8b 44 24 0c                   mov eax, dword ptr [esp + 12]
c010419f: e8 9f fe ff ff                call 0xc0104043 <InsertIntoAvl>
c01041a4: 83 7b 0c 01                   cmp dword ptr [ebx + 12], 1
c01041a8: 7e 63                         jle 0xc010420d <SplitLargePageEntryIntoMultip
c01041aa: 83 ec 0c                      sub esp, 12
c01041ad: 68 a0 07 11 c0                push 3222341536
c01041b2: e8 0e 49 00 00                call 0xc0108ac5 <LogWriteSerial>
c01041b7: c7 04 24 24 00 00 00          mov dword ptr [esp], 36
c01041be: e8 8c f7 ff ff                call 0xc010394f <AllocHeap>
```

```
c0104215 <GetVirtEntry.isra.0>:
c0104215: 57                            push edi
c0104216: 56                            push esi
c0104217: 53                            push ebx
c0104218: 83 ec 40                      sub esp, 64
c010421b: 89 c6                         mov esi, eax
c010421d: 8d 7c 24 20                   lea edi, [esp + 32]
c0104221: b9 08 00 00 00                mov ecx, 8
c0104226: 31 c0                         xor eax, eax
c0104228: f3 ab                         rep  stosd dword ptr es:[edi], eax
c010422a: 81 e2 00 f0 ff ff             and edx, 4294963200
c0104230: 89 54 24 1c                   mov dword ptr [esp + 28], edx
c0104234: c7 44 24 28 01 00 00 00       mov dword ptr [esp + 40], 1
c010423c: 53                            push ebx
c010423d: 53                            push ebx
c010423e: 8d 5c 24 24                   lea ebx, [esp + 36]
c0104242: 53                            push ebx
c0104243: 56                            push esi
c0104244: e8 b7 de ff ff                call 0xc0102100 <TreeGet>
c0104249: 83 c4 10                      add esp, 16
c010424c: 85 c0                         test eax, eax
c010424e: 75 47                         jne 0xc0104297 <GetVirtEntry.isra.0+0x82>
c0104250: 0f 21 d8                      mov eax, dr3
c0104253: 83 ec 0c                      sub esp, 12
c0104256: c1 e0 06                      shl eax, 6
c0104259: 05 e4 40 11 c0                add eax, 3222356196
c010425e: 50                            push eax
c010425f: e8 f6 26 00 00                call 0xc010695a <AcquireSpinlock>
c0104264: 0f 21 d8                      mov eax, dr3
c0104267: 5a                            pop edx
c0104268: 59                            pop ecx
c0104269: 53                            push ebx
c010426a: c1 e0 06                      shl eax, 6
c010426d: ff b0 e0 40 11 c0             push dword ptr [eax - 1072611104]
c0104273: e8 88 de ff ff                call 0xc0102100 <TreeGet>
c0104278: 89 44 24 1c                   mov dword ptr [esp + 28], eax
c010427c: 0f 21 da                      mov edx, dr3
c010427f: c1 e2 06                      shl edx, 6
c0104282: 81 c2 e4 40 11 c0             add edx, 3222356196
c0104288: 89 14 24                      mov dword ptr [esp], edx
c010428b: e8 1a 27 00 00                call 0xc01069aa <ReleaseSpinlock>
c0104290: 83 c4 10                      add esp, 16
c0104293: 8b 44 24 0c                   mov eax, dword ptr [esp + 12]
c0104297: 83 c4 40                      add esp, 64
c010429a: 5b                            pop ebx
c010429b: 5e                            pop esi
c010429c: 5f                            pop edi
c010429d: c3                            ret

c010429e <AllocVirtRange.isra.0>:
c010429e: 53                            push ebx
c010429f: 83 ec 08                      sub esp, 8
c01042a2: c1 e0 0c                      shl eax, 12
c01042a5: 85 d2                         test edx, edx
c01042a7: 74 17                         je 0xc01042c0 <AllocVirtRange.isra.0+0x22>
c01042a9: 8b 1d 04 31 11 c0             mov ebx, dword ptr [-1072615164]
c01042af: 01 d8                         add eax, ebx
c01042b1: a3 04 31 11 c0                mov dword ptr [3222352132], eax
c01042b6: 50                            push eax
c01042b7: 50                            push eax
c01042b8: 53                            push ebx
c01042b9: 68 b3 07 11 c0                push 3222341555
c01042be: eb 15                         jmp 0xc01042d5 <AllocVirtRange.isra.0+0x37>
c01042c0: 8b 1d 00 31 11 c0             mov ebx, dword ptr [-1072615168]
c01042c6: 01 d8                         add eax, ebx
c01042c8: a3 00 31 11 c0                mov dword ptr [3222352128], eax
c01042cd: 50                            push eax
c01042ce: 50                            push eax
c01042cf: 53                            push ebx
c01042d0: 68 c7 07 11 c0                push 3222341575
c01042d5: e8 eb 47 00 00                call 0xc0108ac5 <LogWriteSerial>
```

```
c0104321: 5a                            pop edx
c0104322: 5b                            pop ebx
c0104323: 5e                            pop esi
c0104324: e9 44 94 00 00                jmp 0xc010d76d <ArchInitVas>
c0104329: 58                            pop eax
c010432a: 5b                            pop ebx
c010432b: 5e                            pop esi
c010432c: c3                            ret

c010432d <CreateVas>:
c010432d: 83 ec 28                      sub esp, 40
c0104330: 6a 24                         push 36
c0104332: e8 18 f6 ff ff                call 0xc010394f <AllocHeap>
c0104337: 5a                            pop edx
c0104338: 59                            pop ecx
c0104339: 6a 00                         push 0
c010433b: 50                            push eax
c010433c: 89 44 24 1c                   mov dword ptr [esp + 28], eax
c0104340: e8 9f ff ff ff                call 0xc01042e4 <CreateVasEx>
c0104345: 8b 44 24 1c                   mov eax, dword ptr [esp + 28]
c0104349: 83 c4 2c                      add esp, 44
c010434c: c3                            ret

c010434d <FindVirtToEvictRecursive>:
c010434d: 55                            push ebp
c010434e: 57                            push edi
c010434f: 56                            push esi
c0104350: 53                            push ebx
c0104351: 83 ec 2c                      sub esp, 44
c0104354: 8b 74 24 44                   mov esi, dword ptr [esp + 68]
c0104358: 8b 6c 24 48                   mov ebp, dword ptr [esp + 72]
c010435c: 85 f6                         test esi, esi
c010435e: 0f 84 55 01 00 00             je 0xc01044b9 <FindVirtToEvictRecursive+0x16c
c0104364: 83 7d 00 09                   cmp dword ptr [ebp], 9
c0104368: 0f 8e 4b 01 00 00             jle 0xc01044b9 <FindVirtToEvictRecursive+0x16
c010436e: 8b 44 24 50                   mov eax, dword ptr [esp + 80]
c0104372: ff 00                         inc dword ptr [eax]
c0104374: 8b 5e 08                      mov ebx, dword ptr [esi + 8]
c0104377: 8b 7b 08                      mov edi, dword ptr [ebx + 8]
c010437a: 85 ff                         test edi, edi
c010437c: 74 22                         je 0xc01043a0 <FindVirtToEvictRecursive+0x53>
c010437e: 50                            push eax
c010437f: 50                            push eax
c0104380: ff 74 24 5c                   push dword ptr [esp + 92]
c0104384: ff 74 24 5c                   push dword ptr [esp + 92]
c0104388: ff 74 24 5c                   push dword ptr [esp + 92]
c010438c: 55                            push ebp
c010438d: ff 36                         push dword ptr [esi]
c010438f: ff 74 24 5c                   push dword ptr [esp + 92]
c0104393: e8 b5 ff ff ff                call 0xc010434d <FindVirtToEvictRecursive>
c0104398: 8b 76 04                      mov esi, dword ptr [esi + 4]
c010439b: 83 c4 20                      add esp, 32
c010439e: eb bc                         jmp 0xc010435c <FindVirtToEvictRecursive+0xf>
c01043a0: 8a 43 04                      mov al, byte ptr [ebx + 4]
c01043a3: f7 d0                         not eax
c01043a5: a8 03                         test al, 3
c01043a7: 75 d5                         jne 0xc010437e <FindVirtToEvictRecursive+0x31
c01043a9: 8d 44 24 1f                   lea eax, [esp + 31]
c01043ad: 50                            push eax
c01043ae: 8d 44 24 22                   lea eax, [esp + 34]
c01043b2: 50                            push eax
c01043b3: 53                            push ebx
c01043b4: ff 74 24 4c                   push dword ptr [esp + 76]
c01043b8: e8 9b 92 00 00                call 0xc010d658 <ArchGetPageUsageBits>
c01043bd: 8a 4b 05                      mov cl, byte ptr [ebx + 5]
c01043c0: 88 c8                         mov al, cl
c01043c2: 83 e0 04                      and eax, 4
c01043c5: 83 c4 10                      add esp, 16
c01043c8: f6 d8                         neg al
c01043ca: 19 d2                         sbb edx, edx
c01043cc: 83 e2 03                      and edx, 3
```

```
c0104425: 19 c0                         sbb eax, eax
c0104427: 83 e0 ec                      and eax, -20
c010442a: 83 c0 28                      add eax, 40
c010442d: 01 d0                         add eax, edx
c010442f: eb 1c                         jmp 0xc010444d <FindVirtToEvictRecursive+0x10
c0104431: 8d 42 50                      lea eax, [edx + 80]
c0104434: 84 c9                         test cl, cl
c0104436: 75 15                         jne 0xc010444d <FindVirtToEvictRecursive+0x10
c0104438: 80 7c 24 1e 01                cmp byte ptr [esp + 30], 1
c010443d: 19 c0                         sbb eax, eax
c010443f: 83 e0 f6                      and eax, -10
c0104442: 8d 44 02 3c                   lea eax, [edx + eax + 60]
c0104446: eb 05                         jmp 0xc010444d <FindVirtToEvictRecursive+0x10
c0104448: b8 96 00 00 00                mov eax, 150
c010444d: 8b 4d 00                      mov ecx, dword ptr [ebp]
c0104450: 89 4c 24 0c                   mov dword ptr [esp + 12], ecx
c0104454: 31 c9                         xor ecx, ecx
c0104456: 39 44 24 0c                   cmp dword ptr [esp + 12], eax
c010445a: 75 15                         jne 0xc0104471 <FindVirtToEvictRecursive+0x12
c010445c: 8a 0d 20 b1 13 c0             mov cl, byte ptr [-1072451296]
c0104462: 8d 51 01                      lea edx, [ecx + 1]
c0104465: 88 15 20 b1 13 c0             mov byte ptr [-1072451296], dl
c010446b: 80 e1 03                      and cl, 3
c010446e: 0f 94 c1                      sete cl
c0104471: 8b 54 24 54                   mov edx, dword ptr [esp + 84]
c0104475: 39 1c ba                      cmp dword ptr [edx + 4*edi], ebx
c0104478: 74 0a                         je 0xc0104484 <FindVirtToEvictRecursive+0x137
c010447a: 47                            inc edi
c010447b: 83 ff 20                      cmp edi, 32
c010447e: 75 f1                         jne 0xc0104471 <FindVirtToEvictRecursive+0x12
c0104480: 31 ff                         xor edi, edi
c0104482: eb 05                         jmp 0xc0104489 <FindVirtToEvictRecursive+0x13
c0104484: bf 01 00 00 00                mov edi, 1
c0104489: 39 44 24 0c                   cmp dword ptr [esp + 12], eax
c010448d: 7f 08                         jg 0xc0104497 <FindVirtToEvictRecursive+0x14a
c010448f: 84 c9                         test cl, cl
c0104491: 0f 84 e7 fe ff ff             je 0xc010437e <FindVirtToEvictRecursive+0x31>
c0104497: 89 fa                         mov edx, edi
c0104499: 84 d2                         test dl, dl
c010449b: 0f 85 dd fe ff ff             jne 0xc010437e <FindVirtToEvictRecursive+0x31
c01044a1: 8b 7c 24 4c                   mov edi, dword ptr [esp + 76]
c01044a5: 8b 4c 24 40                   mov ecx, dword ptr [esp + 64]
c01044a9: 89 0f                         mov dword ptr [edi], ecx
c01044ab: 89 5f 04                      mov dword ptr [edi + 4], ebx
c01044ae: 89 45 00                      mov dword ptr [ebp], eax
c01044b1: 85 c0                         test eax, eax
c01044b3: 0f 85 c5 fe ff ff             jne 0xc010437e <FindVirtToEvictRecursive+0x31
c01044b9: 83 c4 2c                      add esp, 44
c01044bc: 5b                            pop ebx
c01044bd: 5e                            pop esi
c01044be: 5f                            pop edi
c01044bf: 5d                            pop ebp
c01044c0: c3                            ret

c01044c1 <FindVirtToEvict>:
c01044c1: 55                            push ebp
c01044c2: 57                            push edi
c01044c3: 56                            push esi
c01044c4: 53                            push ebx
c01044c5: 83 ec 1c                      sub esp, 28
c01044c8: 8b 5c 24 30                   mov ebx, dword ptr [esp + 48]
c01044cc: 8b 7c 24 38                   mov edi, dword ptr [esp + 56]
c01044d0: 8b 6c 24 40                   mov ebp, dword ptr [esp + 64]
c01044d4: 31 c9                         xor ecx, ecx
c01044d6: 89 4c 24 0c                   mov dword ptr [esp + 12], ecx
c01044da: 80 7c 24 3c 00                cmp byte ptr [esp + 60], 0
c01044df: 8d 74 24 0c                   lea esi, [esp + 12]
c01044e3: 74 21                         je 0xc0104506 <FindVirtToEvict+0x45>
c01044e5: 0f 21 d8                      mov eax, dr3
c01044e8: 52                            push edx
c01044e9: 52                            push edx
```

```
c0104523: 83 ec 08                  sub esp, 8
c0104526: 8b 54 24 14               mov edx, dword ptr [esp + 20]
c010452a: 8b 44 24 10               mov eax, dword ptr [esp + 16]
c010452e: 8b 00                     mov eax, dword ptr [eax]
c0104530: e8 e0 fc ff ff            call 0xc0104215 <GetVirtEntry.isra.0>
c0104535: 89 c3                     mov ebx, eax
c0104537: 89 c1                     mov ecx, eax
c0104539: 8b 54 24 14               mov edx, dword ptr [esp + 20]
c010453d: 8b 44 24 10               mov eax, dword ptr [esp + 16]
c0104541: e8 b3 fb ff ff            call 0xc01040f9 <SplitLargePageEntryIntoMulti
c0104546: 31 d2                     xor edx, edx
c0104548: 89 53 08                  mov dword ptr [ebx + 8], edx
c010454b: 83 c4 08                  add esp, 8
c010454e: 5b                        pop ebx
c010454f: c3                        ret

c0104550 <SetVirtPermissionsEx>:
c0104550: 55                        push ebp
c0104551: 57                        push edi
c0104552: 56                        push esi
c0104553: 53                        push ebx
c0104554: 83 ec 0c                  sub esp, 12
c0104557: 8b 7c 24 20               mov edi, dword ptr [esp + 32]
c010455b: 8b 74 24 28               mov esi, dword ptr [esp + 40]
c010455f: 8b 54 24 2c               mov edx, dword ptr [esp + 44]
c0104563: 09 f2                     or edx, esi
c0104565: b8 07 00 00 00            mov eax, 7
c010456a: 83 fa 0f                  cmp edx, 15
c010456d: 0f 87 fe 00 00 00         ja 0xc0104671 <SetVirtPermissionsEx+0x121>
c0104573: 8b 54 24 24               mov edx, dword ptr [esp + 36]
c0104577: 8b 07                     mov eax, dword ptr [edi]
c0104579: e8 97 fc ff ff            call 0xc0104215 <GetVirtEntry.isra.0>
c010457e: 89 c3                     mov ebx, eax
c0104580: b8 02 00 00 00            mov eax, 2
c0104585: 85 db                     test ebx, ebx
c0104587: 0f 84 e4 00 00 00         je 0xc0104671 <SetVirtPermissionsEx+0x121>
c010458d: 89 f5                     mov ebp, esi
c010458f: 83 e5 02                  and ebp, 2
c0104592: f6 43 04 04               test byte ptr [ebx + 4], 4
c0104596: 74 1c                     je 0xc01045b4 <SetVirtPermissionsEx+0x64>
c0104598: 8b 43 14                  mov eax, dword ptr [ebx + 20]
c010459b: 80 78 01 00               cmp byte ptr [eax + 1], 0
c010459f: 75 13                     jne 0xc01045b4 <SetVirtPermissionsEx+0x64>
c01045a1: 85 ed                     test ebp, ebp
c01045a3: 74 0f                     je 0xc01045b4 <SetVirtPermissionsEx+0x64>
c01045a5: b8 0b 00 00 00            mov eax, 11
c01045aa: f6 43 05 10               test byte ptr [ebx + 5], 16
c01045ae: 0f 84 bd 00 00 00         je 0xc0104671 <SetVirtPermissionsEx+0x121>
c01045b4: 89 d9                     mov ecx, ebx
c01045b6: 8b 54 24 24               mov edx, dword ptr [esp + 36]
c01045ba: 89 f8                     mov eax, edi
c01045bc: e8 38 fb ff ff            call 0xc01040f9 <SplitLargePageEntryIntoMulti
c01045c1: b0 01                     mov al, 1
c01045c3: f7 c6 01 00 00 00         test esi, 1
c01045c9: 75 12                     jne 0xc01045dd <SetVirtPermissionsEx+0x8d>
c01045cb: 31 c0                     xor eax, eax
c01045cd: f6 44 24 2c 01            test byte ptr [esp + 44], 1
c01045d2: 75 09                     jne 0xc01045dd <SetVirtPermissionsEx+0x8d>
c01045d4: 8a 43 04                  mov al, byte ptr [ebx + 4]
c01045d7: c0 e8 06                  shr al, 6
c01045da: 83 e0 01                  and eax, 1
c01045dd: 83 e0 01                  and eax, 1
c01045e0: c1 e0 06                  shl eax, 6
c01045e3: 8a 53 04                  mov dl, byte ptr [ebx + 4]
c01045e6: 83 e2 bf                  and edx, -65
c01045e9: 09 d0                     or eax, edx
c01045eb: 88 43 04                  mov byte ptr [ebx + 4], al
c01045ee: b2 01                     mov dl, 1
c01045f0: 85 ed                     test ebp, ebp
c01045f2: 75 0e                     jne 0xc0104602 <SetVirtPermissionsEx+0xb2>
c01045f4: 31 d2                     xor edx, edx
```

```
c0104648: 83 e0 01                      and eax, 1
c010464b: 83 e0 01                      and eax, 1
c010464e: d1 e0                         shl eax
c0104650: 8a 53 05                      mov dl, byte ptr [ebx + 5]
c0104653: 83 e2 fd                      and edx, -3
c0104656: 09 d0                         or eax, edx
c0104658: 88 43 05                      mov byte ptr [ebx + 5], al
c010465b: 50                            push eax
c010465c: 50                            push eax
c010465d: 53                            push ebx
c010465e: 57                            push edi
c010465f: e8 75 90 00 00                call 0xc010d6d9 <ArchUpdateMapping>
c0104664: 89 3c 24                      mov dword ptr [esp], edi
c0104667: e8 fc 90 00 00                call 0xc010d768 <ArchFlushTlb>
c010466c: 83 c4 10                      add esp, 16
c010466f: 31 c0                         xor eax, eax
c0104671: 83 c4 0c                      add esp, 12
c0104674: 5b                            pop ebx
c0104675: 5e                            pop esi
c0104676: 5f                            pop edi
c0104677: 5d                            pop ebp
c0104678: c3                            ret

c0104679 <GetVas>:
c0104679: 0f 21 d8                      mov eax, dr3
c010467c: c1 e0 06                      shl eax, 6
c010467f: 8b 80 c0 40 11 c0             mov eax, dword ptr [eax - 1072611136]
c0104685: c3                            ret

c0104686 <CopyVasRecursive>:
c0104686: 55                            push ebp
c0104687: 57                            push edi
c0104688: 56                            push esi
c0104689: 53                            push ebx
c010468a: 81 ec 1c 10 00 00             sub esp, 4124
c0104690: 89 c5                         mov ebp, eax
c0104692: 89 54 24 08                   mov dword ptr [esp + 8], edx
c0104696: 51                            push ecx
c0104697: 51                            push ecx
c0104698: 55                            push ebp
c0104699: 68 d9 07 11 c0                push 3222341593
c010469e: e8 22 44 00 00                call 0xc0108ac5 <LogWriteSerial>
c01046a3: 83 c4 10                      add esp, 16
c01046a6: 85 ed                         test ebp, ebp
c01046a8: 0f 84 7d 01 00 00             je 0xc010482b <CopyVasRecursive+0x1a5>
c01046ae: 8b 5d 08                      mov ebx, dword ptr [ebp + 8]
c01046b1: 50                            push eax
c01046b2: 50                            push eax
c01046b3: 53                            push ebx
c01046b4: 68 f8 07 11 c0                push 3222341624
c01046b9: e8 07 44 00 00                call 0xc0108ac5 <LogWriteSerial>
c01046be: 58                            pop eax
c01046bf: 5a                            pop edx
c01046c0: ff 33                         push dword ptr [ebx]
c01046c2: 68 1e 08 11 c0                push 3222341662
c01046c7: e8 f9 43 00 00                call 0xc0108ac5 <LogWriteSerial>
c01046cc: 83 c4 10                      add esp, 16
c01046cf: 83 7b 08 00                   cmp dword ptr [ebx + 8], 0
c01046d3: 0f 84 b1 00 00 00             je 0xc010478a <CopyVasRecursive+0x104>
c01046d9: 83 ec 0c                      sub esp, 12
c01046dc: 68 4d 08 11 c0                push 3222341709
c01046e1: e8 df 43 00 00                call 0xc0108ac5 <LogWriteSerial>
c01046e6: 83 c4 10                      add esp, 16
c01046e9: f6 43 04 02                   test byte ptr [ebx + 4], 2
c01046ed: 0f 84 89 00 00 00             je 0xc010477c <CopyVasRecursive+0xf6>
c01046f3: 8b 33                         mov esi, dword ptr [ebx]
c01046f5: 8d 7c 24 10                   lea edi, [esp + 16]
c01046f9: b9 00 04 00 00                mov ecx, 1024
c01046fe: f3 a5                         rep  movsd dword ptr es:[edi], dword ptr [esi
c0104700: 8b 53 18                      mov edx, dword ptr [ebx + 24]
c0104703: 89 54 24 0c                   mov dword ptr [esp + 12], edx
```

```
c0104767: ff 30                   push dword ptr [eax]
c0104769: e8 1c d9 ff ff          call 0xc010208a <TreeInsert>
c010476e: 5f                      pop edi
c010476f: 58                      pop eax
c0104770: 53                      push ebx
c0104771: ff 74 24 14             push dword ptr [esp + 20]
c0104775: e8 e9 8f 00 00          call 0xc010d763 <ArchAddMapping>
c010477a: eb 77                   jmp 0xc01047f3 <CopyVasRecursive+0x16d>
c010477c: 57                      push edi
c010477d: 57                      push edi
c010477e: 68 72 08 11 c0          push 3222341746
c0104783: 6a 00                   push 0
c0104785: e8 c4 43 00 00          call 0xc0108b4e <PanicEx>
c010478a: 83 ec 0c                sub esp, 12
c010478d: 68 99 08 11 c0          push 3222341785
c0104792: e8 2e 43 00 00          call 0xc0108ac5 <LogWriteSerial>
c0104797: 83 c4 10                add esp, 16
c010479a: f6 43 06 20             test byte ptr [ebx + 6], 32
c010479e: 75 04                   jne 0xc01047a4 <CopyVasRecursive+0x11e>
c01047a0: 80 4b 04 08             or byte ptr [ebx + 4], 8
c01047a4: ff 43 20                inc dword ptr [ebx + 32]
c01047a7: 56                      push esi
c01047a8: 56                      push esi
c01047a9: 53                      push ebx
c01047aa: 8b 44 24 14             mov eax, dword ptr [esp + 20]
c01047ae: ff 30                   push dword ptr [eax]
c01047b0: e8 d5 d8 ff ff          call 0xc010208a <TreeInsert>
c01047b5: c7 04 24 be 08 11 c0    mov dword ptr [esp], 3222341822
c01047bc: e8 04 43 00 00          call 0xc0108ac5 <LogWriteSerial>
c01047c1: e8 b3 fe ff ff          call 0xc0104679 <GetVas>
c01047c6: 5f                      pop edi
c01047c7: 5a                      pop edx
c01047c8: 53                      push ebx
c01047c9: 50                      push eax
c01047ca: e8 0a 8f 00 00          call 0xc010d6d9 <ArchUpdateMapping>
c01047cf: c7 04 24 e9 08 11 c0    mov dword ptr [esp], 3222341865
c01047d6: e8 ea 42 00 00          call 0xc0108ac5 <LogWriteSerial>
c01047db: 59                      pop ecx
c01047dc: 5e                      pop esi
c01047dd: 53                      push ebx
c01047de: ff 74 24 14             push dword ptr [esp + 20]
c01047e2: e8 7c 8f 00 00          call 0xc010d763 <ArchAddMapping>
c01047e7: c7 04 24 0e 09 11 c0    mov dword ptr [esp], 3222341902
c01047ee: e8 d2 42 00 00          call 0xc0108ac5 <LogWriteSerial>
c01047f3: 83 c4 10                add esp, 16
c01047f6: 50                      push eax
c01047f7: 50                      push eax
c01047f8: ff 75 00                push dword ptr [ebp]
c01047fb: 68 34 09 11 c0          push 3222341940
c0104800: e8 c0 42 00 00          call 0xc0108ac5 <LogWriteSerial>
c0104805: 5a                      pop edx
c0104806: 59                      pop ecx
c0104807: ff 75 04                push dword ptr [ebp + 4]
c010480a: 68 59 09 11 c0          push 3222341977
c010480f: e8 b1 42 00 00          call 0xc0108ac5 <LogWriteSerial>
c0104814: 8b 54 24 18             mov edx, dword ptr [esp + 24]
c0104818: 8b 45 00                mov eax, dword ptr [ebp]
c010481b: e8 66 fe ff ff          call 0xc0104686 <CopyVasRecursive>
c0104820: 8b 6d 04                mov ebp, dword ptr [ebp + 4]
c0104823: 83 c4 10                add esp, 16
c0104826: e9 6b fe ff ff          jmp 0xc0104696 <CopyVasRecursive+0x10>
c010482b: 81 c4 1c 10 00 00       add esp, 4124
c0104831: 5b                      pop ebx
c0104832: 5e                      pop esi
c0104833: 5f                      pop edi
c0104834: 5d                      pop ebp
c0104835: c3                      ret

c0104836 <CopyVas>:
c0104836: 57                      push edi
c0104837: 56                      push esi
```

```
c01048b0: 5b                            pop ebx
c01048b1: 5e                            pop esi
c01048b2: 5f                            pop edi
c01048b3: c3                            ret

c01048b4 <GetVirtPermissions>:
c01048b4: 57                            push edi
c01048b5: 56                            push esi
c01048b6: 53                            push ebx
c01048b7: 83 ec 30                      sub esp, 48
c01048ba: e8 ba fd ff ff                call 0xc0104679 <GetVas>
c01048bf: 8d 58 08                      lea ebx, [eax + 8]
c01048c2: 83 ec 0c                      sub esp, 12
c01048c5: 53                            push ebx
c01048c6: e8 8f 20 00 00                call 0xc010695a <AcquireSpinlock>
c01048cb: e8 a9 fd ff ff                call 0xc0104679 <GetVas>
c01048d0: 8b 54 24 50                   mov edx, dword ptr [esp + 80]
c01048d4: 8b 00                         mov eax, dword ptr [eax]
c01048d6: e8 3a f9 ff ff                call 0xc0104215 <GetVirtEntry.isra.0>
c01048db: 83 c4 10                      add esp, 16
c01048de: 85 c0                         test eax, eax
c01048e0: 75 10                         jne 0xc01048f2 <GetVirtPermissions+0x3e>
c01048e2: 83 ec 0c                      sub esp, 12
c01048e5: 53                            push ebx
c01048e6: e8 bf 20 00 00                call 0xc01069aa <ReleaseSpinlock>
c01048eb: 83 c4 10                      add esp, 16
c01048ee: 31 c0                         xor eax, eax
c01048f0: eb 64                         jmp 0xc0104956 <GetVirtPermissions+0xa2>
c01048f2: 8d 7c 24 0c                   lea edi, [esp + 12]
c01048f6: b9 09 00 00 00                mov ecx, 9
c01048fb: 89 c6                         mov esi, eax
c01048fd: f3 a5                         rep  movsd dword ptr es:[edi], dword ptr [esi
c01048ff: 8b 70 08                      mov esi, dword ptr [eax + 8]
c0104902: 83 ec 0c                      sub esp, 12
c0104905: 53                            push ebx
c0104906: e8 9f 20 00 00                call 0xc01069aa <ReleaseSpinlock>
c010490b: 8a 4c 24 20                   mov cl, byte ptr [esp + 32]
c010490f: 88 ca                         mov dl, cl
c0104911: c0 ea 06                      shr dl, 6
c0104914: 83 e2 01                      and edx, 1
c0104917: 83 c4 10                      add esp, 16
c010491a: 84 c9                         test cl, cl
c010491c: 79 03                         jns 0xc0104921 <GetVirtPermissions+0x6d>
c010491e: 83 ca 02                      or edx, 2
c0104921: 8a 5c 24 11                   mov bl, byte ptr [esp + 17]
c0104925: 89 d8                         mov eax, ebx
c0104927: 83 e0 01                      and eax, 1
c010492a: c1 e0 03                      shl eax, 3
c010492d: 09 d0                         or eax, edx
c010492f: 85 f6                         test esi, esi
c0104931: 74 03                         je 0xc0104936 <GetVirtPermissions+0x82>
c0104933: 83 c8 10                      or eax, 16
c0104936: 80 e1 04                      and cl, 4
c0104939: 74 03                         je 0xc010493e <GetVirtPermissions+0x8a>
c010493b: 83 c8 20                      or eax, 32
c010493e: f6 c3 02                      test bl, 2
c0104941: 74 03                         je 0xc0104946 <GetVirtPermissions+0x92>
c0104943: 83 c8 04                      or eax, 4
c0104946: f6 c3 04                      test bl, 4
c0104949: 75 03                         jne 0xc010494e <GetVirtPermissions+0x9a>
c010494b: 80 cc 01                      or ah, 1
c010494e: 80 e3 10                      and bl, 16
c0104951: 74 03                         je 0xc0104956 <GetVirtPermissions+0xa2>
c0104953: 80 cc 04                      or ah, 4
c0104956: 83 c4 30                      add esp, 48
c0104959: 5b                            pop ebx
c010495a: 5e                            pop esi
c010495b: 5f                            pop edi
c010495c: c3                            ret

c010495d <SetVirtPermissions>:
```

```
c01049a5: e8 cf fc ff ff                call 0xc0104679 <GetVas>
c01049aa: 89 c3                         mov ebx, eax
c01049ac: 8d 70 08                      lea esi, [eax + 8]
c01049af: 83 ec 0c                      sub esp, 12
c01049b2: 56                            push esi
c01049b3: e8 a2 1f 00 00                call 0xc010695a <AcquireSpinlock>
c01049b8: 58                            pop eax
c01049b9: 5a                            pop edx
c01049ba: 57                            push edi
c01049bb: 53                            push ebx
c01049bc: e8 61 fb ff ff                call 0xc0104522 <UnlockVirtEx>
c01049c1: 83 c4 10                      add esp, 16
c01049c4: 89 74 24 10                   mov dword ptr [esp + 16], esi
c01049c8: 5b                            pop ebx
c01049c9: 5e                            pop esi
c01049ca: 5f                            pop edi
c01049cb: e9 da 1f 00 00                jmp 0xc01069aa <ReleaseSpinlock>

c01049d0 <BringIntoMemoryFromCow>:
c01049d0: 55                            push ebp
c01049d1: 57                            push edi
c01049d2: 56                            push esi
c01049d3: 53                            push ebx
c01049d4: 81 ec 0c 10 00 00             sub esp, 4108
c01049da: 89 c3                         mov ebx, eax
c01049dc: 8b 40 20                      mov eax, dword ptr [eax + 32]
c01049df: 83 f8 01                      cmp eax, 1
c01049e2: 75 21                         jne 0xc0104a05 <BringIntoMemoryFromCow+0x35>
c01049e4: 80 63 04 f7                   and byte ptr [ebx + 4], -9
c01049e8: e8 8c fc ff ff                call 0xc0104679 <GetVas>
c01049ed: 56                            push esi
c01049ee: 56                            push esi
c01049ef: 53                            push ebx
c01049f0: 50                            push eax
c01049f1: e8 e3 8c 00 00                call 0xc010d6d9 <ArchUpdateMapping>
c01049f6: e8 7e fc ff ff                call 0xc0104679 <GetVas>
c01049fb: 89 04 24                      mov dword ptr [esp], eax
c01049fe: e8 65 8d 00 00                call 0xc010d768 <ArchFlushTlb>
c0104a03: eb 7e                         jmp 0xc0104a83 <BringIntoMemoryFromCow+0xb3>
c0104a05: 8b 33                         mov esi, dword ptr [ebx]
c0104a07: 89 e7                         mov edi, esp
c0104a09: b9 00 04 00 00                mov ecx, 1024
c0104a0e: f3 a5                         rep  movsd dword ptr es:[edi], dword ptr [esi
c0104a10: 48                            dec eax
c0104a11: 89 43 20                      mov dword ptr [ebx + 32], eax
c0104a14: 48                            dec eax
c0104a15: 75 04                         jne 0xc0104a1b <BringIntoMemoryFromCow+0x4b>
c0104a17: 80 63 04 f7                   and byte ptr [ebx + 4], -9
c0104a1b: 83 ec 0c                      sub esp, 12
c0104a1e: 6a 24                         push 36
c0104a20: e8 2a ef ff ff                call 0xc010394f <AllocHeap>
c0104a25: 89 c5                         mov ebp, eax
c0104a27: b9 09 00 00 00                mov ecx, 9
c0104a2c: 89 c7                         mov edi, eax
c0104a2e: 89 de                         mov esi, ebx
c0104a30: f3 a5                         rep  movsd dword ptr es:[edi], dword ptr [esi
c0104a32: c7 40 20 01 00 00 00          mov dword ptr [eax + 32], 1
c0104a39: e8 2b f1 ff ff                call 0xc0103b69 <AllocPhys>
c0104a3e: 89 45 18                      mov dword ptr [ebp + 24], eax
c0104a41: 80 4d 04 02                   or byte ptr [ebp + 4], 2
c0104a45: e8 2f fc ff ff                call 0xc0104679 <GetVas>
c0104a4a: 89 da                         mov edx, ebx
c0104a4c: e8 4d f6 ff ff                call 0xc010409e <DeleteFromAvl>
c0104a51: 89 1c 24                      mov dword ptr [esp], ebx
c0104a54: e8 1a ef ff ff                call 0xc0103973 <FreeHeap>
c0104a59: e8 1b fc ff ff                call 0xc0104679 <GetVas>
c0104a5e: 5a                            pop edx
c0104a5f: 59                            pop ecx
c0104a60: 53                            push ebx
c0104a61: 50                            push eax
c0104a62: e8 72 8c 00 00                call 0xc010d6d9 <ArchUpdateMapping>
```

```
c0104aaa: 68 fb 09 11 c0              push 3222342139
c0104aaf: e8 11 40 00 00              call 0xc0108ac5 <LogWriteSerial>
c0104ab4: 89 d8                       mov eax, ebx
c0104ab6: e8 15 ff ff ff              call 0xc01049d0 <BringIntoMemoryFromCow>
c0104abb: eb 7b                       jmp 0xc0104b38 <BringIntoMemory+0xa7>
c0104abd: 88 c2                       mov dl, al
c0104abf: 83 e2 05                    and edx, 5
c0104ac2: 80 fa 04                    cmp dl, 4
c0104ac5: 75 7b                       jne 0xc0104b42 <BringIntoMemory+0xb1>
c0104ac7: 83 ec 0c                    sub esp, 12
c0104aca: 68 04 0a 11 c0              push 3222342148
c0104acf: e8 f1 3f 00 00              call 0xc0108ac5 <LogWriteSerial>
c0104ad4: e8 a0 fb ff ff              call 0xc0104679 <GetVas>
c0104ad9: 89 d9                       mov ecx, ebx
c0104adb: 8b 54 24 20                 mov edx, dword ptr [esp + 32]
c0104adf: e8 15 f6 ff ff              call 0xc01040f9 <SplitLargePageEntryIntoMulti
c0104ae4: 80 4b 05 40                 or byte ptr [ebx + 5], 64
c0104ae8: e8 8c fb ff ff              call 0xc0104679 <GetVas>
c0104aed: 59                          pop ecx
c0104aee: 5e                          pop esi
c0104aef: 53                          push ebx
c0104af0: 50                          push eax
c0104af1: e8 e3 8b 00 00              call 0xc010d6d9 <ArchUpdateMapping>
c0104af6: e8 7e fb ff ff              call 0xc0104679 <GetVas>
c0104afb: 89 04 24                    mov dword ptr [esp], eax
c0104afe: e8 65 8c 00 00              call 0xc010d768 <ArchFlushTlb>
c0104b03: 8b 73 10                    mov esi, dword ptr [ebx + 16]
c0104b06: 8b 7b 14                    mov edi, dword ptr [ebx + 20]
c0104b09: 8b 1b                       mov ebx, dword ptr [ebx]
c0104b0b: c7 04 24 18 00 00 00        mov dword ptr [esp], 24
c0104b12: e8 38 ee ff ff              call 0xc010394f <AllocHeap>
c0104b17: 89 58 0c                    mov dword ptr [eax + 12], ebx
c0104b1a: 89 38                       mov dword ptr [eax], edi
c0104b1c: 31 ff                       xor edi, edi
c0104b1e: 89 78 10                    mov dword ptr [eax + 16], edi
c0104b21: 89 70 08                    mov dword ptr [eax + 8], esi
c0104b24: c6 40 14 00                 mov byte ptr [eax + 20], 0
c0104b28: 83 c4 0c                    add esp, 12
c0104b2b: 50                          push eax
c0104b2c: 68 76 57 10 c0              push 3222296438
c0104b31: 6a 01                       push 1
c0104b33: e8 c1 e7 ff ff              call 0xc01032f9 <DeferUntilIrql>
c0104b38: 83 c4 10                    add esp, 16
c0104b3b: 31 c0                       xor eax, eax
c0104b3d: e9 49 01 00 00              jmp 0xc0104c8b <BringIntoMemory+0x1fa>
c0104b42: a8 10                       test al, 16
c0104b44: 74 57                       je 0xc0104b9d <BringIntoMemory+0x10c>
c0104b46: 83 ec 0c                    sub esp, 12
c0104b49: 68 0e 0a 11 c0              push 3222342158
c0104b4e: e8 72 3f 00 00              call 0xc0108ac5 <LogWriteSerial>
c0104b53: 8b 7b 1c                    mov edi, dword ptr [ebx + 28]
c0104b56: 80 4b 05 40                 or byte ptr [ebx + 5], 64
c0104b5a: e8 1a fb ff ff              call 0xc0104679 <GetVas>
c0104b5f: 59                          pop ecx
c0104b60: 5e                          pop esi
c0104b61: 53                          push ebx
c0104b62: 50                          push eax
c0104b63: e8 71 8b 00 00              call 0xc010d6d9 <ArchUpdateMapping>
c0104b68: e8 0c fb ff ff              call 0xc0104679 <GetVas>
c0104b6d: 89 04 24                    mov dword ptr [esp], eax
c0104b70: e8 f3 8b 00 00              call 0xc010d768 <ArchFlushTlb>
c0104b75: e8 a8 f3 ff ff              call 0xc0103f22 <GetSwapfile>
c0104b7a: 89 c6                       mov esi, eax
c0104b7c: 8b 1b                       mov ebx, dword ptr [ebx]
c0104b7e: c7 04 24 18 00 00 00        mov dword ptr [esp], 24
c0104b85: e8 c5 ed ff ff              call 0xc010394f <AllocHeap>
c0104b8a: 89 58 0c                    mov dword ptr [eax + 12], ebx
c0104b8d: 89 30                       mov dword ptr [eax], esi
c0104b8f: 31 d2                       xor edx, edx
c0104b91: 89 50 10                    mov dword ptr [eax + 16], edx
c0104b94: 89 78 08                    mov dword ptr [eax + 8], edi
```

```
c0104c00: 89 43 18                mov dword ptr [ebx + 24], eax
c0104c03: 66 81 4b 04 03 08       or word ptr [ebx + 4], 2051
c0104c09: 57                      push edi
c0104c0a: 57                      push edi
c0104c0b: 53                      push ebx
c0104c0c: 56                      push esi
c0104c0d: e8 c7 8a 00 00          call 0xc010d6d9 <ArchUpdateMapping>
c0104c12: 89 34 24                mov dword ptr [esp], esi
c0104c15: e8 4e 8b 00 00          call 0xc010d768 <ArchFlushTlb>
c0104c1a: b9 00 04 00 00          mov ecx, 1024
c0104c1f: 31 c0                   xor eax, eax
c0104c21: 8b 3b                   mov edi, dword ptr [ebx]
c0104c23: f3 ab                   rep  stosd dword ptr es:[edi], eax
c0104c25: 80 63 05 f7             and byte ptr [ebx + 5], -9
c0104c29: 58                      pop eax
c0104c2a: 5a                      pop edx
c0104c2b: 53                      push ebx
c0104c2c: 56                      push esi
c0104c2d: e8 a7 8a 00 00          call 0xc010d6d9 <ArchUpdateMapping>
c0104c32: 89 34 24                mov dword ptr [esp], esi
c0104c35: e8 2e 8b 00 00          call 0xc010d768 <ArchFlushTlb>
c0104c3a: e9 f9 fe ff ff          jmp 0xc0104b38 <BringIntoMemory+0xa7>
c0104c3f: 52                      push edx
c0104c40: 52                      push edx
c0104c41: 8a 53 05                mov dl, byte ptr [ebx + 5]
c0104c44: c0 ea 06                shr dl, 6
c0104c47: 83 e2 01                and edx, 1
c0104c4a: 52                      push edx
c0104c4b: 88 c2                   mov dl, al
c0104c4d: d0 ea                   shr dl
c0104c4f: 83 e2 01                and edx, 1
c0104c52: 52                      push edx
c0104c53: 0f b6 d1                movzx edx, cl
c0104c56: 52                      push edx
c0104c57: c0 e8 02                shr al, 2
c0104c5a: 83 e0 01                and eax, 1
c0104c5d: 50                      push eax
c0104c5e: ff 33                   push dword ptr [ebx]
c0104c60: 68 21 0a 11 c0          push 3222342177
c0104c65: e8 5b 3e 00 00          call 0xc0108ac5 <LogWriteSerial>
c0104c6a: 83 c4 18                add esp, 24
c0104c6d: ff 33                   push dword ptr [ebx]
c0104c6f: 56                      push esi
c0104c70: e8 48 89 00 00          call 0xc010d5bd <x86GetPageEntry>
c0104c75: 59                      pop ecx
c0104c76: 5b                      pop ebx
c0104c77: ff 30                   push dword ptr [eax]
c0104c79: 68 6a 0a 11 c0          push 3222342250
c0104c7e: e8 42 3e 00 00          call 0xc0108ac5 <LogWriteSerial>
c0104c83: 83 c4 10                add esp, 16
c0104c86: b8 07 00 00 00          mov eax, 7
c0104c8b: 5b                      pop ebx
c0104c8c: 5e                      pop esi
c0104c8d: 5f                      pop edi
c0104c8e: c3                      ret

c0104c8f <LockVirtEx>:
c0104c8f: 53                      push ebx
c0104c90: 83 ec 08                sub esp, 8
c0104c93: 8b 54 24 14             mov edx, dword ptr [esp + 20]
c0104c97: 8b 44 24 10             mov eax, dword ptr [esp + 16]
c0104c9b: 8b 00                   mov eax, dword ptr [eax]
c0104c9d: e8 73 f5 ff ff          call 0xc0104215 <GetVirtEntry.isra.0>
c0104ca2: 89 c3                   mov ebx, eax
c0104ca4: f6 40 04 01             test byte ptr [eax + 4], 1
c0104ca8: 75 38                   jne 0xc0104ce2 <LockVirtEx+0x53>
c0104caa: 89 c1                   mov ecx, eax
c0104cac: 8b 54 24 14             mov edx, dword ptr [esp + 20]
c0104cb0: 8b 44 24 10             mov eax, dword ptr [esp + 16]
c0104cb4: e8 40 f4 ff ff          call 0xc01040f9 <SplitLargePageEntryIntoMulti
c0104cb9: 50                      push eax
```

```
c0104d06: e8 4f 1c 00 00                call 0xc010695a <AcquireSpinlock>
c0104d0b: 5a                            pop edx
c0104d0c: 59                            pop ecx
c0104d0d: ff 74 24 18                   push dword ptr [esp + 24]
c0104d11: 53                            push ebx
c0104d12: e8 78 ff ff ff                call 0xc0104c8f <LockVirtEx>
c0104d17: 88 c3                         mov bl, al
c0104d19: 89 34 24                      mov dword ptr [esp], esi
c0104d1c: e8 89 1c 00 00                call 0xc01069aa <ReleaseSpinlock>
c0104d21: 88 d8                         mov al, bl
c0104d23: 83 c4 14                      add esp, 20
c0104d26: 5b                            pop ebx
c0104d27: 5e                            pop esi
c0104d28: c3                            ret

c0104d29 <GetPhysFromVirt>:
c0104d29: 56                            push esi
c0104d2a: 53                            push ebx
c0104d2b: 50                            push eax
c0104d2c: e8 48 f9 ff ff                call 0xc0104679 <GetVas>
c0104d31: 89 c6                         mov esi, eax
c0104d33: 8d 58 08                      lea ebx, [eax + 8]
c0104d36: 83 ec 0c                      sub esp, 12
c0104d39: 53                            push ebx
c0104d3a: e8 1b 1c 00 00                call 0xc010695a <AcquireSpinlock>
c0104d3f: 8b 54 24 20                   mov edx, dword ptr [esp + 32]
c0104d43: 8b 06                         mov eax, dword ptr [esi]
c0104d45: e8 cb f4 ff ff                call 0xc0104215 <GetVirtEntry.isra.0>
c0104d4a: 8b 70 18                      mov esi, dword ptr [eax + 24]
c0104d4d: 8b 54 24 20                   mov edx, dword ptr [esp + 32]
c0104d51: c1 ea 0c                      shr edx, 12
c0104d54: 8b 00                         mov eax, dword ptr [eax]
c0104d56: c1 e8 0c                      shr eax, 12
c0104d59: 83 c4 10                      add esp, 16
c0104d5c: 39 d0                         cmp eax, edx
c0104d5e: 73 07                         jae 0xc0104d67 <GetPhysFromVirt+0x3e>
c0104d60: 29 c2                         sub edx, eax
c0104d62: c1 e2 0c                      shl edx, 12
c0104d65: 01 d6                         add esi, edx
c0104d67: 83 ec 0c                      sub esp, 12
c0104d6a: 53                            push ebx
c0104d6b: e8 3a 1c 00 00                call 0xc01069aa <ReleaseSpinlock>
c0104d70: 89 f0                         mov eax, esi
c0104d72: 83 c4 14                      add esp, 20
c0104d75: 5b                            pop ebx
c0104d76: 5e                            pop esi
c0104d77: c3                            ret

c0104d78 <MapVirtEx>:
c0104d78: 55                            push ebp
c0104d79: 57                            push edi
c0104d7a: 56                            push esi
c0104d7b: 53                            push ebx
c0104d7c: 81 ec 8c 00 00 00             sub esp, 140
c0104d82: 8b 9c 24 b0 00 00 00          mov ebx, dword ptr [esp + 176]
c0104d89: 8b 84 24 bc 00 00 00          mov eax, dword ptr [esp + 188]
c0104d90: 31 f6                         xor esi, esi
c0104d92: 89 30                         mov dword ptr [eax], esi
c0104d94: 83 bc 24 a4 00 00 00 00       cmp dword ptr [esp + 164], 0
c0104d9c: 74 0c                         je 0xc0104daa <MapVirtEx+0x32>
c0104d9e: f7 c3 80 04 00 00             test ebx, 1152
c0104da4: 0f 84 bc 00 00 00             je 0xc0104e66 <MapVirtEx+0xee>
c0104daa: 89 d8                         mov eax, ebx
c0104dac: 25 90 00 00 00                and eax, 144
c0104db1: 89 44 24 0c                   mov dword ptr [esp + 12], eax
c0104db5: 83 c0 80                      add eax, -128
c0104db8: 0f 84 a8 00 00 00             je 0xc0104e66 <MapVirtEx+0xee>
c0104dbe: 89 d8                         mov eax, ebx
c0104dc0: f7 d0                         not eax
c0104dc2: a8 a0                         test al, -96
c0104dc4: 0f 84 9c 00 00 00             je 0xc0104e66 <MapVirtEx+0xee>
```

```
c0104e34: 84 c2                         test dl, al
c0104e36: 75 2e                         jne 0xc0104e66 <MapVirtEx+0xee>
c0104e38: 89 d8                         mov eax, ebx
c0104e3a: f7 d0                         not eax
c0104e3c: a9 10 10 00 00                test eax, 4112
c0104e41: 74 23                         je 0xc0104e66 <MapVirtEx+0xee>
c0104e43: 83 7c 24 18 00                cmp dword ptr [esp + 24], 0
c0104e48: 74 4f                         je 0xc0104e99 <MapVirtEx+0x121>
c0104e4a: 8b 84 24 b4 00 00 00          mov eax, dword ptr [esp + 180]
c0104e51: 8b 40 30                      mov eax, dword ptr [eax + 48]
c0104e54: 8b 40 58                      mov eax, dword ptr [eax + 88]
c0104e57: c1 e8 0f                      shr eax, 15
c0104e5a: 83 f8 01                      cmp eax, 1
c0104e5d: 74 0e                         je 0xc0104e6d <MapVirtEx+0xf5>
c0104e5f: 83 f8 04                      cmp eax, 4
c0104e62: 74 09                         je 0xc0104e6d <MapVirtEx+0xf5>
c0104e64: eb 13                         jmp 0xc0104e79 <MapVirtEx+0x101>
c0104e66: b8 07 00 00 00                mov eax, 7
c0104e6b: eb 11                         jmp 0xc0104e7e <MapVirtEx+0x106>
c0104e6d: 8b 84 24 b4 00 00 00          mov eax, dword ptr [esp + 180]
c0104e74: 80 38 00                      cmp byte ptr [eax], 0
c0104e77: 75 15                         jne 0xc0104e8e <MapVirtEx+0x116>
c0104e79: b8 0b 00 00 00                mov eax, 11
c0104e7e: 8b 9c 24 bc 00 00 00          mov ebx, dword ptr [esp + 188]
c0104e85: 89 03                         mov dword ptr [ebx], eax
c0104e87: 31 c0                         xor eax, eax
c0104e89: e9 af 04 00 00                jmp 0xc010533d <MapVirtEx+0x5c5>
c0104e8e: 80 78 01 00                   cmp byte ptr [eax + 1], 0
c0104e92: 75 05                         jne 0xc0104e99 <MapVirtEx+0x121>
c0104e94: f6 c3 02                      test bl, 2
c0104e97: 75 e0                         jne 0xc0104e79 <MapVirtEx+0x101>
c0104e99: 83 bc 24 a8 00 00 00 00       cmp dword ptr [esp + 168], 0
c0104ea1: 0f 84 05 01 00 00             je 0xc0104fac <MapVirtEx+0x234>
c0104ea7: 8d 7c 24 60                   lea edi, [esp + 96]
c0104eab: b9 08 00 00 00                mov ecx, 8
c0104eb0: 31 c0                         xor eax, eax
c0104eb2: f3 ab                         rep  stosd dword ptr es:[edi], eax
c0104eb4: 8b 84 24 a8 00 00 00          mov eax, dword ptr [esp + 168]
c0104ebb: 89 44 24 5c                   mov dword ptr [esp + 92], eax
c0104ebf: c7 44 24 68 01 00 00 00       mov dword ptr [esp + 104], 1
c0104ec7: 8b 84 24 a0 00 00 00          mov eax, dword ptr [esp + 160]
c0104ece: 8d 78 08                      lea edi, [eax + 8]
c0104ed1: 83 ec 0c                      sub esp, 12
c0104ed4: 57                            push edi
c0104ed5: e8 80 1a 00 00                call 0xc010695a <AcquireSpinlock>
c0104eda: 83 c4 10                      add esp, 16
c0104edd: 31 ed                         xor ebp, ebp
c0104edf: 39 ac 24 ac 00 00 00          cmp dword ptr [esp + 172], ebp
c0104ee6: 74 29                         je 0xc0104f11 <MapVirtEx+0x199>
c0104ee8: 51                            push ecx
c0104ee9: 51                            push ecx
c0104eea: 8d 44 24 64                   lea eax, [esp + 100]
c0104eee: 50                            push eax
c0104eef: 8b 84 24 ac 00 00 00          mov eax, dword ptr [esp + 172]
c0104ef6: ff 30                         push dword ptr [eax]
c0104ef8: e8 f0 d1 ff ff                call 0xc01020ed <TreeContains>
c0104efd: 89 c6                         mov esi, eax
c0104eff: 83 c4 10                      add esp, 16
c0104f02: 84 c0                         test al, al
c0104f04: 75 0d                         jne 0xc0104f13 <MapVirtEx+0x19b>
c0104f06: 81 44 24 5c 00 10 00 00       add dword ptr [esp + 92], 4096
c0104f0e: 45                            inc ebp
c0104f0f: eb ce                         jmp 0xc0104edf <MapVirtEx+0x167>
c0104f11: 31 f6                         xor esi, esi
c0104f13: 83 ec 0c                      sub esp, 12
c0104f16: 57                            push edi
c0104f17: e8 8e 1a 00 00                call 0xc01069aa <ReleaseSpinlock>
c0104f1c: 83 c4 10                      add esp, 16
c0104f1f: 89 f0                         mov eax, esi
c0104f21: 84 c0                         test al, al
c0104f23: 75 79                         jne 0xc0104f9e <MapVirtEx+0x226>
```

```
c0104f81: 0f 21 d8                  mov eax, dr3
c0104f84: 83 ec 0c                  sub esp, 12
c0104f87: c1 e0 06                  shl eax, 6
c0104f8a: 05 e4 40 11 c0            add eax, 3222356196
c0104f8f: 50                        push eax
c0104f90: e8 15 1a 00 00            call 0xc01069aa <ReleaseSpinlock>
c0104f95: 83 c4 10                  add esp, 16
c0104f98: 89 f8                     mov eax, edi
c0104f9a: 84 c0                     test al, al
c0104f9c: 74 29                     je 0xc0104fc7 <MapVirtEx+0x24f>
c0104f9e: b8 08 00 00 00            mov eax, 8
c0104fa3: f6 c3 40                  test bl, 64
c0104fa6: 0f 85 d2 fe ff ff         jne 0xc0104e7e <MapVirtEx+0x106>
c0104fac: 89 da                     mov edx, ebx
c0104fae: 81 e2 00 01 00 00         and edx, 256
c0104fb4: 8b 84 24 ac 00 00 00      mov eax, dword ptr [esp + 172]
c0104fbb: e8 de f2 ff ff            call 0xc010429e <AllocVirtRange.isra.0>
c0104fc0: 89 84 24 a8 00 00 00      mov dword ptr [esp + 168], eax
c0104fc7: 83 bc 24 ac 00 00 00 02   cmp dword ptr [esp + 172], 2
c0104fcf: 0f 97 c2                  seta dl
c0104fd2: 83 7c 24 0c 10            cmp dword ptr [esp + 12], 16
c0104fd7: 0f 95 c0                  setne al
c0104fda: 84 c2                     test dl, al
c0104fdc: 74 15                     je 0xc0104ff3 <MapVirtEx+0x27b>
c0104fde: c7 44 24 30 01 00 00 00   mov dword ptr [esp + 48], 1
c0104fe6: 8b 84 24 ac 00 00 00      mov eax, dword ptr [esp + 172]
c0104fed: 89 44 24 14               mov dword ptr [esp + 20], eax
c0104ff1: eb 13                     jmp 0xc0105006 <MapVirtEx+0x28e>
c0104ff3: 8b 84 24 ac 00 00 00      mov eax, dword ptr [esp + 172]
c0104ffa: 89 44 24 30               mov dword ptr [esp + 48], eax
c0104ffe: c7 44 24 14 01 00 00 00   mov dword ptr [esp + 20], 1
c0105006: 89 d8                     mov eax, ebx
c0105008: d1 f8                     sar eax
c010500a: 89 d9                     mov ecx, ebx
c010500c: c1 f9 03                  sar ecx, 3
c010500f: 89 4c 24 20               mov dword ptr [esp + 32], ecx
c0105013: 89 d9                     mov ecx, ebx
c0105015: c1 f9 05                  sar ecx, 5
c0105018: 89 4c 24 24               mov dword ptr [esp + 36], ecx
c010501c: 89 df                     mov edi, ebx
c010501e: c1 ff 02                  sar edi, 2
c0105021: 89 7c 24 28               mov dword ptr [esp + 40], edi
c0105025: 89 d9                     mov ecx, ebx
c0105027: c1 f9 0c                  sar ecx, 12
c010502a: 89 4c 24 34               mov dword ptr [esp + 52], ecx
c010502e: 89 df                     mov edi, ebx
c0105030: c1 ff 0b                  sar edi, 11
c0105033: 89 7c 24 38               mov dword ptr [esp + 56], edi
c0105037: 89 d9                     mov ecx, ebx
c0105039: c1 f9 0a                  sar ecx, 10
c010503c: 89 4c 24 2c               mov dword ptr [esp + 44], ecx
c0105040: 8b 7c 24 24               mov edi, dword ptr [esp + 36]
c0105044: 83 e7 01                  and edi, 1
c0105047: 89 7c 24 3c               mov dword ptr [esp + 60], edi
c010504b: 8b 4c 24 28               mov ecx, dword ptr [esp + 40]
c010504f: 83 e1 01                  and ecx, 1
c0105052: 89 4c 24 40               mov dword ptr [esp + 64], ecx
c0105056: 8b 7c 24 20               mov edi, dword ptr [esp + 32]
c010505a: 83 e7 01                  and edi, 1
c010505d: 89 7c 24 44               mov dword ptr [esp + 68], edi
c0105061: 89 c1                     mov ecx, eax
c0105063: 83 e1 01                  and ecx, 1
c0105066: 89 4c 24 48               mov dword ptr [esp + 72], ecx
c010506a: 8b bc 24 a8 00 00 00      mov edi, dword ptr [esp + 168]
c0105071: 89 7c 24 0c               mov dword ptr [esp + 12], edi
c0105075: 31 ed                     xor ebp, ebp
c0105077: 89 6c 24 10               mov dword ptr [esp + 16], ebp
c010507b: c1 e0 07                  shl eax, 7
c010507e: 0f b6 c0                  movzx eax, al
c0105081: 89 44 24 4c               mov dword ptr [esp + 76], eax
c0105085: 8b 74 24 30               mov esi, dword ptr [esp + 48]
```

```
c01050fe: 83 e2 01                  and edx, 1
c0105101: 89 56 08                  mov dword ptr [esi + 8], edx
c0105104: 8a 56 04                  mov dl, byte ptr [esi + 4]
c0105107: 83 e2 fc                  and edx, -4
c010510a: 09 c2                     or edx, eax
c010510c: 88 56 04                  mov byte ptr [esi + 4], dl
c010510f: 83 c4 10                  add esp, 16
c0105112: 31 d2                     xor edx, edx
c0105114: 83 7c 24 1c 00            cmp dword ptr [esp + 28], 0
c0105119: 75 04                     jne 0xc010511f <MapVirtEx+0x3a7>
c010511b: 89 fa                     mov edx, edi
c010511d: 31 ff                     xor edi, edi
c010511f: 85 d2                     test edx, edx
c0105121: 75 0f                     jne 0xc0105132 <MapVirtEx+0x3ba>
c0105123: 84 c0                     test al, al
c0105125: 74 0b                     je 0xc0105132 <MapVirtEx+0x3ba>
c0105127: e8 3d ea ff ff            call 0xc0103b69 <AllocPhys>
c010512c: 89 c2                     mov edx, eax
c010512e: 80 4e 04 02               or byte ptr [esi + 4], 2
c0105132: 8b 44 24 0c               mov eax, dword ptr [esp + 12]
c0105136: 89 06                     mov dword ptr [esi], eax
c0105138: 89 d9                     mov ecx, ebx
c010513a: c1 e9 08                  shr ecx, 8
c010513d: 83 f1 01                  xor ecx, 1
c0105140: 89 56 18                  mov dword ptr [esi + 24], edx
c0105143: c7 46 20 01 00 00 00      mov dword ptr [esi + 32], 1
c010514a: 89 6e 10                  mov dword ptr [esi + 16], ebp
c010514d: 8b 84 24 b4 00 00 00      mov eax, dword ptr [esp + 180]
c0105154: 89 46 14                  mov dword ptr [esi + 20], eax
c0105157: 89 dd                     mov ebp, ebx
c0105159: c1 e5 06                  shl ebp, 6
c010515c: 83 e5 40                  and ebp, 64
c010515f: 8b 44 24 24               mov eax, dword ptr [esp + 36]
c0105163: c1 e0 02                  shl eax, 2
c0105166: 83 e0 04                  and eax, 4
c0105169: 09 c5                     or ebp, eax
c010516b: 8b 44 24 4c               mov eax, dword ptr [esp + 76]
c010516f: 09 c5                     or ebp, eax
c0105171: 8b 44 24 20               mov eax, dword ptr [esp + 32]
c0105175: c1 e0 08                  shl eax, 8
c0105178: 25 00 01 00 00            and eax, 256
c010517d: 09 c5                     or ebp, eax
c010517f: 8b 44 24 28               mov eax, dword ptr [esp + 40]
c0105183: c1 e0 09                  shl eax, 9
c0105186: 25 00 02 00 00            and eax, 512
c010518b: 09 e8                     or eax, ebp
c010518d: 83 e1 01                  and ecx, 1
c0105190: 89 cd                     mov ebp, ecx
c0105192: c1 e5 0a                  shl ebp, 10
c0105195: 09 e8                     or eax, ebp
c0105197: 8b 6c 24 2c               mov ebp, dword ptr [esp + 44]
c010519b: c1 e5 0c                  shl ebp, 12
c010519e: 81 e5 00 10 00 00         and ebp, 4096
c01051a4: 09 e8                     or eax, ebp
c01051a6: 8b 6c 24 2c               mov ebp, dword ptr [esp + 44]
c01051aa: c1 e5 0d                  shl ebp, 13
c01051ad: 81 e5 00 20 00 00         and ebp, 8192
c01051b3: 09 e8                     or eax, ebp
c01051b5: 8b 6c 24 38               mov ebp, dword ptr [esp + 56]
c01051b9: c1 e5 14                  shl ebp, 20
c01051bc: 81 e5 00 00 10 00         and ebp, 1048576
c01051c2: 09 e8                     or eax, ebp
c01051c4: 8b 6c 24 34               mov ebp, dword ptr [esp + 52]
c01051c8: c1 e5 15                  shl ebp, 21
c01051cb: 81 e5 00 00 20 00         and ebp, 2097152
c01051d1: 09 e8                     or eax, ebp
c01051d3: 8b 6e 04                  mov ebp, dword ptr [esi + 4]
c01051d6: 81 e5 2b 80 c0 ff         and ebp, 4290805803
c01051dc: 09 e8                     or eax, ebp
c01051de: 89 46 04                  mov dword ptr [esi + 4], eax
c01051e1: 8b 44 24 14               mov eax, dword ptr [esp + 20]
```

```
c010523b: e8 85 38 00 00              call 0xc0108ac5 <LogWriteSerial>
c0105240: 83 c4 40                    add esp, 64
c0105243: 89 dd                       mov ebp, ebx
c0105245: 81 e5 00 02 00 00           and ebp, 512
c010524b: 75 16                       jne 0xc0105263 <MapVirtEx+0x4eb>
c010524d: 83 ec 0c                    sub esp, 12
c0105250: 8b 84 24 ac 00 00 00        mov eax, dword ptr [esp + 172]
c0105257: 83 c0 08                    add eax, 8
c010525a: 50                          push eax
c010525b: e8 fa 16 00 00              call 0xc010695a <AcquireSpinlock>
c0105260: 83 c4 10                    add esp, 16
c0105263: 89 f2                       mov edx, esi
c0105265: 8b 84 24 a0 00 00 00        mov eax, dword ptr [esp + 160]
c010526c: e8 d2 ed ff ff              call 0xc0104043 <InsertIntoAvl>
c0105271: 50                          push eax
c0105272: 50                          push eax
c0105273: 56                          push esi
c0105274: ff b4 24 ac 00 00 00        push dword ptr [esp + 172]
c010527b: e8 e3 84 00 00              call 0xc010d763 <ArchAddMapping>
c0105280: 83 c4 10                    add esp, 16
c0105283: 83 7e 08 00                 cmp dword ptr [esi + 8], 0
c0105287: 74 5e                       je 0xc01052e7 <MapVirtEx+0x56f>
c0105289: f6 c3 80                    test bl, -128
c010528c: 75 59                       jne 0xc01052e7 <MapVirtEx+0x56f>
c010528e: e8 e6 f3 ff ff              call 0xc0104679 <GetVas>
c0105293: 39 84 24 a0 00 00 00        cmp dword ptr [esp + 160], eax
c010529a: 75 3b                       jne 0xc01052d7 <MapVirtEx+0x55f>
c010529c: 6a 00                       push 0
c010529e: 6a 02                       push 2
c01052a0: ff 36                       push dword ptr [esi]
c01052a2: ff b4 24 ac 00 00 00        push dword ptr [esp + 172]
c01052a9: e8 a2 f2 ff ff              call 0xc0104550 <SetVirtPermissionsEx>
c01052ae: 8b 4e 0c                    mov ecx, dword ptr [esi + 12]
c01052b1: c1 e1 0c                    shl ecx, 12
c01052b4: 31 c0                       xor eax, eax
c01052b6: 8b 3e                       mov edi, dword ptr [esi]
c01052b8: f3 aa                       rep  stosb byte ptr es:[edi], al
c01052ba: 83 c4 10                    add esp, 16
c01052bd: 80 7e 04 00                 cmp byte ptr [esi + 4], 0
c01052c1: 78 24                       js 0xc01052e7 <MapVirtEx+0x56f>
c01052c3: 6a 02                       push 2
c01052c5: 6a 00                       push 0
c01052c7: ff 36                       push dword ptr [esi]
c01052c9: ff b4 24 ac 00 00 00        push dword ptr [esp + 172]
c01052d0: e8 7b f2 ff ff              call 0xc0104550 <SetVirtPermissionsEx>
c01052d5: eb 0d                       jmp 0xc01052e4 <MapVirtEx+0x56c>
c01052d7: 83 ec 0c                    sub esp, 12
c01052da: 68 e2 0a 11 c0              push 3222342370
c01052df: e8 f9 37 00 00              call 0xc0108add <LogDeveloperWarning>
c01052e4: 83 c4 10                    add esp, 16
c01052e7: 85 ed                       test ebp, ebp
c01052e9: 75 16                       jne 0xc0105301 <MapVirtEx+0x589>
c01052eb: 83 ec 0c                    sub esp, 12
c01052ee: 8b 84 24 ac 00 00 00        mov eax, dword ptr [esp + 172]
c01052f5: 83 c0 08                    add eax, 8
c01052f8: 50                          push eax
c01052f9: e8 ac 16 00 00              call 0xc01069aa <ReleaseSpinlock>
c01052fe: 83 c4 10                    add esp, 16
c0105301: ff 44 24 10                 inc dword ptr [esp + 16]
c0105305: 81 44 24 0c 00 10 00 00     add dword ptr [esp + 12], 4096
c010530d: e9 73 fd ff ff              jmp 0xc0105085 <MapVirtEx+0x30d>
c0105312: e8 62 f3 ff ff              call 0xc0104679 <GetVas>
c0105317: 39 84 24 a0 00 00 00        cmp dword ptr [esp + 160], eax
c010531e: 74 09                       je 0xc0105329 <MapVirtEx+0x5b1>
c0105320: 8b 84 24 a8 00 00 00        mov eax, dword ptr [esp + 168]
c0105327: eb 14                       jmp 0xc010533d <MapVirtEx+0x5c5>
c0105329: 83 ec 0c                    sub esp, 12
c010532c: ff b4 24 ac 00 00 00        push dword ptr [esp + 172]
c0105333: e8 30 84 00 00              call 0xc010d768 <ArchFlushTlb>
c0105338: 83 c4 10                    add esp, 16
c010533b: eb e3                       jmp 0xc0105320 <MapVirtEx+0x5a8>
```

```
c0105383: 57                            push edi
c0105384: 56                            push esi
c0105385: 53                            push ebx
c0105386: 83 ec 24                      sub esp, 36
c0105389: 89 c6                         mov esi, eax
c010538b: 89 d5                         mov ebp, edx
c010538d: 89 4c 24 14                   mov dword ptr [esp + 20], ecx
c0105391: 6a 00                         push 0
c0105393: 6a 00                         push 0
c0105395: 68 13 02 00 00                push 531
c010539a: 68 00 10 00 00                push 4096
c010539f: 6a 00                         push 0
c01053a1: 6a 00                         push 0
c01053a3: e8 a0 ff ff ff                call 0xc0105348 <MapVirt>
c01053a8: 89 c3                         mov ebx, eax
c01053aa: b9 00 04 00 00                mov ecx, 1024
c01053af: 89 c7                         mov edi, eax
c01053b1: f3 a5                         rep  movsd dword ptr es:[edi], dword ptr [esi
c01053b3: 83 c4 14                      add esp, 20
c01053b6: 6a 18                         push 24
c01053b8: e8 92 e5 ff ff                call 0xc010394f <AllocHeap>
c01053bd: 89 58 0c                      mov dword ptr [eax + 12], ebx
c01053c0: 89 28                         mov dword ptr [eax], ebp
c01053c2: c7 40 10 01 00 00 00          mov dword ptr [eax + 16], 1
c01053c9: 8b 54 24 1c                   mov edx, dword ptr [esp + 28]
c01053cd: 89 50 08                      mov dword ptr [eax + 8], edx
c01053d0: c6 40 14 00                   mov byte ptr [eax + 20], 0
c01053d4: 83 c4 0c                      add esp, 12
c01053d7: 50                            push eax
c01053d8: 68 76 57 10 c0                push 3222296438
c01053dd: 6a 01                         push 1
c01053df: e8 15 df ff ff                call 0xc01032f9 <DeferUntilIrql>
c01053e4: 83 c4 2c                      add esp, 44
c01053e7: 5b                            pop ebx
c01053e8: 5e                            pop esi
c01053e9: 5f                            pop edi
c01053ea: 5d                            pop ebp
c01053eb: c3                            ret

c01053ec <DereferenceEntry.part.0>:
c01053ec: 57                            push edi
c01053ed: 56                            push esi
c01053ee: 53                            push ebx
c01053ef: 89 c6                         mov esi, eax
c01053f1: 89 d3                         mov ebx, edx
c01053f3: 8a 42 04                      mov al, byte ptr [edx + 4]
c01053f6: f7 d0                         not eax
c01053f8: a8 85                         test al, -123
c01053fa: 75 0d                         jne 0xc0105409 <DereferenceEntry.part.0+0x1d>
c01053fc: 8b 4a 10                      mov ecx, dword ptr [edx + 16]
c01053ff: 8b 52 14                      mov edx, dword ptr [edx + 20]
c0105402: 8b 03                         mov eax, dword ptr [ebx]
c0105404: e8 79 ff ff ff                call 0xc0105382 <DeferDiskWrite>
c0105409: 31 ff                         xor edi, edi
c010540b: f6 43 04 01                   test byte ptr [ebx + 4], 1
c010540f: 74 11                         je 0xc0105422 <DereferenceEntry.part.0+0x36>
c0105411: 52                            push edx
c0105412: 52                            push edx
c0105413: 53                            push ebx
c0105414: 56                            push esi
c0105415: e8 a8 82 00 00                call 0xc010d6c2 <ArchUnmap>
c010541a: 83 c4 10                      add esp, 16
c010541d: bf 01 00 00 00                mov edi, 1
c0105422: f6 43 04 10                   test byte ptr [ebx + 4], 16
c0105426: 74 14                         je 0xc010543c <DereferenceEntry.part.0+0x50>
c0105428: 50                            push eax
c0105429: 50                            push eax
c010542a: 8b 43 18                      mov eax, dword ptr [ebx + 24]
c010542d: c1 e8 0c                      shr eax, 12
c0105430: 31 d2                         xor edx, edx
c0105432: 52                            push edx
```

```
c0105477: 56                            push esi
c0105478: 53                            push ebx
c0105479: 83 ec 0c                      sub esp, 12
c010547c: 8b 5c 24 20                   mov ebx, dword ptr [esp + 32]
c0105480: 31 f6                         xor esi, esi
c0105482: 31 ff                         xor edi, edi
c0105484: 3b 74 24 28                   cmp esi, dword ptr [esp + 40]
c0105488: 74 4e                         je 0xc01054d8 <UnmapVirtEx+0x63>
c010548a: 89 f2                         mov edx, esi
c010548c: c1 e2 0c                      shl edx, 12
c010548f: 03 54 24 24                   add edx, dword ptr [esp + 36]
c0105493: 8b 03                         mov eax, dword ptr [ebx]
c0105495: e8 7b ed ff ff                call 0xc0104215 <GetVirtEntry.isra.0>
c010549a: 89 c5                         mov ebp, eax
c010549c: 85 c0                         test eax, eax
c010549e: 75 0e                         jne 0xc01054ae <UnmapVirtEx+0x39>
c01054a0: f6 44 24 2c 01                test byte ptr [esp + 44], 1
c01054a5: 75 2e                         jne 0xc01054d5 <UnmapVirtEx+0x60>
c01054a7: b8 07 00 00 00                mov eax, 7
c01054ac: eb 42                         jmp 0xc01054f0 <UnmapVirtEx+0x7b>
c01054ae: 89 c1                         mov ecx, eax
c01054b0: 8b 54 24 24                   mov edx, dword ptr [esp + 36]
c01054b4: 89 d8                         mov eax, ebx
c01054b6: e8 3e ec ff ff                call 0xc01040f9 <SplitLargePageEntryIntoMulti
c01054bb: 8b 45 20                      mov eax, dword ptr [ebp + 32]
c01054be: 8d 50 ff                      lea edx, [eax - 1]
c01054c1: 89 55 20                      mov dword ptr [ebp + 32], edx
c01054c4: 31 c0                         xor eax, eax
c01054c6: 85 d2                         test edx, edx
c01054c8: 75 09                         jne 0xc01054d3 <UnmapVirtEx+0x5e>
c01054ca: 89 ea                         mov edx, ebp
c01054cc: 89 d8                         mov eax, ebx
c01054ce: e8 19 ff ff ff                call 0xc01053ec <DereferenceEntry.part.0>
c01054d3: 09 c7                         or edi, eax
c01054d5: 46                            inc esi
c01054d6: eb ac                         jmp 0xc0105484 <UnmapVirtEx+0xf>
c01054d8: 89 f8                         mov eax, edi
c01054da: 84 c0                         test al, al
c01054dc: 75 04                         jne 0xc01054e2 <UnmapVirtEx+0x6d>
c01054de: 31 c0                         xor eax, eax
c01054e0: eb 0e                         jmp 0xc01054f0 <UnmapVirtEx+0x7b>
c01054e2: 83 ec 0c                      sub esp, 12
c01054e5: 53                            push ebx
c01054e6: e8 7d 82 00 00                call 0xc010d768 <ArchFlushTlb>
c01054eb: 83 c4 10                      add esp, 16
c01054ee: eb ee                         jmp 0xc01054de <UnmapVirtEx+0x69>
c01054f0: 83 c4 0c                      add esp, 12
c01054f3: 5b                            pop ebx
c01054f4: 5e                            pop esi
c01054f5: 5f                            pop edi
c01054f6: 5d                            pop ebp
c01054f7: c3                            ret

c01054f8 <UnmapVirt>:
c01054f8: 56                            push esi
c01054f9: 53                            push ebx
c01054fa: 83 ec 14                      sub esp, 20
c01054fd: e8 77 f1 ff ff                call 0xc0104679 <GetVas>
c0105502: 89 c3                         mov ebx, eax
c0105504: 8d 70 08                      lea esi, [eax + 8]
c0105507: 83 ec 0c                      sub esp, 12
c010550a: 56                            push esi
c010550b: e8 4a 14 00 00                call 0xc010695a <AcquireSpinlock>
c0105510: 6a 00                         push 0
c0105512: 8b 44 24 38                   mov eax, dword ptr [esp + 56]
c0105516: 8d 90 ff 0f 00 00             lea edx, [eax + 4095]
c010551c: c1 ea 0c                      shr edx, 12
c010551f: 52                            push edx
c0105520: ff 74 24 38                   push dword ptr [esp + 56]
c0105524: 53                            push ebx
c0105525: e8 4b ff ff ff                call 0xc0105475 <UnmapVirtEx>
```

```
c0105572: 8d 51 ff                  lea edx, [ecx - 1]
c0105575: 89 56 20                  mov dword ptr [esi + 32], edx
c0105578: 83 c4 10                  add esp, 16
c010557b: 85 d2                     test edx, edx
c010557d: 75 07                     jne 0xc0105586 <WipeUsermodePagesRecursive+0x
c010557f: 89 f2                     mov edx, esi
c0105581: e8 66 fe ff ff            call 0xc01053ec <DereferenceEntry.part.0>
c0105586: 81 3e ff ff ff 0f         cmp dword ptr [esi], 268435455
c010558c: 77 05                     ja 0xc0105593 <WipeUsermodePagesRecursive+0x5
c010558e: 8b 5b 04                  mov ebx, dword ptr [ebx + 4]
c0105591: eb b3                     jmp 0xc0105546 <WipeUsermodePagesRecursive+0x
c0105593: 8b 03                     mov eax, dword ptr [ebx]
c0105595: e8 a7 ff ff ff            call 0xc0105541 <WipeUsermodePagesRecursive>
c010559a: 81 3e ff ff bf bf         cmp dword ptr [esi], 3217031167
c01055a0: 76 ec                     jbe 0xc010558e <WipeUsermodePagesRecursive+0x
c01055a2: 58                        pop eax
c01055a3: 5b                        pop ebx
c01055a4: 5e                        pop esi
c01055a5: c3                        ret

c01055a6 <WipeUsermodePages>:
c01055a6: 56                        push esi
c01055a7: 53                        push ebx
c01055a8: 50                        push eax
c01055a9: e8 cb f0 ff ff            call 0xc0104679 <GetVas>
c01055ae: 89 c3                     mov ebx, eax
c01055b0: 8d 70 08                  lea esi, [eax + 8]
c01055b3: 83 ec 0c                  sub esp, 12
c01055b6: 56                        push esi
c01055b7: e8 9e 13 00 00            call 0xc010695a <AcquireSpinlock>
c01055bc: e8 b8 f0 ff ff            call 0xc0104679 <GetVas>
c01055c1: 8b 00                     mov eax, dword ptr [eax]
c01055c3: 8b 40 04                  mov eax, dword ptr [eax + 4]
c01055c6: e8 76 ff ff ff            call 0xc0105541 <WipeUsermodePagesRecursive>
c01055cb: 89 1c 24                  mov dword ptr [esp], ebx
c01055ce: e8 95 81 00 00            call 0xc010d768 <ArchFlushTlb>
c01055d3: 89 34 24                  mov dword ptr [esp], esi
c01055d6: e8 cf 13 00 00            call 0xc01069aa <ReleaseSpinlock>
c01055db: 31 c0                     xor eax, eax
c01055dd: 83 c4 14                  add esp, 20
c01055e0: 5b                        pop ebx
c01055e1: 5e                        pop esi
c01055e2: c3                        ret

c01055e3 <EvictPage>:
c01055e3: 55                        push ebp
c01055e4: 57                        push edi
c01055e5: 56                        push esi
c01055e6: 53                        push ebx
c01055e7: 83 ec 24                  sub esp, 36
c01055ea: 8b 6c 24 38               mov ebp, dword ptr [esp + 56]
c01055ee: 8b 5c 24 3c               mov ebx, dword ptr [esp + 60]
c01055f2: ff 33                     push dword ptr [ebx]
c01055f4: 68 29 0b 11 c0            push 3222342441
c01055f9: e8 c7 34 00 00            call 0xc0108ac5 <LogWriteSerial>
c01055fe: 8d 45 08                  lea eax, [ebp + 8]
c0105601: 89 c6                     mov esi, eax
c0105603: 89 04 24                  mov dword ptr [esp], eax
c0105606: e8 4f 13 00 00            call 0xc010695a <AcquireSpinlock>
c010560b: 8a 43 04                  mov al, byte ptr [ebx + 4]
c010560e: 83 c4 10                  add esp, 16
c0105611: a8 04                     test al, 4
c0105613: 74 34                     je 0xc0105649 <EvictPage+0x66>
c0105615: 8b 43 04                  mov eax, dword ptr [ebx + 4]
c0105618: 66 25 80 10               and ax, 4224
c010561c: 66 83 c0 80               add ax, -128
c0105620: 75 0d                     jne 0xc010562f <EvictPage+0x4c>
c0105622: 8b 4b 10                  mov ecx, dword ptr [ebx + 16]
c0105625: 8b 53 14                  mov edx, dword ptr [ebx + 20]
c0105628: 8b 03                     mov eax, dword ptr [ebx]
c010562a: e8 53 fd ff ff            call 0xc0105382 <DeferDiskWrite>
```

```
c0105684: 55                            push ebp
c0105685: e8 38 80 00 00                call 0xc010d6c2 <ArchUnmap>
c010568a: 5a                            pop edx
c010568b: ff 73 18                      push dword ptr [ebx + 24]
c010568e: e8 34 e4 ff ff                call 0xc0103ac7 <DeallocPhys>
c0105693: 89 2c 24                      mov dword ptr [esp], ebp
c0105696: e8 cd 80 00 00                call 0xc010d768 <ArchFlushTlb>
c010569b: 83 c4 10                      add esp, 16
c010569e: 83 ec 0c                      sub esp, 12
c01056a1: 68 41 0b 11 c0                push 3222342465
c01056a6: e8 1a 34 00 00                call 0xc0108ac5 <LogWriteSerial>
c01056ab: 89 34 24                      mov dword ptr [esp], esi
c01056ae: e8 f7 12 00 00                call 0xc01069aa <ReleaseSpinlock>
c01056b3: c7 44 24 40 54 0b 11 c0       mov dword ptr [esp + 64], 3222342484
c01056bb: 83 c4 2c                      add esp, 44
c01056be: 5b                            pop ebx
c01056bf: 5e                            pop esi
c01056c0: 5f                            pop edi
c01056c1: 5d                            pop ebp
c01056c2: e9 fe 33 00 00                jmp 0xc0108ac5 <LogWriteSerial>

c01056c7 <EvictVirt>:
c01056c7: 53                            push ebx
c01056c8: 83 ec 18                      sub esp, 24
c01056cb: e8 52 e8 ff ff                call 0xc0103f22 <GetSwapfile>
c01056d0: 85 c0                         test eax, eax
c01056d2: 0f 84 99 00 00 00             je 0xc0105771 <EvictVirt+0xaa>
c01056d8: c7 44 24 04 10 27 00 00       mov dword ptr [esp + 4], 10000
c01056e0: 31 d2                         xor edx, edx
c01056e2: 89 54 24 0c                   mov dword ptr [esp + 12], edx
c01056e6: e8 8e ef ff ff                call 0xc0104679 <GetVas>
c01056eb: 83 ec 0c                      sub esp, 12
c01056ee: 83 c0 08                      add eax, 8
c01056f1: 50                            push eax
c01056f2: e8 63 12 00 00                call 0xc010695a <AcquireSpinlock>
c01056f7: e8 7d ef ff ff                call 0xc0104679 <GetVas>
c01056fc: c7 04 24 a0 b0 13 c0          mov dword ptr [esp], 3222515872
c0105703: 6a 01                         push 1
c0105705: 8d 54 24 1c                   lea edx, [esp + 28]
c0105709: 52                            push edx
c010570a: 8d 54 24 1c                   lea edx, [esp + 28]
c010570e: 52                            push edx
c010570f: 50                            push eax
c0105710: e8 ac ed ff ff                call 0xc01044c1 <FindVirtToEvict>
c0105715: 83 c4 20                      add esp, 32
c0105718: e8 5c ef ff ff                call 0xc0104679 <GetVas>
c010571d: 83 ec 0c                      sub esp, 12
c0105720: 83 c0 08                      add eax, 8
c0105723: 50                            push eax
c0105724: e8 81 12 00 00                call 0xc01069aa <ReleaseSpinlock>
c0105729: 8b 5c 24 1c                   mov ebx, dword ptr [esp + 28]
c010572d: 83 c4 10                      add esp, 16
c0105730: 85 db                         test ebx, ebx
c0105732: 74 3d                         je 0xc0105771 <EvictVirt+0xaa>
c0105734: a1 84 b0 13 c0                mov eax, dword ptr [3222515844]
c0105739: 8d 50 01                      lea edx, [eax + 1]
c010573c: 89 15 84 b0 13 c0             mov dword ptr [-1072451452], edx
c0105742: b9 20 00 00 00                mov ecx, 32
c0105747: 99                            cdq
c0105748: f7 f9                         idiv ecx
c010574a: 89 1c 95 a0 b0 13 c0          mov dword ptr [4*edx - 1072451424], ebx
c0105751: 50                            push eax
c0105752: 50                            push eax
c0105753: 53                            push ebx
c0105754: ff 74 24 14                   push dword ptr [esp + 20]
c0105758: e8 86 fe ff ff                call 0xc01055e3 <EvictPage>
c010575d: 8a 43 06                      mov al, byte ptr [ebx + 6]
c0105760: 8d 50 01                      lea edx, [eax + 1]
c0105763: 83 e2 0f                      and edx, 15
c0105766: 83 e0 f0                      and eax, -16
c0105769: 09 d0                         or eax, edx
```

```
c01057ae: e8 95 fb ff ff              call 0xc0105348 <MapVirt>
c01057b3: 89 44 24 28                 mov dword ptr [esp + 40], eax
c01057b7: 83 c4 20                    add esp, 32
c01057ba: 8d 74 24 10                 lea esi, [esp + 16]
c01057be: 50                          push eax
c01057bf: ff 75 10                    push dword ptr [ebp + 16]
c01057c2: 8b 45 08                    mov eax, dword ptr [ebp + 8]
c01057c5: 31 d2                       xor edx, edx
c01057c7: 52                          push edx
c01057c8: 50                          push eax
c01057c9: 6a 00                       push 0
c01057cb: 68 00 10 00 00              push 4096
c01057d0: ff 74 24 20                 push dword ptr [esp + 32]
c01057d4: 56                          push esi
c01057d5: e8 d6 3f 00 00              call 0xc01097b0 <CreateKernelTransfer>
c01057da: 83 c4 1c                    add esp, 28
c01057dd: b8 cb a2 10 c0              mov eax, 3222315723
c01057e2: 83 fb 01                    cmp ebx, 1
c01057e5: 75 05                       jne 0xc01057ec <PerformDeferredAccess+0x76>
c01057e7: b8 da a2 10 c0              mov eax, 3222315738
c01057ec: 57                          push edi
c01057ed: 57                          push edi
c01057ee: 56                          push esi
c01057ef: ff 75 00                    push dword ptr [ebp]
c01057f2: ff d0                       call eax
c01057f4: 83 c4 10                    add esp, 16
c01057f7: 85 c0                       test eax, eax
c01057f9: 74 1a                       je 0xc0105815 <PerformDeferredAccess+0x9f>
c01057fb: 8b 45 04                    mov eax, dword ptr [ebp + 4]
c01057fe: f6 40 04 10                 test byte ptr [eax + 4], 16
c0105802: 74 07                       je 0xc010580b <PerformDeferredAccess+0x95>
c0105804: 83 ec 0c                    sub esp, 12
c0105807: 6a 19                       push 25
c0105809: eb 05                       jmp 0xc0105810 <PerformDeferredAccess+0x9a>
c010580b: 83 ec 0c                    sub esp, 12
c010580e: 6a 0b                       push 11
c0105810: e8 8a 33 00 00              call 0xc0108b9f <Panic>
c0105815: 4b                          dec ebx
c0105816: 75 14                       jne 0xc010582c <PerformDeferredAccess+0xb6>
c0105818: 53                          push ebx
c0105819: 53                          push ebx
c010581a: 68 00 10 00 00              push 4096
c010581f: ff 75 0c                    push dword ptr [ebp + 12]
c0105822: e8 d1 fc ff ff              call 0xc01054f8 <UnmapVirt>
c0105827: e9 3c 01 00 00              jmp 0xc0105968 <PerformDeferredAccess+0x1f2>
c010582c: 83 ec 0c                    sub esp, 12
c010582f: 68 7a 0b 11 c0              push 3222342522
c0105834: e8 8c 32 00 00              call 0xc0108ac5 <LogWriteSerial>
c0105839: e8 3b ee ff ff              call 0xc0104679 <GetVas>
c010583e: 89 44 24 10                 mov dword ptr [esp + 16], eax
c0105842: 83 c0 08                    add eax, 8
c0105845: 89 44 24 14                 mov dword ptr [esp + 20], eax
c0105849: 89 04 24                    mov dword ptr [esp], eax
c010584c: e8 09 11 00 00              call 0xc010695a <AcquireSpinlock>
c0105851: 8b 55 0c                    mov edx, dword ptr [ebp + 12]
c0105854: 8b 44 24 10                 mov eax, dword ptr [esp + 16]
c0105858: 8b 00                       mov eax, dword ptr [eax]
c010585a: e8 b6 e9 ff ff              call 0xc0104215 <GetVirtEntry.isra.0>
c010585f: 89 c3                       mov ebx, eax
c0105861: c7 40 08 01 00 00 00        mov dword ptr [eax + 8], 1
c0105868: e8 fc e2 ff ff              call 0xc0103b69 <AllocPhys>
c010586d: 89 43 18                    mov dword ptr [ebx + 24], eax
c0105870: 8b 43 04                    mov eax, dword ptr [ebx + 4]
c0105873: 66 25 ec f7                 and ax, 63468
c0105877: 66 0d 03 08                 or ax, 2051
c010587b: 66 89 43 04                 mov word ptr [ebx + 4], ax
c010587f: 58                          pop eax
c0105880: 5a                          pop edx
c0105881: 53                          push ebx
c0105882: ff 74 24 0c                 push dword ptr [esp + 12]
c0105886: e8 4e 7e 00 00              call 0xc010d6d9 <ArchUpdateMapping>
```

```
c01058d9: 68 91 0b 11 c0                push 3222342545
c01058de: e8 e2 31 00 00                call 0xc0108ac5 <LogWriteSerial>
c01058e3: 59                            pop ecx
c01058e4: 5e                            pop esi
c01058e5: 53                            push ebx
c01058e6: ff 74 24 0c                   push dword ptr [esp + 12]
c01058ea: e8 ea 7d 00 00                call 0xc010d6d9 <ArchUpdateMapping>
c01058ef: 5f                            pop edi
c01058f0: ff 74 24 0c                   push dword ptr [esp + 12]
c01058f4: e8 6f 7e 00 00                call 0xc010d768 <ArchFlushTlb>
c01058f9: 83 c4 10                      add esp, 16
c01058fc: 80 7c 24 0f 10                cmp byte ptr [esp + 15], 16
c0105901: 74 09                         je 0xc010590c <PerformDeferredAccess+0x196>
c0105903: 80 63 05 9f                   and byte ptr [ebx + 5], -97
c0105907: 31 c0                         xor eax, eax
c0105909: 89 43 08                      mov dword ptr [ebx + 8], eax
c010590c: 83 ec 0c                      sub esp, 12
c010590f: ff 74 24 10                   push dword ptr [esp + 16]
c0105913: e8 92 10 00 00                call 0xc01069aa <ReleaseSpinlock>
c0105918: 5f                            pop edi
c0105919: 58                            pop eax
c010591a: 68 00 10 00 00                push 4096
c010591f: ff 74 24 14                   push dword ptr [esp + 20]
c0105923: e8 d0 fb ff ff                call 0xc01054f8 <UnmapVirt>
c0105928: 83 c4 10                      add esp, 16
c010592b: 80 7c 24 0f 10                cmp byte ptr [esp + 15], 16
c0105930: 75 39                         jne 0xc010596b <PerformDeferredAccess+0x1f5>
c0105932: 50                            push eax
c0105933: ff 75 0c                      push dword ptr [ebp + 12]
c0105936: ff 73 1c                      push dword ptr [ebx + 28]
c0105939: ff 74 24 0c                   push dword ptr [esp + 12]
c010593d: e8 79 2d 00 00                call 0xc01086bb <RelocatePage>
c0105942: 5a                            pop edx
c0105943: ff 74 24 10                   push dword ptr [esp + 16]
c0105947: e8 0e 10 00 00                call 0xc010695a <AcquireSpinlock>
c010594c: 80 63 05 9f                   and byte ptr [ebx + 5], -97
c0105950: 59                            pop ecx
c0105951: 5b                            pop ebx
c0105952: ff 75 0c                      push dword ptr [ebp + 12]
c0105955: ff 74 24 0c                   push dword ptr [esp + 12]
c0105959: e8 c4 eb ff ff                call 0xc0104522 <UnlockVirtEx>
c010595e: 5e                            pop esi
c010595f: ff 74 24 10                   push dword ptr [esp + 16]
c0105963: e8 42 10 00 00                call 0xc01069aa <ReleaseSpinlock>
c0105968: 83 c4 10                      add esp, 16
c010596b: 83 ec 0c                      sub esp, 12
c010596e: 55                            push ebp
c010596f: e8 ff df ff ff                call 0xc0103973 <FreeHeap>
c0105974: 83 c4 4c                      add esp, 76
c0105977: 5b                            pop ebx
c0105978: 5e                            pop esi
c0105979: 5f                            pop edi
c010597a: 5d                            pop ebp
c010597b: c3                            ret

c010597c <SetVas>:
c010597c: 0f 21 d8                      mov eax, dr3
c010597f: c1 e0 06                      shl eax, 6
c0105982: 8b 54 24 04                   mov edx, dword ptr [esp + 4]
c0105986: 89 90 c0 40 11 c0             mov dword ptr [eax - 1072611136], edx
c010598c: e9 de 7b 00 00                jmp 0xc010d56f <ArchSetVas>

c0105991 <GetKernelVas>:
c0105991: a1 24 b1 13 c0                mov eax, dword ptr [3222516004]
c0105996: c3                            ret

c0105997 <InitVirt>:
c0105997: 53                            push ebx
c0105998: 83 ec 08                      sub esp, 8
c010599b: 0f 21 db                      mov ebx, dr3
c010599e: e8 aa c6 ff ff                call 0xc010204d <TreeCreate>
```

```
c01059f9: 52                            push edx
c01059fa: 68 a9 0b 11 c0                push 3222342569
c01059ff: 6a 0c                         push 12
c0105a01: e8 48 31 00 00                call 0xc0108b4e <PanicEx>
c0105a06: e8 6e ec ff ff                call 0xc0104679 <GetVas>
c0105a0b: 89 c3                         mov ebx, eax
c0105a0d: 8d 70 08                      lea esi, [eax + 8]
c0105a10: 83 ec 0c                      sub esp, 12
c0105a13: 56                            push esi
c0105a14: e8 41 0f 00 00                call 0xc010695a <AcquireSpinlock>
c0105a19: ff 05 80 b0 13 c0             inc dword ptr [-1072451456]
c0105a1f: 0f 21 d8                      mov eax, dr3
c0105a22: 83 c4 0c                      add esp, 12
c0105a25: c1 e0 06                      shl eax, 6
c0105a28: ff b0 c4 40 11 c0             push dword ptr [eax - 1072611132]
c0105a2e: 57                            push edi
c0105a2f: 68 41 0c 11 c0                push 3222342721
c0105a34: e8 8c 30 00 00                call 0xc0108ac5 <LogWriteSerial>
c0105a39: 89 fa                         mov edx, edi
c0105a3b: 8b 03                         mov eax, dword ptr [ebx]
c0105a3d: e8 d3 e7 ff ff                call 0xc0104215 <GetVirtEntry.isra.0>
c0105a42: 89 c2                         mov edx, eax
c0105a44: 83 c4 10                      add esp, 16
c0105a47: 85 c0                         test eax, eax
c0105a49: 75 0d                         jne 0xc0105a58 <HandleVirtFault+0x79>
c0105a4b: 89 44 24 0c                   mov dword ptr [esp + 12], eax
c0105a4f: e8 6c d8 ff ff                call 0xc01032c0 <UnhandledFault>
c0105a54: 8b 54 24 0c                   mov edx, dword ptr [esp + 12]
c0105a58: f6 42 05 40                   test byte ptr [edx + 5], 64
c0105a5c: 74 27                         je 0xc0105a85 <HandleVirtFault+0xa6>
c0105a5e: 83 ec 0c                      sub esp, 12
c0105a61: 68 5c 0c 11 c0                push 3222342748
c0105a66: e8 5a 30 00 00                call 0xc0108ac5 <LogWriteSerial>
c0105a6b: ff 0d 80 b0 13 c0             dec dword ptr [-1072451456]
c0105a71: 89 34 24                      mov dword ptr [esp], esi
c0105a74: e8 31 0f 00 00                call 0xc01069aa <ReleaseSpinlock>
c0105a79: 83 c4 2c                      add esp, 44
c0105a7c: 5b                            pop ebx
c0105a7d: 5e                            pop esi
c0105a7e: 5f                            pop edi
c0105a7f: 5d                            pop ebp
c0105a80: e9 59 1f 00 00                jmp 0xc01079de <Schedule>
c0105a85: 89 e9                         mov ecx, ebp
c0105a87: d1 e9                         shr ecx
c0105a89: 83 e1 01                      and ecx, 1
c0105a8c: 50                            push eax
c0105a8d: 50                            push eax
c0105a8e: 55                            push ebp
c0105a8f: 57                            push edi
c0105a90: 89 d8                         mov eax, ebx
c0105a92: e8 fa ef ff ff                call 0xc0104a91 <BringIntoMemory>
c0105a97: 83 c4 10                      add esp, 16
c0105a9a: 85 c0                         test eax, eax
c0105a9c: 74 05                         je 0xc0105aa3 <HandleVirtFault+0xc4>
c0105a9e: e8 1d d8 ff ff                call 0xc01032c0 <UnhandledFault>
c0105aa3: ff 0d 80 b0 13 c0             dec dword ptr [-1072451456]
c0105aa9: 89 74 24 30                   mov dword ptr [esp + 48], esi
c0105aad: 83 c4 1c                      add esp, 28
c0105ab0: 5b                            pop ebx
c0105ab1: 5e                            pop esi
c0105ab2: 5f                            pop edi
c0105ab3: 5d                            pop ebp
c0105ab4: e9 f1 0e 00 00                jmp 0xc01069aa <ReleaseSpinlock>

c0105ab9 <IsVirtInitialised>:
c0105ab9: a0 21 b1 13 c0                mov al, byte ptr [3222516001]
c0105abe: c3                            ret

c0105abf <BytesToPages>:
c0105abf: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c0105ac3: 05 ff 0f 00 00                add eax, 4095
```

```
c0105b05: 83 ec 0c                  sub esp, 12
c0105b08: 50                        push eax
c0105b09: e8 ef b5 ff ff            call 0xc01010fd <isspace>
c0105b0e: 83 c4 10                  add esp, 16
c0105b11: 85 c0                     test eax, eax
c0105b13: 74 e4                     je 0xc0105af9 <atoi+0x11>
c0105b15: 43                        inc ebx
c0105b16: eb d9                     jmp 0xc0105af1 <atoi+0x9>
c0105b18: 31 ff                     xor edi, edi
c0105b1a: 3c 2d                     cmp al, 45
c0105b1c: 75 06                     jne 0xc0105b24 <atoi+0x3c>
c0105b1e: 43                        inc ebx
c0105b1f: bf 01 00 00 00            mov edi, 1
c0105b24: 01 f3                     add ebx, esi
c0105b26: 31 f6                     xor esi, esi
c0105b28: 0f be 03                  movsx eax, byte ptr [ebx]
c0105b2b: 84 c0                     test al, al
c0105b2d: 75 0a                     jne 0xc0105b39 <atoi+0x51>
c0105b2f: 89 f8                     mov eax, edi
c0105b31: 84 c0                     test al, al
c0105b33: 74 21                     je 0xc0105b56 <atoi+0x6e>
c0105b35: f7 de                     neg esi
c0105b37: eb 1d                     jmp 0xc0105b56 <atoi+0x6e>
c0105b39: 83 ec 0c                  sub esp, 12
c0105b3c: 50                        push eax
c0105b3d: e8 6a b5 ff ff            call 0xc01010ac <isdigit>
c0105b42: 83 c4 10                  add esp, 16
c0105b45: 85 c0                     test eax, eax
c0105b47: 74 e6                     je 0xc0105b2f <atoi+0x47>
c0105b49: 6b f6 0a                  imul esi, esi, 10
c0105b4c: 0f be 03                  movsx eax, byte ptr [ebx]
c0105b4f: 8d 74 06 d0               lea esi, [esi + eax - 48]
c0105b53: 43                        inc ebx
c0105b54: eb d2                     jmp 0xc0105b28 <atoi+0x40>
c0105b56: 89 f0                     mov eax, esi
c0105b58: 5b                        pop ebx
c0105b59: 5e                        pop esi
c0105b5a: 5f                        pop edi
c0105b5b: c3                        ret

c0105b5c <rand>:
c0105b5c: 69 0d 0c 31 11 c0 a5 2b 35 8b imul ecx, dword ptr [-1072615156], 2335517605
c0105b66: 69 05 08 31 11 c0 d6 c9 48 02 imul eax, dword ptr [-1072615160], 38324694
c0105b70: 01 c1                     add ecx, eax
c0105b72: b8 a5 2b 35 8b            mov eax, 2335517605
c0105b77: f7 25 08 31 11 c0         mul dword ptr [-1072615160]
c0105b7d: 01 ca                     add edx, ecx
c0105b7f: 05 7d 12 fd 98            add eax, 2566722173
c0105b84: 81 d2 48 6e 8b cc         adc edx, 3431689800
c0105b8a: a3 08 31 11 c0            mov dword ptr [3222352136], eax
c0105b8f: 89 15 0c 31 11 c0         mov dword ptr [-1072615156], edx
c0105b95: 89 d0                     mov eax, edx
c0105b97: d1 e8                     shr eax
c0105b99: c3                        ret

c0105b9a <srand>:
c0105b9a: 8b 44 24 04               mov eax, dword ptr [esp + 4]
c0105b9e: a3 08 31 11 c0            mov dword ptr [3222352136], eax
c0105ba3: 31 c0                     xor eax, eax
c0105ba5: a3 0c 31 11 c0            mov dword ptr [3222352140], eax
c0105baa: c3                        ret

c0105bab <MergeSort>:
c0105bab: 55                        push ebp
c0105bac: 57                        push edi
c0105bad: 56                        push esi
c0105bae: 53                        push ebx
c0105baf: 83 ec 3c                  sub esp, 60
c0105bb2: 89 44 24 14               mov dword ptr [esp + 20], eax
c0105bb6: 89 14 24                  mov dword ptr [esp], edx
c0105bb9: 89 4c 24 04               mov dword ptr [esp + 4], ecx
```

```
c0105c19: e8 8d ff ff ff              call 0xc0105bab <MergeSort>
c0105c1e: 8d 46 01                    lea eax, [esi + 1]
c0105c21: 89 44 24 28                 mov dword ptr [esp + 40], eax
c0105c25: 8b 44 24 14                 mov eax, dword ptr [esp + 20]
c0105c29: 29 f8                       sub eax, edi
c0105c2b: 89 44 24 2c                 mov dword ptr [esp + 44], eax
c0105c2f: 8b 44 24 28                 mov eax, dword ptr [esp + 40]
c0105c33: 0f af c3                    imul eax, ebx
c0105c36: 89 44 24 14                 mov dword ptr [esp + 20], eax
c0105c3a: 8b 44 24 2c                 mov eax, dword ptr [esp + 44]
c0105c3e: 0f af c3                    imul eax, ebx
c0105c41: 89 44 24 18                 mov dword ptr [esp + 24], eax
c0105c45: 83 c4 10                    add esp, 16
c0105c48: 81 7c 24 04 ff 03 00 00     cmp dword ptr [esp + 4], 1023
c0105c50: 7f 15                       jg 0xc0105c67 <MergeSort+0xbc>
c0105c52: 83 ec 0c                    sub esp, 12
c0105c55: ff 74 24 10                 push dword ptr [esp + 16]
c0105c59: e8 f1 dc ff ff              call 0xc010394f <AllocHeap>
c0105c5e: 89 44 24 1c                 mov dword ptr [esp + 28], eax
c0105c62: 83 c4 10                    add esp, 16
c0105c65: eb 28                       jmp 0xc0105c8f <MergeSort+0xe4>
c0105c67: 80 7c 24 10 01              cmp byte ptr [esp + 16], 1
c0105c6c: 19 c0                       sbb eax, eax
c0105c6e: 83 e0 10                    and eax, 16
c0105c71: 83 c0 03                    add eax, 3
c0105c74: 57                          push edi
c0105c75: 57                          push edi
c0105c76: 6a 00                       push 0
c0105c78: 6a 00                       push 0
c0105c7a: 50                          push eax
c0105c7b: ff 74 24 18                 push dword ptr [esp + 24]
c0105c7f: 6a 00                       push 0
c0105c81: 6a 00                       push 0
c0105c83: e8 c0 f6 ff ff              call 0xc0105348 <MapVirt>
c0105c88: 89 44 24 2c                 mov dword ptr [esp + 44], eax
c0105c8c: 83 c4 20                    add esp, 32
c0105c8f: 81 7c 24 08 ff 03 00 00     cmp dword ptr [esp + 8], 1023
c0105c97: 7f 13                       jg 0xc0105cac <MergeSort+0x101>
c0105c99: 83 ec 0c                    sub esp, 12
c0105c9c: ff 74 24 14                 push dword ptr [esp + 20]
c0105ca0: e8 aa dc ff ff              call 0xc010394f <AllocHeap>
c0105ca5: 89 c5                       mov ebp, eax
c0105ca7: 83 c4 10                    add esp, 16
c0105caa: eb 26                       jmp 0xc0105cd2 <MergeSort+0x127>
c0105cac: 80 7c 24 10 01              cmp byte ptr [esp + 16], 1
c0105cb1: 19 c0                       sbb eax, eax
c0105cb3: 83 e0 10                    and eax, 16
c0105cb6: 83 c0 03                    add eax, 3
c0105cb9: 56                          push esi
c0105cba: 56                          push esi
c0105cbb: 6a 00                       push 0
c0105cbd: 6a 00                       push 0
c0105cbf: 50                          push eax
c0105cc0: ff 74 24 1c                 push dword ptr [esp + 28]
c0105cc4: 6a 00                       push 0
c0105cc6: 6a 00                       push 0
c0105cc8: e8 7b f6 ff ff              call 0xc0105348 <MapVirt>
c0105ccd: 89 c5                       mov ebp, eax
c0105ccf: 83 c4 20                    add esp, 32
c0105cd2: 8b 04 24                    mov eax, dword ptr [esp]
c0105cd5: 0f af c3                    imul eax, ebx
c0105cd8: 8b 54 24 14                 mov edx, dword ptr [esp + 20]
c0105cdc: 01 d0                       add eax, edx
c0105cde: 8b 7c 24 0c                 mov edi, dword ptr [esp + 12]
c0105ce2: 89 c6                       mov esi, eax
c0105ce4: 8b 4c 24 04                 mov ecx, dword ptr [esp + 4]
c0105ce8: f3 a4                       rep  movsb byte ptr es:[edi], byte ptr [esi]
c0105cea: 8b 74 24 20                 mov esi, dword ptr [esp + 32]
c0105cee: 0f af f3                    imul esi, ebx
c0105cf1: 01 d6                       add esi, edx
c0105cf3: 89 ef                       mov edi, ebp
```

```
c0105d46: 85 c0                   test eax, eax
c0105d48: 8b 54 24 2c             mov edx, dword ptr [esp + 44]
c0105d4c: 7f 07                   jg 0xc0105d55 <MergeSort+0x1aa>
c0105d4e: 89 d9                   mov ecx, ebx
c0105d50: f3 a4                   rep  movsb byte ptr es:[edi], byte ptr [esi]
c0105d52: 42                      inc edx
c0105d53: eb 0c                   jmp 0xc0105d61 <MergeSort+0x1b6>
c0105d55: 8b 74 24 28             mov esi, dword ptr [esp + 40]
c0105d59: 89 d9                   mov ecx, ebx
c0105d5b: f3 a4                   rep  movsb byte ptr es:[edi], byte ptr [esi]
c0105d5d: ff 44 24 10             inc dword ptr [esp + 16]
c0105d61: ff 04 24                inc dword ptr [esp]
c0105d64: 01 5c 24 20             add dword ptr [esp + 32], ebx
c0105d68: eb 9d                   jmp 0xc0105d07 <MergeSort+0x15c>
c0105d6a: 8b 04 24                mov eax, dword ptr [esp]
c0105d6d: 0f af c3                imul eax, ebx
c0105d70: 8b 7c 24 14             mov edi, dword ptr [esp + 20]
c0105d74: 01 f8                   add eax, edi
c0105d76: 89 c7                   mov edi, eax
c0105d78: 89 de                   mov esi, ebx
c0105d7a: 0f af f2                imul esi, edx
c0105d7d: 8b 44 24 0c             mov eax, dword ptr [esp + 12]
c0105d81: 01 c6                   add esi, eax
c0105d83: 89 d0                   mov eax, edx
c0105d85: 8b 4c 24 18             mov ecx, dword ptr [esp + 24]
c0105d89: 39 c8                   cmp eax, ecx
c0105d8b: 73 07                   jae 0xc0105d94 <MergeSort+0x1e9>
c0105d8d: 89 d9                   mov ecx, ebx
c0105d8f: f3 a4                   rep  movsb byte ptr es:[edi], byte ptr [esi]
c0105d91: 40                      inc eax
c0105d92: eb f1                   jmp 0xc0105d85 <MergeSort+0x1da>
c0105d94: 31 c0                   xor eax, eax
c0105d96: 39 d1                   cmp ecx, edx
c0105d98: 72 04                   jb 0xc0105d9e <MergeSort+0x1f3>
c0105d9a: 89 c8                   mov eax, ecx
c0105d9c: 29 d0                   sub eax, edx
c0105d9e: 8b 14 24                mov edx, dword ptr [esp]
c0105da1: 01 d0                   add eax, edx
c0105da3: 0f af c3                imul eax, ebx
c0105da6: 8b 54 24 14             mov edx, dword ptr [esp + 20]
c0105daa: 01 c2                   add edx, eax
c0105dac: 89 d0                   mov eax, edx
c0105dae: 8b 74 24 10             mov esi, dword ptr [esp + 16]
c0105db2: 0f af f3                imul esi, ebx
c0105db5: 01 ee                   add esi, ebp
c0105db7: 8b 4c 24 1c             mov ecx, dword ptr [esp + 28]
c0105dbb: 39 4c 24 10             cmp dword ptr [esp + 16], ecx
c0105dbf: 73 0e                   jae 0xc0105dcf <MergeSort+0x224>
c0105dc1: 89 c7                   mov edi, eax
c0105dc3: 89 d9                   mov ecx, ebx
c0105dc5: f3 a4                   rep  movsb byte ptr es:[edi], byte ptr [esi]
c0105dc7: ff 44 24 10             inc dword ptr [esp + 16]
c0105dcb: 89 f8                   mov eax, edi
c0105dcd: eb e8                   jmp 0xc0105db7 <MergeSort+0x20c>
c0105dcf: 81 7c 24 04 ff 03 00 00 cmp dword ptr [esp + 4], 1023
c0105dd7: 7f 0e                   jg 0xc0105de7 <MergeSort+0x23c>
c0105dd9: 83 ec 0c                sub esp, 12
c0105ddc: ff 74 24 18             push dword ptr [esp + 24]
c0105de0: e8 8e db ff ff          call 0xc0103973 <FreeHeap>
c0105de5: eb 0f                   jmp 0xc0105df6 <MergeSort+0x24b>
c0105de7: 50                      push eax
c0105de8: 50                      push eax
c0105de9: ff 74 24 0c             push dword ptr [esp + 12]
c0105ded: ff 74 24 18             push dword ptr [esp + 24]
c0105df1: e8 02 f7 ff ff          call 0xc01054f8 <UnmapVirt>
c0105df6: 83 c4 10                add esp, 16
c0105df9: 81 7c 24 08 ff 03 00 00 cmp dword ptr [esp + 8], 1023
c0105e01: 7f 10                   jg 0xc0105e13 <MergeSort+0x268>
c0105e03: 89 6c 24 50             mov dword ptr [esp + 80], ebp
c0105e07: 83 c4 3c                add esp, 60
c0105e0a: 5b                      pop ebx
```

```
c0105e4b: 89 5c 24 0c                  mov dword ptr [esp + 12], ebx
c0105e4f: 89 54 24 08                  mov dword ptr [esp + 8], edx
c0105e53: 31 d2                        xor edx, edx
c0105e55: 5b                           pop ebx
c0105e56: e9 50 fd ff ff               jmp 0xc0105bab <MergeSort>

c0105e5b <qsort_pageable>:
c0105e5b: 53                           push ebx
c0105e5c: 8b 44 24 08                  mov eax, dword ptr [esp + 8]
c0105e60: 8b 54 24 10                  mov edx, dword ptr [esp + 16]
c0105e64: 8b 4c 24 0c                  mov ecx, dword ptr [esp + 12]
c0105e68: 49                           dec ecx
c0105e69: c7 44 24 10 01 00 00 00      mov dword ptr [esp + 16], 1
c0105e71: 8b 5c 24 14                  mov ebx, dword ptr [esp + 20]
c0105e75: 89 5c 24 0c                  mov dword ptr [esp + 12], ebx
c0105e79: 89 54 24 08                  mov dword ptr [esp + 8], edx
c0105e7d: 31 d2                        xor edx, edx
c0105e7f: 5b                           pop ebx
c0105e80: e9 26 fd ff ff               jmp 0xc0105bab <MergeSort>

c0105e85 <bsearch>:
c0105e85: 55                           push ebp
c0105e86: 57                           push edi
c0105e87: 56                           push esi
c0105e88: 53                           push ebx
c0105e89: 83 ec 0c                     sub esp, 12
c0105e8c: 8b 44 24 28                  mov eax, dword ptr [esp + 40]
c0105e90: 8d 78 ff                     lea edi, [eax - 1]
c0105e93: 31 ed                        xor ebp, ebp
c0105e95: 89 fb                        mov ebx, edi
c0105e97: 29 eb                        sub ebx, ebp
c0105e99: d1 eb                        shr ebx
c0105e9b: 01 eb                        add ebx, ebp
c0105e9d: 8b 74 24 2c                  mov esi, dword ptr [esp + 44]
c0105ea1: 0f af f3                     imul esi, ebx
c0105ea4: 03 74 24 24                  add esi, dword ptr [esp + 36]
c0105ea8: 50                           push eax
c0105ea9: 50                           push eax
c0105eaa: 56                           push esi
c0105eab: ff 74 24 2c                  push dword ptr [esp + 44]
c0105eaf: ff 54 24 40                  call dword ptr [esp + 64]
c0105eb3: 83 c4 10                     add esp, 16
c0105eb6: 85 c0                        test eax, eax
c0105eb8: 74 10                        je 0xc0105eca <bsearch+0x45>
c0105eba: 79 05                        jns 0xc0105ec1 <bsearch+0x3c>
c0105ebc: 8d 7b ff                     lea edi, [ebx - 1]
c0105ebf: eb 03                        jmp 0xc0105ec4 <bsearch+0x3f>
c0105ec1: 8d 6b 01                     lea ebp, [ebx + 1]
c0105ec4: 39 ef                        cmp edi, ebp
c0105ec6: 73 cd                        jae 0xc0105e95 <bsearch+0x10>
c0105ec8: 31 f6                        xor esi, esi
c0105eca: 89 f0                        mov eax, esi
c0105ecc: 83 c4 0c                     add esp, 12
c0105ecf: 5b                           pop ebx
c0105ed0: 5e                           pop esi
c0105ed1: 5f                           pop edi
c0105ed2: 5d                           pop ebp
c0105ed3: c3                           ret

c0105ed4 <MailboxWaitGettableInternal>:
c0105ed4: 57                           push edi
c0105ed5: 56                           push esi
c0105ed6: 53                           push ebx
c0105ed7: 89 c6                        mov esi, eax
c0105ed9: 89 d7                        mov edi, edx
c0105edb: 83 ec 0c                     sub esp, 12
c0105ede: 68 9a 0c 11 c0               push 3222342810
c0105ee3: e8 dd 2b 00 00               call 0xc0108ac5 <LogWriteSerial>
c0105ee8: 5a                           pop edx
c0105ee9: 59                           pop ecx
c0105eea: 57                           push edi
```

```
c0105f3c: 5f                            pop edi
c0105f3d: c3                            ret

c0105f3e <MailboxWaitGettable>:
c0105f3e: 56                            push esi
c0105f3f: 83 ec 18                      sub esp, 24
c0105f42: 8b 74 24 20                   mov esi, dword ptr [esp + 32]
c0105f46: 8b 54 24 24                   mov edx, dword ptr [esp + 36]
c0105f4a: 89 f0                         mov eax, esi
c0105f4c: e8 83 ff ff ff                call 0xc0105ed4 <MailboxWaitGettableInternal>
c0105f51: 85 c0                         test eax, eax
c0105f53: 75 1f                         jne 0xc0105f74 <MailboxWaitGettable+0x36>
c0105f55: 89 44 24 0c                   mov dword ptr [esp + 12], eax
c0105f59: 83 ec 0c                      sub esp, 12
c0105f5c: ff 76 14                      push dword ptr [esi + 20]
c0105f5f: e8 4f 09 00 00                call 0xc01068b3 <ReleaseSemaphore>
c0105f64: 58                            pop eax
c0105f65: ff 76 20                      push dword ptr [esi + 32]
c0105f68: e8 46 09 00 00                call 0xc01068b3 <ReleaseSemaphore>
c0105f6d: 83 c4 10                      add esp, 16
c0105f70: 8b 44 24 0c                   mov eax, dword ptr [esp + 12]
c0105f74: 83 c4 18                      add esp, 24
c0105f77: 5e                            pop esi
c0105f78: c3                            ret

c0105f79 <MailboxWaitAddableInternal>:
c0105f79: 57                            push edi
c0105f7a: 56                            push esi
c0105f7b: 53                            push ebx
c0105f7c: 89 c6                         mov esi, eax
c0105f7e: 89 d7                         mov edi, edx
c0105f80: 83 ec 0c                      sub esp, 12
c0105f83: 68 ff 0c 11 c0                push 3222342911
c0105f88: e8 38 2b 00 00                call 0xc0108ac5 <LogWriteSerial>
c0105f8d: 5a                            pop edx
c0105f8e: 59                            pop ecx
c0105f8f: 57                            push edi
c0105f90: ff 76 1c                      push dword ptr [esi + 28]
c0105f93: e8 a1 07 00 00                call 0xc0106739 <AcquireSemaphore>
c0105f98: 83 c4 10                      add esp, 16
c0105f9b: 85 c0                         test eax, eax
c0105f9d: 74 0c                         je 0xc0105fab <MailboxWaitAddableInternal+0x3
c0105f9f: 89 c3                         mov ebx, eax
c0105fa1: 83 ec 0c                      sub esp, 12
c0105fa4: 68 21 0d 11 c0                push 3222342945
c0105fa9: eb 2a                         jmp 0xc0105fd5 <MailboxWaitAddableInternal+0x
c0105fab: 50                            push eax
c0105fac: 50                            push eax
c0105fad: 57                            push edi
c0105fae: ff 76 18                      push dword ptr [esi + 24]
c0105fb1: e8 83 07 00 00                call 0xc0106739 <AcquireSemaphore>
c0105fb6: 89 c3                         mov ebx, eax
c0105fb8: 83 c4 10                      add esp, 16
c0105fbb: 85 c0                         test eax, eax
c0105fbd: 74 0e                         je 0xc0105fcd <MailboxWaitAddableInternal+0x5
c0105fbf: 83 ec 0c                      sub esp, 12
c0105fc2: ff 76 1c                      push dword ptr [esi + 28]
c0105fc5: e8 e9 08 00 00                call 0xc01068b3 <ReleaseSemaphore>
c0105fca: 83 c4 10                      add esp, 16
c0105fcd: 83 ec 0c                      sub esp, 12
c0105fd0: 68 41 0d 11 c0                push 3222342977
c0105fd5: e8 eb 2a 00 00                call 0xc0108ac5 <LogWriteSerial>
c0105fda: 83 c4 10                      add esp, 16
c0105fdd: 89 d8                         mov eax, ebx
c0105fdf: 5b                            pop ebx
c0105fe0: 5e                            pop esi
c0105fe1: 5f                            pop edi
c0105fe2: c3                            ret

c0105fe3 <MailboxWaitAddable>:
c0105fe3: 56                            push esi
```

```
c0106030: 89 c3                   mov ebx, eax
c0106032: 89 34 24                mov dword ptr [esp], esi
c0106035: e8 15 d9 ff ff          call 0xc010394f <AllocHeap>
c010603a: 89 44 24 1c             mov dword ptr [esp + 28], eax
c010603e: 83 c4 0c                add esp, 12
c0106041: 56                      push esi
c0106042: 56                      push esi
c0106043: 68 61 0d 11 c0          push 3222343009
c0106048: e8 8c 06 00 00          call 0xc01066d9 <CreateSemaphore>
c010604d: 89 44 24 18             mov dword ptr [esp + 24], eax
c0106051: 83 c4 0c                add esp, 12
c0106054: 6a 00                   push 0
c0106056: 56                      push esi
c0106057: 68 68 0d 11 c0          push 3222343016
c010605c: e8 78 06 00 00          call 0xc01066d9 <CreateSemaphore>
c0106061: 89 c5                   mov ebp, eax
c0106063: 83 c4 0c                add esp, 12
c0106066: 6a 00                   push 0
c0106068: 6a 01                   push 1
c010606a: 68 70 0d 11 c0          push 3222343024
c010606f: e8 65 06 00 00          call 0xc01066d9 <CreateSemaphore>
c0106074: 89 c7                   mov edi, eax
c0106076: 83 c4 0c                add esp, 12
c0106079: 6a 00                   push 0
c010607b: 6a 01                   push 1
c010607d: 68 76 0d 11 c0          push 3222343030
c0106082: e8 52 06 00 00          call 0xc01066d9 <CreateSemaphore>
c0106087: 89 44 24 14             mov dword ptr [esp + 20], eax
c010608b: 83 c4 0c                add esp, 12
c010608e: 6a 00                   push 0
c0106090: 6a 01                   push 1
c0106092: 68 7c 0d 11 c0          push 3222343036
c0106097: e8 3d 06 00 00          call 0xc01066d9 <CreateSemaphore>
c010609c: 8b 4c 24 1c             mov ecx, dword ptr [esp + 28]
c01060a0: 89 0b                   mov dword ptr [ebx], ecx
c01060a2: 89 73 04                mov dword ptr [ebx + 4], esi
c01060a5: 31 d2                   xor edx, edx
c01060a7: 89 53 08                mov dword ptr [ebx + 8], edx
c01060aa: 89 53 0c                mov dword ptr [ebx + 12], edx
c01060ad: 89 53 10                mov dword ptr [ebx + 16], edx
c01060b0: 8b 54 24 18             mov edx, dword ptr [esp + 24]
c01060b4: 89 53 14                mov dword ptr [ebx + 20], edx
c01060b7: 89 6b 18                mov dword ptr [ebx + 24], ebp
c01060ba: 89 7b 1c                mov dword ptr [ebx + 28], edi
c01060bd: 8b 7c 24 14             mov edi, dword ptr [esp + 20]
c01060c1: 89 7b 20                mov dword ptr [ebx + 32], edi
c01060c4: 89 43 24                mov dword ptr [ebx + 36], eax
c01060c7: 89 d8                   mov eax, ebx
c01060c9: 83 c4 2c                add esp, 44
c01060cc: 5b                      pop ebx
c01060cd: 5e                      pop esi
c01060ce: 5f                      pop edi
c01060cf: 5d                      pop ebp
c01060d0: c3                      ret

c01060d1 <MailboxDestroy>:
c01060d1: 53                      push ebx
c01060d2: 83 ec 10                sub esp, 16
c01060d5: 8b 5c 24 18             mov ebx, dword ptr [esp + 24]
c01060d9: 6a 00                   push 0
c01060db: ff 73 14                push dword ptr [ebx + 20]
c01060de: e8 f0 07 00 00          call 0xc01068d3 <DestroySemaphore>
c01060e3: 58                      pop eax
c01060e4: 5a                      pop edx
c01060e5: 6a 00                   push 0
c01060e7: ff 73 18                push dword ptr [ebx + 24]
c01060ea: e8 e4 07 00 00          call 0xc01068d3 <DestroySemaphore>
c01060ef: 59                      pop ecx
c01060f0: 58                      pop eax
c01060f1: 6a 01                   push 1
c01060f3: ff 73 1c                push dword ptr [ebx + 28]
```

```
c010613c: 75 10                         jne 0xc010614e <MailboxAddMany+0x2e>
c010613e: c7 44 24 0c 07 00 00 00       mov dword ptr [esp + 12], 7
c0106146: 85 db                         test ebx, ebx
c0106148: 0f 84 c9 00 00 00             je 0xc0106217 <MailboxAddMany+0xf7>
c010614e: 8b 54 24 34                   mov edx, dword ptr [esp + 52]
c0106152: 8b 44 24 30                   mov eax, dword ptr [esp + 48]
c0106156: e8 1e fe ff ff                call 0xc0105f79 <MailboxWaitAddableInternal>
c010615b: 89 44 24 0c                   mov dword ptr [esp + 12], eax
c010615f: 85 c0                         test eax, eax
c0106161: 0f 85 b0 00 00 00             jne 0xc0106217 <MailboxAddMany+0xf7>
c0106167: be 01 00 00 00                mov esi, 1
c010616c: 31 ff                         xor edi, edi
c010616e: 39 fd                         cmp ebp, edi
c0106170: 75 20                         jne 0xc0106192 <MailboxAddMany+0x72>
c0106172: 39 f3                         cmp ebx, esi
c0106174: 75 1c                         jne 0xc0106192 <MailboxAddMany+0x72>
c0106176: 50                            push eax
c0106177: 50                            push eax
c0106178: 6a ff                         push -1
c010617a: 8b 44 24 3c                   mov eax, dword ptr [esp + 60]
c010617e: ff 70 24                      push dword ptr [eax + 36]
c0106181: e8 b3 05 00 00                call 0xc0106739 <AcquireSemaphore>
c0106186: 8b 4c 24 48                   mov ecx, dword ptr [esp + 72]
c010618a: 8d 2c 31                      lea ebp, [ecx + esi]
c010618d: 83 c4 10                      add esp, 16
c0106190: eb 1f                         jmp 0xc01061b1 <MailboxAddMany+0x91>
c0106192: 50                            push eax
c0106193: 50                            push eax
c0106194: 6a 00                         push 0
c0106196: 8b 44 24 3c                   mov eax, dword ptr [esp + 60]
c010619a: ff 70 18                      push dword ptr [eax + 24]
c010619d: e8 97 05 00 00                call 0xc0106739 <AcquireSemaphore>
c01061a2: 83 c4 10                      add esp, 16
c01061a5: 85 c0                         test eax, eax
c01061a7: 75 cd                         jne 0xc0106176 <MailboxAddMany+0x56>
c01061a9: 83 c6 01                      add esi, 1
c01061ac: 83 d7 00                      adc edi, 0
c01061af: eb bd                         jmp 0xc010616e <MailboxAddMany+0x4e>
c01061b1: 8b 44 24 30                   mov eax, dword ptr [esp + 48]
c01061b5: 8b 10                         mov edx, dword ptr [eax]
c01061b7: 8b 40 10                      mov eax, dword ptr [eax + 16]
c01061ba: 8a 19                         mov bl, byte ptr [ecx]
c01061bc: 88 1c 02                      mov byte ptr [edx + eax], bl
c01061bf: 8b 44 24 30                   mov eax, dword ptr [esp + 48]
c01061c3: 8b 40 10                      mov eax, dword ptr [eax + 16]
c01061c6: 40                            inc eax
c01061c7: 8b 5c 24 30                   mov ebx, dword ptr [esp + 48]
c01061cb: 99                            cdq
c01061cc: f7 7b 04                      idiv dword ptr [ebx + 4]
c01061cf: 89 53 10                      mov dword ptr [ebx + 16], edx
c01061d2: ff 43 08                      inc dword ptr [ebx + 8]
c01061d5: 41                            inc ecx
c01061d6: 39 e9                         cmp ecx, ebp
c01061d8: 75 d7                         jne 0xc01061b1 <MailboxAddMany+0x91>
c01061da: 83 ec 0c                      sub esp, 12
c01061dd: ff 73 24                      push dword ptr [ebx + 36]
c01061e0: e8 ce 06 00 00                call 0xc01068b3 <ReleaseSemaphore>
c01061e5: 58                            pop eax
c01061e6: 8b 44 24 3c                   mov eax, dword ptr [esp + 60]
c01061ea: ff 70 1c                      push dword ptr [eax + 28]
c01061ed: e8 c1 06 00 00                call 0xc01068b3 <ReleaseSemaphore>
c01061f2: e8 50 14 00 00                call 0xc0107647 <LockScheduler>
c01061f7: 5a                            pop edx
c01061f8: 59                            pop ecx
c01061f9: 56                            push esi
c01061fa: 8b 44 24 3c                   mov eax, dword ptr [esp + 60]
c01061fe: ff 70 14                      push dword ptr [eax + 20]
c0106201: e8 2c 06 00 00                call 0xc0106832 <ReleaseSemaphoreEx>
c0106206: e8 90 14 00 00                call 0xc010769b <UnlockScheduler>
c010620b: 8b 44 24 54                   mov eax, dword ptr [esp + 84]
c010620f: 89 30                         mov dword ptr [eax], esi
```

```
c0106250: 89 f9                         mov ecx, edi
c0106252: 88 0c 02                      mov byte ptr [edx + eax], cl
c0106255: 8b 43 10                      mov eax, dword ptr [ebx + 16]
c0106258: 40                            inc eax
c0106259: 99                            cdq
c010625a: f7 7b 04                      idiv dword ptr [ebx + 4]
c010625d: 89 53 10                      mov dword ptr [ebx + 16], edx
c0106260: ff 43 08                      inc dword ptr [ebx + 8]
c0106263: 5a                            pop edx
c0106264: ff 73 24                      push dword ptr [ebx + 36]
c0106267: e8 47 06 00 00                call 0xc01068b3 <ReleaseSemaphore>
c010626c: 59                            pop ecx
c010626d: ff 73 1c                      push dword ptr [ebx + 28]
c0106270: e8 3e 06 00 00                call 0xc01068b3 <ReleaseSemaphore>
c0106275: 5f                            pop edi
c0106276: ff 73 14                      push dword ptr [ebx + 20]
c0106279: e8 35 06 00 00                call 0xc01068b3 <ReleaseSemaphore>
c010627e: 83 c4 10                      add esp, 16
c0106281: 89 f0                         mov eax, esi
c0106283: 5b                            pop ebx
c0106284: 5e                            pop esi
c0106285: 5f                            pop edi
c0106286: c3                            ret

c0106287 <MailboxGet>:
c0106287: 56                            push esi
c0106288: 53                            push ebx
c0106289: 50                            push eax
c010628a: 8b 5c 24 10                   mov ebx, dword ptr [esp + 16]
c010628e: 8b 54 24 14                   mov edx, dword ptr [esp + 20]
c0106292: 89 d8                         mov eax, ebx
c0106294: e8 3b fc ff ff                call 0xc0105ed4 <MailboxWaitGettableInternal>
c0106299: 89 c6                         mov esi, eax
c010629b: 85 c0                         test eax, eax
c010629d: 75 46                         jne 0xc01062e5 <MailboxGet+0x5e>
c010629f: 51                            push ecx
c01062a0: 51                            push ecx
c01062a1: 6a ff                         push -1
c01062a3: ff 73 24                      push dword ptr [ebx + 36]
c01062a6: e8 8e 04 00 00                call 0xc0106739 <AcquireSemaphore>
c01062ab: 8b 13                         mov edx, dword ptr [ebx]
c01062ad: 8b 43 0c                      mov eax, dword ptr [ebx + 12]
c01062b0: 8a 14 02                      mov dl, byte ptr [edx + eax]
c01062b3: 8b 44 24 28                   mov eax, dword ptr [esp + 40]
c01062b7: 88 10                         mov byte ptr [eax], dl
c01062b9: 8b 43 0c                      mov eax, dword ptr [ebx + 12]
c01062bc: 40                            inc eax
c01062bd: 99                            cdq
c01062be: f7 7b 04                      idiv dword ptr [ebx + 4]
c01062c1: 89 53 0c                      mov dword ptr [ebx + 12], edx
c01062c4: ff 4b 08                      dec dword ptr [ebx + 8]
c01062c7: 58                            pop eax
c01062c8: ff 73 24                      push dword ptr [ebx + 36]
c01062cb: e8 e3 05 00 00                call 0xc01068b3 <ReleaseSemaphore>
c01062d0: 58                            pop eax
c01062d1: ff 73 20                      push dword ptr [ebx + 32]
c01062d4: e8 da 05 00 00                call 0xc01068b3 <ReleaseSemaphore>
c01062d9: 58                            pop eax
c01062da: ff 73 18                      push dword ptr [ebx + 24]
c01062dd: e8 d1 05 00 00                call 0xc01068b3 <ReleaseSemaphore>
c01062e2: 83 c4 10                      add esp, 16
c01062e5: 89 f0                         mov eax, esi
c01062e7: 5a                            pop edx
c01062e8: 5b                            pop ebx
c01062e9: 5e                            pop esi
c01062ea: c3                            ret

c01062eb <MailboxGetMany>:
c01062eb: 55                            push ebp
c01062ec: 57                            push edi
c01062ed: 56                            push esi
```

```
c0106351: 50                            push eax
c0106352: 6a ff                         push -1
c0106354: ff 75 24                      push dword ptr [ebp + 36]
c0106357: e8 dd 03 00 00                call 0xc0106739 <AcquireSemaphore>
c010635c: 8b 4c 24 48                   mov ecx, dword ptr [esp + 72]
c0106360: 8d 04 31                      lea eax, [ecx + esi]
c0106363: 89 44 24 18                   mov dword ptr [esp + 24], eax
c0106367: 83 c4 10                      add esp, 16
c010636a: eb 1b                         jmp 0xc0106387 <MailboxGetMany+0x9c>
c010636c: 50                            push eax
c010636d: 50                            push eax
c010636e: 6a 00                         push 0
c0106370: ff 75 14                      push dword ptr [ebp + 20]
c0106373: e8 c1 03 00 00                call 0xc0106739 <AcquireSemaphore>
c0106378: 83 c4 10                      add esp, 16
c010637b: 85 c0                         test eax, eax
c010637d: 75 d1                         jne 0xc0106350 <MailboxGetMany+0x65>
c010637f: 83 c6 01                      add esi, 1
c0106382: 83 d7 00                      adc edi, 0
c0106385: eb bd                         jmp 0xc0106344 <MailboxGetMany+0x59>
c0106387: 8b 55 00                      mov edx, dword ptr [ebp]
c010638a: 8b 45 0c                      mov eax, dword ptr [ebp + 12]
c010638d: 8a 04 02                      mov al, byte ptr [edx + eax]
c0106390: 88 01                         mov byte ptr [ecx], al
c0106392: 8b 45 0c                      mov eax, dword ptr [ebp + 12]
c0106395: 40                            inc eax
c0106396: 99                            cdq
c0106397: f7 7d 04                      idiv dword ptr [ebp + 4]
c010639a: 89 55 0c                      mov dword ptr [ebp + 12], edx
c010639d: ff 4d 08                      dec dword ptr [ebp + 8]
c01063a0: 41                            inc ecx
c01063a1: 39 4c 24 08                   cmp dword ptr [esp + 8], ecx
c01063a5: 75 e0                         jne 0xc0106387 <MailboxGetMany+0x9c>
c01063a7: 83 ec 0c                      sub esp, 12
c01063aa: ff 75 24                      push dword ptr [ebp + 36]
c01063ad: e8 01 05 00 00                call 0xc01068b3 <ReleaseSemaphore>
c01063b2: 58                            pop eax
c01063b3: ff 75 20                      push dword ptr [ebp + 32]
c01063b6: e8 f8 04 00 00                call 0xc01068b3 <ReleaseSemaphore>
c01063bb: e8 87 12 00 00                call 0xc0107647 <LockScheduler>
c01063c0: 5a                            pop edx
c01063c1: 59                            pop ecx
c01063c2: 56                            push esi
c01063c3: ff 75 18                      push dword ptr [ebp + 24]
c01063c6: e8 67 04 00 00                call 0xc0106832 <ReleaseSemaphoreEx>
c01063cb: e8 cb 12 00 00                call 0xc010769b <UnlockScheduler>
c01063d0: 8b 44 24 54                   mov eax, dword ptr [esp + 84]
c01063d4: 89 30                         mov dword ptr [eax], esi
c01063d6: 89 78 04                      mov dword ptr [eax + 4], edi
c01063d9: 83 c4 10                      add esp, 16
c01063dc: 89 d8                         mov eax, ebx
c01063de: 83 c4 1c                      add esp, 28
c01063e1: 5b                            pop ebx
c01063e2: 5e                            pop esi
c01063e3: 5f                            pop edi
c01063e4: 5d                            pop ebp
c01063e5: c3                            ret

c01063e6 <MailboxAccess>:
c01063e6: 55                            push ebp
c01063e7: 89 e5                         mov ebp, esp
c01063e9: 57                            push edi
c01063ea: 56                            push esi
c01063eb: 53                            push ebx
c01063ec: 83 ec 3c                      sub esp, 60
c01063ef: 8b 7d 0c                      mov edi, dword ptr [ebp + 12]
c01063f2: 8b 47 14                      mov eax, dword ptr [edi + 20]
c01063f5: 89 45 c4                      mov dword ptr [ebp - 60], eax
c01063f8: 83 7f 08 00                   cmp dword ptr [edi + 8], 0
c01063fc: 75 2a                         jne 0xc0106428 <MailboxAccess+0x42>
c01063fe: 83 7f 04 00                   cmp dword ptr [edi + 4], 0
```

```
c0106460: b9 00 01 00 00                mov ecx, 256
c0106465: 8b 5d d0                      mov ebx, dword ptr [ebp - 48]
c0106468: 39 d9                         cmp ecx, ebx
c010646a: b9 00 00 00 00                mov ecx, 0
c010646f: 1b 4d d4                      sbb ecx, dword ptr [ebp - 44]
c0106472: 73 07                         jae 0xc010647b <MailboxAccess+0x95>
c0106474: b8 00 01 00 00                mov eax, 256
c0106479: 31 d2                         xor edx, edx
c010647b: 83 7d c4 01                   cmp dword ptr [ebp - 60], 1
c010647f: 0f 85 88 00 00 00             jne 0xc010650d <MailboxAccess+0x127>
c0106485: 52                            push edx
c0106486: 50                            push eax
c0106487: 57                            push edi
c0106488: ff 75 cc                      push dword ptr [ebp - 52]
c010648b: e8 63 30 00 00                call 0xc01094f3 <PerformTransfer>
c0106490: 8b 4d d0                      mov ecx, dword ptr [ebp - 48]
c0106493: 8b 5d d4                      mov ebx, dword ptr [ebp - 44]
c0106496: 2b 4f 04                      sub ecx, dword ptr [edi + 4]
c0106499: 1b 5f 08                      sbb ebx, dword ptr [edi + 8]
c010649c: 58                            pop eax
c010649d: 5a                            pop edx
c010649e: 8d 45 e0                      lea eax, [ebp - 32]
c01064a1: 50                            push eax
c01064a2: 53                            push ebx
c01064a3: 51                            push ecx
c01064a4: 89 4d b8                      mov dword ptr [ebp - 72], ecx
c01064a7: 89 5d bc                      mov dword ptr [ebp - 68], ebx
c01064aa: ff 75 cc                      push dword ptr [ebp - 52]
c01064ad: 89 f0                         mov eax, esi
c01064af: f7 d8                         neg eax
c01064b1: 50                            push eax
c01064b2: ff 75 08                      push dword ptr [ebp + 8]
c01064b5: e8 66 fc ff ff                call 0xc0106120 <MailboxAddMany>
c01064ba: 89 45 d0                      mov dword ptr [ebp - 48], eax
c01064bd: 8b 45 e0                      mov eax, dword ptr [ebp - 32]
c01064c0: 8b 55 e4                      mov edx, dword ptr [ebp - 28]
c01064c3: 83 c4 20                      add esp, 32
c01064c6: 8b 4d b8                      mov ecx, dword ptr [ebp - 72]
c01064c9: 8b 5d bc                      mov ebx, dword ptr [ebp - 68]
c01064cc: 39 da                         cmp edx, ebx
c01064ce: 75 08                         jne 0xc01064d8 <MailboxAccess+0xf2>
c01064d0: 39 c8                         cmp eax, ecx
c01064d2: 0f 84 94 00 00 00             je 0xc010656c <MailboxAccess+0x186>
c01064d8: 39 c1                         cmp ecx, eax
c01064da: 89 de                         mov esi, ebx
c01064dc: 19 d6                         sbb esi, edx
c01064de: 73 1b                         jae 0xc01064fb <MailboxAccess+0x115>
c01064e0: 57                            push edi
c01064e1: 51                            push ecx
c01064e2: 50                            push eax
c01064e3: 68 84 0d 11 c0                push 3222343044
c01064e8: e8 d8 25 00 00                call 0xc0108ac5 <LogWriteSerial>
c01064ed: 58                            pop eax
c01064ee: 5a                            pop edx
c01064ef: 68 9b 0d 11 c0                push 3222343067
c01064f4: 6a 00                         push 0
c01064f6: e8 53 26 00 00                call 0xc0108b4e <PanicEx>
c01064fb: 56                            push esi
c01064fc: 29 c1                         sub ecx, eax
c01064fe: 19 d3                         sbb ebx, edx
c0106500: 53                            push ebx
c0106501: 51                            push ecx
c0106502: 57                            push edi
c0106503: e8 cc 2f 00 00                call 0xc01094d4 <RevertTransfer>
c0106508: 83 c4 10                      add esp, 16
c010650b: eb 5f                         jmp 0xc010656c <MailboxAccess+0x186>
c010650d: 51                            push ecx
c010650e: 51                            push ecx
c010650f: 8d 4d e0                      lea ecx, [ebp - 32]
c0106512: 51                            push ecx
c0106513: 52                            push edx
```

```
c010656a: eb 08                   jmp 0xc0106574 <MailboxAccess+0x18e>
c010656c: 83 7d d0 00             cmp dword ptr [ebp - 48], 0
c0106570: 74 dd                   je 0xc010654f <MailboxAccess+0x169>
c0106572: eb b9                   jmp 0xc010652d <MailboxAccess+0x147>
c0106574: 8b 45 d0                mov eax, dword ptr [ebp - 48]
c0106577: 8d 65 f4                lea esp, [ebp - 12]
c010657a: 5b                      pop ebx
c010657b: 5e                      pop esi
c010657c: 5f                      pop edi
c010657d: 5d                      pop ebp
c010657e: c3                      ret

c010657f <CreateMessageBox>:
c010657f: 55                      push ebp
c0106580: 57                      push edi
c0106581: 56                      push esi
c0106582: 53                      push ebx
c0106583: 83 ec 18                sub esp, 24
c0106586: 6a 2c                   push 44
c0106588: e8 c2 d3 ff ff          call 0xc010394f <AllocHeap>
c010658d: 89 c3                   mov ebx, eax
c010658f: 58                      pop eax
c0106590: ff 74 24 2c             push dword ptr [esp + 44]
c0106594: e8 5c ad ff ff          call 0xc01012f5 <strdup>
c0106599: 89 c5                   mov ebp, eax
c010659b: e8 98 b4 ff ff          call 0xc0101a38 <ListCreate>
c01065a0: 89 c6                   mov esi, eax
c01065a2: 83 c4 0c                add esp, 12
c01065a5: 68 00 00 00 40          push 1073741824
c01065aa: 68 00 00 00 40          push 1073741824
c01065af: 68 b9 0d 11 c0          push 3222343097
c01065b4: e8 20 01 00 00          call 0xc01066d9 <CreateSemaphore>
c01065b9: 89 c2                   mov edx, eax
c01065bb: b9 0b 00 00 00          mov ecx, 11
c01065c0: 31 c0                   xor eax, eax
c01065c2: 89 df                   mov edi, ebx
c01065c4: f3 ab                   rep  stosd dword ptr es:[edi], eax
c01065c6: 89 2b                   mov dword ptr [ebx], ebp
c01065c8: 8b 44 24 34             mov eax, dword ptr [esp + 52]
c01065cc: 89 43 04                mov dword ptr [ebx + 4], eax
c01065cf: 89 73 08                mov dword ptr [ebx + 8], esi
c01065d2: 89 53 28                mov dword ptr [ebx + 40], edx
c01065d5: 83 c4 0c                add esp, 12
c01065d8: 6a 03                   push 3
c01065da: 68 c1 0d 11 c0          push 3222343105
c01065df: 8d 43 0c                lea eax, [ebx + 12]
c01065e2: 50                      push eax
c01065e3: e8 57 03 00 00          call 0xc010693f <InitSpinlock>
c01065e8: 89 d8                   mov eax, ebx
c01065ea: 83 c4 1c                add esp, 28
c01065ed: 5b                      pop ebx
c01065ee: 5e                      pop esi
c01065ef: 5f                      pop edi
c01065f0: 5d                      pop ebp
c01065f1: c3                      ret

c01065f2 <DestroyMessageBox>:
c01065f2: 53                      push ebx
c01065f3: 83 ec 14                sub esp, 20
c01065f6: 8b 5c 24 1c             mov ebx, dword ptr [esp + 28]
c01065fa: ff 73 08                push dword ptr [ebx + 8]
c01065fd: e8 ae b5 ff ff          call 0xc0101bb0 <ListDestroy>
c0106602: 58                      pop eax
c0106603: ff 33                   push dword ptr [ebx]
c0106605: e8 69 d3 ff ff          call 0xc0103973 <FreeHeap>
c010660a: 89 5c 24 20             mov dword ptr [esp + 32], ebx
c010660e: 83 c4 18                add esp, 24
c0106611: 5b                      pop ebx
c0106612: e9 5c d3 ff ff          jmp 0xc0103973 <FreeHeap>

c0106617 <SendMessage>:
```

```
c0106664: 5e                            pop esi
c0106665: 5f                            pop edi
c0106666: 5d                            pop ebp
c0106667: c3                            ret

c0106668 <ReceiveMessage>:
c0106668: 55                            push ebp
c0106669: 57                            push edi
c010666a: 56                            push esi
c010666b: 53                            push ebx
c010666c: 83 ec 14                      sub esp, 20
c010666f: 8b 74 24 28                   mov esi, dword ptr [esp + 40]
c0106673: 6a ff                         push -1
c0106675: ff 76 28                      push dword ptr [esi + 40]
c0106678: e8 bc 00 00 00                call 0xc0106739 <AcquireSemaphore>
c010667d: 89 c5                         mov ebp, eax
c010667f: 83 c4 10                      add esp, 16
c0106682: 85 c0                         test eax, eax
c0106684: 75 49                         jne 0xc01066cf <ReceiveMessage+0x67>
c0106686: 8d 7e 0c                      lea edi, [esi + 12]
c0106689: 83 ec 0c                      sub esp, 12
c010668c: 57                            push edi
c010668d: e8 c8 02 00 00                call 0xc010695a <AcquireSpinlock>
c0106692: 58                            pop eax
c0106693: ff 76 08                      push dword ptr [esi + 8]
c0106696: e8 3e b5 ff ff                call 0xc0101bd9 <ListGetNextNode>
c010669b: 89 04 24                      mov dword ptr [esp], eax
c010669e: e8 52 b5 ff ff                call 0xc0101bf5 <ListGetDataFromNode>
c01066a3: 89 c3                         mov ebx, eax
c01066a5: 5a                            pop edx
c01066a6: 59                            pop ecx
c01066a7: 6a 00                         push 0
c01066a9: ff 76 08                      push dword ptr [esi + 8]
c01066ac: e8 77 b4 ff ff                call 0xc0101b28 <ListDeleteIndex>
c01066b1: 89 3c 24                      mov dword ptr [esp], edi
c01066b4: e8 f1 02 00 00                call 0xc01069aa <ReleaseSpinlock>
c01066b9: 8b 4e 04                      mov ecx, dword ptr [esi + 4]
c01066bc: 8b 7c 24 34                   mov edi, dword ptr [esp + 52]
c01066c0: 89 de                         mov esi, ebx
c01066c2: f3 a4                         rep  movsb byte ptr es:[edi], byte ptr [esi]
c01066c4: 89 1c 24                      mov dword ptr [esp], ebx
c01066c7: e8 a7 d2 ff ff                call 0xc0103973 <FreeHeap>
c01066cc: 83 c4 10                      add esp, 16
c01066cf: 89 e8                         mov eax, ebp
c01066d1: 83 c4 0c                      add esp, 12
c01066d4: 5b                            pop ebx
c01066d5: 5e                            pop esi
c01066d6: 5f                            pop edi
c01066d7: 5d                            pop ebp
c01066d8: c3                            ret

c01066d9 <CreateSemaphore>:
c01066d9: 53                            push ebx
c01066da: 83 ec 14                      sub esp, 20
c01066dd: 6a 18                         push 24
c01066df: e8 6b d2 ff ff                call 0xc010394f <AllocHeap>
c01066e4: 89 c3                         mov ebx, eax
c01066e6: 8b 44 24 20                   mov eax, dword ptr [esp + 32]
c01066ea: 89 03                         mov dword ptr [ebx], eax
c01066ec: 8b 44 24 24                   mov eax, dword ptr [esp + 36]
c01066f0: 89 43 04                      mov dword ptr [ebx + 4], eax
c01066f3: 8b 44 24 28                   mov eax, dword ptr [esp + 40]
c01066f7: 89 43 08                      mov dword ptr [ebx + 8], eax
c01066fa: 58                            pop eax
c01066fb: 5a                            pop edx
c01066fc: 6a 02                         push 2
c01066fe: 8d 43 0c                      lea eax, [ebx + 12]
c0106701: 50                            push eax
c0106702: e8 1b 14 00 00                call 0xc0107b22 <ThreadListInit>
c0106707: 89 d8                         mov eax, ebx
c0106709: 83 c4 18                      add esp, 24
```

```
c010673d: 83 ec 0c                  sub esp, 12
c0106740: 8b 74 24 20               mov esi, dword ptr [esp + 32]
c0106744: 8b 6c 24 24               mov ebp, dword ptr [esp + 36]
c0106748: e8 22 cc ff ff            call 0xc010336f <GetIrql>
c010674d: 85 c0                     test eax, eax
c010674f: 74 17                     je 0xc0106768 <AcquireSemaphore+0x2f>
c0106751: 8b 1e                     mov ebx, dword ptr [esi]
c0106753: e8 17 cc ff ff            call 0xc010336f <GetIrql>
c0106758: 57                        push edi
c0106759: 53                        push ebx
c010675a: 50                        push eax
c010675b: 68 c9 0d 11 c0            push 3222343113
c0106760: e8 60 23 00 00            call 0xc0108ac5 <LogWriteSerial>
c0106765: 83 c4 10                  add esp, 16
c0106768: e8 da 0e 00 00            call 0xc0107647 <LockScheduler>
c010676d: 0f 21 d8                  mov eax, dr3
c0106770: c1 e0 06                  shl eax, 6
c0106773: 8b 98 c4 40 11 c0         mov ebx, dword ptr [eax - 1072611132]
c0106779: 85 db                     test ebx, ebx
c010677b: 75 20                     jne 0xc010679d <AcquireSemaphore+0x64>
c010677d: 8b 46 08                  mov eax, dword ptr [esi + 8]
c0106780: 3b 46 04                  cmp eax, dword ptr [esi + 4]
c0106783: 7d 0e                     jge 0xc0106793 <AcquireSemaphore+0x5a>
c0106785: 40                        inc eax
c0106786: 89 46 08                  mov dword ptr [esi + 8], eax
c0106789: e8 0d 0f 00 00            call 0xc010769b <UnlockScheduler>
c010678e: e9 88 00 00 00            jmp 0xc010681b <AcquireSemaphore+0xe2>
c0106793: 83 ec 0c                  sub esp, 12
c0106796: 6a 13                     push 19
c0106798: e8 02 24 00 00            call 0xc0108b9f <Panic>
c010679d: c6 43 44 00               mov byte ptr [ebx + 68], 0
c01067a1: 8b 46 08                  mov eax, dword ptr [esi + 8]
c01067a4: 3b 46 04                  cmp eax, dword ptr [esi + 4]
c01067a7: 7d 06                     jge 0xc01067af <AcquireSemaphore+0x76>
c01067a9: 40                        inc eax
c01067aa: 89 46 08                  mov dword ptr [esi + 8], eax
c01067ad: eb 61                     jmp 0xc0106810 <AcquireSemaphore+0xd7>
c01067af: 89 73 48                  mov dword ptr [ebx + 72], esi
c01067b2: 85 ed                     test ebp, ebp
c01067b4: 75 06                     jne 0xc01067bc <AcquireSemaphore+0x83>
c01067b6: c6 43 44 01               mov byte ptr [ebx + 68], 1
c01067ba: eb 54                     jmp 0xc0106810 <AcquireSemaphore+0xd7>
c01067bc: 83 fd ff                  cmp ebp, -1
c01067bf: 8d 46 0c                  lea eax, [esi + 12]
c01067c2: 75 12                     jne 0xc01067d6 <AcquireSemaphore+0x9d>
c01067c4: 51                        push ecx
c01067c5: 51                        push ecx
c01067c6: 53                        push ebx
c01067c7: 50                        push eax
c01067c8: e8 8b 13 00 00            call 0xc0107b58 <ThreadListInsert>
c01067cd: c7 04 24 03 00 00 00      mov dword ptr [esp], 3
c01067d4: eb 32                     jmp 0xc0106808 <AcquireSemaphore+0xcf>
c01067d6: 52                        push edx
c01067d7: 52                        push edx
c01067d8: 53                        push ebx
c01067d9: 50                        push eax
c01067da: e8 79 13 00 00            call 0xc0107b58 <ThreadListInsert>
c01067df: e8 64 15 00 00            call 0xc0107d48 <GetSystemTimer>
c01067e4: 89 c6                     mov esi, eax
c01067e6: 89 d7                     mov edi, edx
c01067e8: b8 40 42 0f 00            mov eax, 1000000
c01067ed: f7 ed                     imul ebp
c01067ef: 01 f0                     add eax, esi
c01067f1: 11 fa                     adc edx, edi
c01067f3: 89 43 64                  mov dword ptr [ebx + 100], eax
c01067f6: 89 53 68                  mov dword ptr [ebx + 104], edx
c01067f9: 89 1c 24                  mov dword ptr [esp], ebx
c01067fc: e8 9e 15 00 00            call 0xc0107d9f <QueueForSleep>
c0106801: c7 04 24 04 00 00 00      mov dword ptr [esp], 4
c0106808: e8 9c 0b 00 00            call 0xc01073a9 <BlockThread>
c010680d: 83 c4 10                  add esp, 16
```

```
c010684c: 75 17                         jne 0xc0106865 <ReleaseSemaphoreEx+0x33>
c010684e: 8b 47 08                      mov eax, dword ptr [edi + 8]
c0106851: 85 c0                         test eax, eax
c0106853: 75 0a                         jne 0xc010685f <ReleaseSemaphoreEx+0x2d>
c0106855: 83 ec 0c                      sub esp, 12
c0106858: 6a 1a                         push 26
c010685a: e8 40 23 00 00                call 0xc0108b9f <Panic>
c010685f: 48                            dec eax
c0106860: 89 47 08                      mov dword ptr [edi + 8], eax
c0106863: eb 3a                         jmp 0xc010689f <ReleaseSemaphoreEx+0x6d>
c0106865: 83 ec 0c                      sub esp, 12
c0106868: 8d 47 0c                      lea eax, [edi + 12]
c010686b: 50                            push eax
c010686c: e8 36 13 00 00                call 0xc0107ba7 <ThreadListDeleteTop>
c0106871: 89 c3                         mov ebx, eax
c0106873: 83 c4 10                      add esp, 16
c0106876: 83 78 24 04                   cmp dword ptr [eax + 36], 4
c010687a: 75 17                         jne 0xc0106893 <ReleaseSemaphoreEx+0x61>
c010687c: 83 ec 0c                      sub esp, 12
c010687f: 50                            push eax
c0106880: e8 3d 15 00 00                call 0xc0107dc2 <TryDequeueForSleep>
c0106885: 83 c4 10                      add esp, 16
c0106888: 84 c0                         test al, al
c010688a: 74 13                         je 0xc010689f <ReleaseSemaphoreEx+0x6d>
c010688c: c7 43 24 01 00 00 00          mov dword ptr [ebx + 36], 1
c0106893: 83 ec 0c                      sub esp, 12
c0106896: 53                            push ebx
c0106897: e8 25 0b 00 00                call 0xc01073c1 <UnblockThread>
c010689c: 83 c4 10                      add esp, 16
c010689f: 39 f5                         cmp ebp, esi
c01068a1: 74 06                         je 0xc01068a9 <ReleaseSemaphoreEx+0x77>
c01068a3: 83 7f 08 00                   cmp dword ptr [edi + 8], 0
c01068a7: 7f 9e                         jg 0xc0106847 <ReleaseSemaphoreEx+0x15>
c01068a9: 89 f0                         mov eax, esi
c01068ab: 83 c4 0c                      add esp, 12
c01068ae: 5b                            pop ebx
c01068af: 5e                            pop esi
c01068b0: 5f                            pop edi
c01068b1: 5d                            pop ebp
c01068b2: c3                            ret

c01068b3 <ReleaseSemaphore>:
c01068b3: 53                            push ebx
c01068b4: 83 ec 08                      sub esp, 8
c01068b7: 8b 5c 24 10                   mov ebx, dword ptr [esp + 16]
c01068bb: e8 87 0d 00 00                call 0xc0107647 <LockScheduler>
c01068c0: 52                            push edx
c01068c1: 52                            push edx
c01068c2: 6a 01                         push 1
c01068c4: 53                            push ebx
c01068c5: e8 68 ff ff ff                call 0xc0106832 <ReleaseSemaphoreEx>
c01068ca: 83 c4 18                      add esp, 24
c01068cd: 5b                            pop ebx
c01068ce: e9 c8 0d 00 00                jmp 0xc010769b <UnlockScheduler>

c01068d3 <DestroySemaphore>:
c01068d3: 56                            push esi
c01068d4: 53                            push ebx
c01068d5: 51                            push ecx
c01068d6: 8b 5c 24 10                   mov ebx, dword ptr [esp + 16]
c01068da: 8b 74 24 14                   mov esi, dword ptr [esp + 20]
c01068de: e8 64 0d 00 00                call 0xc0107647 <LockScheduler>
c01068e3: 83 fe 01                      cmp esi, 1
c01068e6: 75 0b                         jne 0xc01068f3 <DestroySemaphore+0x20>
c01068e8: be 1e 00 00 00                mov esi, 30
c01068ed: 83 7b 08 00                   cmp dword ptr [ebx + 8], 0
c01068f1: eb 10                         jmp 0xc0106903 <DestroySemaphore+0x30>
c01068f3: 83 fe 02                      cmp esi, 2
c01068f6: 75 0d                         jne 0xc0106905 <DestroySemaphore+0x32>
c01068f8: be 1e 00 00 00                mov esi, 30
c01068fd: 8b 43 04                      mov eax, dword ptr [ebx + 4]
```

```
c010693f <InitSpinlock>:
c010693f: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c0106943: 31 d2                         xor edx, edx
c0106945: 89 10                         mov dword ptr [eax], edx
c0106947: 8b 54 24 0c                   mov edx, dword ptr [esp + 12]
c010694b: 89 50 14                      mov dword ptr [eax + 20], edx
c010694e: 83 c0 04                      add eax, 4
c0106951: 89 44 24 04                   mov dword ptr [esp + 4], eax
c0106955: e9 65 a8 ff ff                jmp 0xc01011bf <strcpy>

c010695a <AcquireSpinlock>:
c010695a: 56                            push esi
c010695b: 53                            push ebx
c010695c: 52                            push edx
c010695d: 8b 5c 24 10                   mov ebx, dword ptr [esp + 16]
c0106961: 83 3b 00                      cmp dword ptr [ebx], 0
c0106964: 74 0d                         je 0xc0106973 <AcquireSpinlock+0x19>
c0106966: 50                            push eax
c0106967: 50                            push eax
c0106968: 83 c3 04                      add ebx, 4
c010696b: 53                            push ebx
c010696c: 6a 24                         push 36
c010696e: e8 db 21 00 00                call 0xc0108b4e <PanicEx>
c0106973: 83 ec 0c                      sub esp, 12
c0106976: ff 73 14                      push dword ptr [ebx + 20]
c0106979: e8 fe c9 ff ff                call 0xc010337c <RaiseIrql>
c010697e: 89 c6                         mov esi, eax
c0106980: 8b 43 14                      mov eax, dword ptr [ebx + 20]
c0106983: 83 c4 10                      add esp, 16
c0106986: 39 f0                         cmp eax, esi
c0106988: 7e 0c                         jle 0xc0106996 <AcquireSpinlock+0x3c>
c010698a: 83 ec 0c                      sub esp, 12
c010698d: 50                            push eax
c010698e: e8 e9 c9 ff ff                call 0xc010337c <RaiseIrql>
c0106993: 83 c4 10                      add esp, 16
c0106996: 83 ec 0c                      sub esp, 12
c0106999: 53                            push ebx
c010699a: e8 21 7c 00 00                call 0xc010e5c0 <ArchSpinlockAcquire>
c010699f: 89 73 18                      mov dword ptr [ebx + 24], esi
c01069a2: 89 f0                         mov eax, esi
c01069a4: 83 c4 14                      add esp, 20
c01069a7: 5b                            pop ebx
c01069a8: 5e                            pop esi
c01069a9: c3                            ret

c01069aa <ReleaseSpinlock>:
c01069aa: 53                            push ebx
c01069ab: 83 ec 08                      sub esp, 8
c01069ae: 8b 44 24 10                   mov eax, dword ptr [esp + 16]
c01069b2: 83 38 00                      cmp dword ptr [eax], 0
c01069b5: 75 0d                         jne 0xc01069c4 <ReleaseSpinlock+0x1a>
c01069b7: 52                            push edx
c01069b8: 52                            push edx
c01069b9: 83 c0 04                      add eax, 4
c01069bc: 50                            push eax
c01069bd: 6a 25                         push 37
c01069bf: e8 8a 21 00 00                call 0xc0108b4e <PanicEx>
c01069c4: 8b 58 18                      mov ebx, dword ptr [eax + 24]
c01069c7: 83 ec 0c                      sub esp, 12
c01069ca: 50                            push eax
c01069cb: e8 08 7c 00 00                call 0xc010e5d8 <ArchSpinlockRelease>
c01069d0: 89 5c 24 20                   mov dword ptr [esp + 32], ebx
c01069d4: 83 c4 18                      add esp, 24
c01069d7: 5b                            pop ebx
c01069d8: e9 db c9 ff ff                jmp 0xc01033b8 <LowerIrql>

c01069dd <IsSpinlockHeld>:
c01069dd: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c01069e1: 83 38 00                      cmp dword ptr [eax], 0
c01069e4: 0f 95 c0                      setne al
```

```
c0106a31 <CleanerThread>:
c0106a31: 83 ec 1c                  sub esp, 28
c0106a34: 50                        push eax
c0106a35: 50                        push eax
c0106a36: 8d 44 24 14               lea eax, [esp + 20]
c0106a3a: 50                        push eax
c0106a3b: ff 35 28 b1 13 c0         push dword ptr [-1072451288]
c0106a41: e8 22 fc ff ff            call 0xc0106668 <ReceiveMessage>
c0106a46: 8b 44 24 1c               mov eax, dword ptr [esp + 28]
c0106a4a: 8b 50 0c                  mov edx, dword ptr [eax + 12]
c0106a4d: 59                        pop ecx
c0106a4e: 59                        pop ecx
c0106a4f: 52                        push edx
c0106a50: 8b 00                     mov eax, dword ptr [eax]
c0106a52: 29 d0                     sub eax, edx
c0106a54: 50                        push eax
c0106a55: e8 9e ea ff ff            call 0xc01054f8 <UnmapVirt>
c0106a5a: 58                        pop eax
c0106a5b: 8b 44 24 18               mov eax, dword ptr [esp + 24]
c0106a5f: ff 70 34                  push dword ptr [eax + 52]
c0106a62: e8 0c cf ff ff            call 0xc0103973 <FreeHeap>
c0106a67: 58                        pop eax
c0106a68: ff 74 24 18               push dword ptr [esp + 24]
c0106a6c: e8 02 cf ff ff            call 0xc0103973 <FreeHeap>
c0106a71: 83 c4 10                  add esp, 16
c0106a74: eb be                     jmp 0xc0106a34 <CleanerThread+0x3>

c0106a76 <TerminateThread>:
c0106a76: 83 ec 0c                  sub esp, 12
c0106a79: e8 c9 0b 00 00            call 0xc0107647 <LockScheduler>
c0106a7e: 0f 21 d8                  mov eax, dr3
c0106a81: 8b 54 24 10               mov edx, dword ptr [esp + 16]
c0106a85: c1 e0 06                  shl eax, 6
c0106a88: 39 90 c4 40 11 c0         cmp dword ptr [eax - 1072611132], edx
c0106a8e: 75 23                     jne 0xc0106ab3 <TerminateThread+0x3d>
c0106a90: 50                        push eax
c0106a91: 50                        push eax
c0106a92: 8d 44 24 18               lea eax, [esp + 24]
c0106a96: 50                        push eax
c0106a97: ff 35 28 b1 13 c0         push dword ptr [-1072451288]
c0106a9d: e8 75 fb ff ff            call 0xc0106617 <SendMessage>
c0106aa2: c7 04 24 05 00 00 00      mov dword ptr [esp], 5
c0106aa9: e8 fb 08 00 00            call 0xc01073a9 <BlockThread>
c0106aae: 83 c4 10                  add esp, 16
c0106ab1: eb 04                     jmp 0xc0106ab7 <TerminateThread+0x41>
c0106ab3: c6 42 46 01               mov byte ptr [edx + 70], 1
c0106ab7: e8 df 0b 00 00            call 0xc010769b <UnlockScheduler>
c0106abc: 83 c4 0c                  add esp, 12
c0106abf: c3                        ret

c0106ac0 <InitCleaner>:
c0106ac0: 83 ec 14                  sub esp, 20
c0106ac3: 6a 04                     push 4
c0106ac5: 68 f6 0d 11 c0            push 3222343158
c0106aca: e8 b0 fa ff ff            call 0xc010657f <CreateMessageBox>
c0106acf: a3 28 b1 13 c0            mov dword ptr [3222516008], eax
c0106ad4: e8 a0 db ff ff            call 0xc0104679 <GetVas>
c0106ad9: 68 f6 0d 11 c0            push 3222343158
c0106ade: 50                        push eax
c0106adf: 6a 00                     push 0
c0106ae1: 68 31 6a 10 c0            push 3222301233
c0106ae6: e8 5d 0e 00 00            call 0xc0107948 <CreateThread>
c0106aeb: 83 c4 2c                  add esp, 44
c0106aee: c3                        ret

c0106aef <IdleThread>:
c0106aef: 83 ec 0c                  sub esp, 12
c0106af2: e8 bc 7a 00 00            call 0xc010e5b3 <ArchStallProcessor>
c0106af7: eb f9                     jmp 0xc0106af2 <IdleThread+0x3>
```

```
c0106b3d: 53                            push ebx
c0106b3e: 83 ec 10                      sub esp, 16
c0106b41: 89 c6                         mov esi, eax
c0106b43: 68 34 b1 13 c0                push 3222516020
c0106b48: e8 0d fe ff ff                call 0xc010695a <AcquireSpinlock>
c0106b4d: 8b 1d 10 31 11 c0             mov ebx, dword ptr [-1072615152]
c0106b53: 8d 43 01                      lea eax, [ebx + 1]
c0106b56: a3 10 31 11 c0                mov dword ptr [3222352144], eax
c0106b5b: c7 04 24 34 b1 13 c0          mov dword ptr [esp], 3222516020
c0106b62: e8 43 fe ff ff                call 0xc01069aa <ReleaseSpinlock>
c0106b67: 58                            pop eax
c0106b68: 5a                            pop edx
c0106b69: 6a ff                         push -1
c0106b6b: ff 35 2c b1 13 c0             push dword ptr [-1072451284]
c0106b71: e8 c3 fb ff ff                call 0xc0106739 <AcquireSemaphore>
c0106b76: c7 04 24 08 00 00 00          mov dword ptr [esp], 8
c0106b7d: e8 cd cd ff ff                call 0xc010394f <AllocHeap>
c0106b82: 89 18                         mov dword ptr [eax], ebx
c0106b84: 89 70 04                      mov dword ptr [eax + 4], esi
c0106b87: 59                            pop ecx
c0106b88: 5e                            pop esi
c0106b89: 50                            push eax
c0106b8a: ff 35 30 b1 13 c0             push dword ptr [-1072451280]
c0106b90: e8 f5 b4 ff ff                call 0xc010208a <TreeInsert>
c0106b95: 58                            pop eax
c0106b96: ff 35 2c b1 13 c0             push dword ptr [-1072451284]
c0106b9c: e8 12 fd ff ff                call 0xc01068b3 <ReleaseSemaphore>
c0106ba1: 89 d8                         mov eax, ebx
c0106ba3: 83 c4 14                      add esp, 20
c0106ba6: 5b                            pop ebx
c0106ba7: 5e                            pop esi
c0106ba8: c3                            ret

c0106ba9 <LockProcess>:
c0106ba9: 83 ec 14                      sub esp, 20
c0106bac: 6a ff                         push -1
c0106bae: 8b 44 24 1c                   mov eax, dword ptr [esp + 28]
c0106bb2: ff 70 14                      push dword ptr [eax + 20]
c0106bb5: e8 7f fb ff ff                call 0xc0106739 <AcquireSemaphore>
c0106bba: 83 c4 1c                      add esp, 28
c0106bbd: c3                            ret

c0106bbe <UnlockProcess>:
c0106bbe: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c0106bc2: 8b 40 14                      mov eax, dword ptr [eax + 20]
c0106bc5: 89 44 24 04                   mov dword ptr [esp + 4], eax
c0106bc9: e9 e5 fc ff ff                jmp 0xc01068b3 <ReleaseSemaphore>

c0106bce <InitProcess>:
c0106bce: 83 ec 10                      sub esp, 16
c0106bd1: 6a 03                         push 3
c0106bd3: 68 0a 0e 11 c0                push 3222343178
c0106bd8: 68 34 b1 13 c0                push 3222516020
c0106bdd: e8 5d fd ff ff                call 0xc010693f <InitSpinlock>
c0106be2: 83 c4 0c                      add esp, 12
c0106be5: 6a 00                         push 0
c0106be7: 6a 01                         push 1
c0106be9: 68 0e 0e 11 c0                push 3222343182
c0106bee: e8 e6 fa ff ff                call 0xc01066d9 <CreateSemaphore>
c0106bf3: a3 2c b1 13 c0                mov dword ptr [3222516012], eax
c0106bf8: e8 50 b4 ff ff                call 0xc010204d <TreeCreate>
c0106bfd: a3 30 b1 13 c0                mov dword ptr [3222516016], eax
c0106c02: 5a                            pop edx
c0106c03: 59                            pop ecx
c0106c04: 68 22 6b 10 c0                push 3222301474
c0106c09: 50                            push eax
c0106c0a: e8 6c b4 ff ff                call 0xc010207b <TreeSetComparator>
c0106c0f: 83 c4 1c                      add esp, 28
c0106c12: c3                            ret

c0106c13 <AddThreadToProcess>:
```

```
c0106c59: ff 73 04                  push dword ptr [ebx + 4]
c0106c5c: e8 e1 ff ff ff            call 0xc0106c42 <RecursivelyKillRemainingThre
c0106c61: 8b 43 08                  mov eax, dword ptr [ebx + 8]
c0106c64: 83 c4 10                  add esp, 16
c0106c67: 83 78 24 05               cmp dword ptr [eax + 36], 5
c0106c6b: 74 13                     je 0xc0106c80 <RecursivelyKillRemainingThread
c0106c6d: 80 78 46 00               cmp byte ptr [eax + 70], 0
c0106c71: 75 0d                     jne 0xc0106c80 <RecursivelyKillRemainingThrea
c0106c73: 89 44 24 10               mov dword ptr [esp + 16], eax
c0106c77: 83 c4 08                  add esp, 8
c0106c7a: 5b                        pop ebx
c0106c7b: e9 f6 fd ff ff            jmp 0xc0106a76 <TerminateThread>
c0106c80: 83 c4 08                  add esp, 8
c0106c83: 5b                        pop ebx
c0106c84: c3                        ret

c0106c85 <GetProcess>:
c0106c85: 0f 21 d8                  mov eax, dr3
c0106c88: c1 e0 06                  shl eax, 6
c0106c8b: 8b 80 c4 40 11 c0         mov eax, dword ptr [eax - 1072611132]
c0106c91: 85 c0                     test eax, eax
c0106c93: 74 03                     je 0xc0106c98 <GetProcess+0x13>
c0106c95: 8b 40 4c                  mov eax, dword ptr [eax + 76]
c0106c98: c3                        ret

c0106c99 <KillProcess>:
c0106c99: 53                        push ebx
c0106c9a: 83 ec 08                  sub esp, 8
c0106c9d: 8b 54 24 10               mov edx, dword ptr [esp + 16]
c0106ca1: e8 df ff ff ff            call 0xc0106c85 <GetProcess>
c0106ca6: 89 c3                     mov ebx, eax
c0106ca8: 89 50 20                  mov dword ptr [eax + 32], edx
c0106cab: e8 e1 ec ff ff            call 0xc0105991 <GetKernelVas>
c0106cb0: 6a 00                     push 0
c0106cb2: 6a 00                     push 0
c0106cb4: 6a 00                     push 0
c0106cb6: 6a 00                     push 0
c0106cb8: 68 1a 0e 11 c0            push 3222343194
c0106cbd: 50                        push eax
c0106cbe: 53                        push ebx
c0106cbf: 68 d0 6e 10 c0            push 3222302416
c0106cc4: e8 25 0b 00 00            call 0xc01077ee <CreateThreadEx>
c0106cc9: 0f 21 d8                  mov eax, dr3
c0106ccc: c1 e0 06                  shl eax, 6
c0106ccf: 8b 80 c4 40 11 c0         mov eax, dword ptr [eax - 1072611132]
c0106cd5: 89 44 24 30               mov dword ptr [esp + 48], eax
c0106cd9: 83 c4 28                  add esp, 40
c0106cdc: 5b                        pop ebx
c0106cdd: e9 94 fd ff ff            jmp 0xc0106a76 <TerminateThread>

c0106ce2 <GetFdTable>:
c0106ce2: 8b 44 24 04               mov eax, dword ptr [esp + 4]
c0106ce6: 85 c0                     test eax, eax
c0106ce8: 74 03                     je 0xc0106ced <GetFdTable+0xb>
c0106cea: 8b 40 1c                  mov eax, dword ptr [eax + 28]
c0106ced: c3                        ret

c0106cee <GetProcessFromPid>:
c0106cee: 83 ec 34                  sub esp, 52
c0106cf1: 6a ff                     push -1
c0106cf3: ff 35 2c b1 13 c0         push dword ptr [-1072451284]
c0106cf9: e8 3b fa ff ff            call 0xc0106739 <AcquireSemaphore>
c0106cfe: 31 c0                     xor eax, eax
c0106d00: 89 44 24 2c               mov dword ptr [esp + 44], eax
c0106d04: 8b 44 24 40               mov eax, dword ptr [esp + 64]
c0106d08: 89 44 24 28               mov dword ptr [esp + 40], eax
c0106d0c: 5a                        pop edx
c0106d0d: 59                        pop ecx
c0106d0e: 8d 44 24 20               lea eax, [esp + 32]
c0106d12: 50                        push eax
c0106d13: ff 35 30 b1 13 c0         push dword ptr [-1072451280]
```

```
c0106d67: 89 04 24                mov dword ptr [esp], eax
c0106d6a: e8 3a fe ff ff          call 0xc0106ba9 <LockProcess>
c0106d6f: 8b 03                   mov eax, dword ptr [ebx]
c0106d71: 89 46 04                mov dword ptr [esi + 4], eax
c0106d74: 59                      pop ecx
c0106d75: 58                      pop eax
c0106d76: 56                      push esi
c0106d77: ff 73 0c                push dword ptr [ebx + 12]
c0106d7a: e8 0b b3 ff ff          call 0xc010208a <TreeInsert>
c0106d7f: 58                      pop eax
c0106d80: ff 73 18                push dword ptr [ebx + 24]
c0106d83: e8 2b fb ff ff          call 0xc01068b3 <ReleaseSemaphore>
c0106d88: 89 1c 24                mov dword ptr [esp], ebx
c0106d8b: e8 2e fe ff ff          call 0xc0106bbe <UnlockProcess>
c0106d90: 83 c4 14                add esp, 20
c0106d93: 5b                      pop ebx
c0106d94: 5e                      pop esi
c0106d95: c3                      ret
c0106d96: c3                      ret

c0106d97 <ReapProcess>:
c0106d97: 56                      push esi
c0106d98: 53                      push ebx
c0106d99: 83 ec 1c                sub esp, 28
c0106d9c: 89 c3                   mov ebx, eax
c0106d9e: 6a 02                   push 2
c0106da0: ff 70 18                push dword ptr [eax + 24]
c0106da3: e8 2b fb ff ff          call 0xc01068d3 <DestroySemaphore>
c0106da8: 5e                      pop esi
c0106da9: ff 73 08                push dword ptr [ebx + 8]
c0106dac: e8 1b ed ff ff          call 0xc0105acc <DestroyVas>
c0106db1: 58                      pop eax
c0106db2: ff 73 1c                push dword ptr [ebx + 28]
c0106db5: e8 15 22 00 00          call 0xc0108fcf <DestroyFdTable>
c0106dba: 8b 33                   mov esi, dword ptr [ebx]
c0106dbc: 58                      pop eax
c0106dbd: 5a                      pop edx
c0106dbe: 6a ff                   push -1
c0106dc0: ff 35 2c b1 13 c0       push dword ptr [-1072451284]
c0106dc6: e8 6e f9 ff ff          call 0xc0106739 <AcquireSemaphore>
c0106dcb: 31 c9                   xor ecx, ecx
c0106dcd: 89 4c 24 1c             mov dword ptr [esp + 28], ecx
c0106dd1: 89 74 24 18             mov dword ptr [esp + 24], esi
c0106dd5: 5e                      pop esi
c0106dd6: 58                      pop eax
c0106dd7: 8d 44 24 10             lea eax, [esp + 16]
c0106ddb: 50                      push eax
c0106ddc: ff 35 30 b1 13 c0       push dword ptr [-1072451280]
c0106de2: e8 19 b3 ff ff          call 0xc0102100 <TreeGet>
c0106de7: 89 c6                   mov esi, eax
c0106de9: 5a                      pop edx
c0106dea: 59                      pop ecx
c0106deb: 50                      push eax
c0106dec: ff 35 30 b1 13 c0       push dword ptr [-1072451280]
c0106df2: e8 d5 b2 ff ff          call 0xc01020cc <TreeDelete>
c0106df7: 89 34 24                mov dword ptr [esp], esi
c0106dfa: e8 74 cb ff ff          call 0xc0103973 <FreeHeap>
c0106dff: 5e                      pop esi
c0106e00: ff 35 2c b1 13 c0       push dword ptr [-1072451284]
c0106e06: e8 a8 fa ff ff          call 0xc01068b3 <ReleaseSemaphore>
c0106e0b: 8b 43 04                mov eax, dword ptr [ebx + 4]
c0106e0e: 83 c4 10                add esp, 16
c0106e11: 85 c0                   test eax, eax
c0106e13: 74 17                   je 0xc0106e2c <ReapProcess+0x95>
c0106e15: 83 ec 0c                sub esp, 12
c0106e18: 50                      push eax
c0106e19: e8 d0 fe ff ff          call 0xc0106cee <GetProcessFromPid>
c0106e1e: 5a                      pop edx
c0106e1f: 59                      pop ecx
c0106e20: 53                      push ebx
c0106e21: ff 70 0c                push dword ptr [eax + 12]
```

```
c0106e62: 83 ec 0c                   sub esp, 12
c0106e65: 53                         push ebx
c0106e66: e8 3e fd ff ff             call 0xc0106ba9 <LockProcess>
c0106e6b: 83 c4 10                   add esp, 16
c0106e6e: 80 7b 24 00                cmp byte ptr [ebx + 36], 0
c0106e72: 74 2e                      je 0xc0106ea2 <RecursivelyTryReap.isra.0+0x54
c0106e74: 39 3b                      cmp dword ptr [ebx], edi
c0106e76: 74 05                      je 0xc0106e7d <RecursivelyTryReap.isra.0+0x2f
c0106e78: 83 ff ff                   cmp edi, -1
c0106e7b: 75 25                      jne 0xc0106ea2 <RecursivelyTryReap.isra.0+0x5
c0106e7d: 8b 43 20                   mov eax, dword ptr [ebx + 32]
c0106e80: 89 45 00                   mov dword ptr [ebp], eax
c0106e83: 8b 13                      mov edx, dword ptr [ebx]
c0106e85: 89 54 24 0c                mov dword ptr [esp + 12], edx
c0106e89: 83 ec 0c                   sub esp, 12
c0106e8c: 53                         push ebx
c0106e8d: e8 2c fd ff ff             call 0xc0106bbe <UnlockProcess>
c0106e92: 89 d8                      mov eax, ebx
c0106e94: e8 fe fe ff ff             call 0xc0106d97 <ReapProcess>
c0106e99: 83 c4 10                   add esp, 16
c0106e9c: 8b 54 24 0c                mov edx, dword ptr [esp + 12]
c0106ea0: eb 24                      jmp 0xc0106ec6 <RecursivelyTryReap.isra.0+0x7
c0106ea2: 83 ec 0c                   sub esp, 12
c0106ea5: 53                         push ebx
c0106ea6: e8 13 fd ff ff             call 0xc0106bbe <UnlockProcess>
c0106eab: 89 e9                      mov ecx, ebp
c0106ead: 89 fa                      mov edx, edi
c0106eaf: 8b 06                      mov eax, dword ptr [esi]
c0106eb1: e8 98 ff ff ff             call 0xc0106e4e <RecursivelyTryReap.isra.0>
c0106eb6: 89 c2                      mov edx, eax
c0106eb8: 83 c4 10                   add esp, 16
c0106ebb: 85 c0                      test eax, eax
c0106ebd: 75 07                      jne 0xc0106ec6 <RecursivelyTryReap.isra.0+0x7
c0106ebf: 8b 76 04                   mov esi, dword ptr [esi + 4]
c0106ec2: eb 97                      jmp 0xc0106e5b <RecursivelyTryReap.isra.0+0xd
c0106ec4: 31 d2                      xor edx, edx
c0106ec6: 89 d0                      mov eax, edx
c0106ec8: 83 c4 1c                   add esp, 28
c0106ecb: 5b                         pop ebx
c0106ecc: 5e                         pop esi
c0106ecd: 5f                         pop edi
c0106ece: 5d                         pop ebp
c0106ecf: c3                         ret

c0106ed0 <KillProcessHelper>:
c0106ed0: 53                         push ebx
c0106ed1: 83 ec 14                   sub esp, 20
c0106ed4: 8b 5c 24 1c                mov ebx, dword ptr [esp + 28]
c0106ed8: 8b 43 10                   mov eax, dword ptr [ebx + 16]
c0106edb: ff 70 04                   push dword ptr [eax + 4]
c0106ede: e8 5f fd ff ff             call 0xc0106c42 <RecursivelyKillRemainingThre
c0106ee3: 8b 43 0c                   mov eax, dword ptr [ebx + 12]
c0106ee6: 8b 40 04                   mov eax, dword ptr [eax + 4]
c0106ee9: e8 52 fe ff ff             call 0xc0106d40 <RecursivelyMakeChildrenOrpha
c0106eee: 58                         pop eax
c0106eef: ff 73 10                   push dword ptr [ebx + 16]
c0106ef2: e8 1c b2 ff ff             call 0xc0102113 <TreeDestroy>
c0106ef7: 58                         pop eax
c0106ef8: ff 73 0c                   push dword ptr [ebx + 12]
c0106efb: e8 13 b2 ff ff             call 0xc0102113 <TreeDestroy>
c0106f00: 58                         pop eax
c0106f01: ff 73 08                   push dword ptr [ebx + 8]
c0106f04: e8 c3 eb ff ff             call 0xc0105acc <DestroyVas>
c0106f09: c6 43 24 01                mov byte ptr [ebx + 36], 1
c0106f0d: 8b 43 04                   mov eax, dword ptr [ebx + 4]
c0106f10: 83 c4 10                   add esp, 16
c0106f13: 85 c0                      test eax, eax
c0106f15: 75 09                      jne 0xc0106f20 <KillProcessHelper+0x50>
c0106f17: 89 d8                      mov eax, ebx
c0106f19: e8 79 fe ff ff             call 0xc0106d97 <ReapProcess>
c0106f1e: eb 15                      jmp 0xc0106f35 <KillProcessHelper+0x65>
```

```
c0106f74: e8 b4 d3 ff ff                call 0xc010432d <CreateVas>
c0106f79: 89 43 08                      mov dword ptr [ebx + 8], eax
c0106f7c: 89 73 04                      mov dword ptr [ebx + 4], esi
c0106f7f: e8 c9 b0 ff ff                call 0xc010204d <TreeCreate>
c0106f84: 89 43 0c                      mov dword ptr [ebx + 12], eax
c0106f87: e8 c1 b0 ff ff                call 0xc010204d <TreeCreate>
c0106f8c: 89 43 10                      mov dword ptr [ebx + 16], eax
c0106f8f: 83 c4 0c                      add esp, 12
c0106f92: 68 00 00 00 40                push 1073741824
c0106f97: 68 00 00 00 40                push 1073741824
c0106f9c: 68 2f 0e 11 c0                push 3222343215
c0106fa1: e8 33 f7 ff ff                call 0xc01066d9 <CreateSemaphore>
c0106fa6: 89 43 18                      mov dword ptr [ebx + 24], eax
c0106fa9: 31 c9                         xor ecx, ecx
c0106fab: 89 4b 20                      mov dword ptr [ebx + 32], ecx
c0106fae: c6 43 24 00                   mov byte ptr [ebx + 36], 0
c0106fb2: 89 d8                         mov eax, ebx
c0106fb4: e8 83 fb ff ff                call 0xc0106b3c <InsertIntoProcessTable.const
c0106fb9: 89 03                         mov dword ptr [ebx], eax
c0106fbb: e8 7a 1f 00 00                call 0xc0108f3a <CreateFdTable>
c0106fc0: 89 43 1c                      mov dword ptr [ebx + 28], eax
c0106fc3: 83 c4 10                      add esp, 16
c0106fc6: 85 f6                         test esi, esi
c0106fc8: 74 45                         je 0xc010700f <CreateProcess+0xc1>
c0106fca: 83 ec 0c                      sub esp, 12
c0106fcd: 56                            push esi
c0106fce: e8 1b fd ff ff                call 0xc0106cee <GetProcessFromPid>
c0106fd3: 89 c6                         mov esi, eax
c0106fd5: 89 04 24                      mov dword ptr [esp], eax
c0106fd8: e8 cc fb ff ff                call 0xc0106ba9 <LockProcess>
c0106fdd: 58                            pop eax
c0106fde: 5a                            pop edx
c0106fdf: 53                            push ebx
c0106fe0: ff 76 0c                      push dword ptr [esi + 12]
c0106fe3: e8 a2 b0 ff ff                call 0xc010208a <TreeInsert>
c0106fe8: 8b 46 28                      mov eax, dword ptr [esi + 40]
c0106feb: 89 43 28                      mov dword ptr [ebx + 40], eax
c0106fee: 83 c4 10                      add esp, 16
c0106ff1: 85 c0                         test eax, eax
c0106ff3: 74 0c                         je 0xc0107001 <CreateProcess+0xb3>
c0106ff5: 83 ec 0c                      sub esp, 12
c0106ff8: 50                            push eax
c0106ff9: e8 10 34 00 00                call 0xc010a40e <ReferenceVnode>
c0106ffe: 83 c4 10                      add esp, 16
c0107001: 83 ec 0c                      sub esp, 12
c0107004: 56                            push esi
c0107005: e8 b4 fb ff ff                call 0xc0106bbe <UnlockProcess>
c010700a: 83 c4 10                      add esp, 16
c010700d: eb 05                         jmp 0xc0107014 <CreateProcess+0xc6>
c010700f: 31 c9                         xor ecx, ecx
c0107011: 89 4b 28                      mov dword ptr [ebx + 40], ecx
c0107014: 89 d8                         mov eax, ebx
c0107016: 5a                            pop edx
c0107017: 5b                            pop ebx
c0107018: 5e                            pop esi
c0107019: c3                            ret

c010701a <CreateProcessWithEntryPoint>:
c010701a: 53                            push ebx
c010701b: 83 ec 14                      sub esp, 20
c010701e: ff 74 24 1c                   push dword ptr [esp + 28]
c0107022: e8 27 ff ff ff                call 0xc0106f4e <CreateProcess>
c0107027: 89 c3                         mov ebx, eax
c0107029: 68 3f 0e 11 c0                push 3222343231
c010702e: ff 70 08                      push dword ptr [eax + 8]
c0107031: ff 74 24 30                   push dword ptr [esp + 48]
c0107035: ff 74 24 30                   push dword ptr [esp + 48]
c0107039: e8 0a 09 00 00                call 0xc0107948 <CreateThread>
c010703e: 83 c4 18                      add esp, 24
c0107041: 50                            push eax
c0107042: 53                            push ebx
```

```
c0107098: 68 00 00 00 40              push 1073741824
c010709d: 68 2f 0e 11 c0              push 3222343215
c01070a2: e8 32 f6 ff ff              call 0xc01066d9 <CreateSemaphore>
c01070a7: 89 43 18                    mov dword ptr [ebx + 24], eax
c01070aa: 31 c9                       xor ecx, ecx
c01070ac: 89 4b 20                    mov dword ptr [ebx + 32], ecx
c01070af: c6 43 24 00                 mov byte ptr [ebx + 36], 0
c01070b3: 89 d8                       mov eax, ebx
c01070b5: e8 82 fa ff ff              call 0xc0106b3c <InsertIntoProcessTable.const
c01070ba: 89 03                       mov dword ptr [ebx], eax
c01070bc: e8 79 1e 00 00              call 0xc0108f3a <CreateFdTable>
c01070c1: 89 43 1c                    mov dword ptr [ebx + 28], eax
c01070c4: 83 c4 10                    add esp, 16
c01070c7: 85 f6                       test esi, esi
c01070c9: 74 31                       je 0xc01070fc <CreateProcessEx+0xad>
c01070cb: 83 ec 0c                    sub esp, 12
c01070ce: 56                          push esi
c01070cf: e8 1a fc ff ff              call 0xc0106cee <GetProcessFromPid>
c01070d4: 89 c6                       mov esi, eax
c01070d6: 58                          pop eax
c01070d7: 5a                          pop edx
c01070d8: 53                          push ebx
c01070d9: ff 76 0c                    push dword ptr [esi + 12]
c01070dc: e8 a9 af ff ff              call 0xc010208a <TreeInsert>
c01070e1: 8b 46 28                    mov eax, dword ptr [esi + 40]
c01070e4: 89 43 28                    mov dword ptr [ebx + 40], eax
c01070e7: 83 c4 10                    add esp, 16
c01070ea: 85 c0                       test eax, eax
c01070ec: 74 13                       je 0xc0107101 <CreateProcessEx+0xb2>
c01070ee: 83 ec 0c                    sub esp, 12
c01070f1: 50                          push eax
c01070f2: e8 17 33 00 00              call 0xc010a40e <ReferenceVnode>
c01070f7: 83 c4 10                    add esp, 16
c01070fa: eb 05                       jmp 0xc0107101 <CreateProcessEx+0xb2>
c01070fc: 31 c9                       xor ecx, ecx
c01070fe: 89 4b 28                    mov dword ptr [ebx + 40], ecx
c0107101: 89 d8                       mov eax, ebx
c0107103: 5a                          pop edx
c0107104: 5b                          pop ebx
c0107105: 5e                          pop esi
c0107106: c3                          ret

c0107107 <ForkProcess>:
c0107107: 53                          push ebx
c0107108: 83 ec 14                    sub esp, 20
c010710b: 68 49 0e 11 c0              push 3222343241
c0107110: e8 b0 19 00 00              call 0xc0108ac5 <LogWriteSerial>
c0107115: e8 6b fb ff ff              call 0xc0106c85 <GetProcess>
c010711a: 89 04 24                    mov dword ptr [esp], eax
c010711d: e8 87 fa ff ff              call 0xc0106ba9 <LockProcess>
c0107122: c7 04 24 67 0e 11 c0        mov dword ptr [esp], 3222343271
c0107129: e8 97 19 00 00              call 0xc0108ac5 <LogWriteSerial>
c010712e: e8 52 fb ff ff              call 0xc0106c85 <GetProcess>
c0107133: 5a                          pop edx
c0107134: 59                          pop ecx
c0107135: ff 30                       push dword ptr [eax]
c0107137: 68 7a 0e 11 c0              push 3222343290
c010713c: e8 84 19 00 00              call 0xc0108ac5 <LogWriteSerial>
c0107141: e8 3f fb ff ff              call 0xc0106c85 <GetProcess>
c0107146: 5b                          pop ebx
c0107147: ff 30                       push dword ptr [eax]
c0107149: e8 01 ff ff ff              call 0xc010704f <CreateProcessEx>
c010714e: 89 c3                       mov ebx, eax
c0107150: 58                          pop eax
c0107151: 5a                          pop edx
c0107152: ff 33                       push dword ptr [ebx]
c0107154: 68 89 0e 11 c0              push 3222343305
c0107159: e8 67 19 00 00              call 0xc0108ac5 <LogWriteSerial>
c010715e: 59                          pop ecx
c010715f: ff 73 08                    push dword ptr [ebx + 8]
c0107162: e8 65 e9 ff ff              call 0xc0105acc <DestroyVas>
```

```
c01071cf: 74 02                         je 0xc01071d3 <GetPid+0xc>
c01071d1: 8b 02                         mov eax, dword ptr [edx]
c01071d3: c3                            ret

c01071d4 <WaitProcess>:
c01071d4: 55                            push ebp
c01071d5: 57                            push edi
c01071d6: 56                            push esi
c01071d7: 53                            push ebx
c01071d8: 83 ec 0c                      sub esp, 12
c01071db: e8 a5 fa ff ff                call 0xc0106c85 <GetProcess>
c01071e0: 89 c6                         mov esi, eax
c01071e2: 31 db                         xor ebx, ebx
c01071e4: 8b 6c 24 28                   mov ebp, dword ptr [esp + 40]
c01071e8: 83 e5 01                      and ebp, 1
c01071eb: 4d                            dec ebp
c01071ec: 50                            push eax
c01071ed: 50                            push eax
c01071ee: 55                            push ebp
c01071ef: ff 76 18                      push dword ptr [esi + 24]
c01071f2: e8 42 f5 ff ff                call 0xc0106739 <AcquireSemaphore>
c01071f7: 83 c4 10                      add esp, 16
c01071fa: 85 c0                         test eax, eax
c01071fc: 75 37                         jne 0xc0107235 <WaitProcess+0x61>
c01071fe: 83 ec 0c                      sub esp, 12
c0107201: 56                            push esi
c0107202: e8 a2 f9 ff ff                call 0xc0106ba9 <LockProcess>
c0107207: 8b 46 0c                      mov eax, dword ptr [esi + 12]
c010720a: 8b 40 04                      mov eax, dword ptr [eax + 4]
c010720d: 8b 4c 24 34                   mov ecx, dword ptr [esp + 52]
c0107211: 8b 54 24 30                   mov edx, dword ptr [esp + 48]
c0107215: e8 34 fc ff ff                call 0xc0106e4e <RecursivelyTryReap.isra.0>
c010721a: 89 c7                         mov edi, eax
c010721c: 89 34 24                      mov dword ptr [esp], esi
c010721f: e8 9a f9 ff ff                call 0xc0106bbe <UnlockProcess>
c0107224: 83 c4 10                      add esp, 16
c0107227: 85 ff                         test edi, edi
c0107229: 75 0c                         jne 0xc0107237 <WaitProcess+0x63>
c010722b: 83 7c 24 20 ff                cmp dword ptr [esp + 32], -1
c0107230: 74 ba                         je 0xc01071ec <WaitProcess+0x18>
c0107232: 43                            inc ebx
c0107233: eb b7                         jmp 0xc01071ec <WaitProcess+0x18>
c0107235: 31 ff                         xor edi, edi
c0107237: 85 db                         test ebx, ebx
c0107239: 74 11                         je 0xc010724c <WaitProcess+0x78>
c010723b: 83 ec 0c                      sub esp, 12
c010723e: ff 76 18                      push dword ptr [esi + 24]
c0107241: e8 6d f6 ff ff                call 0xc01068b3 <ReleaseSemaphore>
c0107246: 4b                            dec ebx
c0107247: 83 c4 10                      add esp, 16
c010724a: eb eb                         jmp 0xc0107237 <WaitProcess+0x63>
c010724c: 89 f8                         mov eax, edi
c010724e: 83 c4 0c                      add esp, 12
c0107251: 5b                            pop ebx
c0107252: 5e                            pop esi
c0107253: 5f                            pop edi
c0107254: 5d                            pop ebp
c0107255: c3                            ret

c0107256 <InitProgramLoader>:
c0107256: 83 ec 0c                      sub esp, 12
c0107259: 68 50 b1 13 c0                push 3222516048
c010725e: 6a 00                         push 0
c0107260: 6a 00                         push 0
c0107262: 68 14 0f 11 c0                push 3222343444
c0107267: e8 e1 2d 00 00                call 0xc010a04d <OpenFile>
c010726c: 83 c4 10                      add esp, 16
c010726f: 85 c0                         test eax, eax
c0107271: 74 0e                         je 0xc0107281 <InitProgramLoader+0x2b>
c0107273: 50                            push eax
c0107274: 50                            push eax
```

```
c01072c4: 25 96 00 00 00                and eax, 150
c01072c9: c3                            ret
c01072ca: b8 32 00 00 00                mov eax, 50
c01072cf: c3                            ret

c01072d0 <UpdateTimesliceExpiry>:
c01072d0: 55                            push ebp
c01072d1: 57                            push edi
c01072d2: 56                            push esi
c01072d3: 53                            push ebx
c01072d4: 83 ec 0c                      sub esp, 12
c01072d7: 0f 21 d8                      mov eax, dr3
c01072da: c1 e0 06                      shl eax, 6
c01072dd: 8b b0 c4 40 11 c0             mov esi, dword ptr [eax - 1072611132]
c01072e3: e8 60 0a 00 00                call 0xc0107d48 <GetSystemTimer>
c01072e8: 03 46 5c                      add eax, dword ptr [esi + 92]
c01072eb: 13 56 60                      adc edx, dword ptr [esi + 96]
c01072ee: 89 c1                         mov ecx, eax
c01072f0: 89 d3                         mov ebx, edx
c01072f2: 8b 7e 38                      mov edi, dword ptr [esi + 56]
c01072f5: 81 ff ff 00 00 00             cmp edi, 255
c01072fb: 74 18                         je 0xc0107315 <UpdateTimesliceExpiry+0x45>
c01072fd: bd 04 00 00 00                mov ebp, 4
c0107302: 89 f8                         mov eax, edi
c0107304: 99                            cdq
c0107305: f7 fd                         idiv ebp
c0107307: 89 c7                         mov edi, eax
c0107309: 83 c7 14                      add edi, 20
c010730c: b8 40 42 0f 00                mov eax, 1000000
c0107311: f7 ef                         imul edi
c0107313: eb 04                         jmp 0xc0107319 <UpdateTimesliceExpiry+0x49>
c0107315: 31 c0                         xor eax, eax
c0107317: 31 d2                         xor edx, edx
c0107319: 01 c1                         add ecx, eax
c010731b: 11 d3                         adc ebx, edx
c010731d: 89 4e 54                      mov dword ptr [esi + 84], ecx
c0107320: 89 5e 58                      mov dword ptr [esi + 88], ebx
c0107323: 31 c0                         xor eax, eax
c0107325: 89 46 5c                      mov dword ptr [esi + 92], eax
c0107328: 89 46 60                      mov dword ptr [esi + 96], eax
c010732b: 83 c4 0c                      add esp, 12
c010732e: 5b                            pop ebx
c010732f: 5e                            pop esi
c0107330: 5f                            pop edi
c0107331: 5d                            pop ebp
c0107332: c3                            ret

c0107333 <SwitchToNewTask>:
c0107333: 55                            push ebp
c0107334: 57                            push edi
c0107335: 56                            push esi
c0107336: 53                            push ebx
c0107337: 83 ec 18                      sub esp, 24
c010733a: 89 c6                         mov esi, eax
c010733c: 89 d3                         mov ebx, edx
c010733e: 31 c9                         xor ecx, ecx
c0107340: 89 4a 24                      mov dword ptr [edx + 36], ecx
c0107343: 68 e4 b1 13 c0                push 3222516196
c0107348: e8 5a 08 00 00                call 0xc0107ba7 <ThreadListDeleteTop>
c010734d: 0f 21 df                      mov edi, dr3
c0107350: c1 e7 06                      shl edi, 6
c0107353: 8d af c0 40 11 c0             lea ebp, [edi - 1072611136]
c0107359: c7 04 24 90 b1 13 c0          mov dword ptr [esp], 3222516112
c0107360: e8 f5 f5 ff ff                call 0xc010695a <AcquireSpinlock>
c0107365: 8b 43 08                      mov eax, dword ptr [ebx + 8]
c0107368: 83 c4 10                      add esp, 16
c010736b: 3b 46 08                      cmp eax, dword ptr [esi + 8]
c010736e: 74 0c                         je 0xc010737c <SwitchToNewTask+0x49>
c0107370: 83 ec 0c                      sub esp, 12
c0107373: 50                            push eax
c0107374: e8 03 e6 ff ff                call 0xc010597c <SetVas>
```

```
c01073c5: 8b 5c 24 10                  mov ebx, dword ptr [esp + 16]
c01073c9: 83 7b 24 04                  cmp dword ptr [ebx + 36], 4
c01073cd: 75 0c                        jne 0xc01073db <UnblockThread+0x1a>
c01073cf: 83 ec 0c                     sub esp, 12
c01073d2: 53                           push ebx
c01073d3: e8 46 f5 ff ff               call 0xc010691e <CancelSemaphoreOfThread>
c01073d8: 83 c4 10                     add esp, 16
c01073db: 50                           push eax
c01073dc: 50                           push eax
c01073dd: 53                           push ebx
c01073de: 68 e4 b1 13 c0               push 3222516196
c01073e3: e8 70 07 00 00               call 0xc0107b58 <ThreadListInsert>
c01073e8: 0f 21 d8                     mov eax, dr3
c01073eb: c1 e0 06                     shl eax, 6
c01073ee: 8b 80 c4 40 11 c0            mov eax, dword ptr [eax - 1072611132]
c01073f4: 83 c4 10                     add esp, 16
c01073f7: 8b 40 38                     mov eax, dword ptr [eax + 56]
c01073fa: 39 43 38                     cmp dword ptr [ebx + 56], eax
c01073fd: 7d 09                        jge 0xc0107408 <UnblockThread+0x47>
c01073ff: 83 c4 08                     add esp, 8
c0107402: 5b                           pop ebx
c0107403: e9 90 c0 ff ff               jmp 0xc0103498 <PostponeScheduleUntilStandard
c0107408: 83 c4 08                     add esp, 8
c010740b: 5b                           pop ebx
c010740c: c3                           ret

c010740d <UnblockThreadGiftingTimeslice>:
c010740d: 57                           push edi
c010740e: 56                           push esi
c010740f: 53                           push ebx
c0107410: 83 ec 10                     sub esp, 16
c0107413: 8b 5c 24 20                  mov ebx, dword ptr [esp + 32]
c0107417: e8 2c 09 00 00               call 0xc0107d48 <GetSystemTimer>
c010741c: 89 c6                        mov esi, eax
c010741e: 89 d7                        mov edi, edx
c0107420: 0f 21 d8                     mov eax, dr3
c0107423: c1 e0 06                     shl eax, 6
c0107426: 8b 80 c4 40 11 c0            mov eax, dword ptr [eax - 1072611132]
c010742c: 8b 50 58                     mov edx, dword ptr [eax + 88]
c010742f: 8b 40 54                     mov eax, dword ptr [eax + 84]
c0107432: 89 44 24 08                  mov dword ptr [esp + 8], eax
c0107436: 89 54 24 0c                  mov dword ptr [esp + 12], edx
c010743a: 39 74 24 08                  cmp dword ptr [esp + 8], esi
c010743e: 8b 44 24 0c                  mov eax, dword ptr [esp + 12]
c0107442: 19 f8                        sbb eax, edi
c0107444: 72 18                        jb 0xc010745e <UnblockThreadGiftingTimeslice+
c0107446: 8b 43 5c                     mov eax, dword ptr [ebx + 92]
c0107449: 8b 53 60                     mov edx, dword ptr [ebx + 96]
c010744c: 29 f0                        sub eax, esi
c010744e: 19 fa                        sbb edx, edi
c0107450: 03 44 24 08                  add eax, dword ptr [esp + 8]
c0107454: 13 54 24 0c                  adc edx, dword ptr [esp + 12]
c0107458: 89 43 5c                     mov dword ptr [ebx + 92], eax
c010745b: 89 53 60                     mov dword ptr [ebx + 96], edx
c010745e: 83 7b 24 04                  cmp dword ptr [ebx + 36], 4
c0107462: 75 0c                        jne 0xc0107470 <UnblockThreadGiftingTimeslice
c0107464: 83 ec 0c                     sub esp, 12
c0107467: 53                           push ebx
c0107468: e8 b1 f4 ff ff               call 0xc010691e <CancelSemaphoreOfThread>
c010746d: 83 c4 10                     add esp, 16
c0107470: 50                           push eax
c0107471: 50                           push eax
c0107472: 53                           push ebx
c0107473: 68 e4 b1 13 c0               push 3222516196
c0107478: e8 be 06 00 00               call 0xc0107b3b <ThreadListInsertAtFront>
c010747d: 0f 21 d8                     mov eax, dr3
c0107480: c1 e0 06                     shl eax, 6
c0107483: 8b 80 c4 40 11 c0            mov eax, dword ptr [eax - 1072611132]
c0107489: 83 c4 10                     add esp, 16
c010748c: 8b 40 38                     mov eax, dword ptr [eax + 56]
c010748f: 39 43 38                     cmp dword ptr [ebx + 56], eax
```

```
c01074ee: 11 51 30                      adc dword ptr [ecx + 48], edx
c01074f1: 5a                            pop edx
c01074f2: 5e                            pop esi
c01074f3: 5f                            pop edi
c01074f4: c3                            ret

c01074f5 <ScheduleWithLockHeld>:
c01074f5: 55                            push ebp
c01074f6: 57                            push edi
c01074f7: 56                            push esi
c01074f8: 53                            push ebx
c01074f9: 81 ec 8c 00 00 00             sub esp, 140
c01074ff: e8 6b be ff ff                call 0xc010336f <GetIrql>
c0107504: 83 f8 03                      cmp eax, 3
c0107507: 75 18                         jne 0xc0107521 <ScheduleWithLockHeld+0x2c>
c0107509: 0f 21 d8                      mov eax, dr3
c010750c: c1 e0 06                      shl eax, 6
c010750f: 8b 98 c4 40 11 c0             mov ebx, dword ptr [eax - 1072611132]
c0107515: 8b 35 e4 b1 13 c0             mov esi, dword ptr [-1072451100]
c010751b: 85 db                         test ebx, ebx
c010751d: 75 29                         jne 0xc0107548 <ScheduleWithLockHeld+0x53>
c010751f: eb 17                         jmp 0xc0107538 <ScheduleWithLockHeld+0x43>
c0107521: e8 49 be ff ff                call 0xc010336f <GetIrql>
c0107526: 52                            push edx
c0107527: 52                            push edx
c0107528: 50                            push eax
c0107529: 68 44 0f 11 c0                push 3222343492
c010752e: e8 92 15 00 00                call 0xc0108ac5 <LogWriteSerial>
c0107533: 83 c4 10                      add esp, 16
c0107536: eb d1                         jmp 0xc0107509 <ScheduleWithLockHeld+0x14>
c0107538: 85 f6                         test esi, esi
c010753a: 0f 84 84 00 00 00             je 0xc01075c4 <ScheduleWithLockHeld+0xcf>
c0107540: 89 f2                         mov edx, esi
c0107542: 8d 44 24 14                   lea eax, [esp + 20]
c0107546: eb 77                         jmp 0xc01075bf <ScheduleWithLockHeld+0xca>
c0107548: 39 f3                         cmp ebx, esi
c010754a: 74 78                         je 0xc01075c4 <ScheduleWithLockHeld+0xcf>
c010754c: 85 f6                         test esi, esi
c010754e: 74 74                         je 0xc01075c4 <ScheduleWithLockHeld+0xcf>
c0107550: 8b 7b 54                      mov edi, dword ptr [ebx + 84]
c0107553: 8b 43 58                      mov eax, dword ptr [ebx + 88]
c0107556: 89 44 24 0c                   mov dword ptr [esp + 12], eax
c010755a: e8 e9 07 00 00                call 0xc0107d48 <GetSystemTimer>
c010755f: 89 c5                         mov ebp, eax
c0107561: 89 d0                         mov eax, edx
c0107563: 0f 21 da                      mov edx, dr3
c0107566: c1 e2 06                      shl edx, 6
c0107569: 8b 8a c4 40 11 c0             mov ecx, dword ptr [edx - 1072611132]
c010756f: 8b 51 3c                      mov edx, dword ptr [ecx + 60]
c0107572: 85 d2                         test edx, edx
c0107574: 74 2a                         je 0xc01075a0 <ScheduleWithLockHeld+0xab>
c0107576: 39 fd                         cmp ebp, edi
c0107578: 1b 44 24 0c                   sbb eax, dword ptr [esp + 12]
c010757c: 0f 93 c0                      setae al
c010757f: 0f b6 c0                      movzx eax, al
c0107582: 8d 44 00 ff                   lea eax, [eax + eax - 1]
c0107586: 03 41 38                      add eax, dword ptr [ecx + 56]
c0107589: 89 c7                         mov edi, eax
c010758b: 89 d0                         mov eax, edx
c010758d: e8 18 fd ff ff                call 0xc01072aa <GetMinPriorityValueForPolicy
c0107592: 39 c7                         cmp edi, eax
c0107594: 7c 0a                         jl 0xc01075a0 <ScheduleWithLockHeld+0xab>
c0107596: 83 c0 64                      add eax, 100
c0107599: 39 c7                         cmp edi, eax
c010759b: 7f 03                         jg 0xc01075a0 <ScheduleWithLockHeld+0xab>
c010759d: 89 79 38                      mov dword ptr [ecx + 56], edi
c01075a0: e8 11 ff ff ff                call 0xc01074b6 <UpdateThreadTimeUsed>
c01075a5: 83 7b 24 00                   cmp dword ptr [ebx + 36], 0
c01075a9: 75 10                         jne 0xc01075bb <ScheduleWithLockHeld+0xc6>
c01075ab: 50                            push eax
c01075ac: 50                            push eax
```

```
c01075f8: e8 1d fa ff ff                call 0xc010701a <CreateProcessWithEntryPoint>
c01075fd: 83 c4 1c                      add esp, 28
c0107600: c3                            ret

c0107601 <PreventScheduler>:
c0107601: 83 ec 18                      sub esp, 24
c0107604: 68 ac b1 13 c0                push 3222516140
c0107609: e8 4c f3 ff ff                call 0xc010695a <AcquireSpinlock>
c010760e: ff 05 88 b1 13 c0             inc dword ptr [-1072451192]
c0107614: c7 04 24 ac b1 13 c0          mov dword ptr [esp], 3222516140
c010761b: e8 8a f3 ff ff                call 0xc01069aa <ReleaseSpinlock>
c0107620: 83 c4 1c                      add esp, 28
c0107623: c3                            ret

c0107624 <UnpreventScheduler>:
c0107624: 83 ec 18                      sub esp, 24
c0107627: 68 ac b1 13 c0                push 3222516140
c010762c: e8 29 f3 ff ff                call 0xc010695a <AcquireSpinlock>
c0107631: ff 0d 88 b1 13 c0             dec dword ptr [-1072451192]
c0107637: c7 04 24 ac b1 13 c0          mov dword ptr [esp], 3222516140
c010763e: e8 67 f3 ff ff                call 0xc01069aa <ReleaseSpinlock>
c0107643: 83 c4 1c                      add esp, 28
c0107646: c3                            ret

c0107647 <LockScheduler>:
c0107647: 83 ec 18                      sub esp, 24
c010764a: 68 ac b1 13 c0                push 3222516140
c010764f: e8 06 f3 ff ff                call 0xc010695a <AcquireSpinlock>
c0107654: 83 c4 10                      add esp, 16
c0107657: 83 3d 8c b1 13 c0 00          cmp dword ptr [-1072451188], 0
c010765e: 75 24                         jne 0xc0107684 <LockScheduler+0x3d>
c0107660: 83 ec 0c                      sub esp, 12
c0107663: 68 c8 b1 13 c0                push 3222516168
c0107668: e8 ed f2 ff ff                call 0xc010695a <AcquireSpinlock>
c010766d: a1 c4 b1 13 c0                mov eax, dword ptr [3222516164]
c0107672: a3 e0 b1 13 c0                mov dword ptr [3222516192], eax
c0107677: a1 dc b1 13 c0                mov eax, dword ptr [3222516188]
c010767c: a3 c4 b1 13 c0                mov dword ptr [3222516164], eax
c0107681: 83 c4 10                      add esp, 16
c0107684: ff 05 8c b1 13 c0             inc dword ptr [-1072451188]
c010768a: 83 ec 0c                      sub esp, 12
c010768d: 68 ac b1 13 c0                push 3222516140
c0107692: e8 13 f3 ff ff                call 0xc01069aa <ReleaseSpinlock>
c0107697: 83 c4 1c                      add esp, 28
c010769a: c3                            ret

c010769b <UnlockScheduler>:
c010769b: 83 ec 18                      sub esp, 24
c010769e: 68 ac b1 13 c0                push 3222516140
c01076a3: e8 b2 f2 ff ff                call 0xc010695a <AcquireSpinlock>
c01076a8: a1 8c b1 13 c0                mov eax, dword ptr [3222516108]
c01076ad: 48                            dec eax
c01076ae: a3 8c b1 13 c0                mov dword ptr [3222516108], eax
c01076b3: 83 c4 10                      add esp, 16
c01076b6: 85 c0                         test eax, eax
c01076b8: 75 24                         jne 0xc01076de <UnlockScheduler+0x43>
c01076ba: a1 e0 b1 13 c0                mov eax, dword ptr [3222516192]
c01076bf: a3 c4 b1 13 c0                mov dword ptr [3222516164], eax
c01076c4: e8 a6 bc ff ff                call 0xc010336f <GetIrql>
c01076c9: a3 e0 b1 13 c0                mov dword ptr [3222516192], eax
c01076ce: 83 ec 0c                      sub esp, 12
c01076d1: 68 c8 b1 13 c0                push 3222516168
c01076d6: e8 cf f2 ff ff                call 0xc01069aa <ReleaseSpinlock>
c01076db: 83 c4 10                      add esp, 16
c01076de: 83 ec 0c                      sub esp, 12
c01076e1: 68 ac b1 13 c0                push 3222516140
c01076e6: e8 bf f2 ff ff                call 0xc01069aa <ReleaseSpinlock>
c01076eb: 83 c4 1c                      add esp, 28
c01076ee: c3                            ret

c01076ef <ThreadInitialisationHandler>:
```

```
c0107757: 50                            push eax
c0107758: e8 28 fb ff ff                call 0xc0107285 <LoadProgramLoaderIntoAddress
c010775d: 83 c4 10                      add esp, 16
c0107760: 85 c0                         test eax, eax
c0107762: 74 18                         je 0xc010777c <ThreadExecuteInUsermode+0x39>
c0107764: 83 ec 0c                      sub esp, 12
c0107767: 68 69 0f 11 c0                push 3222343529
c010776c: e8 6c 13 00 00                call 0xc0108add <LogDeveloperWarning>
c0107771: 89 1c 24                      mov dword ptr [esp], ebx
c0107774: e8 fd f2 ff ff                call 0xc0106a76 <TerminateThread>
c0107779: 83 c4 10                      add esp, 16
c010777c: 83 ec 0c                      sub esp, 12
c010777f: 68 00 00 40 00                push 4194304
c0107784: e8 36 e3 ff ff                call 0xc0105abf <BytesToPages>
c0107789: c1 e0 0c                      shl eax, 12
c010778c: 89 04 24                      mov dword ptr [esp], eax
c010778f: e8 2b e3 ff ff                call 0xc0105abf <BytesToPages>
c0107794: c1 e0 0c                      shl eax, 12
c0107797: 5a                            pop edx
c0107798: 59                            pop ecx
c0107799: 6a 00                         push 0
c010779b: 6a 00                         push 0
c010779d: 68 07 01 00 00                push 263
c01077a2: 50                            push eax
c01077a3: ba 00 00 00 10                mov edx, 268435456
c01077a8: 29 c2                         sub edx, eax
c01077aa: 52                            push edx
c01077ab: 6a 00                         push 0
c01077ad: e8 96 db ff ff                call 0xc0105348 <MapVirt>
c01077b2: 83 c4 20                      add esp, 32
c01077b5: e8 8d fe ff ff                call 0xc0107647 <LockScheduler>
c01077ba: c7 43 04 00 00 00 10          mov dword ptr [ebx + 4], 268435456
c01077c1: e8 d5 fe ff ff                call 0xc010769b <UnlockScheduler>
c01077c6: e8 ae ce ff ff                call 0xc0104679 <GetVas>
c01077cb: 83 ec 0c                      sub esp, 12
c01077ce: 50                            push eax
c01077cf: e8 94 5f 00 00                call 0xc010d768 <ArchFlushTlb>
c01077d4: 83 c4 0c                      add esp, 12
c01077d7: ff 74 24 24                   push dword ptr [esp + 36]
c01077db: 68 00 00 00 10                push 268435456
c01077e0: ff 74 24 18                   push dword ptr [esp + 24]
c01077e4: e8 57 6e 00 00                call 0xc010e640 <ArchSwitchToUsermode>
c01077e9: 83 c4 28                      add esp, 40
c01077ec: 5b                            pop ebx
c01077ed: c3                            ret

c01077ee <CreateThreadEx>:
c01077ee: 57                            push edi
c01077ef: 56                            push esi
c01077f0: 53                            push ebx
c01077f1: 8b 74 24 20                   mov esi, dword ptr [esp + 32]
c01077f5: 83 ec 0c                      sub esp, 12
c01077f8: 6a 6c                         push 108
c01077fa: e8 50 c1 ff ff                call 0xc010394f <AllocHeap>
c01077ff: 89 c3                         mov ebx, eax
c0107801: 8b 44 24 24                   mov eax, dword ptr [esp + 36]
c0107805: 89 43 28                      mov dword ptr [ebx + 40], eax
c0107808: 8b 44 24 20                   mov eax, dword ptr [esp + 32]
c010780c: 89 43 10                      mov dword ptr [ebx + 16], eax
c010780f: c7 43 24 01 00 00 00          mov dword ptr [ebx + 36], 1
c0107816: 31 ff                         xor edi, edi
c0107818: 89 7b 2c                      mov dword ptr [ebx + 44], edi
c010781b: 89 7b 30                      mov dword ptr [ebx + 48], edi
c010781e: 89 7b 5c                      mov dword ptr [ebx + 92], edi
c0107821: 89 7b 60                      mov dword ptr [ebx + 96], edi
c0107824: 58                            pop eax
c0107825: ff 74 24 28                   push dword ptr [esp + 40]
c0107829: e8 c7 9a ff ff                call 0xc01012f5 <strdup>
c010782e: 89 43 34                      mov dword ptr [ebx + 52], eax
c0107831: 8b 44 24 38                   mov eax, dword ptr [esp + 56]
c0107835: 89 43 38                      mov dword ptr [ebx + 56], eax
```

```
c01078a7: c7 04 24 5c b1 13 c0          mov dword ptr [esp], 3222516060
c01078ae: e8 f7 f0 ff ff                call 0xc01069aa <ReleaseSpinlock>
c01078b3: 89 7b 20                      mov dword ptr [ebx + 32], edi
c01078b6: 83 c4 10                      add esp, 16
c01078b9: 31 c0                         xor eax, eax
c01078bb: 83 7c 24 2c 00                cmp dword ptr [esp + 44], 0
c01078c0: 75 16                         jne 0xc01078d8 <CreateThreadEx+0xea>
c01078c2: 83 ec 0c                      sub esp, 12
c01078c5: 68 00 40 00 00                push 16384
c01078ca: e8 f0 e1 ff ff                call 0xc0105abf <BytesToPages>
c01078cf: c1 e0 0c                      shl eax, 12
c01078d2: c1 e8 0a                      shr eax, 10
c01078d5: 83 c4 10                      add esp, 16
c01078d8: 83 ec 0c                      sub esp, 12
c01078db: c1 e0 0a                      shl eax, 10
c01078de: 50                            push eax
c01078df: e8 db e1 ff ff                call 0xc0105abf <BytesToPages>
c01078e4: c1 e0 0c                      shl eax, 12
c01078e7: 89 c7                         mov edi, eax
c01078e9: 58                            pop eax
c01078ea: 5a                            pop edx
c01078eb: 6a 00                         push 0
c01078ed: 6a 00                         push 0
c01078ef: 6a 13                         push 19
c01078f1: 57                            push edi
c01078f2: 6a 00                         push 0
c01078f4: 6a 00                         push 0
c01078f6: e8 4d da ff ff                call 0xc0105348 <MapVirt>
c01078fb: 01 f8                         add eax, edi
c01078fd: 89 03                         mov dword ptr [ebx], eax
c01078ff: 89 7b 0c                      mov dword ptr [ebx + 12], edi
c0107902: 83 c4 14                      add esp, 20
c0107905: 50                            push eax
c0107906: e8 e5 6c 00 00                call 0xc010e5f0 <ArchPrepareStack>
c010790b: 89 43 04                      mov dword ptr [ebx + 4], eax
c010790e: 83 c4 10                      add esp, 16
c0107911: 85 f6                         test esi, esi
c0107913: 74 0e                         je 0xc0107923 <CreateThreadEx+0x135>
c0107915: 51                            push ecx
c0107916: 51                            push ecx
c0107917: 53                            push ebx
c0107918: 56                            push esi
c0107919: e8 f5 f2 ff ff                call 0xc0106c13 <AddThreadToProcess>
c010791e: 83 c4 10                      add esp, 16
c0107921: eb 05                         jmp 0xc0107928 <CreateThreadEx+0x13a>
c0107923: 31 d2                         xor edx, edx
c0107925: 89 53 4c                      mov dword ptr [ebx + 76], edx
c0107928: e8 1a fd ff ff                call 0xc0107647 <LockScheduler>
c010792d: 50                            push eax
c010792e: 50                            push eax
c010792f: 53                            push ebx
c0107930: 68 e4 b1 13 c0                push 3222516196
c0107935: e8 1e 02 00 00                call 0xc0107b58 <ThreadListInsert>
c010793a: e8 5c fd ff ff                call 0xc010769b <UnlockScheduler>
c010793f: 83 c4 10                      add esp, 16
c0107942: 89 d8                         mov eax, ebx
c0107944: 5b                            pop ebx
c0107945: 5e                            pop esi
c0107946: 5f                            pop edi
c0107947: c3                            ret

c0107948 <CreateThread>:
c0107948: 83 ec 0c                      sub esp, 12
c010794b: e8 35 f3 ff ff                call 0xc0106c85 <GetProcess>
c0107950: 6a 00                         push 0
c0107952: 6a 1e                         push 30
c0107954: 6a 00                         push 0
c0107956: 50                            push eax
c0107957: ff 74 24 2c                   push dword ptr [esp + 44]
c010795b: ff 74 24 2c                   push dword ptr [esp + 44]
c010795f: ff 74 24 2c                   push dword ptr [esp + 44]
```

```
c01079b3: 89 43 34                  mov dword ptr [ebx + 52], eax
c01079b6: 8b 45 08                  mov eax, dword ptr [ebp + 8]
c01079b9: 89 43 08                  mov dword ptr [ebx + 8], eax
c01079bc: 89 6b 4c                  mov dword ptr [ebx + 76], ebp
c01079bf: e8 83 fc ff ff            call 0xc0107647 <LockScheduler>
c01079c4: 5e                        pop esi
c01079c5: 5f                        pop edi
c01079c6: 53                        push ebx
c01079c7: 68 e4 b1 13 c0            push 3222516196
c01079cc: e8 87 01 00 00            call 0xc0107b58 <ThreadListInsert>
c01079d1: 83 c4 2c                  add esp, 44
c01079d4: 5b                        pop ebx
c01079d5: 5e                        pop esi
c01079d6: 5f                        pop edi
c01079d7: 5d                        pop ebp
c01079d8: e9 be fc ff ff            jmp 0xc010769b <UnlockScheduler>

c01079dd <UnassignThreadToCpu>:
c01079dd: c3                        ret

c01079de <Schedule>:
c01079de: 83 ec 0c                  sub esp, 12
c01079e1: e8 89 b9 ff ff            call 0xc010336f <GetIrql>
c01079e6: 83 f8 02                  cmp eax, 2
c01079e9: 7f 09                     jg 0xc01079f4 <Schedule+0x16>
c01079eb: 83 3d 88 b1 13 c0 00      cmp dword ptr [-1072451192], 0
c01079f2: 7e 08                     jle 0xc01079fc <Schedule+0x1e>
c01079f4: 83 c4 0c                  add esp, 12
c01079f7: e9 9c ba ff ff            jmp 0xc0103498 <PostponeScheduleUntilStandard
c01079fc: e8 46 fc ff ff            call 0xc0107647 <LockScheduler>
c0107a01: e8 ef fa ff ff            call 0xc01074f5 <ScheduleWithLockHeld>
c0107a06: e8 90 fc ff ff            call 0xc010769b <UnlockScheduler>
c0107a0b: 0f 21 d8                  mov eax, dr3
c0107a0e: c1 e0 06                  shl eax, 6
c0107a11: 8b 80 c4 40 11 c0         mov eax, dword ptr [eax - 1072611132]
c0107a17: 80 78 46 00               cmp byte ptr [eax + 70], 0
c0107a1b: 74 20                     je 0xc0107a3d <Schedule+0x5f>
c0107a1d: 0f 21 d8                  mov eax, dr3
c0107a20: 83 ec 0c                  sub esp, 12
c0107a23: c1 e0 06                  shl eax, 6
c0107a26: ff b0 c4 40 11 c0         push dword ptr [eax - 1072611132]
c0107a2c: e8 45 f0 ff ff            call 0xc0106a76 <TerminateThread>
c0107a31: c7 04 24 01 00 00 00      mov dword ptr [esp], 1
c0107a38: e8 62 11 00 00            call 0xc0108b9f <Panic>
c0107a3d: 83 c4 0c                  add esp, 12
c0107a40: c3                        ret

c0107a41 <InitScheduler>:
c0107a41: 83 ec 14                  sub esp, 20
c0107a44: 6a 00                     push 0
c0107a46: 68 e4 b1 13 c0            push 3222516196
c0107a4b: e8 d2 00 00 00            call 0xc0107b22 <ThreadListInit>
c0107a50: 83 c4 0c                  add esp, 12
c0107a53: 6a 03                     push 3
c0107a55: 68 92 0f 11 c0            push 3222343570
c0107a5a: 68 c8 b1 13 c0            push 3222516168
c0107a5f: e8 db ee ff ff            call 0xc010693f <InitSpinlock>
c0107a64: 83 c4 0c                  add esp, 12
c0107a67: 6a 03                     push 3
c0107a69: 68 9c 0f 11 c0            push 3222343580
c0107a6e: 68 ac b1 13 c0            push 3222516140
c0107a73: e8 c7 ee ff ff            call 0xc010693f <InitSpinlock>
c0107a78: 83 c4 0c                  add esp, 12
c0107a7b: 6a 29                     push 41
c0107a7d: 68 a7 0f 11 c0            push 3222343591
c0107a82: 68 90 b1 13 c0            push 3222516112
c0107a87: e8 b3 ee ff ff            call 0xc010693f <InitSpinlock>
c0107a8c: 83 c4 1c                  add esp, 28
c0107a8f: c3                        ret

c0107a90 <StartMultitasking>:
```

```
c0107aea: 7d 02                         jge 0xc0107aee <SetThreadPriority+0x42>
c0107aec: 89 f0                         mov eax, esi
c0107aee: be ff 00 00 00                mov esi, 255
c0107af3: 85 c9                         test ecx, ecx
c0107af5: 74 03                         je 0xc0107afa <SetThreadPriority+0x4e>
c0107af7: 8d 72 64                      lea esi, [edx + 100]
c0107afa: 39 f0                         cmp eax, esi
c0107afc: 7e 02                         jle 0xc0107b00 <SetThreadPriority+0x54>
c0107afe: 89 f0                         mov eax, esi
c0107b00: 83 f9 ff                      cmp ecx, -1
c0107b03: 74 03                         je 0xc0107b08 <SetThreadPriority+0x5c>
c0107b05: 89 4b 3c                      mov dword ptr [ebx + 60], ecx
c0107b08: 83 f8 ff                      cmp eax, -1
c0107b0b: 74 03                         je 0xc0107b10 <SetThreadPriority+0x64>
c0107b0d: 89 43 38                      mov dword ptr [ebx + 56], eax
c0107b10: 31 c0                         xor eax, eax
c0107b12: 5b                            pop ebx
c0107b13: 5e                            pop esi
c0107b14: c3                            ret

c0107b15 <GetThread>:
c0107b15: 0f 21 d8                      mov eax, dr3
c0107b18: c1 e0 06                      shl eax, 6
c0107b1b: 8b 80 c4 40 11 c0             mov eax, dword ptr [eax - 1072611132]
c0107b21: c3                            ret

c0107b22 <ThreadListInit>:
c0107b22: 57                            push edi
c0107b23: 8b 54 24 08                   mov edx, dword ptr [esp + 8]
c0107b27: b9 03 00 00 00                mov ecx, 3
c0107b2c: 31 c0                         xor eax, eax
c0107b2e: 89 d7                         mov edi, edx
c0107b30: f3 ab                         rep  stosd dword ptr es:[edi], eax
c0107b32: 8b 44 24 0c                   mov eax, dword ptr [esp + 12]
c0107b36: 89 42 08                      mov dword ptr [edx + 8], eax
c0107b39: 5f                            pop edi
c0107b3a: c3                            ret

c0107b3b <ThreadListInsertAtFront>:
c0107b3b: 53                            push ebx
c0107b3c: 8b 44 24 08                   mov eax, dword ptr [esp + 8]
c0107b40: 8b 54 24 0c                   mov edx, dword ptr [esp + 12]
c0107b44: 8b 08                         mov ecx, dword ptr [eax]
c0107b46: 85 c9                         test ecx, ecx
c0107b48: 75 03                         jne 0xc0107b4d <ThreadListInsertAtFront+0x12>
c0107b4a: 89 50 04                      mov dword ptr [eax + 4], edx
c0107b4d: 8b 58 08                      mov ebx, dword ptr [eax + 8]
c0107b50: 89 4c 9a 14                   mov dword ptr [edx + 4*ebx + 20], ecx
c0107b54: 89 10                         mov dword ptr [eax], edx
c0107b56: 5b                            pop ebx
c0107b57: c3                            ret

c0107b58 <ThreadListInsert>:
c0107b58: 53                            push ebx
c0107b59: 8b 44 24 08                   mov eax, dword ptr [esp + 8]
c0107b5d: 8b 54 24 0c                   mov edx, dword ptr [esp + 12]
c0107b61: 8b 48 04                      mov ecx, dword ptr [eax + 4]
c0107b64: 8b 58 08                      mov ebx, dword ptr [eax + 8]
c0107b67: 85 c9                         test ecx, ecx
c0107b69: 75 04                         jne 0xc0107b6f <ThreadListInsert+0x17>
c0107b6b: 89 10                         mov dword ptr [eax], edx
c0107b6d: eb 04                         jmp 0xc0107b73 <ThreadListInsert+0x1b>
c0107b6f: 89 54 99 14                   mov dword ptr [ecx + 4*ebx + 20], edx
c0107b73: 89 50 04                      mov dword ptr [eax + 4], edx
c0107b76: 8b 40 08                      mov eax, dword ptr [eax + 8]
c0107b79: 31 c9                         xor ecx, ecx
c0107b7b: 89 4c 82 14                   mov dword ptr [edx + 4*eax + 20], ecx
c0107b7f: 5b                            pop ebx
c0107b80: c3                            ret

c0107b81 <ThreadListContains>:
```

```
c0107bc2: c3                            ret

c0107bc3 <ThreadListDelete>:
c0107bc3: 55                            push ebp
c0107bc4: 57                            push edi
c0107bc5: 56                            push esi
c0107bc6: 53                            push ebx
c0107bc7: 83 ec 0c                      sub esp, 12
c0107bca: 8b 54 24 20                   mov edx, dword ptr [esp + 32]
c0107bce: 8b 3a                         mov edi, dword ptr [edx]
c0107bd0: 89 f8                         mov eax, edi
c0107bd2: 31 c9                         xor ecx, ecx
c0107bd4: 85 c0                         test eax, eax
c0107bd6: 74 10                         je 0xc0107be8 <ThreadListDelete+0x25>
c0107bd8: 39 44 24 24                   cmp dword ptr [esp + 36], eax
c0107bdc: 74 0d                         je 0xc0107beb <ThreadListDelete+0x28>
c0107bde: 41                            inc ecx
c0107bdf: 8b 5a 08                      mov ebx, dword ptr [edx + 8]
c0107be2: 8b 44 98 14                   mov eax, dword ptr [eax + 4*ebx + 20]
c0107be6: eb ec                         jmp 0xc0107bd4 <ThreadListDelete+0x11>
c0107be8: 83 c9 ff                      or ecx, -1
c0107beb: 89 f8                         mov eax, edi
c0107bed: 31 f6                         xor esi, esi
c0107bef: 31 ed                         xor ebp, ebp
c0107bf1: 85 c0                         test eax, eax
c0107bf3: 74 2d                         je 0xc0107c22 <ThreadListDelete+0x5f>
c0107bf5: 8b 5a 08                      mov ebx, dword ptr [edx + 8]
c0107bf8: 39 ce                         cmp esi, ecx
c0107bfa: 8d 5b 04                      lea ebx, [ebx + 4]
c0107bfd: 75 1a                         jne 0xc0107c19 <ThreadListDelete+0x56>
c0107bff: 8b 4c 98 04                   mov ecx, dword ptr [eax + 4*ebx + 4]
c0107c03: 39 f8                         cmp eax, edi
c0107c05: 75 04                         jne 0xc0107c0b <ThreadListDelete+0x48>
c0107c07: 89 0a                         mov dword ptr [edx], ecx
c0107c09: eb 04                         jmp 0xc0107c0f <ThreadListDelete+0x4c>
c0107c0b: 89 4c 9d 04                   mov dword ptr [ebp + 4*ebx + 4], ecx
c0107c0f: 3b 42 04                      cmp eax, dword ptr [edx + 4]
c0107c12: 75 18                         jne 0xc0107c2c <ThreadListDelete+0x69>
c0107c14: 89 6a 04                      mov dword ptr [edx + 4], ebp
c0107c17: eb 13                         jmp 0xc0107c2c <ThreadListDelete+0x69>
c0107c19: 46                            inc esi
c0107c1a: 89 c5                         mov ebp, eax
c0107c1c: 8b 44 98 04                   mov eax, dword ptr [eax + 4*ebx + 4]
c0107c20: eb cf                         jmp 0xc0107bf1 <ThreadListDelete+0x2e>
c0107c22: 83 ec 0c                      sub esp, 12
c0107c25: 6a 15                         push 21
c0107c27: e8 73 0f 00 00                call 0xc0108b9f <Panic>
c0107c2c: 83 c4 0c                      add esp, 12
c0107c2f: 5b                            pop ebx
c0107c30: 5e                            pop esi
c0107c31: 5f                            pop edi
c0107c32: 5d                            pop ebp
c0107c33: c3                            ret

c0107c34 <HandleSleepWakeups>:
c0107c34: 57                            push edi
c0107c35: 56                            push esi
c0107c36: 53                            push ebx
c0107c37: 8b 5c 24 10                   mov ebx, dword ptr [esp + 16]
c0107c3b: 0f 21 d8                      mov eax, dr3
c0107c3e: c1 e0 06                      shl eax, 6
c0107c41: 83 b8 c4 40 11 c0 00          cmp dword ptr [eax - 1072611132], 0
c0107c48: 74 6a                         je 0xc0107cb4 <HandleSleepWakeups+0x80>
c0107c4a: e8 f8 f9 ff ff                call 0xc0107647 <LockScheduler>
c0107c4f: a1 f0 b1 13 c0                mov eax, dword ptr [3222516208]
c0107c54: 85 c0                         test eax, eax
c0107c56: 7e 06                         jle 0xc0107c5e <HandleSleepWakeups+0x2a>
c0107c58: 48                            dec eax
c0107c59: a3 f0 b1 13 c0                mov dword ptr [3222516208], eax
c0107c5e: 8b 33                         mov esi, dword ptr [ebx]
c0107c60: 8b 7b 04                      mov edi, dword ptr [ebx + 4]
```

```
c0107cb5: 5e                            pop esi
c0107cb6: 5f                            pop edi
c0107cb7: c3                            ret

c0107cb8 <ReceivedTimer>:
c0107cb8: 57                            push edi
c0107cb9: 56                            push esi
c0107cba: 51                            push ecx
c0107cbb: 8b 74 24 10                   mov esi, dword ptr [esp + 16]
c0107cbf: 8b 7c 24 14                   mov edi, dword ptr [esp + 20]
c0107cc3: 0f 21 d8                      mov eax, dr3
c0107cc6: 85 c0                         test eax, eax
c0107cc8: 75 28                         jne 0xc0107cf2 <ReceivedTimer+0x3a>
c0107cca: 83 ec 0c                      sub esp, 12
c0107ccd: 68 0c b2 13 c0                push 3222516236
c0107cd2: e8 83 ec ff ff                call 0xc010695a <AcquireSpinlock>
c0107cd7: 01 35 f8 b1 13 c0             add dword ptr [-1072451080], esi
c0107cdd: 11 3d fc b1 13 c0             adc dword ptr [-1072451076], edi
c0107ce3: c7 04 24 0c b2 13 c0          mov dword ptr [esp], 3222516236
c0107cea: e8 bb ec ff ff                call 0xc01069aa <ReleaseSpinlock>
c0107cef: 83 c4 10                      add esp, 16
c0107cf2: 0f 21 d8                      mov eax, dr3
c0107cf5: c1 e0 06                      shl eax, 6
c0107cf8: 8b 80 c4 40 11 c0             mov eax, dword ptr [eax - 1072611132]
c0107cfe: 85 c0                         test eax, eax
c0107d00: 74 23                         je 0xc0107d25 <ReceivedTimer+0x6d>
c0107d02: 8b 50 54                      mov edx, dword ptr [eax + 84]
c0107d05: 8b 40 58                      mov eax, dword ptr [eax + 88]
c0107d08: 85 c0                         test eax, eax
c0107d0a: 75 04                         jne 0xc0107d10 <ReceivedTimer+0x58>
c0107d0c: 85 d2                         test edx, edx
c0107d0e: 74 15                         je 0xc0107d25 <ReceivedTimer+0x6d>
c0107d10: 39 15 f8 b1 13 c0             cmp dword ptr [-1072451080], edx
c0107d16: 8b 15 fc b1 13 c0             mov edx, dword ptr [-1072451076]
c0107d1c: 19 c2                         sbb edx, eax
c0107d1e: 72 05                         jb 0xc0107d25 <ReceivedTimer+0x6d>
c0107d20: e8 73 b7 ff ff                call 0xc0103498 <PostponeScheduleUntilStandar
c0107d25: e8 a9 b7 ff ff                call 0xc01034d3 <GetNumberInDeferQueue>
c0107d2a: 83 f8 07                      cmp eax, 7
c0107d2d: 7f 15                         jg 0xc0107d44 <ReceivedTimer+0x8c>
c0107d2f: 52                            push edx
c0107d30: 68 f8 b1 13 c0                push 3222516216
c0107d35: 68 34 7c 10 c0                push 3222305844
c0107d3a: 6a 00                         push 0
c0107d3c: e8 b8 b5 ff ff                call 0xc01032f9 <DeferUntilIrql>
c0107d41: 83 c4 10                      add esp, 16
c0107d44: 58                            pop eax
c0107d45: 5e                            pop esi
c0107d46: 5f                            pop edi
c0107d47: c3                            ret

c0107d48 <GetSystemTimer>:
c0107d48: 57                            push edi
c0107d49: 56                            push esi
c0107d4a: 83 ec 10                      sub esp, 16
c0107d4d: 68 0c b2 13 c0                push 3222516236
c0107d52: e8 03 ec ff ff                call 0xc010695a <AcquireSpinlock>
c0107d57: 8b 35 f8 b1 13 c0             mov esi, dword ptr [-1072451080]
c0107d5d: 8b 3d fc b1 13 c0             mov edi, dword ptr [-1072451076]
c0107d63: c7 04 24 0c b2 13 c0          mov dword ptr [esp], 3222516236
c0107d6a: e8 3b ec ff ff                call 0xc01069aa <ReleaseSpinlock>
c0107d6f: 89 f0                         mov eax, esi
c0107d71: 89 fa                         mov edx, edi
c0107d73: 83 c4 14                      add esp, 20
c0107d76: 5e                            pop esi
c0107d77: 5f                            pop edi
c0107d78: c3                            ret

c0107d79 <InitTimer>:
c0107d79: 83 ec 10                      sub esp, 16
c0107d7c: 6a 28                         push 40
```

```
c0107dca: a1 00 b2 13 c0                mov eax, dword ptr [3222516224]
c0107dcf: 85 c0                         test eax, eax
c0107dd1: 74 1f                         je 0xc0107df2 <TryDequeueForSleep+0x30>
c0107dd3: 3b 44 24 10                   cmp eax, dword ptr [esp + 16]
c0107dd7: 75 14                         jne 0xc0107ded <TryDequeueForSleep+0x2b>
c0107dd9: 52                            push edx
c0107dda: 52                            push edx
c0107ddb: 50                            push eax
c0107ddc: 68 00 b2 13 c0                push 3222516224
c0107de1: e8 dd fd ff ff                call 0xc0107bc3 <ThreadListDelete>
c0107de6: 83 c4 10                      add esp, 16
c0107de9: b0 01                         mov al, 1
c0107deb: eb 05                         jmp 0xc0107df2 <TryDequeueForSleep+0x30>
c0107ded: 8b 40 18                      mov eax, dword ptr [eax + 24]
c0107df0: eb dd                         jmp 0xc0107dcf <TryDequeueForSleep+0xd>
c0107df2: 83 c4 0c                      add esp, 12
c0107df5: c3                            ret

c0107df6 <SleepUntil>:
c0107df6: 56                            push esi
c0107df7: 53                            push ebx
c0107df8: 51                            push ecx
c0107df9: 8b 74 24 10                   mov esi, dword ptr [esp + 16]
c0107dfd: 8b 5c 24 14                   mov ebx, dword ptr [esp + 20]
c0107e01: e8 42 ff ff ff                call 0xc0107d48 <GetSystemTimer>
c0107e06: 39 c6                         cmp esi, eax
c0107e08: 89 d8                         mov eax, ebx
c0107e0a: 19 d0                         sbb eax, edx
c0107e0c: 73 04                         jae 0xc0107e12 <SleepUntil+0x1c>
c0107e0e: 31 c0                         xor eax, eax
c0107e10: eb 56                         jmp 0xc0107e68 <SleepUntil+0x72>
c0107e12: e8 30 f8 ff ff                call 0xc0107647 <LockScheduler>
c0107e17: 0f 21 d8                      mov eax, dr3
c0107e1a: c1 e0 06                      shl eax, 6
c0107e1d: 8b 80 c4 40 11 c0             mov eax, dword ptr [eax - 1072611132]
c0107e23: 89 70 64                      mov dword ptr [eax + 100], esi
c0107e26: 89 58 68                      mov dword ptr [eax + 104], ebx
c0107e29: 0f 21 d8                      mov eax, dr3
c0107e2c: 83 ec 0c                      sub esp, 12
c0107e2f: c1 e0 06                      shl eax, 6
c0107e32: ff b0 c4 40 11 c0             push dword ptr [eax - 1072611132]
c0107e38: e8 62 ff ff ff                call 0xc0107d9f <QueueForSleep>
c0107e3d: c7 04 24 02 00 00 00          mov dword ptr [esp], 2
c0107e44: e8 60 f5 ff ff                call 0xc01073a9 <BlockThread>
c0107e49: e8 4d f8 ff ff                call 0xc010769b <UnlockScheduler>
c0107e4e: 0f 21 d8                      mov eax, dr3
c0107e51: c1 e0 06                      shl eax, 6
c0107e54: 8b 80 c4 40 11 c0             mov eax, dword ptr [eax - 1072611132]
c0107e5a: 83 c4 10                      add esp, 16
c0107e5d: 80 78 45 00                   cmp byte ptr [eax + 69], 0
c0107e61: 74 ab                         je 0xc0107e0e <SleepUntil+0x18>
c0107e63: b8 21 00 00 00                mov eax, 33
c0107e68: 5a                            pop edx
c0107e69: 5b                            pop ebx
c0107e6a: 5e                            pop esi
c0107e6b: c3                            ret

c0107e6c <SleepNano>:
c0107e6c: 57                            push edi
c0107e6d: 56                            push esi
c0107e6e: 50                            push eax
c0107e6f: 8b 74 24 10                   mov esi, dword ptr [esp + 16]
c0107e73: 8b 7c 24 14                   mov edi, dword ptr [esp + 20]
c0107e77: e8 cc fe ff ff                call 0xc0107d48 <GetSystemTimer>
c0107e7c: 01 f0                         add eax, esi
c0107e7e: 11 fa                         adc edx, edi
c0107e80: 89 44 24 10                   mov dword ptr [esp + 16], eax
c0107e84: 89 54 24 14                   mov dword ptr [esp + 20], edx
c0107e88: 5a                            pop edx
c0107e89: 5e                            pop esi
c0107e8a: 5f                            pop edi
```

```
c0107ed9: 56                            push esi
c0107eda: 53                            push ebx
c0107edb: 83 ec 20                      sub esp, 32
c0107ede: 89 e7                         mov edi, esp
c0107ee0: b9 1e 00 00 00                mov ecx, 30
c0107ee5: 31 db                         xor ebx, ebx
c0107ee7: 88 d8                         mov al, bl
c0107ee9: f3 aa                         rep  stosb byte ptr es:[edi], al
c0107eeb: c6 04 24 02                   mov byte ptr [esp], 2
c0107eef: a0 14 31 11 c0                mov al, byte ptr [3222352148]
c0107ef4: 88 44 24 1e                   mov byte ptr [esp + 30], al
c0107ef8: a0 48 b2 13 c0                mov al, byte ptr [3222516296]
c0107efd: 88 44 24 1f                   mov byte ptr [esp + 31], al
c0107f01: 50                            push eax
c0107f02: 6a 1a                         push 26
c0107f04: 68 28 b2 13 c0                push 3222516264
c0107f09: 8d 74 24 0c                   lea esi, [esp + 12]
c0107f0d: 8d 44 24 10                   lea eax, [esp + 16]
c0107f11: 50                            push eax
c0107f12: e8 a1 93 ff ff                call 0xc01012b8 <strncpy>
c0107f17: 83 ec 20                      sub esp, 32
c0107f1a: b9 08 00 00 00                mov ecx, 8
c0107f1f: 89 e7                         mov edi, esp
c0107f21: f3 a5                         rep  movsd dword ptr es:[edi], dword ptr [esi
c0107f23: e8 ad 0c 00 00                call 0xc0108bd5 <SendVideoMessage>
c0107f28: 31 d2                         xor edx, edx
c0107f2a: 89 15 44 b2 13 c0             mov dword ptr [-1072451004], edx
c0107f30: ba 28 b2 13 c0                mov edx, 3222516264
c0107f35: b9 1a 00 00 00                mov ecx, 26
c0107f3a: 89 d7                         mov edi, edx
c0107f3c: 88 d8                         mov al, bl
c0107f3e: f3 aa                         rep  stosb byte ptr es:[edi], al
c0107f40: 83 c4 50                      add esp, 80
c0107f43: 5b                            pop ebx
c0107f44: 5e                            pop esi
c0107f45: 5f                            pop edi
c0107f46: c3                            ret
c0107f47: c3                            ret

c0107f48 <Putchar>:
c0107f48: 89 c1                         mov ecx, eax
c0107f4a: 8b 15 44 b2 13 c0             mov edx, dword ptr [-1072451004]
c0107f50: 8d 42 01                      lea eax, [edx + 1]
c0107f53: a3 44 b2 13 c0                mov dword ptr [3222516292], eax
c0107f58: 88 8a 28 b2 13 c0             mov byte ptr [edx - 1072451032], cl
c0107f5e: 83 f8 19                      cmp eax, 25
c0107f61: 7e 05                         jle 0xc0107f68 <Putchar+0x20>
c0107f63: e9 67 ff ff ff                jmp 0xc0107ecf <Flush>
c0107f68: c3                            ret

c0107f69 <ConsoleDriverThread>:
c0107f69: 55                            push ebp
c0107f6a: 89 e5                         mov ebp, esp
c0107f6c: 57                            push edi
c0107f6d: 56                            push esi
c0107f6e: 53                            push ebx
c0107f6f: 83 ec 7c                      sub esp, 124
c0107f72: 31 f6                         xor esi, esi
c0107f74: 31 db                         xor ebx, ebx
c0107f76: 89 65 84                      mov dword ptr [ebp - 124], esp
c0107f79: 81 ec 00 01 00 00             sub esp, 256
c0107f7f: 89 65 88                      mov dword ptr [ebp - 120], esp
c0107f82: 8d 7d a8                      lea edi, [ebp - 88]
c0107f85: 50                            push eax
c0107f86: 6a 00                         push 0
c0107f88: 6a 00                         push 0
c0107f8a: 6a 00                         push 0
c0107f8c: 6a 00                         push 0
c0107f8e: 68 00 01 00 00                push 256
c0107f93: ff 75 88                      push dword ptr [ebp - 120]
c0107f96: 57                            push edi
```

```
c0107ff8: 3c 5b                   cmp al, 91
c0107ffa: 75 0a                   jne 0xc0108006 <ConsoleDriverThread+0x9d>
c0107ffc: 83 7d 90 0d             cmp dword ptr [ebp - 112], 13
c0108000: 0f 8e c1 01 00 00       jle 0xc01081c7 <ConsoleDriverThread+0x25e>
c0108006: 8b 45 90                mov eax, dword ptr [ebp - 112]
c0108009: c6 44 05 98 00          mov byte ptr [ebp + eax - 104], 0
c010800e: 80 7d 98 5b             cmp byte ptr [ebp - 104], 91
c0108012: 75 64                   jne 0xc0108078 <ConsoleDriverThread+0x10f>
c0108014: 53                      push ebx
c0108015: 53                      push ebx
c0108016: 68 df 0f 11 c0          push 3222343647
c010801b: 8d 5d 98                lea ebx, [ebp - 104]
c010801e: 53                      push ebx
c010801f: e8 7d 91 ff ff          call 0xc01011a1 <strcmp>
c0108024: 89 c2                   mov edx, eax
c0108026: 83 c4 10                add esp, 16
c0108029: 85 c0                   test eax, eax
c010802b: 75 52                   jne 0xc010807f <ConsoleDriverThread+0x116>
c010802d: 31 c9                   xor ecx, ecx
c010802f: 89 0d 44 b2 13 c0       mov dword ptr [-1072451004], ecx
c0108035: bb 28 b2 13 c0          mov ebx, 3222516264
c010803a: b9 1a 00 00 00          mov ecx, 26
c010803f: 31 c0                   xor eax, eax
c0108041: 89 df                   mov edi, ebx
c0108043: f3 aa                   rep  stosb byte ptr es:[edi], al
c0108045: 8d 7d c8                lea edi, [ebp - 56]
c0108048: b9 08 00 00 00          mov ecx, 8
c010804d: 89 d0                   mov eax, edx
c010804f: f3 ab                   rep  stosd dword ptr es:[edi], eax
c0108051: a0 14 31 11 c0          mov al, byte ptr [3222352148]
c0108056: 88 45 cc                mov byte ptr [ebp - 52], al
c0108059: a0 48 b2 13 c0          mov al, byte ptr [3222516296]
c010805e: 88 45 cd                mov byte ptr [ebp - 51], al
c0108061: 83 ec 20                sub esp, 32
c0108064: 8d 75 c8                lea esi, [ebp - 56]
c0108067: b9 08 00 00 00          mov ecx, 8
c010806c: 89 e7                   mov edi, esp
c010806e: f3 a5                   rep  movsd dword ptr es:[edi], dword ptr [esi
c0108070: e8 60 0b 00 00          call 0xc0108bd5 <SendVideoMessage>
c0108075: 83 c4 20                add esp, 32
c0108078: 31 db                   xor ebx, ebx
c010807a: e9 48 01 00 00          jmp 0xc01081c7 <ConsoleDriverThread+0x25e>
c010807f: 52                      push edx
c0108080: 52                      push edx
c0108081: 68 e3 0f 11 c0          push 3222343651
c0108086: 53                      push ebx
c0108087: e8 15 91 ff ff          call 0xc01011a1 <strcmp>
c010808c: 83 c4 10                add esp, 16
c010808f: 85 c0                   test eax, eax
c0108091: 75 15                   jne 0xc01080a8 <ConsoleDriverThread+0x13f>
c0108093: e8 37 fe ff ff          call 0xc0107ecf <Flush>
c0108098: c6 05 48 b2 13 c0 00    mov byte ptr [-1072451000], 0
c010809f: c6 05 14 31 11 c0 07    mov byte ptr [-1072615148], 7
c01080a6: eb d0                   jmp 0xc0108078 <ConsoleDriverThread+0x10f>
c01080a8: 83 ec 0c                sub esp, 12
c01080ab: 53                      push ebx
c01080ac: e8 26 91 ff ff          call 0xc01011d7 <strlen>
c01080b1: 83 c4 10                add esp, 16
c01080b4: 83 f8 03                cmp eax, 3
c01080b7: 0f 86 8d 00 00 00       jbe 0xc010814a <ConsoleDriverThread+0x1e1>
c01080bd: 83 ec 0c                sub esp, 12
c01080c0: 53                      push ebx
c01080c1: e8 11 91 ff ff          call 0xc01011d7 <strlen>
c01080c6: 83 c4 10                add esp, 16
c01080c9: 80 7c 05 97 6d          cmp byte ptr [ebp + eax - 105], 109
c01080ce: 75 7a                   jne 0xc010814a <ConsoleDriverThread+0x1e1>
c01080d0: e8 fa fd ff ff          call 0xc0107ecf <Flush>
c01080d5: c7 45 c8 00 04 02 06    mov dword ptr [ebp - 56], 100795392
c01080dc: c7 45 cc 01 05 03 07    mov dword ptr [ebp - 52], 117638401
c01080e3: 83 ec 0c                sub esp, 12
c01080e6: 8d 45 99                lea eax, [ebp - 103]
```

```
c010814e: e8 84 90 ff ff              call 0xc01011d7 <strlen>
c0108153: 83 c4 10                    add esp, 16
c0108156: 83 f8 03                    cmp eax, 3
c0108159: 76 3f                       jbe 0xc010819a <ConsoleDriverThread+0x231>
c010815b: 83 ec 0c                    sub esp, 12
c010815e: 53                          push ebx
c010815f: e8 73 90 ff ff              call 0xc01011d7 <strlen>
c0108164: 83 c4 10                    add esp, 16
c0108167: 80 7c 05 97 48              cmp byte ptr [ebp + eax - 105], 72
c010816c: 75 2c                       jne 0xc010819a <ConsoleDriverThread+0x231>
c010816e: 83 ec 0c                    sub esp, 12
c0108171: 8d 45 99                    lea eax, [ebp - 103]
c0108174: 50                          push eax
c0108175: e8 6e d9 ff ff              call 0xc0105ae8 <atoi>
c010817a: 89 c6                       mov esi, eax
c010817c: 83 c4 10                    add esp, 16
c010817f: b8 01 00 00 00              mov eax, 1
c0108184: 8a 54 05 98                 mov dl, byte ptr [ebp + eax - 104]
c0108188: 84 d2                       test dl, dl
c010818a: 0f 84 e8 fe ff ff           je 0xc0108078 <ConsoleDriverThread+0x10f>
c0108190: 80 fa 3b                    cmp dl, 59
c0108193: 8d 40 01                    lea eax, [eax + 1]
c0108196: 75 ec                       jne 0xc0108184 <ConsoleDriverThread+0x21b>
c0108198: eb 45                       jmp 0xc01081df <ConsoleDriverThread+0x276>
c010819a: b8 1b 00 00 00              mov eax, 27
c010819f: e8 a4 fd ff ff              call 0xc0107f48 <Putchar>
c01081a4: 43                          inc ebx
c01081a5: 0f be 43 ff                 movsx eax, byte ptr [ebx - 1]
c01081a9: 84 c0                       test al, al
c01081ab: 75 f2                       jne 0xc010819f <ConsoleDriverThread+0x236>
c01081ad: e9 c6 fe ff ff              jmp 0xc0108078 <ConsoleDriverThread+0x10f>
c01081b2: 3c 1b                       cmp al, 27
c01081b4: 74 0a                       je 0xc01081c0 <ConsoleDriverThread+0x257>
c01081b6: e8 8d fd ff ff              call 0xc0107f48 <Putchar>
c01081bb: 89 75 90                    mov dword ptr [ebp - 112], esi
c01081be: eb 07                       jmp 0xc01081c7 <ConsoleDriverThread+0x25e>
c01081c0: 31 c0                       xor eax, eax
c01081c2: 89 45 90                    mov dword ptr [ebp - 112], eax
c01081c5: b3 01                       mov bl, 1
c01081c7: ff 45 8c                    inc dword ptr [ebp - 116]
c01081ca: 8b 75 90                    mov esi, dword ptr [ebp - 112]
c01081cd: e9 e0 fd ff ff              jmp 0xc0107fb2 <ConsoleDriverThread+0x49>
c01081d2: e8 f8 fc ff ff              call 0xc0107ecf <Flush>
c01081d7: 8b 65 84                    mov esp, dword ptr [ebp - 124]
c01081da: e9 97 fd ff ff              jmp 0xc0107f76 <ConsoleDriverThread+0xd>
c01081df: 8d 4d 98                    lea ecx, [ebp - 104]
c01081e2: 01 c8                       add eax, ecx
c01081e4: 80 38 00                    cmp byte ptr [eax], 0
c01081e7: 0f 84 8b fe ff ff           je 0xc0108078 <ConsoleDriverThread+0x10f>
c01081ed: 83 ec 0c                    sub esp, 12
c01081f0: 50                          push eax
c01081f1: e8 f2 d8 ff ff              call 0xc0105ae8 <atoi>
c01081f6: 89 c3                       mov ebx, eax
c01081f8: e8 d2 fc ff ff              call 0xc0107ecf <Flush>
c01081fd: 8d 7d c8                    lea edi, [ebp - 56]
c0108200: b9 08 00 00 00              mov ecx, 8
c0108205: 31 c0                       xor eax, eax
c0108207: f3 ab                       rep  stosd dword ptr es:[edi], eax
c0108209: c6 45 c8 03                 mov byte ptr [ebp - 56], 3
c010820d: 4b                          dec ebx
c010820e: 89 5d cc                    mov dword ptr [ebp - 52], ebx
c0108211: 8d 46 ff                    lea eax, [esi - 1]
c0108214: 89 45 d0                    mov dword ptr [ebp - 48], eax
c0108217: 83 ec 20                    sub esp, 32
c010821a: 8d 75 c8                    lea esi, [ebp - 56]
c010821d: b9 08 00 00 00              mov ecx, 8
c0108222: 89 e7                       mov edi, esp
c0108224: f3 a5                       rep  movsd dword ptr es:[edi], dword ptr [esi
c0108226: e8 aa 09 00 00              call 0xc0108bd5 <SendVideoMessage>
c010822b: 83 c4 30                    add esp, 48
c010822e: e9 45 fe ff ff              jmp 0xc0108078 <ConsoleDriverThread+0x10f>
```

```
c0108290: 50                            push eax
c0108291: 6a 00                         push 0
c0108293: 68 69 7f 10 c0                push 3222306665
c0108298: e8 ab f6 ff ff                call 0xc0107948 <CreateThread>
c010829d: c6 05 49 b2 13 c0 01          mov byte ptr [-1072450999], 1
c01082a4: 31 c0                         xor eax, eax
c01082a6: a3 44 b2 13 c0                mov dword ptr [3222516292], eax
c01082ab: ba 28 b2 13 c0                mov edx, 3222516264
c01082b0: b9 1a 00 00 00                mov ecx, 26
c01082b5: 31 c0                         xor eax, eax
c01082b7: 89 d7                         mov edi, edx
c01082b9: f3 aa                         rep  stosb byte ptr es:[edi], al
c01082bb: 83 c4 38                      add esp, 56
c01082be: 5f                            pop edi
c01082bf: c3                            ret

c01082c0 <SendKeystrokeConsole>:
c01082c0: 53                            push ebx
c01082c1: 83 ec 38                      sub esp, 56
c01082c4: 8b 44 24 40                   mov eax, dword ptr [esp + 64]
c01082c8: 88 44 24 0c                   mov byte ptr [esp + 12], al
c01082cc: 80 3d 49 b2 13 c0 00          cmp byte ptr [-1072450999], 0
c01082d3: 74 2b                         je 0xc0108300 <SendKeystrokeConsole+0x40>
c01082d5: 8d 5c 24 10                   lea ebx, [esp + 16]
c01082d9: 50                            push eax
c01082da: 6a 01                         push 1
c01082dc: 6a 00                         push 0
c01082de: 6a 00                         push 0
c01082e0: 6a 00                         push 0
c01082e2: 6a 01                         push 1
c01082e4: 8d 44 24 24                   lea eax, [esp + 36]
c01082e8: 50                            push eax
c01082e9: 53                            push ebx
c01082ea: e8 c1 14 00 00                call 0xc01097b0 <CreateKernelTransfer>
c01082ef: 89 1c 24                      mov dword ptr [esp], ebx
c01082f2: ff 35 4c b2 13 c0             push dword ptr [-1072450996]
c01082f8: e8 dd 1f 00 00                call 0xc010a2da <WriteFile>
c01082fd: 83 c4 20                      add esp, 32
c0108300: 83 c4 38                      add esp, 56
c0108303: 5b                            pop ebx
c0108304: c3                            ret

c0108305 <DriverTableComparatorByRelocationPoint>:
c0108305: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c0108309: 8b 48 04                      mov ecx, dword ptr [eax + 4]
c010830c: 8b 44 24 08                   mov eax, dword ptr [esp + 8]
c0108310: 8b 50 04                      mov edx, dword ptr [eax + 4]
c0108313: b8 01 00 00 00                mov eax, 1
c0108318: 39 ca                         cmp edx, ecx
c010831a: 72 04                         jb 0xc0108320 <DriverTableComparatorByRelocat
c010831c: 39 d1                         cmp ecx, edx
c010831e: 19 c0                         sbb eax, eax
c0108320: c3                            ret

c0108321 <BinarySearchComparator>:
c0108321: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c0108325: 8b 10                         mov edx, dword ptr [eax]
c0108327: c1 ea 0c                      shr edx, 12
c010832a: 8b 44 24 08                   mov eax, dword ptr [esp + 8]
c010832e: 8b 00                         mov eax, dword ptr [eax]
c0108330: c1 e8 0c                      shr eax, 12
c0108333: b9 01 00 00 00                mov ecx, 1
c0108338: 39 d0                         cmp eax, edx
c010833a: 72 04                         jb 0xc0108340 <BinarySearchComparator+0x1f>
c010833c: 39 c2                         cmp edx, eax
c010833e: 19 c9                         sbb ecx, ecx
c0108340: 89 c8                         mov eax, ecx
c0108342: c3                            ret

c0108343 <GetDriverAddressWithLockHeld>:
c0108343: 83 ec 24                      sub esp, 36
```

```
c010839c: e9 00 8e ff ff                jmp 0xc01011a1 <strcmp>

c01083a1 <GetDriverAddress>:
c01083a1: 83 ec 24                      sub esp, 36
c01083a4: 6a ff                         push -1
c01083a6: ff 35 5c b2 13 c0             push dword ptr [-1072450980]
c01083ac: e8 88 e3 ff ff                call 0xc0106739 <AcquireSemaphore>
c01083b1: 8b 44 24 30                   mov eax, dword ptr [esp + 48]
c01083b5: e8 89 ff ff ff                call 0xc0108343 <GetDriverAddressWithLockHeld
c01083ba: 89 44 24 1c                   mov dword ptr [esp + 28], eax
c01083be: 58                            pop eax
c01083bf: ff 35 5c b2 13 c0             push dword ptr [-1072450980]
c01083c5: e8 e9 e4 ff ff                call 0xc01068b3 <ReleaseSemaphore>
c01083ca: 8b 44 24 1c                   mov eax, dword ptr [esp + 28]
c01083ce: 83 c4 2c                      add esp, 44
c01083d1: c3                            ret

c01083d2 <InitSymbolTable>:
c01083d2: 83 ec 20                      sub esp, 32
c01083d5: 6a 00                         push 0
c01083d7: 6a 01                         push 1
c01083d9: 68 eb 0f 11 c0                push 3222343659
c01083de: e8 f6 e2 ff ff                call 0xc01066d9 <CreateSemaphore>
c01083e3: a3 5c b2 13 c0                mov dword ptr [3222516316], eax
c01083e8: 83 c4 0c                      add esp, 12
c01083eb: 6a 00                         push 0
c01083ed: 6a 01                         push 1
c01083ef: 68 f5 0f 11 c0                push 3222343669
c01083f4: e8 e0 e2 ff ff                call 0xc01066d9 <CreateSemaphore>
c01083f9: a3 58 b2 13 c0                mov dword ptr [3222516312], eax
c01083fe: e8 4a 9c ff ff                call 0xc010204d <TreeCreate>
c0108403: a3 54 b2 13 c0                mov dword ptr [3222516308], eax
c0108408: e8 40 9c ff ff                call 0xc010204d <TreeCreate>
c010840d: a3 50 b2 13 c0                mov dword ptr [3222516304], eax
c0108412: 59                            pop ecx
c0108413: 5a                            pop edx
c0108414: 68 88 83 10 c0                push 3222307720
c0108419: 50                            push eax
c010841a: e8 5c 9c ff ff                call 0xc010207b <TreeSetComparator>
c010841f: 8d 44 24 1c                   lea eax, [esp + 28]
c0108423: 50                            push eax
c0108424: 6a 00                         push 0
c0108426: 6a 00                         push 0
c0108428: 68 ff 0f 11 c0                push 3222343679
c010842d: e8 1b 1c 00 00                call 0xc010a04d <OpenFile>
c0108432: 83 c4 20                      add esp, 32
c0108435: 85 c0                         test eax, eax
c0108437: 74 0a                         je 0xc0108443 <InitSymbolTable+0x71>
c0108439: 83 ec 0c                      sub esp, 12
c010843c: 6a 17                         push 23
c010843e: e8 5c 07 00 00                call 0xc0108b9f <Panic>
c0108443: 50                            push eax
c0108444: 50                            push eax
c0108445: 6a 00                         push 0
c0108447: ff 74 24 18                   push dword ptr [esp + 24]
c010844b: e8 5c 4d 00 00                call 0xc010d1ac <ArchLoadSymbols>
c0108450: 5a                            pop edx
c0108451: ff 74 24 18                   push dword ptr [esp + 24]
c0108455: e8 92 1e 00 00                call 0xc010a2ec <CloseFile>
c010845a: 83 c4 2c                      add esp, 44
c010845d: c3                            ret

c010845e <AddSymbol>:
c010845e: 57                            push edi
c010845f: 56                            push esi
c0108460: 53                            push ebx
c0108461: 8b 74 24 10                   mov esi, dword ptr [esp + 16]
c0108465: 8b 7c 24 14                   mov edi, dword ptr [esp + 20]
c0108469: 89 f3                         mov ebx, esi
c010846b: 0f be 03                      movsx eax, byte ptr [ebx]
c010846e: 84 c0                         test al, al
```

```
c01084bd: e8 77 e2 ff ff             call 0xc0106739 <AcquireSemaphore>
c01084c2: 5e                         pop esi
c01084c3: 5f                         pop edi
c01084c4: 53                         push ebx
c01084c5: ff 35 50 b2 13 c0          push dword ptr [-1072450992]
c01084cb: e8 1d 9c ff ff             call 0xc01020ed <TreeContains>
c01084d0: 83 c4 10                   add esp, 16
c01084d3: 84 c0                      test al, al
c01084d5: 74 0b                      je 0xc01084e2 <AddSymbol+0x84>
c01084d7: 83 ec 0c                   sub esp, 12
c01084da: 53                         push ebx
c01084db: e8 93 b4 ff ff             call 0xc0103973 <FreeHeap>
c01084e0: eb 0e                      jmp 0xc01084f0 <AddSymbol+0x92>
c01084e2: 50                         push eax
c01084e3: 50                         push eax
c01084e4: 53                         push ebx
c01084e5: ff 35 50 b2 13 c0          push dword ptr [-1072450992]
c01084eb: e8 9a 9b ff ff             call 0xc010208a <TreeInsert>
c01084f0: 83 c4 10                   add esp, 16
c01084f3: a1 58 b2 13 c0             mov eax, dword ptr [3222516312]
c01084f8: 89 44 24 10                mov dword ptr [esp + 16], eax
c01084fc: 5b                         pop ebx
c01084fd: 5e                         pop esi
c01084fe: 5f                         pop edi
c01084ff: e9 af e3 ff ff             jmp 0xc01068b3 <ReleaseSemaphore>
c0108504: 5b                         pop ebx
c0108505: 5e                         pop esi
c0108506: 5f                         pop edi
c0108507: c3                         ret

c0108508 <GetSymbolAddress>:
c0108508: 53                         push ebx
c0108509: 83 ec 20                   sub esp, 32
c010850c: 31 c0                      xor eax, eax
c010850e: 89 44 24 14                mov dword ptr [esp + 20], eax
c0108512: 8b 44 24 28                mov eax, dword ptr [esp + 40]
c0108516: 89 44 24 10                mov dword ptr [esp + 16], eax
c010851a: 6a ff                      push -1
c010851c: ff 35 58 b2 13 c0          push dword ptr [-1072450984]
c0108522: e8 12 e2 ff ff             call 0xc0106739 <AcquireSemaphore>
c0108527: 5a                         pop edx
c0108528: 59                         pop ecx
c0108529: 8d 44 24 10                lea eax, [esp + 16]
c010852d: 50                         push eax
c010852e: ff 35 50 b2 13 c0          push dword ptr [-1072450992]
c0108534: e8 c7 9b ff ff             call 0xc0102100 <TreeGet>
c0108539: 89 c3                      mov ebx, eax
c010853b: 58                         pop eax
c010853c: ff 35 58 b2 13 c0          push dword ptr [-1072450984]
c0108542: e8 6c e3 ff ff             call 0xc01068b3 <ReleaseSemaphore>
c0108547: 83 c4 10                   add esp, 16
c010854a: 31 c0                      xor eax, eax
c010854c: 85 db                      test ebx, ebx
c010854e: 74 03                      je 0xc0108553 <GetSymbolAddress+0x4b>
c0108550: 8b 43 04                   mov eax, dword ptr [ebx + 4]
c0108553: 83 c4 18                   add esp, 24
c0108556: 5b                         pop ebx
c0108557: c3                         ret

c0108558 <RequireDriver>:
c0108558: 57                         push edi
c0108559: 56                         push esi
c010855a: 53                         push ebx
c010855b: 83 ec 18                   sub esp, 24
c010855e: 8b 7c 24 28                mov edi, dword ptr [esp + 40]
c0108562: 57                         push edi
c0108563: 68 0f 10 11 c0             push 3222343695
c0108568: e8 58 05 00 00             call 0xc0108ac5 <LogWriteSerial>
c010856d: 58                         pop eax
c010856e: 5a                         pop edx
c010856f: 6a ff                      push -1
```

```
c01085ce: 89 03                         mov dword ptr [ebx], eax
c01085d0: 31 c0                         xor eax, eax
c01085d2: 89 43 08                      mov dword ptr [ebx + 8], eax
c01085d5: 89 43 04                      mov dword ptr [ebx + 4], eax
c01085d8: 6a 00                         push 0
c01085da: 8d 43 08                      lea eax, [ebx + 8]
c01085dd: 50                            push eax
c01085de: ff 74 24 24                   push dword ptr [esp + 36]
c01085e2: 8d 43 04                      lea eax, [ebx + 4]
c01085e5: 50                            push eax
c01085e6: e8 91 45 00 00                call 0xc010cb7c <ArchLoadDriver>
c01085eb: 89 c6                         mov esi, eax
c01085ed: 83 c4 20                      add esp, 32
c01085f0: 85 c0                         test eax, eax
c01085f2: 75 2e                         jne 0xc0108622 <RequireDriver+0xca>
c01085f4: 50                            push eax
c01085f5: ff 73 04                      push dword ptr [ebx + 4]
c01085f8: 57                            push edi
c01085f9: 68 25 10 11 c0                push 3222343717
c01085fe: e8 c2 04 00 00                call 0xc0108ac5 <LogWriteSerial>
c0108603: 5a                            pop edx
c0108604: 59                            pop ecx
c0108605: 53                            push ebx
c0108606: ff 35 54 b2 13 c0             push dword ptr [-1072450988]
c010860c: e8 79 9a ff ff                call 0xc010208a <TreeInsert>
c0108611: 5f                            pop edi
c0108612: 58                            pop eax
c0108613: ff 73 04                      push dword ptr [ebx + 4]
c0108616: ff 74 24 18                   push dword ptr [esp + 24]
c010861a: e8 8d 4b 00 00                call 0xc010d1ac <ArchLoadSymbols>
c010861f: 83 c4 10                      add esp, 16
c0108622: 83 ec 0c                      sub esp, 12
c0108625: ff 35 5c b2 13 c0             push dword ptr [-1072450980]
c010862b: e8 83 e2 ff ff                call 0xc01068b3 <ReleaseSemaphore>
c0108630: 83 c4 10                      add esp, 16
c0108633: 89 f0                         mov eax, esi
c0108635: 83 c4 10                      add esp, 16
c0108638: 5b                            pop ebx
c0108639: 5e                            pop esi
c010863a: 5f                            pop edi
c010863b: c3                            ret

c010863c <SortRelocationTable>:
c010863c: 83 ec 0c                      sub esp, 12
c010863f: 8b 44 24 10                   mov eax, dword ptr [esp + 16]
c0108643: 68 22 6b 10 c0                push 3222301474
c0108648: 6a 08                         push 8
c010864a: ff 70 04                      push dword ptr [eax + 4]
c010864d: ff 70 08                      push dword ptr [eax + 8]
c0108650: e8 06 d8 ff ff                call 0xc0105e5b <qsort_pageable>
c0108655: 83 c4 1c                      add esp, 28
c0108658: c3                            ret

c0108659 <AddToRelocationTable>:
c0108659: 53                            push ebx
c010865a: 8b 44 24 08                   mov eax, dword ptr [esp + 8]
c010865e: 8b 48 04                      mov ecx, dword ptr [eax + 4]
c0108661: 8b 50 08                      mov edx, dword ptr [eax + 8]
c0108664: 8b 5c 24 0c                   mov ebx, dword ptr [esp + 12]
c0108668: 89 1c ca                      mov dword ptr [edx + 8*ecx], ebx
c010866b: 8b 48 04                      mov ecx, dword ptr [eax + 4]
c010866e: 8b 50 08                      mov edx, dword ptr [eax + 8]
c0108671: 8b 5c 24 10                   mov ebx, dword ptr [esp + 16]
c0108675: 89 5c ca 04                   mov dword ptr [edx + 8*ecx + 4], ebx
c0108679: ff 40 04                      inc dword ptr [eax + 4]
c010867c: 5b                            pop ebx
c010867d: c3                            ret

c010867e <CreateRelocationTable>:
c010867e: 56                            push esi
c010867f: 53                            push ebx
```

```
c01086be: 53                            push ebx
c01086bf: 83 ec 34                      sub esp, 52
c01086c2: 8b 5c 24 50                   mov ebx, dword ptr [esp + 80]
c01086c6: 6a ff                         push -1
c01086c8: ff 35 5c b2 13 c0             push dword ptr [-1072450980]
c01086ce: e8 66 e0 ff ff                call 0xc0106739 <AcquireSemaphore>
c01086d3: 5e                            pop esi
c01086d4: 5f                            pop edi
c01086d5: 68 05 83 10 c0                push 3222307589
c01086da: ff 35 54 b2 13 c0             push dword ptr [-1072450988]
c01086e0: e8 96 99 ff ff                call 0xc010207b <TreeSetComparator>
c01086e5: 8d 7c 24 24                   lea edi, [esp + 36]
c01086e9: b9 03 00 00 00                mov ecx, 3
c01086ee: 31 c0                         xor eax, eax
c01086f0: f3 ab                         rep  stosd dword ptr es:[edi], eax
c01086f2: 8b 44 24 54                   mov eax, dword ptr [esp + 84]
c01086f6: 89 44 24 28                   mov dword ptr [esp + 40], eax
c01086fa: 5d                            pop ebp
c01086fb: 58                            pop eax
c01086fc: 8d 7c 24 1c                   lea edi, [esp + 28]
c0108700: 57                            push edi
c0108701: ff 35 54 b2 13 c0             push dword ptr [-1072450988]
c0108707: e8 f4 99 ff ff                call 0xc0102100 <TreeGet>
c010870c: 89 c6                         mov esi, eax
c010870e: 58                            pop eax
c010870f: ff 35 5c b2 13 c0             push dword ptr [-1072450980]
c0108715: e8 99 e1 ff ff                call 0xc01068b3 <ReleaseSemaphore>
c010871a: 83 c4 10                      add esp, 16
c010871d: 85 f6                         test esi, esi
c010871f: 75 09                         jne 0xc010872a <RelocatePage+0x6f>
c0108721: 51                            push ecx
c0108722: 51                            push ecx
c0108723: 68 47 10 11 c0                push 3222343751
c0108728: eb 57                         jmp 0xc0108781 <RelocatePage+0xc6>
c010872a: 8b 6e 08                      mov ebp, dword ptr [esi + 8]
c010872d: 89 5c 24 14                   mov dword ptr [esp + 20], ebx
c0108731: 83 ec 0c                      sub esp, 12
c0108734: 68 54 10 11 c0                push 3222343764
c0108739: e8 87 03 00 00                call 0xc0108ac5 <LogWriteSerial>
c010873e: c7 04 24 21 83 10 c0          mov dword ptr [esp], 3222307617
c0108745: 6a 08                         push 8
c0108747: ff 75 04                      push dword ptr [ebp + 4]
c010874a: ff 75 08                      push dword ptr [ebp + 8]
c010874d: 57                            push edi
c010874e: e8 32 d7 ff ff                call 0xc0105e85 <bsearch>
c0108753: 83 c4 20                      add esp, 32
c0108756: 85 c0                         test eax, eax
c0108758: 74 07                         je 0xc0108761 <RelocatePage+0xa6>
c010875a: 89 df                         mov edi, ebx
c010875c: c1 ef 0c                      shr edi, 12
c010875f: eb 36                         jmp 0xc0108797 <RelocatePage+0xdc>
c0108761: 50                            push eax
c0108762: 50                            push eax
c0108763: 53                            push ebx
c0108764: 68 6d 10 11 c0                push 3222343789
c0108769: e8 57 03 00 00                call 0xc0108ac5 <LogWriteSerial>
c010876e: c7 04 24 96 10 11 c0          mov dword ptr [esp], 3222343830
c0108775: e8 4b 03 00 00                call 0xc0108ac5 <LogWriteSerial>
c010877a: 58                            pop eax
c010877b: 5a                            pop edx
c010877c: 68 da 10 11 c0                push 3222343898
c0108781: 6a 09                         push 9
c0108783: e8 c6 03 00 00                call 0xc0108b4e <PanicEx>
c0108788: 83 ea 03                      sub edx, 3
c010878b: 39 d7                         cmp edi, edx
c010878d: 75 15                         jne 0xc01087a4 <RelocatePage+0xe9>
c010878f: 3b 45 08                      cmp eax, dword ptr [ebp + 8]
c0108792: 74 10                         je 0xc01087a4 <RelocatePage+0xe9>
c0108794: 83 e8 08                      sub eax, 8
c0108797: 8b 10                         mov edx, dword ptr [eax]
c0108799: 89 d1                         mov ecx, edx
```

```
c01087ea: c1 e9 0c                      shr ecx, 12
c01087ed: 39 cf                         cmp edi, ecx
c01087ef: 75 55                         jne 0xc0108846 <RelocatePage+0x18b>
c01087f1: 83 c0 05                      add eax, 5
c01087f4: c1 e8 0c                      shr eax, 12
c01087f7: 39 c7                         cmp edi, eax
c01087f9: 74 37                         je 0xc0108832 <RelocatePage+0x177>
c01087fb: 8d ab 00 10 00 00             lea ebp, [ebx + 4096]
c0108801: 83 ec 0c                      sub esp, 12
c0108804: 55                            push ebp
c0108805: e8 eb c4 ff ff                call 0xc0104cf5 <LockVirt>
c010880a: 83 f0 01                      xor eax, 1
c010880d: 88 44 24 17                   mov byte ptr [esp + 23], al
c0108811: 89 2c 24                      mov dword ptr [esp], ebp
c0108814: e8 9b c0 ff ff                call 0xc01048b4 <GetVirtPermissions>
c0108819: 83 c4 10                      add esp, 16
c010881c: 31 d2                         xor edx, edx
c010881e: a8 02                         test al, 2
c0108820: 75 10                         jne 0xc0108832 <RelocatePage+0x177>
c0108822: 51                            push ecx
c0108823: 6a 00                         push 0
c0108825: 6a 02                         push 2
c0108827: 55                            push ebp
c0108828: e8 30 c1 ff ff                call 0xc010495d <SetVirtPermissions>
c010882d: 83 c4 10                      add esp, 16
c0108830: b2 01                         mov dl, 1
c0108832: 8b 4e 04                      mov ecx, dword ptr [esi + 4]
c0108835: 8b 06                         mov eax, dword ptr [esi]
c0108837: 89 08                         mov dword ptr [eax], ecx
c0108839: 8b 44 24 0c                   mov eax, dword ptr [esp + 12]
c010883d: 3b 06                         cmp eax, dword ptr [esi]
c010883f: 74 0c                         je 0xc010884d <RelocatePage+0x192>
c0108841: 83 c6 08                      add esi, 8
c0108844: eb a0                         jmp 0xc01087e6 <RelocatePage+0x12b>
c0108846: 8d 48 fd                      lea ecx, [eax - 3]
c0108849: 39 cf                         cmp edi, ecx
c010884b: 74 a4                         je 0xc01087f1 <RelocatePage+0x136>
c010884d: 83 7c 24 08 00                cmp dword ptr [esp + 8], 0
c0108852: 75 16                         jne 0xc010886a <RelocatePage+0x1af>
c0108854: 88 54 24 08                   mov byte ptr [esp + 8], dl
c0108858: 52                            push edx
c0108859: 6a 02                         push 2
c010885b: 6a 00                         push 0
c010885d: 53                            push ebx
c010885e: e8 fa c0 ff ff                call 0xc010495d <SetVirtPermissions>
c0108863: 83 c4 10                      add esp, 16
c0108866: 8a 54 24 08                   mov dl, byte ptr [esp + 8]
c010886a: 84 d2                         test dl, dl
c010886c: 74 14                         je 0xc0108882 <RelocatePage+0x1c7>
c010886e: 50                            push eax
c010886f: 6a 02                         push 2
c0108871: 6a 00                         push 0
c0108873: 8d 83 00 10 00 00             lea eax, [ebx + 4096]
c0108879: 50                            push eax
c010887a: e8 de c0 ff ff                call 0xc010495d <SetVirtPermissions>
c010887f: 83 c4 10                      add esp, 16
c0108882: 80 7c 24 07 00                cmp byte ptr [esp + 7], 0
c0108887: 74 12                         je 0xc010889b <RelocatePage+0x1e0>
c0108889: 83 ec 0c                      sub esp, 12
c010888c: 81 c3 00 10 00 00             add ebx, 4096
c0108892: 53                            push ebx
c0108893: e8 06 c1 ff ff                call 0xc010499e <UnlockVirt>
c0108898: 83 c4 10                      add esp, 16
c010889b: 83 c4 2c                      add esp, 44
c010889e: 5b                            pop ebx
c010889f: 5e                            pop esi
c01088a0: 5f                            pop edi
c01088a1: 5d                            pop ebp
c01088a2: c3                            ret

c01088a3 <LogChar>:
```

```
c01088de: 88 4c 24 0f                mov byte ptr [esp + 15], cl
c01088e2: 8d 4c 24 14                lea ecx, [esp + 20]
c01088e6: 89 cf                      mov edi, ecx
c01088e8: 41                         inc ecx
c01088e9: 89 c5                      mov ebp, eax
c01088eb: 31 d2                      xor edx, edx
c01088ed: f7 f3                      div ebx
c01088ef: 39 dd                      cmp ebp, ebx
c01088f1: 73 f5                      jae 0xc01088e8 <LogInt+0x15>
c01088f3: c6 01 00                   mov byte ptr [ecx], 0
c01088f6: 89 f0                      mov eax, esi
c01088f8: 31 d2                      xor edx, edx
c01088fa: f7 f3                      div ebx
c01088fc: 49                         dec ecx
c01088fd: 8a 92 28 11 11 c0          mov dl, byte ptr [edx - 1072623320]
c0108903: 88 11                      mov byte ptr [ecx], dl
c0108905: 89 f2                      mov edx, esi
c0108907: 89 c6                      mov esi, eax
c0108909: 39 da                      cmp edx, ebx
c010890b: 73 e9                      jae 0xc01088f6 <LogInt+0x23>
c010890d: 0f b6 5c 24 0f             movzx ebx, byte ptr [esp + 15]
c0108912: 0f be 07                   movsx eax, byte ptr [edi]
c0108915: 84 c0                      test al, al
c0108917: 74 0a                      je 0xc0108923 <LogInt+0x50>
c0108919: 47                         inc edi
c010891a: 89 da                      mov edx, ebx
c010891c: e8 82 ff ff ff             call 0xc01088a3 <LogChar>
c0108921: eb ef                      jmp 0xc0108912 <LogInt+0x3f>
c0108923: 83 c4 2c                   add esp, 44
c0108926: 5b                         pop ebx
c0108927: 5e                         pop esi
c0108928: 5f                         pop edi
c0108929: 5d                         pop ebp
c010892a: c3                         ret

c010892b <LogWriteSerialVa>:
c010892b: 55                         push ebp
c010892c: 57                         push edi
c010892d: 56                         push esi
c010892e: 53                         push ebx
c010892f: 83 ec 1c                   sub esp, 28
c0108932: 8b 7c 24 30                mov edi, dword ptr [esp + 48]
c0108936: 8b 5c 24 34                mov ebx, dword ptr [esp + 52]
c010893a: 8b 44 24 38                mov eax, dword ptr [esp + 56]
c010893e: 89 44 24 04                mov dword ptr [esp + 4], eax
c0108942: 8a 44 24 04                mov al, byte ptr [esp + 4]
c0108946: 88 44 24 03                mov byte ptr [esp + 3], al
c010894a: 85 ff                      test edi, edi
c010894c: 75 05                      jne 0xc0108953 <LogWriteSerialVa+0x28>
c010894e: bf 39 11 11 c0             mov edi, 3222343993
c0108953: 80 3d 15 31 11 c0 00       cmp byte ptr [-1072615147], 0
c010895a: 74 2d                      je 0xc0108989 <LogWriteSerialVa+0x5e>
c010895c: 50                         push eax
c010895d: 6a 29                      push 41
c010895f: 68 3e 11 11 c0             push 3222343998
c0108964: 68 60 b2 13 c0             push 3222516320
c0108969: e8 d1 df ff ff             call 0xc010693f <InitSpinlock>
c010896e: 83 c4 0c                   add esp, 12
c0108971: 6a 00                      push 0
c0108973: 6a 01                      push 1
c0108975: 68 42 11 11 c0             push 3222344002
c010897a: e8 5a dd ff ff             call 0xc01066d9 <CreateSemaphore>
c010897f: c6 05 15 31 11 c0 00       mov byte ptr [-1072615147], 0
c0108986: 83 c4 10                   add esp, 16
c0108989: 80 7c 24 04 00             cmp byte ptr [esp + 4], 0
c010898e: 75 1d                      jne 0xc01089ad <LogWriteSerialVa+0x82>
c0108990: 83 ec 0c                   sub esp, 12
c0108993: 68 60 b2 13 c0             push 3222516320
c0108998: e8 bd df ff ff             call 0xc010695a <AcquireSpinlock>
c010899d: 83 c4 10                   add esp, 16
c01089a0: 31 f6                      xor esi, esi
```

```
c01089fc: 74 2a                         je 0xc0108a28 <LogWriteSerialVa+0xfd>
c01089fe: 3c 4c                         cmp al, 76
c0108a00: 74 49                         je 0xc0108a4b <LogWriteSerialVa+0x120>
c0108a02: eb 6f                         jmp 0xc0108a73 <LogWriteSerialVa+0x148>
c0108a04: 3c 75                         cmp al, 117
c0108a06: 74 52                         je 0xc0108a5a <LogWriteSerialVa+0x12f>
c0108a08: 7f 18                         jg 0xc0108a22 <LogWriteSerialVa+0xf7>
c0108a0a: 3c 6c                         cmp al, 108
c0108a0c: 74 3d                         je 0xc0108a4b <LogWriteSerialVa+0x120>
c0108a0e: 3c 73                         cmp al, 115
c0108a10: 75 61                         jne 0xc0108a73 <LogWriteSerialVa+0x148>
c0108a12: 8d 6b 04                      lea ebp, [ebx + 4]
c0108a15: 8b 1b                         mov ebx, dword ptr [ebx]
c0108a17: 0f b6 44 24 03                movzx eax, byte ptr [esp + 3]
c0108a1c: 89 44 24 0c                   mov dword ptr [esp + 12], eax
c0108a20: eb 11                         jmp 0xc0108a33 <LogWriteSerialVa+0x108>
c0108a22: 3c 78                         cmp al, 120
c0108a24: 74 20                         je 0xc0108a46 <LogWriteSerialVa+0x11b>
c0108a26: eb 4b                         jmp 0xc0108a73 <LogWriteSerialVa+0x148>
c0108a28: 8b 54 24 08                   mov edx, dword ptr [esp + 8]
c0108a2c: b8 25 00 00 00                mov eax, 37
c0108a31: eb 61                         jmp 0xc0108a94 <LogWriteSerialVa+0x169>
c0108a33: 0f be 03                      movsx eax, byte ptr [ebx]
c0108a36: 84 c0                         test al, al
c0108a38: 74 b0                         je 0xc01089ea <LogWriteSerialVa+0xbf>
c0108a3a: 43                            inc ebx
c0108a3b: 8b 54 24 0c                   mov edx, dword ptr [esp + 12]
c0108a3f: e8 5f fe ff ff                call 0xc01088a3 <LogChar>
c0108a44: eb ed                         jmp 0xc0108a33 <LogWriteSerialVa+0x108>
c0108a46: 8d 6b 04                      lea ebp, [ebx + 4]
c0108a49: eb 03                         jmp 0xc0108a4e <LogWriteSerialVa+0x123>
c0108a4b: 8d 6b 08                      lea ebp, [ebx + 8]
c0108a4e: 0f b6 4c 24 03                movzx ecx, byte ptr [esp + 3]
c0108a53: ba 10 00 00 00                mov edx, 16
c0108a58: eb 0d                         jmp 0xc0108a67 <LogWriteSerialVa+0x13c>
c0108a5a: 8d 6b 04                      lea ebp, [ebx + 4]
c0108a5d: 0f b6 4c 24 03                movzx ecx, byte ptr [esp + 3]
c0108a62: ba 0a 00 00 00                mov edx, 10
c0108a67: 8b 03                         mov eax, dword ptr [ebx]
c0108a69: e8 65 fe ff ff                call 0xc01088d3 <LogInt>
c0108a6e: e9 77 ff ff ff                jmp 0xc01089ea <LogWriteSerialVa+0xbf>
c0108a73: 0f b6 54 24 03                movzx edx, byte ptr [esp + 3]
c0108a78: 89 54 24 0c                   mov dword ptr [esp + 12], edx
c0108a7c: b8 25 00 00 00                mov eax, 37
c0108a81: e8 1d fe ff ff                call 0xc01088a3 <LogChar>
c0108a86: 0f be 45 00                   movsx eax, byte ptr [ebp]
c0108a8a: 8b 54 24 0c                   mov edx, dword ptr [esp + 12]
c0108a8e: eb 04                         jmp 0xc0108a94 <LogWriteSerialVa+0x169>
c0108a90: 8b 54 24 08                   mov edx, dword ptr [esp + 8]
c0108a94: e8 0a fe ff ff                call 0xc01088a3 <LogChar>
c0108a99: e9 4e ff ff ff                jmp 0xc01089ec <LogWriteSerialVa+0xc1>
c0108a9e: 80 7c 24 04 00                cmp byte ptr [esp + 4], 0
c0108aa3: 75 14                         jne 0xc0108ab9 <LogWriteSerialVa+0x18e>
c0108aa5: c7 44 24 30 60 b2 13 c0       mov dword ptr [esp + 48], 3222516320
c0108aad: 83 c4 1c                      add esp, 28
c0108ab0: 5b                            pop ebx
c0108ab1: 5e                            pop esi
c0108ab2: 5f                            pop edi
c0108ab3: 5d                            pop ebp
c0108ab4: e9 f1 de ff ff                jmp 0xc01069aa <ReleaseSpinlock>
c0108ab9: 83 c4 1c                      add esp, 28
c0108abc: 5b                            pop ebx
c0108abd: 5e                            pop esi
c0108abe: 5f                            pop edi
c0108abf: 5d                            pop ebp
c0108ac0: e9 5f eb ff ff                jmp 0xc0107624 <UnpreventScheduler>

c0108ac5 <LogWriteSerial>:
c0108ac5: 83 ec 0c                      sub esp, 12
c0108ac8: 8d 44 24 14                   lea eax, [esp + 20]
c0108acc: 52                            push edx
```

```
c0108b11: ff 74 24 1c                  push dword ptr [esp + 28]
c0108b15: e8 11 fe ff ff               call 0xc010892b <LogWriteSerialVa>
c0108b1a: 83 c4 1c                     add esp, 28
c0108b1d: c3                           ret

c0108b1e <SetGraphicalPanicHandler>:
c0108b1e: b8 04 00 00 00               mov eax, 4
c0108b23: 83 3d 7c b2 13 c0 00         cmp dword ptr [-1072450948], 0
c0108b2a: 75 0b                        jne 0xc0108b37 <SetGraphicalPanicHandler+0x19
c0108b2c: 8b 44 24 04                  mov eax, dword ptr [esp + 4]
c0108b30: a3 7c b2 13 c0               mov dword ptr [3222516348], eax
c0108b35: 31 c0                        xor eax, eax
c0108b37: c3                           ret

c0108b38 <GetPanicMessageFromCode>:
c0108b38: 8b 54 24 04                  mov edx, dword ptr [esp + 4]
c0108b3c: b8 7f 11 11 c0               mov eax, 3222344063
c0108b41: 83 fa 29                     cmp edx, 41
c0108b44: 7f 07                        jg 0xc0108b4d <GetPanicMessageFromCode+0x15>
c0108b46: 8b 04 95 80 02 11 c0         mov eax, dword ptr [4*edx - 1072627072]
c0108b4d: c3                           ret

c0108b4e <PanicEx>:
c0108b4e: 56                           push esi
c0108b4f: 53                           push ebx
c0108b50: 83 ec 08                     sub esp, 8
c0108b53: 8b 5c 24 14                  mov ebx, dword ptr [esp + 20]
c0108b57: 8b 74 24 18                  mov esi, dword ptr [esp + 24]
c0108b5b: 56                           push esi
c0108b5c: 53                           push ebx
c0108b5d: 68 80 11 11 c0               push 3222344064
c0108b62: e8 5e ff ff ff               call 0xc0108ac5 <LogWriteSerial>
c0108b67: c7 04 24 29 00 00 00         mov dword ptr [esp], 41
c0108b6e: e8 09 a8 ff ff               call 0xc010337c <RaiseIrql>
c0108b73: 83 c4 0c                     add esp, 12
c0108b76: 56                           push esi
c0108b77: 53                           push ebx
c0108b78: 68 8d 11 11 c0               push 3222344077
c0108b7d: e8 43 ff ff ff               call 0xc0108ac5 <LogWriteSerial>
c0108b82: a1 7c b2 13 c0               mov eax, dword ptr [3222516348]
c0108b87: 83 c4 10                     add esp, 16
c0108b8a: 85 c0                        test eax, eax
c0108b8c: 74 09                        je 0xc0108b97 <PanicEx+0x49>
c0108b8e: 52                           push edx
c0108b8f: 52                           push edx
c0108b90: 56                           push esi
c0108b91: 53                           push ebx
c0108b92: ff d0                        call eax
c0108b94: 83 c4 10                     add esp, 16
c0108b97: fa                           cli
c0108b98: e8 16 5a 00 00               call 0xc010e5b3 <ArchStallProcessor>
c0108b9d: eb f8                        jmp 0xc0108b97 <PanicEx+0x49>

c0108b9f <Panic>:
c0108b9f: 83 ec 0c                     sub esp, 12
c0108ba2: 8b 4c 24 10                  mov ecx, dword ptr [esp + 16]
c0108ba6: 51                           push ecx
c0108ba7: e8 8c ff ff ff               call 0xc0108b38 <GetPanicMessageFromCode>
c0108bac: 52                           push edx
c0108bad: 50                           push eax
c0108bae: 51                           push ecx
c0108baf: e8 9a ff ff ff               call 0xc0108b4e <PanicEx>

c0108bb4 <InitVideoConsole>:
c0108bb4: 83 ec 10                     sub esp, 16
c0108bb7: 8b 44 24 14                  mov eax, dword ptr [esp + 20]
c0108bbb: a3 9c b2 13 c0               mov dword ptr [3222516380], eax
c0108bc0: 6a 03                        push 3
c0108bc2: 68 87 16 11 c0               push 3222345351
c0108bc7: 68 80 b2 13 c0               push 3222516352
c0108bcc: e8 6e dd ff ff               call 0xc010693f <InitSpinlock>
```

```
c0108c1e: c6 04 24 01                  mov byte ptr [esp], 1
c0108c22: 8b 44 24 30                  mov eax, dword ptr [esp + 48]
c0108c26: 88 44 24 04                  mov byte ptr [esp + 4], al
c0108c2a: c6 44 24 05 07               mov byte ptr [esp + 5], 7
c0108c2f: 83 ec 20                     sub esp, 32
c0108c32: 8d 74 24 20                  lea esi, [esp + 32]
c0108c36: b9 08 00 00 00               mov ecx, 8
c0108c3b: 89 e7                        mov edi, esp
c0108c3d: f3 a5                        rep  movsd dword ptr es:[edi], dword ptr [esi
c0108c3f: e8 91 ff ff ff               call 0xc0108bd5 <SendVideoMessage>
c0108c44: 83 c4 44                     add esp, 68
c0108c47: 5e                           pop esi
c0108c48: 5f                           pop edi
c0108c49: c3                           ret

c0108c4a <AppendNumberToString.isra.0>:
c0108c4a: 81 fa e7 03 00 00            cmp edx, 999
c0108c50: 7f 7e                        jg 0xc0108cd0 <AppendNumberToString.isra.0+0x
c0108c52: 55                           push ebp
c0108c53: 57                           push edi
c0108c54: 56                           push esi
c0108c55: 53                           push ebx
c0108c56: 83 ec 2c                     sub esp, 44
c0108c59: 89 c5                        mov ebp, eax
c0108c5b: 89 d1                        mov ecx, edx
c0108c5d: 31 d2                        xor edx, edx
c0108c5f: 89 54 24 1c                  mov dword ptr [esp + 28], edx
c0108c63: 83 f9 09                     cmp ecx, 9
c0108c66: 7f 09                        jg 0xc0108c71 <AppendNumberToString.isra.0+0x
c0108c68: 83 c1 30                     add ecx, 48
c0108c6b: 88 4c 24 1c                  mov byte ptr [esp + 28], cl
c0108c6f: eb 4a                        jmp 0xc0108cbb <AppendNumberToString.isra.0+0
c0108c71: bf 0a 00 00 00               mov edi, 10
c0108c76: 89 c8                        mov eax, ecx
c0108c78: 99                           cdq
c0108c79: f7 ff                        idiv edi
c0108c7b: 89 c3                        mov ebx, eax
c0108c7d: 8d 42 30                     lea eax, [edx + 48]
c0108c80: 88 44 24 0f                  mov byte ptr [esp + 15], al
c0108c84: 83 f9 63                     cmp ecx, 99
c0108c87: 7f 0d                        jg 0xc0108c96 <AppendNumberToString.isra.0+0x
c0108c89: 83 c3 30                     add ebx, 48
c0108c8c: 88 5c 24 1c                  mov byte ptr [esp + 28], bl
c0108c90: 88 44 24 1d                  mov byte ptr [esp + 29], al
c0108c94: eb 25                        jmp 0xc0108cbb <AppendNumberToString.isra.0+0
c0108c96: be 64 00 00 00               mov esi, 100
c0108c9b: 89 c8                        mov eax, ecx
c0108c9d: 99                           cdq
c0108c9e: f7 fe                        idiv esi
c0108ca0: 83 c0 30                     add eax, 48
c0108ca3: 88 44 24 1c                  mov byte ptr [esp + 28], al
c0108ca7: 89 d8                        mov eax, ebx
c0108ca9: 99                           cdq
c0108caa: f7 ff                        idiv edi
c0108cac: 83 c2 30                     add edx, 48
c0108caf: 88 54 24 1d                  mov byte ptr [esp + 29], dl
c0108cb3: 8a 44 24 0f                  mov al, byte ptr [esp + 15]
c0108cb7: 88 44 24 1e                  mov byte ptr [esp + 30], al
c0108cbb: 50                           push eax
c0108cbc: 50                           push eax
c0108cbd: 8d 44 24 24                  lea eax, [esp + 36]
c0108cc1: 50                           push eax
c0108cc2: 55                           push ebp
c0108cc3: e8 cb 85 ff ff               call 0xc0101293 <strcat>
c0108cc8: 83 c4 3c                     add esp, 60
c0108ccb: 5b                           pop ebx
c0108ccc: 5e                           pop esi
c0108ccd: 5f                           pop edi
c0108cce: 5d                           pop ebp
c0108ccf: c3                           ret
c0108cd0: c3                           ret
```

```
c0108d21: 31 c0                         xor eax, eax
c0108d23: 89 d7                         mov edi, edx
c0108d25: f3 ab                         rep  stosd dword ptr es:[edi], eax
c0108d27: 83 c4 18                      add esp, 24
c0108d2a: 5f                            pop edi
c0108d2b: c3                            ret

c0108d2c <GenerateNewMountedDiskName>:
c0108d2c: 56                            push esi
c0108d2d: 53                            push ebx
c0108d2e: 83 ec 1c                      sub esp, 28
c0108d31: 68 96 16 11 c0                push 3222345366
c0108d36: 8d 5c 24 0c                   lea ebx, [esp + 12]
c0108d3a: 53                            push ebx
c0108d3b: e8 7f 84 ff ff                call 0xc01011bf <strcpy>
c0108d40: c7 04 24 e0 b2 13 c0          mov dword ptr [esp], 3222516448
c0108d47: e8 0e dc ff ff                call 0xc010695a <AcquireSpinlock>
c0108d4c: 8b 35 a0 b2 13 c0             mov esi, dword ptr [-1072450912]
c0108d52: 8d 46 01                      lea eax, [esi + 1]
c0108d55: a3 a0 b2 13 c0                mov dword ptr [3222516384], eax
c0108d5a: c7 04 24 e0 b2 13 c0          mov dword ptr [esp], 3222516448
c0108d61: e8 44 dc ff ff                call 0xc01069aa <ReleaseSpinlock>
c0108d66: 89 f2                         mov edx, esi
c0108d68: 89 d8                         mov eax, ebx
c0108d6a: e8 db fe ff ff                call 0xc0108c4a <AppendNumberToString.isra.0>
c0108d6f: 89 1c 24                      mov dword ptr [esp], ebx
c0108d72: e8 7e 85 ff ff                call 0xc01012f5 <strdup>
c0108d77: 83 c4 24                      add esp, 36
c0108d7a: 5b                            pop ebx
c0108d7b: 5e                            pop esi
c0108d7c: c3                            ret

c0108d7d <GenerateNewRawDiskName>:
c0108d7d: 57                            push edi
c0108d7e: 56                            push esi
c0108d7f: 53                            push ebx
c0108d80: 83 ec 10                      sub esp, 16
c0108d83: 8b 5c 24 20                   mov ebx, dword ptr [esp + 32]
c0108d87: c7 04 24 72 61 77 2d          mov dword ptr [esp], 762798450
c0108d8e: 8d 7c 24 04                   lea edi, [esp + 4]
c0108d92: b9 03 00 00 00                mov ecx, 3
c0108d97: 31 c0                         xor eax, eax
c0108d99: f3 ab                         rep  stosd dword ptr es:[edi], eax
c0108d9b: 83 fb 07                      cmp ebx, 7
c0108d9e: 76 05                         jbe 0xc0108da5 <GenerateNewRawDiskName+0x28>
c0108da0: bb 07 00 00 00                mov ebx, 7
c0108da5: 50                            push eax
c0108da6: 50                            push eax
c0108da7: ff 34 9d 40 03 11 c0          push dword ptr [4*ebx - 1072626880]
c0108dae: 8d 74 24 0c                   lea esi, [esp + 12]
c0108db2: 56                            push esi
c0108db3: e8 db 84 ff ff                call 0xc0101293 <strcat>
c0108db8: c7 04 24 e0 b2 13 c0          mov dword ptr [esp], 3222516448
c0108dbf: e8 96 db ff ff                call 0xc010695a <AcquireSpinlock>
c0108dc4: 8b 3c 9d c0 b2 13 c0          mov edi, dword ptr [4*ebx - 1072450880]
c0108dcb: 8d 47 01                      lea eax, [edi + 1]
c0108dce: 89 04 9d c0 b2 13 c0          mov dword ptr [4*ebx - 1072450880], eax
c0108dd5: c7 04 24 e0 b2 13 c0          mov dword ptr [esp], 3222516448
c0108ddc: e8 c9 db ff ff                call 0xc01069aa <ReleaseSpinlock>
c0108de1: 89 fa                         mov edx, edi
c0108de3: 89 f0                         mov eax, esi
c0108de5: e8 60 fe ff ff                call 0xc0108c4a <AppendNumberToString.isra.0>
c0108dea: 5a                            pop edx
c0108deb: 59                            pop ecx
c0108dec: 56                            push esi
c0108ded: 68 9a 16 11 c0                push 3222345370
c0108df2: e8 ce fc ff ff                call 0xc0108ac5 <LogWriteSerial>
c0108df7: 89 34 24                      mov dword ptr [esp], esi
c0108dfa: e8 f6 84 ff ff                call 0xc01012f5 <strdup>
c0108dff: 83 c4 20                      add esp, 32
c0108e02: 5b                            pop ebx
```

```
c0108e48: 52                            push edx
c0108e49: 50                            push eax
c0108e4a: 6a 00                         push 0
c0108e4c: 6a 00                         push 0
c0108e4e: 56                            push esi
c0108e4f: e8 36 97 ff ff                call 0xc010258a <CreatePartition>
c0108e54: 8b 40 30                      mov eax, dword ptr [eax + 48]
c0108e57: 89 44 24 3c                   mov dword ptr [esp + 60], eax
c0108e5b: 83 c4 30                      add esp, 48
c0108e5e: 31 c0                         xor eax, eax
c0108e60: e8 6c fe ff ff                call 0xc0108cd1 <GetPartitionNameString>
c0108e65: 83 ec 0c                      sub esp, 12
c0108e68: 6a 00                         push 0
c0108e6a: 6a 00                         push 0
c0108e6c: 50                            push eax
c0108e6d: 8d 44 24 24                   lea eax, [esp + 36]
c0108e71: 50                            push eax
c0108e72: ff 76 30                      push dword ptr [esi + 48]
c0108e75: e8 b5 16 00 00                call 0xc010a52f <VnodeOpCreate>
c0108e7a: 83 c4 20                      add esp, 32
c0108e7d: eb 42                         jmp 0xc0108ec1 <CreateDiskPartitions+0xbb>
c0108e7f: 83 ec 0c                      sub esp, 12
c0108e82: 68 cc 16 11 c0                push 3222345420
c0108e87: e8 39 fc ff ff                call 0xc0108ac5 <LogWriteSerial>
c0108e8c: 83 c4 10                      add esp, 16
c0108e8f: 31 ff                         xor edi, edi
c0108e91: 8b 04 bb                      mov eax, dword ptr [ebx + 4*edi]
c0108e94: 85 c0                         test eax, eax
c0108e96: 74 29                         je 0xc0108ec1 <CreateDiskPartitions+0xbb>
c0108e98: 8b 40 30                      mov eax, dword ptr [eax + 48]
c0108e9b: 89 44 24 0c                   mov dword ptr [esp + 12], eax
c0108e9f: 89 f8                         mov eax, edi
c0108ea1: e8 2b fe ff ff                call 0xc0108cd1 <GetPartitionNameString>
c0108ea6: 83 ec 0c                      sub esp, 12
c0108ea9: 6a 00                         push 0
c0108eab: 6a 00                         push 0
c0108ead: 50                            push eax
c0108eae: 8d 44 24 24                   lea eax, [esp + 36]
c0108eb2: 50                            push eax
c0108eb3: ff 76 30                      push dword ptr [esi + 48]
c0108eb6: e8 74 16 00 00                call 0xc010a52f <VnodeOpCreate>
c0108ebb: 47                            inc edi
c0108ebc: 83 c4 20                      add esp, 32
c0108ebf: eb d0                         jmp 0xc0108e91 <CreateDiskPartitions+0x8b>
c0108ec1: 83 c4 10                      add esp, 16
c0108ec4: 5b                            pop ebx
c0108ec5: 5e                            pop esi
c0108ec6: 5f                            pop edi
c0108ec7: c3                            ret

c0108ec8 <InitDiskPartitionHelper>:
c0108ec8: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c0108ecc: 31 d2                         xor edx, edx
c0108ece: 89 50 40                      mov dword ptr [eax + 64], edx
c0108ed1: c3                            ret

c0108ed2 <DiskFollowHelper>:
c0108ed2: 56                            push esi
c0108ed3: 53                            push ebx
c0108ed4: 53                            push ebx
c0108ed5: 8b 74 24 10                   mov esi, dword ptr [esp + 16]
c0108ed9: 31 db                         xor ebx, ebx
c0108edb: 39 5e 40                      cmp dword ptr [esi + 64], ebx
c0108ede: 7e 1e                         jle 0xc0108efe <DiskFollowHelper+0x2c>
c0108ee0: 51                            push ecx
c0108ee1: 51                            push ecx
c0108ee2: ff 74 24 20                   push dword ptr [esp + 32]
c0108ee6: ff 74 9e 20                   push dword ptr [esi + 4*ebx + 32]
c0108eea: e8 b2 82 ff ff                call 0xc01011a1 <strcmp>
c0108eef: 83 c4 10                      add esp, 16
c0108ef2: 85 c0                         test eax, eax
```

```
c0108f39: c3                            ret

c0108f3a <CreateFdTable>:
c0108f3a: 53                            push ebx
c0108f3b: 83 ec 14                      sub esp, 20
c0108f3e: 6a 08                         push 8
c0108f40: e8 0a aa ff ff                call 0xc010394f <AllocHeap>
c0108f45: 89 c3                         mov ebx, eax
c0108f47: 83 c4 0c                      add esp, 12
c0108f4a: 6a 00                         push 0
c0108f4c: 6a 01                         push 1
c0108f4e: 68 03 17 11 c0                push 3222345475
c0108f53: e8 81 d7 ff ff                call 0xc01066d9 <CreateSemaphore>
c0108f58: 89 03                         mov dword ptr [ebx], eax
c0108f5a: 58                            pop eax
c0108f5b: 5a                            pop edx
c0108f5c: 6a 00                         push 0
c0108f5e: 6a 00                         push 0
c0108f60: 6a 03                         push 3
c0108f62: 68 00 20 00 00                push 8192
c0108f67: 6a 00                         push 0
c0108f69: 6a 00                         push 0
c0108f6b: e8 d8 c3 ff ff                call 0xc0105348 <MapVirt>
c0108f70: 89 43 04                      mov dword ptr [ebx + 4], eax
c0108f73: 83 c4 20                      add esp, 32
c0108f76: 31 c0                         xor eax, eax
c0108f78: 8b 53 04                      mov edx, dword ptr [ebx + 4]
c0108f7b: 31 c9                         xor ecx, ecx
c0108f7d: 89 0c 02                      mov dword ptr [edx + eax], ecx
c0108f80: 83 c0 08                      add eax, 8
c0108f83: 3d 00 20 00 00                cmp eax, 8192
c0108f88: 75 ee                         jne 0xc0108f78 <CreateFdTable+0x3e>
c0108f8a: 89 d8                         mov eax, ebx
c0108f8c: 83 c4 08                      add esp, 8
c0108f8f: 5b                            pop ebx
c0108f90: c3                            ret

c0108f91 <CopyFdTable>:
c0108f91: 55                            push ebp
c0108f92: 57                            push edi
c0108f93: 56                            push esi
c0108f94: 53                            push ebx
c0108f95: 83 ec 0c                      sub esp, 12
c0108f98: 8b 6c 24 20                   mov ebp, dword ptr [esp + 32]
c0108f9c: e8 99 ff ff ff                call 0xc0108f3a <CreateFdTable>
c0108fa1: 89 c3                         mov ebx, eax
c0108fa3: 50                            push eax
c0108fa4: 50                            push eax
c0108fa5: 6a ff                         push -1
c0108fa7: ff 75 00                      push dword ptr [ebp]
c0108faa: e8 8a d7 ff ff                call 0xc0106739 <AcquireSemaphore>
c0108faf: 8b 75 04                      mov esi, dword ptr [ebp + 4]
c0108fb2: b9 00 08 00 00                mov ecx, 2048
c0108fb7: 8b 7b 04                      mov edi, dword ptr [ebx + 4]
c0108fba: f3 a5                         rep  movsd dword ptr es:[edi], dword ptr [esi
c0108fbc: 5a                            pop edx
c0108fbd: ff 75 00                      push dword ptr [ebp]
c0108fc0: e8 ee d8 ff ff                call 0xc01068b3 <ReleaseSemaphore>
c0108fc5: 89 d8                         mov eax, ebx
c0108fc7: 83 c4 1c                      add esp, 28
c0108fca: 5b                            pop ebx
c0108fcb: 5e                            pop esi
c0108fcc: 5f                            pop edi
c0108fcd: 5d                            pop ebp
c0108fce: c3                            ret

c0108fcf <DestroyFdTable>:
c0108fcf: 56                            push esi
c0108fd0: 53                            push ebx
c0108fd1: 83 ec 0c                      sub esp, 12
c0108fd4: 8b 5c 24 18                   mov ebx, dword ptr [esp + 24]
```

```
c0109029: 83 c4 14                      add esp, 20
c010902c: 5b                            pop ebx
c010902d: 5e                            pop esi
c010902e: c3                            ret

c010902f <CreateFd>:
c010902f: 55                            push ebp
c0109030: 57                            push edi
c0109031: 56                            push esi
c0109032: 53                            push ebx
c0109033: 83 ec 0c                      sub esp, 12
c0109036: 8b 6c 24 20                   mov ebp, dword ptr [esp + 32]
c010903a: 8b 7c 24 24                   mov edi, dword ptr [esp + 36]
c010903e: 8b 74 24 2c                   mov esi, dword ptr [esp + 44]
c0109042: 81 e6 ff fe ff ff             and esi, 4294967039
c0109048: 75 6c                         jne 0xc01090b6 <CreateFd+0x87>
c010904a: 50                            push eax
c010904b: 50                            push eax
c010904c: 6a ff                         push -1
c010904e: ff 75 00                      push dword ptr [ebp]
c0109051: e8 e3 d6 ff ff                call 0xc0106739 <AcquireSemaphore>
c0109056: 8b 45 04                      mov eax, dword ptr [ebp + 4]
c0109059: 83 c4 10                      add esp, 16
c010905c: 31 db                         xor ebx, ebx
c010905e: 83 38 00                      cmp dword ptr [eax], 0
c0109061: 75 32                         jne 0xc0109095 <CreateFd+0x66>
c0109063: 89 38                         mov dword ptr [eax], edi
c0109065: 8b 45 04                      mov eax, dword ptr [ebp + 4]
c0109068: 8b 54 24 2c                   mov edx, dword ptr [esp + 44]
c010906c: 89 54 d8 04                   mov dword ptr [eax + 8*ebx + 4], edx
c0109070: 83 ec 0c                      sub esp, 12
c0109073: ff 75 00                      push dword ptr [ebp]
c0109076: e8 38 d8 ff ff                call 0xc01068b3 <ReleaseSemaphore>
c010907b: 8b 44 24 38                   mov eax, dword ptr [esp + 56]
c010907f: 89 18                         mov dword ptr [eax], ebx
c0109081: 53                            push ebx
c0109082: ff 77 30                      push dword ptr [edi + 48]
c0109085: 57                            push edi
c0109086: 68 0b 17 11 c0                push 3222345483
c010908b: e8 35 fa ff ff                call 0xc0108ac5 <LogWriteSerial>
c0109090: 83 c4 20                      add esp, 32
c0109093: eb 26                         jmp 0xc01090bb <CreateFd+0x8c>
c0109095: 43                            inc ebx
c0109096: 83 c0 08                      add eax, 8
c0109099: 81 fb 00 04 00 00             cmp ebx, 1024
c010909f: 75 bd                         jne 0xc010905e <CreateFd+0x2f>
c01090a1: 83 ec 0c                      sub esp, 12
c01090a4: ff 75 00                      push dword ptr [ebp]
c01090a7: e8 07 d8 ff ff                call 0xc01068b3 <ReleaseSemaphore>
c01090ac: 83 c4 10                      add esp, 16
c01090af: be 18 00 00 00                mov esi, 24
c01090b4: eb 05                         jmp 0xc01090bb <CreateFd+0x8c>
c01090b6: be 07 00 00 00                mov esi, 7
c01090bb: 89 f0                         mov eax, esi
c01090bd: 83 c4 0c                      add esp, 12
c01090c0: 5b                            pop ebx
c01090c1: 5e                            pop esi
c01090c2: 5f                            pop edi
c01090c3: 5d                            pop ebp
c01090c4: c3                            ret

c01090c5 <RemoveFd>:
c01090c5: 56                            push esi
c01090c6: 53                            push ebx
c01090c7: 83 ec 0c                      sub esp, 12
c01090ca: 8b 5c 24 18                   mov ebx, dword ptr [esp + 24]
c01090ce: 8b 74 24 1c                   mov esi, dword ptr [esp + 28]
c01090d2: 6a ff                         push -1
c01090d4: ff 33                         push dword ptr [ebx]
c01090d6: e8 5e d6 ff ff                call 0xc0106739 <AcquireSemaphore>
c01090db: 8b 53 04                      mov edx, dword ptr [ebx + 4]
```

```
c0109129: c3                            ret

c010912a <GetFileFromFd>:
c010912a: 57                            push edi
c010912b: 56                            push esi
c010912c: 53                            push ebx
c010912d: 8b 74 24 10                   mov esi, dword ptr [esp + 16]
c0109131: 8b 5c 24 14                   mov ebx, dword ptr [esp + 20]
c0109135: 8b 7c 24 18                   mov edi, dword ptr [esp + 24]
c0109139: 85 ff                         test edi, edi
c010913b: 74 2e                         je 0xc010916b <GetFileFromFd+0x41>
c010913d: 81 fb ff 03 00 00             cmp ebx, 1023
c0109143: 77 30                         ja 0xc0109175 <GetFileFromFd+0x4b>
c0109145: 50                            push eax
c0109146: 50                            push eax
c0109147: 6a ff                         push -1
c0109149: ff 36                         push dword ptr [esi]
c010914b: e8 e9 d5 ff ff                call 0xc0106739 <AcquireSemaphore>
c0109150: 8b 46 04                      mov eax, dword ptr [esi + 4]
c0109153: 8b 1c d8                      mov ebx, dword ptr [eax + 8*ebx]
c0109156: 5a                            pop edx
c0109157: ff 36                         push dword ptr [esi]
c0109159: e8 55 d7 ff ff                call 0xc01068b3 <ReleaseSemaphore>
c010915e: 83 c4 10                      add esp, 16
c0109161: 83 fb 01                      cmp ebx, 1
c0109164: 19 c0                         sbb eax, eax
c0109166: 83 e0 14                      and eax, 20
c0109169: eb 11                         jmp 0xc010917c <GetFileFromFd+0x52>
c010916b: 31 c9                         xor ecx, ecx
c010916d: 89 0d 00 00 00 00             mov dword ptr [0], ecx
c0109173: 0f 0b                         ud2
c0109175: 31 db                         xor ebx, ebx
c0109177: b8 14 00 00 00                mov eax, 20
c010917c: 89 1f                         mov dword ptr [edi], ebx
c010917e: 5b                            pop ebx
c010917f: 5e                            pop esi
c0109180: 5f                            pop edi
c0109181: c3                            ret

c0109182 <HandleExecFd>:
c0109182: 57                            push edi
c0109183: 56                            push esi
c0109184: 83 ec 1c                      sub esp, 28
c0109187: 8b 74 24 28                   mov esi, dword ptr [esp + 40]
c010918b: 6a ff                         push -1
c010918d: ff 36                         push dword ptr [esi]
c010918f: e8 a5 d5 ff ff                call 0xc0106739 <AcquireSemaphore>
c0109194: 83 c4 10                      add esp, 16
c0109197: 31 ff                         xor edi, edi
c0109199: 8b 46 04                      mov eax, dword ptr [esi + 4]
c010919c: 01 f8                         add eax, edi
c010919e: 8b 10                         mov edx, dword ptr [eax]
c01091a0: 85 d2                         test edx, edx
c01091a2: 74 31                         je 0xc01091d5 <HandleExecFd+0x53>
c01091a4: f6 40 05 01                   test byte ptr [eax + 5], 1
c01091a8: 74 2b                         je 0xc01091d5 <HandleExecFd+0x53>
c01091aa: 31 c9                         xor ecx, ecx
c01091ac: 89 08                         mov dword ptr [eax], ecx
c01091ae: 83 ec 0c                      sub esp, 12
c01091b1: 52                            push edx
c01091b2: e8 35 11 00 00                call 0xc010a2ec <CloseFile>
c01091b7: 83 c4 10                      add esp, 16
c01091ba: 85 c0                         test eax, eax
c01091bc: 74 17                         je 0xc01091d5 <HandleExecFd+0x53>
c01091be: 89 44 24 0c                   mov dword ptr [esp + 12], eax
c01091c2: 83 ec 0c                      sub esp, 12
c01091c5: ff 36                         push dword ptr [esi]
c01091c7: e8 e7 d6 ff ff                call 0xc01068b3 <ReleaseSemaphore>
c01091cc: 83 c4 10                      add esp, 16
c01091cf: 8b 44 24 0c                   mov eax, dword ptr [esp + 12]
c01091d3: eb 1a                         jmp 0xc01091ef <HandleExecFd+0x6d>
```

```
c010921d: 85 c0                         test eax, eax
c010921f: 75 08                         jne 0xc0109229 <DupFd+0x34>
c0109221: 8b 54 24 0c                   mov edx, dword ptr [esp + 12]
c0109225: 85 d2                         test edx, edx
c0109227: 75 14                         jne 0xc010923d <DupFd+0x48>
c0109229: 83 ec 0c                      sub esp, 12
c010922c: ff 33                         push dword ptr [ebx]
c010922e: e8 80 d6 ff ff                call 0xc01068b3 <ReleaseSemaphore>
c0109233: 83 c4 10                      add esp, 16
c0109236: be 14 00 00 00                mov esi, 20
c010923b: eb 4a                         jmp 0xc0109287 <DupFd+0x92>
c010923d: 89 c6                         mov esi, eax
c010923f: 8b 43 04                      mov eax, dword ptr [ebx + 4]
c0109242: 31 ff                         xor edi, edi
c0109244: 83 38 00                      cmp dword ptr [eax], 0
c0109247: 75 20                         jne 0xc0109269 <DupFd+0x74>
c0109249: 89 10                         mov dword ptr [eax], edx
c010924b: 8b 43 04                      mov eax, dword ptr [ebx + 4]
c010924e: 31 d2                         xor edx, edx
c0109250: 89 54 f8 04                   mov dword ptr [eax + 8*edi + 4], edx
c0109254: 83 ec 0c                      sub esp, 12
c0109257: ff 33                         push dword ptr [ebx]
c0109259: e8 55 d6 ff ff                call 0xc01068b3 <ReleaseSemaphore>
c010925e: 8b 44 24 38                   mov eax, dword ptr [esp + 56]
c0109262: 89 38                         mov dword ptr [eax], edi
c0109264: 83 c4 10                      add esp, 16
c0109267: eb 1e                         jmp 0xc0109287 <DupFd+0x92>
c0109269: 47                            inc edi
c010926a: 83 c0 08                      add eax, 8
c010926d: 81 ff 00 04 00 00             cmp edi, 1024
c0109273: 75 cf                         jne 0xc0109244 <DupFd+0x4f>
c0109275: 83 ec 0c                      sub esp, 12
c0109278: ff 33                         push dword ptr [ebx]
c010927a: e8 34 d6 ff ff                call 0xc01068b3 <ReleaseSemaphore>
c010927f: 83 c4 10                      add esp, 16
c0109282: be 18 00 00 00                mov esi, 24
c0109287: 89 f0                         mov eax, esi
c0109289: 83 c4 10                      add esp, 16
c010928c: 5b                            pop ebx
c010928d: 5e                            pop esi
c010928e: 5f                            pop edi
c010928f: c3                            ret

c0109290 <DupFd2>:
c0109290: 55                            push ebp
c0109291: 57                            push edi
c0109292: 56                            push esi
c0109293: 53                            push ebx
c0109294: 83 ec 1c                      sub esp, 28
c0109297: 8b 7c 24 30                   mov edi, dword ptr [esp + 48]
c010929b: 8b 74 24 38                   mov esi, dword ptr [esp + 56]
c010929f: bb 07 00 00 00                mov ebx, 7
c01092a4: f7 44 24 3c ff fe ff ff       test dword ptr [esp + 60], 4294967039
c01092ac: 0f 85 91 00 00 00             jne 0xc0109343 <DupFd2+0xb3>
c01092b2: 52                            push edx
c01092b3: 52                            push edx
c01092b4: 6a ff                         push -1
c01092b6: ff 37                         push dword ptr [edi]
c01092b8: e8 7c d4 ff ff                call 0xc0106739 <AcquireSemaphore>
c01092bd: 83 c4 0c                      add esp, 12
c01092c0: 8d 44 24 0c                   lea eax, [esp + 12]
c01092c4: 50                            push eax
c01092c5: ff 74 24 3c                   push dword ptr [esp + 60]
c01092c9: 57                            push edi
c01092ca: e8 5b fe ff ff                call 0xc010912a <GetFileFromFd>
c01092cf: 89 c3                         mov ebx, eax
c01092d1: 83 c4 10                      add esp, 16
c01092d4: 85 c0                         test eax, eax
c01092d6: 75 08                         jne 0xc01092e0 <DupFd2+0x50>
c01092d8: 8b 6c 24 08                   mov ebp, dword ptr [esp + 8]
c01092dc: 85 ed                         test ebp, ebp
```

```
c0109332: 89 54 f0 04                   mov dword ptr [eax + 8*esi + 4], edx
c0109336: 83 ec 0c                      sub esp, 12
c0109339: ff 37                         push dword ptr [edi]
c010933b: e8 73 d5 ff ff                call 0xc01068b3 <ReleaseSemaphore>
c0109340: 83 c4 10                      add esp, 16
c0109343: 89 d8                         mov eax, ebx
c0109345: 83 c4 1c                      add esp, 28
c0109348: 5b                            pop ebx
c0109349: 5e                            pop esi
c010934a: 5f                            pop edi
c010934b: 5d                            pop ebp
c010934c: c3                            ret

c010934d <CreateFile>:
c010934d: 55                            push ebp
c010934e: 57                            push edi
c010934f: 56                            push esi
c0109350: 53                            push ebx
c0109351: 83 ec 18                      sub esp, 24
c0109354: 8b 74 24 2c                   mov esi, dword ptr [esp + 44]
c0109358: 8b 6c 24 38                   mov ebp, dword ptr [esp + 56]
c010935c: 8b 7c 24 3c                   mov edi, dword ptr [esp + 60]
c0109360: 6a 34                         push 52
c0109362: e8 e8 a5 ff ff                call 0xc010394f <AllocHeap>
c0109367: 89 c3                         mov ebx, eax
c0109369: c7 40 10 01 00 00 00          mov dword ptr [eax + 16], 1
c0109370: 89 70 30                      mov dword ptr [eax + 48], esi
c0109373: 89 e8                         mov eax, ebp
c0109375: 88 03                         mov byte ptr [ebx], al
c0109377: 89 f8                         mov eax, edi
c0109379: 88 43 01                      mov byte ptr [ebx + 1], al
c010937c: 8b 44 24 34                   mov eax, dword ptr [esp + 52]
c0109380: 89 43 04                      mov dword ptr [ebx + 4], eax
c0109383: 8b 44 24 38                   mov eax, dword ptr [esp + 56]
c0109387: 89 43 0c                      mov dword ptr [ebx + 12], eax
c010938a: 31 c0                         xor eax, eax
c010938c: 89 43 08                      mov dword ptr [ebx + 8], eax
c010938f: 83 c4 0c                      add esp, 12
c0109392: 6a 03                         push 3
c0109394: 68 65 17 11 c0                push 3222345573
c0109399: 8d 43 14                      lea eax, [ebx + 20]
c010939c: 50                            push eax
c010939d: e8 9d d5 ff ff                call 0xc010693f <InitSpinlock>
c01093a2: 89 34 24                      mov dword ptr [esp], esi
c01093a5: e8 64 10 00 00                call 0xc010a40e <ReferenceVnode>
c01093aa: 89 d8                         mov eax, ebx
c01093ac: 83 c4 1c                      add esp, 28
c01093af: 5b                            pop ebx
c01093b0: 5e                            pop esi
c01093b1: 5f                            pop edi
c01093b2: 5d                            pop ebp
c01093b3: c3                            ret

c01093b4 <ReferenceFile>:
c01093b4: 56                            push esi
c01093b5: 53                            push ebx
c01093b6: 83 ec 10                      sub esp, 16
c01093b9: 8b 5c 24 1c                   mov ebx, dword ptr [esp + 28]
c01093bd: 8d 73 14                      lea esi, [ebx + 20]
c01093c0: 56                            push esi
c01093c1: e8 94 d5 ff ff                call 0xc010695a <AcquireSpinlock>
c01093c6: ff 43 10                      inc dword ptr [ebx + 16]
c01093c9: 89 74 24 20                   mov dword ptr [esp + 32], esi
c01093cd: 83 c4 14                      add esp, 20
c01093d0: 5b                            pop ebx
c01093d1: 5e                            pop esi
c01093d2: e9 d3 d5 ff ff                jmp 0xc01069aa <ReleaseSpinlock>

c01093d7 <DereferenceFile>:
c01093d7: 56                            push esi
c01093d8: 53                            push ebx
```

```
c010942f: 5b                            pop ebx
c0109430: 5e                            pop esi
c0109431: e9 3d a5 ff ff                jmp 0xc0103973 <FreeHeap>
c0109436: 89 74 24 10                   mov dword ptr [esp + 16], esi
c010943a: 58                            pop eax
c010943b: 5b                            pop ebx
c010943c: 5e                            pop esi
c010943d: e9 68 d5 ff ff                jmp 0xc01069aa <ReleaseSpinlock>

c0109442 <ValidateCopy>:
c0109442: 55                            push ebp
c0109443: 57                            push edi
c0109444: 56                            push esi
c0109445: 53                            push ebx
c0109446: 83 ec 0c                      sub esp, 12
c0109449: 89 c3                         mov ebx, eax
c010944b: 89 d0                         mov eax, edx
c010944d: 89 ce                         mov esi, ecx
c010944f: 89 da                         mov edx, ebx
c0109451: 01 c2                         add edx, eax
c0109453: 0f 92 c1                      setb cl
c0109456: 8d bb 00 00 00 f8             lea edi, [ebx - 134217728]
c010945c: 81 ff ff ff ff b7             cmp edi, 3087007743
c0109462: 77 07                         ja 0xc010946b <ValidateCopy+0x29>
c0109464: 0f b6 c9                      movzx ecx, cl
c0109467: 85 c9                         test ecx, ecx
c0109469: 74 07                         je 0xc0109472 <ValidateCopy+0x30>
c010946b: b8 07 00 00 00                mov eax, 7
c0109470: eb 5a                         jmp 0xc01094cc <ValidateCopy+0x8a>
c0109472: 81 ea 00 00 00 08             sub edx, 134217728
c0109478: 81 fa ff ff ff b7             cmp edx, 3087007743
c010947e: 77 eb                         ja 0xc010946b <ValidateCopy+0x29>
c0109480: 83 ec 0c                      sub esp, 12
c0109483: 50                            push eax
c0109484: e8 36 c6 ff ff                call 0xc0105abf <BytesToPages>
c0109489: 89 c7                         mov edi, eax
c010948b: 81 e3 00 f0 ff ff             and ebx, 4294963200
c0109491: 83 c4 10                      add esp, 16
c0109494: 31 ed                         xor ebp, ebp
c0109496: 39 fd                         cmp ebp, edi
c0109498: 74 30                         je 0xc01094ca <ValidateCopy+0x88>
c010949a: 83 ec 0c                      sub esp, 12
c010949d: 53                            push ebx
c010949e: e8 11 b4 ff ff                call 0xc01048b4 <GetVirtPermissions>
c01094a3: 83 c4 10                      add esp, 16
c01094a6: 85 c0                         test eax, eax
c01094a8: 74 c1                         je 0xc010946b <ValidateCopy+0x29>
c01094aa: 89 c2                         mov edx, eax
c01094ac: f7 d2                         not edx
c01094ae: 80 e2 05                      and dl, 5
c01094b1: 75 b8                         jne 0xc010946b <ValidateCopy+0x29>
c01094b3: 89 f1                         mov ecx, esi
c01094b5: 84 c9                         test cl, cl
c01094b7: 74 08                         je 0xc01094c1 <ValidateCopy+0x7f>
c01094b9: a8 02                         test al, 2
c01094bb: 74 ae                         je 0xc010946b <ValidateCopy+0x29>
c01094bd: a8 08                         test al, 8
c01094bf: 75 aa                         jne 0xc010946b <ValidateCopy+0x29>
c01094c1: 45                            inc ebp
c01094c2: 81 c3 00 10 00 00             add ebx, 4096
c01094c8: eb cc                         jmp 0xc0109496 <ValidateCopy+0x54>
c01094ca: 31 c0                         xor eax, eax
c01094cc: 83 c4 0c                      add esp, 12
c01094cf: 5b                            pop ebx
c01094d0: 5e                            pop esi
c01094d1: 5f                            pop edi
c01094d2: 5d                            pop ebp
c01094d3: c3                            ret

c01094d4 <RevertTransfer>:
c01094d4: 53                            push ebx
```

```
c010951e: 73 07                         jae 0xc0109527 <PerformTransfer+0x34>
c0109520: 89 14 24                      mov dword ptr [esp], edx
c0109523: 89 44 24 04                   mov dword ptr [esp + 4], eax
c0109527: 8b 04 24                      mov eax, dword ptr [esp]
c010952a: 89 44 24 0c                   mov dword ptr [esp + 12], eax
c010952e: 85 c0                         test eax, eax
c0109530: 0f 84 83 00 00 00             je 0xc01095b9 <PerformTransfer+0xc6>
c0109536: 8b 43 14                      mov eax, dword ptr [ebx + 20]
c0109539: 8b 2b                         mov ebp, dword ptr [ebx]
c010953b: 83 7b 18 00                   cmp dword ptr [ebx + 24], 0
c010953f: 75 24                         jne 0xc0109565 <PerformTransfer+0x72>
c0109541: 85 c0                         test eax, eax
c0109543: 75 0c                         jne 0xc0109551 <PerformTransfer+0x5e>
c0109545: 52                            push edx
c0109546: ff 74 24 04                   push dword ptr [esp + 4]
c010954a: ff 74 24 38                   push dword ptr [esp + 56]
c010954e: 55                            push ebp
c010954f: eb 0a                         jmp 0xc010955b <PerformTransfer+0x68>
c0109551: 50                            push eax
c0109552: ff 74 24 04                   push dword ptr [esp + 4]
c0109556: 55                            push ebp
c0109557: ff 74 24 3c                   push dword ptr [esp + 60]
c010955b: e8 04 7d ff ff                call 0xc0101264 <memmove>
c0109560: 83 c4 10                      add esp, 16
c0109563: eb 3d                         jmp 0xc01095a2 <PerformTransfer+0xaf>
c0109565: 85 c0                         test eax, eax
c0109567: 75 1c                         jne 0xc0109585 <PerformTransfer+0x92>
c0109569: b9 01 00 00 00                mov ecx, 1
c010956e: 8b 54 24 0c                   mov edx, dword ptr [esp + 12]
c0109572: 89 e8                         mov eax, ebp
c0109574: e8 c9 fe ff ff                call 0xc0109442 <ValidateCopy>
c0109579: 85 c0                         test eax, eax
c010957b: 75 3e                         jne 0xc01095bb <PerformTransfer+0xc8>
c010957d: 89 ef                         mov edi, ebp
c010957f: 8b 74 24 30                   mov esi, dword ptr [esp + 48]
c0109583: eb 17                         jmp 0xc010959c <PerformTransfer+0xa9>
c0109585: 31 c9                         xor ecx, ecx
c0109587: 8b 54 24 0c                   mov edx, dword ptr [esp + 12]
c010958b: 89 e8                         mov eax, ebp
c010958d: e8 b0 fe ff ff                call 0xc0109442 <ValidateCopy>
c0109592: 85 c0                         test eax, eax
c0109594: 75 25                         jne 0xc01095bb <PerformTransfer+0xc8>
c0109596: 8b 7c 24 30                   mov edi, dword ptr [esp + 48]
c010959a: 89 ee                         mov esi, ebp
c010959c: 8b 4c 24 0c                   mov ecx, dword ptr [esp + 12]
c01095a0: f3 a4                         rep  movsb byte ptr es:[edi], byte ptr [esi]
c01095a2: 8b 04 24                      mov eax, dword ptr [esp]
c01095a5: 31 d2                         xor edx, edx
c01095a7: 29 43 04                      sub dword ptr [ebx + 4], eax
c01095aa: 19 53 08                      sbb dword ptr [ebx + 8], edx
c01095ad: 01 43 0c                      add dword ptr [ebx + 12], eax
c01095b0: 11 53 10                      adc dword ptr [ebx + 16], edx
c01095b3: 8b 44 24 0c                   mov eax, dword ptr [esp + 12]
c01095b7: 01 03                         add dword ptr [ebx], eax
c01095b9: 31 c0                         xor eax, eax
c01095bb: 83 c4 1c                      add esp, 28
c01095be: 5b                            pop ebx
c01095bf: 5e                            pop esi
c01095c0: 5f                            pop edi
c01095c1: 5d                            pop ebp
c01095c2: c3                            ret

c01095c3 <WriteStringToUsermode>:
c01095c3: 57                            push edi
c01095c4: 56                            push esi
c01095c5: 53                            push ebx
c01095c6: 83 ec 3c                      sub esp, 60
c01095c9: 8b 5c 24 4c                   mov ebx, dword ptr [esp + 76]
c01095cd: 8b 74 24 54                   mov esi, dword ptr [esp + 84]
c01095d1: 8b 7c 24 58                   mov edi, dword ptr [esp + 88]
c01095d5: 8b 44 24 50                   mov eax, dword ptr [esp + 80]
```

```
c0109631: 56                            push esi
c0109632: 53                            push ebx
c0109633: e8 bb fe ff ff                call 0xc01094f3 <PerformTransfer>
c0109638: 83 c4 10                      add esp, 16
c010963b: 85 c0                         test eax, eax
c010963d: 75 17                         jne 0xc0109656 <WriteStringToUsermode+0x93>
c010963f: c6 44 24 0f 00                mov byte ptr [esp + 15], 0
c0109644: 6a 00                         push 0
c0109646: 6a 01                         push 1
c0109648: 56                            push esi
c0109649: 8d 44 24 1b                   lea eax, [esp + 27]
c010964d: 50                            push eax
c010964e: e8 a0 fe ff ff                call 0xc01094f3 <PerformTransfer>
c0109653: 83 c4 10                      add esp, 16
c0109656: 83 c4 30                      add esp, 48
c0109659: 5b                            pop ebx
c010965a: 5e                            pop esi
c010965b: 5f                            pop edi
c010965c: c3                            ret

c010965d <ReadStringFromUsermode>:
c010965d: 55                            push ebp
c010965e: 57                            push edi
c010965f: 56                            push esi
c0109660: 53                            push ebx
c0109661: 83 ec 3c                      sub esp, 60
c0109664: 8b 5c 24 50                   mov ebx, dword ptr [esp + 80]
c0109668: 8b 74 24 58                   mov esi, dword ptr [esp + 88]
c010966c: 8b 7c 24 5c                   mov edi, dword ptr [esp + 92]
c0109670: 8b 44 24 54                   mov eax, dword ptr [esp + 84]
c0109674: 89 44 24 10                   mov dword ptr [esp + 16], eax
c0109678: 89 74 24 14                   mov dword ptr [esp + 20], esi
c010967c: 89 7c 24 18                   mov dword ptr [esp + 24], edi
c0109680: 31 c0                         xor eax, eax
c0109682: 89 44 24 1c                   mov dword ptr [esp + 28], eax
c0109686: 89 44 24 20                   mov dword ptr [esp + 32], eax
c010968a: c7 44 24 24 01 00 00 00       mov dword ptr [esp + 36], 1
c0109692: c7 44 24 28 01 00 00 00       mov dword ptr [esp + 40], 1
c010969a: c6 44 24 2c 01                mov byte ptr [esp + 44], 1
c010969f: 31 ed                         xor ebp, ebp
c01096a1: b8 01 00 00 00                mov eax, 1
c01096a6: 39 f0                         cmp eax, esi
c01096a8: b8 00 00 00 00                mov eax, 0
c01096ad: 19 f8                         sbb eax, edi
c01096af: 73 32                         jae 0xc01096e3 <ReadStringFromUsermode+0x86>
c01096b1: c6 44 24 0f 00                mov byte ptr [esp + 15], 0
c01096b6: 6a 00                         push 0
c01096b8: 6a 01                         push 1
c01096ba: 8d 44 24 18                   lea eax, [esp + 24]
c01096be: 50                            push eax
c01096bf: 8d 44 24 1b                   lea eax, [esp + 27]
c01096c3: 50                            push eax
c01096c4: e8 2a fe ff ff                call 0xc01094f3 <PerformTransfer>
c01096c9: 83 c4 10                      add esp, 16
c01096cc: 85 c0                         test eax, eax
c01096ce: 75 19                         jne 0xc01096e9 <ReadStringFromUsermode+0x8c>
c01096d0: 45                            inc ebp
c01096d1: 8a 44 24 0f                   mov al, byte ptr [esp + 15]
c01096d5: 88 44 2b ff                   mov byte ptr [ebx + ebp - 1], al
c01096d9: 83 c6 ff                      add esi, -1
c01096dc: 83 d7 ff                      adc edi, -1
c01096df: 84 c0                         test al, al
c01096e1: 75 be                         jne 0xc01096a1 <ReadStringFromUsermode+0x44>
c01096e3: c6 04 2b 00                   mov byte ptr [ebx + ebp], 0
c01096e7: 31 c0                         xor eax, eax
c01096e9: 83 c4 3c                      add esp, 60
c01096ec: 5b                            pop ebx
c01096ed: 5e                            pop esi
c01096ee: 5f                            pop edi
c01096ef: 5d                            pop ebp
c01096f0: c3                            ret
```

```
c010974f <ReadWordFromUsermode>:
c010974f: 83 ec 2c                      sub esp, 44
c0109752: 8b 44 24 30                   mov eax, dword ptr [esp + 48]
c0109756: 89 04 24                      mov dword ptr [esp], eax
c0109759: c7 44 24 04 04 00 00 00       mov dword ptr [esp + 4], 4
c0109761: 31 c0                         xor eax, eax
c0109763: 89 44 24 08                   mov dword ptr [esp + 8], eax
c0109767: 89 44 24 0c                   mov dword ptr [esp + 12], eax
c010976b: 89 44 24 10                   mov dword ptr [esp + 16], eax
c010976f: c7 44 24 14 01 00 00 00       mov dword ptr [esp + 20], 1
c0109777: c7 44 24 18 01 00 00 00       mov dword ptr [esp + 24], 1
c010977f: c6 44 24 1c 01                mov byte ptr [esp + 28], 1
c0109784: 6a 00                         push 0
c0109786: 6a 04                         push 4
c0109788: 8d 44 24 08                   lea eax, [esp + 8]
c010978c: 50                            push eax
c010978d: ff 74 24 40                   push dword ptr [esp + 64]
c0109791: e8 5d fd ff ff                call 0xc01094f3 <PerformTransfer>
c0109796: 83 c4 10                      add esp, 16
c0109799: 83 7c 24 08 00                cmp dword ptr [esp + 8], 0
c010979e: 75 07                         jne 0xc01097a7 <ReadWordFromUsermode+0x58>
c01097a0: 83 7c 24 04 00                cmp dword ptr [esp + 4], 0
c01097a5: 74 05                         je 0xc01097ac <ReadWordFromUsermode+0x5d>
c01097a7: b8 07 00 00 00                mov eax, 7
c01097ac: 83 c4 2c                      add esp, 44
c01097af: c3                            ret

c01097b0 <CreateKernelTransfer>:
c01097b0: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c01097b4: 8b 54 24 08                   mov edx, dword ptr [esp + 8]
c01097b8: 89 10                         mov dword ptr [eax], edx
c01097ba: 8b 54 24 0c                   mov edx, dword ptr [esp + 12]
c01097be: 8b 4c 24 10                   mov ecx, dword ptr [esp + 16]
c01097c2: 89 50 04                      mov dword ptr [eax + 4], edx
c01097c5: 89 48 08                      mov dword ptr [eax + 8], ecx
c01097c8: 8b 54 24 14                   mov edx, dword ptr [esp + 20]
c01097cc: 8b 4c 24 18                   mov ecx, dword ptr [esp + 24]
c01097d0: 89 50 0c                      mov dword ptr [eax + 12], edx
c01097d3: 89 48 10                      mov dword ptr [eax + 16], ecx
c01097d6: 8b 54 24 1c                   mov edx, dword ptr [esp + 28]
c01097da: 89 50 14                      mov dword ptr [eax + 20], edx
c01097dd: 31 d2                         xor edx, edx
c01097df: 89 50 18                      mov dword ptr [eax + 24], edx
c01097e2: c6 40 1c 01                   mov byte ptr [eax + 28], 1
c01097e6: c2 04 00                      ret 4

c01097e9 <CreateTransferWritingToUser>:
c01097e9: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c01097ed: 8b 54 24 08                   mov edx, dword ptr [esp + 8]
c01097f1: 89 10                         mov dword ptr [eax], edx
c01097f3: 8b 54 24 0c                   mov edx, dword ptr [esp + 12]
c01097f7: 8b 4c 24 10                   mov ecx, dword ptr [esp + 16]
c01097fb: 89 50 04                      mov dword ptr [eax + 4], edx
c01097fe: 89 48 08                      mov dword ptr [eax + 8], ecx
c0109801: 8b 54 24 14                   mov edx, dword ptr [esp + 20]
c0109805: 8b 4c 24 18                   mov ecx, dword ptr [esp + 24]
c0109809: 89 50 0c                      mov dword ptr [eax + 12], edx
c010980c: 89 48 10                      mov dword ptr [eax + 16], ecx
c010980f: 31 d2                         xor edx, edx
c0109811: 89 50 14                      mov dword ptr [eax + 20], edx
c0109814: c7 40 18 01 00 00 00          mov dword ptr [eax + 24], 1
c010981b: c6 40 1c 01                   mov byte ptr [eax + 28], 1
c010981f: c2 04 00                      ret 4

c0109822 <CreateTransferReadingFromUser>:
c0109822: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c0109826: 8b 54 24 08                   mov edx, dword ptr [esp + 8]
c010982a: 89 10                         mov dword ptr [eax], edx
c010982c: 8b 54 24 0c                   mov edx, dword ptr [esp + 12]
c0109830: 8b 4c 24 10                   mov ecx, dword ptr [esp + 16]
c0109834: 89 50 04                      mov dword ptr [eax + 4], edx
```

```
c0109886: 74 0a                         je 0xc0109892 <CheckValidComponentName+0x35>
c0109888: 8a 10                         mov dl, byte ptr [eax]
c010988a: 84 d2                         test dl, dl
c010988c: 75 e4                         jne 0xc0109872 <CheckValidComponentName+0x15>
c010988e: 31 c0                         xor eax, eax
c0109890: eb 05                         jmp 0xc0109897 <CheckValidComponentName+0x3a>
c0109892: b8 07 00 00 00                mov eax, 7
c0109897: 5b                            pop ebx
c0109898: c3                            ret

c0109899 <FileAccess>:
c0109899: 85 d2                         test edx, edx
c010989b: 74 69                         je 0xc0109906 <FileAccess+0x6d>
c010989d: 83 3a 00                      cmp dword ptr [edx], 0
c01098a0: 74 64                         je 0xc0109906 <FileAccess+0x6d>
c01098a2: 56                            push esi
c01098a3: 53                            push ebx
c01098a4: 53                            push ebx
c01098a5: 89 c3                         mov ebx, eax
c01098a7: b8 07 00 00 00                mov eax, 7
c01098ac: 85 db                         test ebx, ebx
c01098ae: 74 52                         je 0xc0109902 <FileAccess+0x69>
c01098b0: 8b 73 30                      mov esi, dword ptr [ebx + 48]
c01098b3: b8 07 00 00 00                mov eax, 7
c01098b8: 85 f6                         test esi, esi
c01098ba: 74 46                         je 0xc0109902 <FileAccess+0x69>
c01098bc: 84 c9                         test cl, cl
c01098be: 75 0c                         jne 0xc01098cc <FileAccess+0x33>
c01098c0: b8 14 00 00 00                mov eax, 20
c01098c5: 80 3b 00                      cmp byte ptr [ebx], 0
c01098c8: 75 0d                         jne 0xc01098d7 <FileAccess+0x3e>
c01098ca: eb 36                         jmp 0xc0109902 <FileAccess+0x69>
c01098cc: b8 14 00 00 00                mov eax, 20
c01098d1: 80 7b 01 00                   cmp byte ptr [ebx + 1], 0
c01098d5: 74 2b                         je 0xc0109902 <FileAccess+0x69>
c01098d7: 8b 86 94 00 00 00             mov eax, dword ptr [esi + 148]
c01098dd: c1 e8 07                      shr eax, 7
c01098e0: 83 f0 01                      xor eax, 1
c01098e3: 83 e0 01                      and eax, 1
c01098e6: 88 42 1c                      mov byte ptr [edx + 28], al
c01098e9: b8 5c a4 10 c0                mov eax, 3222316124
c01098ee: 84 c9                         test cl, cl
c01098f0: 74 05                         je 0xc01098f7 <FileAccess+0x5e>
c01098f2: b8 91 a4 10 c0                mov eax, 3222316177
c01098f7: 51                            push ecx
c01098f8: 51                            push ecx
c01098f9: 52                            push edx
c01098fa: ff 73 30                      push dword ptr [ebx + 48]
c01098fd: ff d0                         call eax
c01098ff: 83 c4 10                      add esp, 16
c0109902: 5a                            pop edx
c0109903: 5b                            pop ebx
c0109904: 5e                            pop esi
c0109905: c3                            ret
c0109906: b8 07 00 00 00                mov eax, 7
c010990b: c3                            ret

c010990c <RootsRead>:
c010990c: 57                            push edi
c010990d: 56                            push esi
c010990e: 53                            push ebx
c010990f: 81 ec 20 01 00 00             sub esp, 288
c0109915: 8b 9c 24 34 01 00 00          mov ebx, dword ptr [esp + 308]
c010991c: 8d 44 24 08                   lea eax, [esp + 8]
c0109920: 83 ec 0c                      sub esp, 12
c0109923: 50                            push eax
c0109924: 6a 00                         push 0
c0109926: 68 0c 01 00 00                push 268
c010992b: ff 73 10                      push dword ptr [ebx + 16]
c010992e: ff 73 0c                      push dword ptr [ebx + 12]
c0109931: e8 42 57 00 00                call 0xc010f078 <__udivmoddi4>
```

```
c01099a4: 68 0c 01 00 00                push 268
c01099a9: 53                            push ebx
c01099aa: 57                            push edi
c01099ab: e9 88 00 00 00                jmp 0xc0109a38 <RootsRead+0x12c>
c01099b0: 52                            push edx
c01099b1: 52                            push edx
c01099b2: 83 e8 02                      sub eax, 2
c01099b5: 50                            push eax
c01099b6: ff 35 18 b3 13 c0             push dword ptr [-1072450792]
c01099bc: e8 4f 82 ff ff                call 0xc0101c10 <ListGetDataAtIndex>
c01099c1: 89 c6                         mov esi, eax
c01099c3: 83 c4 10                      add esp, 16
c01099c6: b8 09 00 00 00                mov eax, 9
c01099cb: 85 f6                         test esi, esi
c01099cd: 74 78                         je 0xc0109a47 <RootsRead+0x13b>
c01099cf: 8b 06                         mov eax, dword ptr [esi]
c01099d1: 8b 40 30                      mov eax, dword ptr [eax + 48]
c01099d4: 8b 40 58                      mov eax, dword ptr [eax + 88]
c01099d7: c1 e8 0f                      shr eax, 15
c01099da: 88 84 24 19 01 00 00          mov byte ptr [esp + 281], al
c01099e1: 8b 06                         mov eax, dword ptr [esi]
c01099e3: 8b 40 30                      mov eax, dword ptr [eax + 48]
c01099e6: 8b 40 54                      mov eax, dword ptr [eax + 84]
c01099e9: 89 44 24 14                   mov dword ptr [esp + 20], eax
c01099ed: 8b 06                         mov eax, dword ptr [esi]
c01099ef: 8b 40 30                      mov eax, dword ptr [eax + 48]
c01099f2: 8b 40 4c                      mov eax, dword ptr [eax + 76]
c01099f5: 89 84 24 1c 01 00 00          mov dword ptr [esp + 284], eax
c01099fc: 83 ec 0c                      sub esp, 12
c01099ff: ff 76 04                      push dword ptr [esi + 4]
c0109a02: e8 d0 77 ff ff                call 0xc01011d7 <strlen>
c0109a07: 88 84 24 28 01 00 00          mov byte ptr [esp + 296], al
c0109a0e: 83 c4 0c                      add esp, 12
c0109a11: 68 00 01 00 00                push 256
c0109a16: ff 76 04                      push dword ptr [esi + 4]
c0109a19: 8d 74 24 20                   lea esi, [esp + 32]
c0109a1d: 8d 44 24 24                   lea eax, [esp + 36]
c0109a21: 50                            push eax
c0109a22: e8 91 78 ff ff                call 0xc01012b8 <strncpy>
c0109a27: c6 84 24 27 01 00 00 00       mov byte ptr [esp + 295], 0
c0109a2f: 6a 00                         push 0
c0109a31: 68 0c 01 00 00                push 268
c0109a36: 53                            push ebx
c0109a37: 56                            push esi
c0109a38: e8 b6 fa ff ff                call 0xc01094f3 <PerformTransfer>
c0109a3d: 83 c4 20                      add esp, 32
c0109a40: eb 05                         jmp 0xc0109a47 <RootsRead+0x13b>
c0109a42: b8 07 00 00 00                mov eax, 7
c0109a47: 81 c4 20 01 00 00             add esp, 288
c0109a4d: 5b                            pop ebx
c0109a4e: 5e                            pop esi
c0109a4f: 5f                            pop edi
c0109a50: c3                            ret

c0109a51 <GetPathComponent.constprop.0>:
c0109a51: 55                            push ebp
c0109a52: 57                            push edi
c0109a53: 56                            push esi
c0109a54: 53                            push ebx
c0109a55: 83 ec 14                      sub esp, 20
c0109a58: 89 c5                         mov ebp, eax
c0109a5a: 89 d7                         mov edi, edx
c0109a5c: 89 ce                         mov esi, ecx
c0109a5e: 8a 5c 24 28                   mov bl, byte ptr [esp + 40]
c0109a62: 50                            push eax
c0109a63: 68 74 17 11 c0                push 3222345588
c0109a68: e8 58 f0 ff ff                call 0xc0108ac5 <LogWriteSerial>
c0109a6d: c6 06 00                      mov byte ptr [esi], 0
c0109a70: 83 c4 10                      add esp, 16
c0109a73: 31 d2                         xor edx, edx
c0109a75: 8b 0f                         mov ecx, dword ptr [edi]
```

```
c0109aba: e9 9e fd ff ff                jmp 0xc010985d <CheckValidComponentName>
c0109abf: b8 0d 00 00 00                mov eax, 13
c0109ac4: 83 c4 0c                      add esp, 12
c0109ac7: 5b                            pop ebx
c0109ac8: 5e                            pop esi
c0109ac9: 5f                            pop edi
c0109aca: 5d                            pop ebp
c0109acb: c3                            ret

c0109acc <NextDevId>:
c0109acc: 53                            push ebx
c0109acd: 83 ec 0c                      sub esp, 12
c0109ad0: 6a 03                         push 3
c0109ad2: 68 97 17 11 c0                push 3222345623
c0109ad7: 68 fc b2 13 c0                push 3222516476
c0109adc: e8 5e ce ff ff                call 0xc010693f <InitSpinlock>
c0109ae1: c7 04 24 fc b2 13 c0          mov dword ptr [esp], 3222516476
c0109ae8: e8 6d ce ff ff                call 0xc010695a <AcquireSpinlock>
c0109aed: 8b 1d 18 31 11 c0             mov ebx, dword ptr [-1072615144]
c0109af3: 8d 43 01                      lea eax, [ebx + 1]
c0109af6: a3 18 31 11 c0                mov dword ptr [3222352152], eax
c0109afb: c7 04 24 fc b2 13 c0          mov dword ptr [esp], 3222516476
c0109b02: e8 a3 ce ff ff                call 0xc01069aa <ReleaseSpinlock>
c0109b07: 89 d8                         mov eax, ebx
c0109b09: 83 c4 18                      add esp, 24
c0109b0c: 5b                            pop ebx
c0109b0d: c3                            ret

c0109b0e <GetMountPointFromName>:
c0109b0e: 56                            push esi
c0109b0f: 53                            push ebx
c0109b10: 50                            push eax
c0109b11: a1 18 b3 13 c0                mov eax, dword ptr [3222516504]
c0109b16: 85 c0                         test eax, eax
c0109b18: 75 04                         jne 0xc0109b1e <GetMountPointFromName+0x10>
c0109b1a: 31 f6                         xor esi, esi
c0109b1c: eb 3d                         jmp 0xc0109b5b <GetMountPointFromName+0x4d>
c0109b1e: 83 ec 0c                      sub esp, 12
c0109b21: 50                            push eax
c0109b22: e8 b2 80 ff ff                call 0xc0101bd9 <ListGetNextNode>
c0109b27: 89 c3                         mov ebx, eax
c0109b29: 83 c4 10                      add esp, 16
c0109b2c: 85 c0                         test eax, eax
c0109b2e: 74 ea                         je 0xc0109b1a <GetMountPointFromName+0xc>
c0109b30: 83 ec 0c                      sub esp, 12
c0109b33: 53                            push ebx
c0109b34: e8 bc 80 ff ff                call 0xc0101bf5 <ListGetDataFromNode>
c0109b39: 89 c6                         mov esi, eax
c0109b3b: 59                            pop ecx
c0109b3c: 58                            pop eax
c0109b3d: ff 76 04                      push dword ptr [esi + 4]
c0109b40: ff 74 24 1c                   push dword ptr [esp + 28]
c0109b44: e8 58 76 ff ff                call 0xc01011a1 <strcmp>
c0109b49: 83 c4 10                      add esp, 16
c0109b4c: 85 c0                         test eax, eax
c0109b4e: 74 0b                         je 0xc0109b5b <GetMountPointFromName+0x4d>
c0109b50: 83 ec 0c                      sub esp, 12
c0109b53: 53                            push ebx
c0109b54: e8 80 80 ff ff                call 0xc0101bd9 <ListGetNextNode>
c0109b59: eb cc                         jmp 0xc0109b27 <GetMountPointFromName+0x19>
c0109b5b: 89 f0                         mov eax, esi
c0109b5d: 5a                            pop edx
c0109b5e: 5b                            pop ebx
c0109b5f: 5e                            pop esi
c0109b60: c3                            ret

c0109b61 <GetVnodeFromPath.part.0>:
c0109b61: 55                            push ebp
c0109b62: 57                            push edi
c0109b63: 56                            push esi
c0109b64: 53                            push ebx
```

```
c0109bbf: e9 36 01 00 00              jmp 0xc0109cfa <GetVnodeFromPath.part.0+0x199
c0109bc4: 8b 10                       mov edx, dword ptr [eax]
c0109bc6: 85 d2                       test edx, edx
c0109bc8: 74 f0                       je 0xc0109bba <GetVnodeFromPath.part.0+0x59>
c0109bca: 8b 5a 30                    mov ebx, dword ptr [edx + 48]
c0109bcd: 83 ec 0c                    sub esp, 12
c0109bd0: 53                          push ebx
c0109bd1: 52                          push edx
c0109bd2: 50                          push eax
c0109bd3: 55                          push ebp
c0109bd4: 68 bc 17 11 c0              push 3222345660
c0109bd9: e8 e7 ee ff ff              call 0xc0108ac5 <LogWriteSerial>
c0109bde: 83 c4 20                    add esp, 32
c0109be1: 85 db                       test ebx, ebx
c0109be3: 74 d5                       je 0xc0109bba <GetVnodeFromPath.part.0+0x59>
c0109be5: 83 ec 0c                    sub esp, 12
c0109be8: 53                          push ebx
c0109be9: e8 20 08 00 00              call 0xc010a40e <ReferenceVnode>
c0109bee: 83 c4 10                    add esp, 16
c0109bf1: 83 ec 0c                    sub esp, 12
c0109bf4: 56                          push esi
c0109bf5: e8 dd 75 ff ff              call 0xc01011d7 <strlen>
c0109bfa: 83 c4 10                    add esp, 16
c0109bfd: 3b 44 24 14                 cmp eax, dword ptr [esp + 20]
c0109c01: 0f 8e 89 00 00 00           jle 0xc0109c90 <GetVnodeFromPath.part.0+0x12f
c0109c07: 51                          push ecx
c0109c08: 51                          push ecx
c0109c09: 56                          push esi
c0109c0a: 68 e3 17 11 c0              push 3222345699
c0109c0f: e8 b1 ee ff ff              call 0xc0108ac5 <LogWriteSerial>
c0109c14: 8d ac 24 af 00 00 00        lea ebp, [esp + 175]
c0109c1b: c7 04 24 2f 00 00 00        mov dword ptr [esp], 47
c0109c22: 89 e9                       mov ecx, ebp
c0109c24: 8d 54 24 24                 lea edx, [esp + 36]
c0109c28: 89 f0                       mov eax, esi
c0109c2a: e8 22 fe ff ff              call 0xc0109a51 <GetPathComponent.constprop.0
c0109c2f: 83 c4 10                    add esp, 16
c0109c32: 85 c0                       test eax, eax
c0109c34: 75 3b                       jne 0xc0109c71 <GetVnodeFromPath.part.0+0x110
c0109c36: 50                          push eax
c0109c37: 56                          push esi
c0109c38: 55                          push ebp
c0109c39: 68 f1 17 11 c0              push 3222345713
c0109c3e: e8 82 ee ff ff              call 0xc0108ac5 <LogWriteSerial>
c0109c43: 58                          pop eax
c0109c44: 5a                          pop edx
c0109c45: 68 6f 17 11 c0              push 3222345583
c0109c4a: 55                          push ebp
c0109c4b: e8 51 75 ff ff              call 0xc01011a1 <strcmp>
c0109c50: 83 c4 10                    add esp, 16
c0109c53: 85 c0                       test eax, eax
c0109c55: 74 9a                       je 0xc0109bf1 <GetVnodeFromPath.part.0+0x90>
c0109c57: 31 d2                       xor edx, edx
c0109c59: 89 54 24 18                 mov dword ptr [esp + 24], edx
c0109c5d: 51                          push ecx
c0109c5e: 55                          push ebp
c0109c5f: 8d 44 24 20                 lea eax, [esp + 32]
c0109c63: 50                          push eax
c0109c64: 53                          push ebx
c0109c65: e8 4f 09 00 00              call 0xc010a5b9 <VnodeOpFollow>
c0109c6a: 83 c4 10                    add esp, 16
c0109c6d: 85 c0                       test eax, eax
c0109c6f: 74 16                       je 0xc0109c87 <GetVnodeFromPath.part.0+0x126>
c0109c71: 89 44 24 0c                 mov dword ptr [esp + 12], eax
c0109c75: 83 ec 0c                    sub esp, 12
c0109c78: 53                          push ebx
c0109c79: e8 d1 09 00 00              call 0xc010a64f <DereferenceVnode>
c0109c7e: 83 c4 10                    add esp, 16
c0109c81: 8b 44 24 0c                 mov eax, dword ptr [esp + 12]
c0109c85: eb 73                       jmp 0xc0109cfa <GetVnodeFromPath.part.0+0x199
c0109c87: 8b 5c 24 18                 mov ebx, dword ptr [esp + 24]
```

```
c0109ce8: 68 9d 17 11 c0                push 3222345629
c0109ced: e8 d3 ed ff ff                call 0xc0108ac5 <LogWriteSerial>
c0109cf2: 83 c4 10                      add esp, 16
c0109cf5: e9 c0 fe ff ff                jmp 0xc0109bba <GetVnodeFromPath.part.0+0x59>
c0109cfa: 81 c4 2c 01 00 00             add esp, 300
c0109d00: 5b                            pop ebx
c0109d01: 5e                            pop esi
c0109d02: 5f                            pop edi
c0109d03: 5d                            pop ebp
c0109d04: c3                            ret

c0109d05 <GetVnodeFromPath>:
c0109d05: 57                            push edi
c0109d06: 56                            push esi
c0109d07: 53                            push ebx
c0109d08: 89 c3                         mov ebx, eax
c0109d0a: 89 d7                         mov edi, edx
c0109d0c: 89 ce                         mov esi, ecx
c0109d0e: 52                            push edx
c0109d0f: 52                            push edx
c0109d10: 50                            push eax
c0109d11: 68 08 18 11 c0                push 3222345736
c0109d16: e8 aa ed ff ff                call 0xc0108ac5 <LogWriteSerial>
c0109d1b: 89 1c 24                      mov dword ptr [esp], ebx
c0109d1e: e8 b4 74 ff ff                call 0xc01011d7 <strlen>
c0109d23: 83 c4 10                      add esp, 16
c0109d26: 85 c0                         test eax, eax
c0109d28: 74 24                         je 0xc0109d4e <GetVnodeFromPath+0x49>
c0109d2a: 83 ec 0c                      sub esp, 12
c0109d2d: 53                            push ebx
c0109d2e: e8 a4 74 ff ff                call 0xc01011d7 <strlen>
c0109d33: 83 c4 10                      add esp, 16
c0109d36: 3d cf 07 00 00                cmp eax, 1999
c0109d3b: 77 18                         ja 0xc0109d55 <GetVnodeFromPath+0x50>
c0109d3d: 89 f0                         mov eax, esi
c0109d3f: 0f b6 c8                      movzx ecx, al
c0109d42: 89 fa                         mov edx, edi
c0109d44: 89 d8                         mov eax, ebx
c0109d46: 5b                            pop ebx
c0109d47: 5e                            pop esi
c0109d48: 5f                            pop edi
c0109d49: e9 13 fe ff ff                jmp 0xc0109b61 <GetVnodeFromPath.part.0>
c0109d4e: b8 07 00 00 00                mov eax, 7
c0109d53: eb 05                         jmp 0xc0109d5a <GetVnodeFromPath+0x55>
c0109d55: b8 0d 00 00 00                mov eax, 13
c0109d5a: 5b                            pop ebx
c0109d5b: 5e                            pop esi
c0109d5c: 5f                            pop edi
c0109d5d: c3                            ret

c0109d5e <RootsFollow>:
c0109d5e: 56                            push esi
c0109d5f: 53                            push ebx
c0109d60: 83 ec 0c                      sub esp, 12
c0109d63: 8b 5c 24 1c                   mov ebx, dword ptr [esp + 28]
c0109d67: 8b 74 24 20                   mov esi, dword ptr [esp + 32]
c0109d6b: 68 71 17 11 c0                push 3222345585
c0109d70: 56                            push esi
c0109d71: e8 2b 74 ff ff                call 0xc01011a1 <strcmp>
c0109d76: 83 c4 10                      add esp, 16
c0109d79: 85 c0                         test eax, eax
c0109d7b: 75 06                         jne 0xc0109d83 <RootsFollow+0x25>
c0109d7d: 8b 44 24 10                   mov eax, dword ptr [esp + 16]
c0109d81: eb 1a                         jmp 0xc0109d9d <RootsFollow+0x3f>
c0109d83: 83 ec 0c                      sub esp, 12
c0109d86: 56                            push esi
c0109d87: e8 82 fd ff ff                call 0xc0109b0e <GetMountPointFromName>
c0109d8c: 83 c4 10                      add esp, 16
c0109d8f: ba 09 00 00 00                mov edx, 9
c0109d94: 85 c0                         test eax, eax
c0109d96: 74 09                         je 0xc0109da1 <RootsFollow+0x43>
```

```
c0109dd8: 85 f6                         test esi, esi
c0109dda: 0f 84 bf 00 00 00             je 0xc0109e9f <AddVfsMount+0xd6>
c0109de0: 85 ed                         test ebp, ebp
c0109de2: 0f 84 b7 00 00 00             je 0xc0109e9f <AddVfsMount+0xd6>
c0109de8: 83 ec 0c                      sub esp, 12
c0109deb: 56                            push esi
c0109dec: e8 e6 73 ff ff                call 0xc01011d7 <strlen>
c0109df1: 83 c4 10                      add esp, 16
c0109df4: bb 0d 00 00 00                mov ebx, 13
c0109df9: 83 f8 7f                      cmp eax, 127
c0109dfc: 0f 87 a2 00 00 00             ja 0xc0109ea4 <AddVfsMount+0xdb>
c0109e02: 89 f0                         mov eax, esi
c0109e04: e8 54 fa ff ff                call 0xc010985d <CheckValidComponentName>
c0109e09: 89 c3                         mov ebx, eax
c0109e0b: 85 c0                         test eax, eax
c0109e0d: 0f 85 91 00 00 00             jne 0xc0109ea4 <AddVfsMount+0xdb>
c0109e13: 83 ec 0c                      sub esp, 12
c0109e16: 68 1c b3 13 c0                push 3222516508
c0109e1b: e8 3a cb ff ff                call 0xc010695a <AcquireSpinlock>
c0109e20: 89 34 24                      mov dword ptr [esp], esi
c0109e23: e8 e6 fc ff ff                call 0xc0109b0e <GetMountPointFromName>
c0109e28: 83 c4 10                      add esp, 16
c0109e2b: 85 c0                         test eax, eax
c0109e2d: 75 59                         jne 0xc0109e88 <AddVfsMount+0xbf>
c0109e2f: 83 ec 0c                      sub esp, 12
c0109e32: 6a 08                         push 8
c0109e34: e8 16 9b ff ff                call 0xc010394f <AllocHeap>
c0109e39: 89 c7                         mov edi, eax
c0109e3b: 89 34 24                      mov dword ptr [esp], esi
c0109e3e: e8 b2 74 ff ff                call 0xc01012f5 <strdup>
c0109e43: 89 47 04                      mov dword ptr [edi + 4], eax
c0109e46: c7 04 24 01 00 00 00          mov dword ptr [esp], 1
c0109e4d: 6a 01                         push 1
c0109e4f: 6a 00                         push 0
c0109e51: 6a 00                         push 0
c0109e53: 55                            push ebp
c0109e54: e8 f4 f4 ff ff                call 0xc010934d <CreateFile>
c0109e59: 89 07                         mov dword ptr [edi], eax
c0109e5b: 83 c4 18                      add esp, 24
c0109e5e: 57                            push edi
c0109e5f: ff 35 18 b3 13 c0             push dword ptr [-1072450792]
c0109e65: e8 0d 7c ff ff                call 0xc0101a77 <ListInsertEnd>
c0109e6a: 58                            pop eax
c0109e6b: 5a                            pop edx
c0109e6c: 56                            push esi
c0109e6d: 68 22 18 11 c0                push 3222345762
c0109e72: e8 4e ec ff ff                call 0xc0108ac5 <LogWriteSerial>
c0109e77: c7 04 24 1c b3 13 c0          mov dword ptr [esp], 3222516508
c0109e7e: e8 27 cb ff ff                call 0xc01069aa <ReleaseSpinlock>
c0109e83: 83 c4 10                      add esp, 16
c0109e86: eb 1c                         jmp 0xc0109ea4 <AddVfsMount+0xdb>
c0109e88: 83 ec 0c                      sub esp, 12
c0109e8b: 68 1c b3 13 c0                push 3222516508
c0109e90: e8 15 cb ff ff                call 0xc01069aa <ReleaseSpinlock>
c0109e95: 83 c4 10                      add esp, 16
c0109e98: bb 08 00 00 00                mov ebx, 8
c0109e9d: eb 05                         jmp 0xc0109ea4 <AddVfsMount+0xdb>
c0109e9f: bb 07 00 00 00                mov ebx, 7
c0109ea4: 89 d8                         mov eax, ebx
c0109ea6: 83 c4 0c                      add esp, 12
c0109ea9: 5b                            pop ebx
c0109eaa: 5e                            pop esi
c0109eab: 5f                            pop edi
c0109eac: 5d                            pop ebp
c0109ead: c3                            ret

c0109eae <InitRootsFilesystem>:
c0109eae: 57                            push edi
c0109eaf: 56                            push esi
c0109eb0: 83 ec 74                      sub esp, 116
c0109eb3: 89 e7                         mov edi, esp
```

```
c0109f2a: 81 c4 84 00 00 00           add esp, 132
c0109f30: 5e                          pop esi
c0109f31: 5f                          pop edi
c0109f32: c3                          ret

c0109f33 <RemoveVfsMount>:
c0109f33: 56                          push esi
c0109f34: 53                          push ebx
c0109f35: 53                          push ebx
c0109f36: 8b 74 24 10                 mov esi, dword ptr [esp + 16]
c0109f3a: bb 07 00 00 00              mov ebx, 7
c0109f3f: 85 f6                       test esi, esi
c0109f41: 0f 84 84 00 00 00           je 0xc0109fcb <RemoveVfsMount+0x98>
c0109f47: 89 f0                       mov eax, esi
c0109f49: e8 0f f9 ff ff              call 0xc010985d <CheckValidComponentName>
c0109f4e: 89 c3                       mov ebx, eax
c0109f50: 85 c0                       test eax, eax
c0109f52: 75 72                       jne 0xc0109fc6 <RemoveVfsMount+0x93>
c0109f54: 83 ec 0c                    sub esp, 12
c0109f57: 68 1c b3 13 c0              push 3222516508
c0109f5c: e8 f9 c9 ff ff              call 0xc010695a <AcquireSpinlock>
c0109f61: 89 34 24                    mov dword ptr [esp], esi
c0109f64: e8 a5 fb ff ff              call 0xc0109b0e <GetMountPointFromName>
c0109f69: 89 c6                       mov esi, eax
c0109f6b: 83 c4 10                    add esp, 16
c0109f6e: 85 c0                       test eax, eax
c0109f70: 75 17                       jne 0xc0109f89 <RemoveVfsMount+0x56>
c0109f72: 83 ec 0c                    sub esp, 12
c0109f75: 68 1c b3 13 c0              push 3222516508
c0109f7a: e8 2b ca ff ff              call 0xc01069aa <ReleaseSpinlock>
c0109f7f: 83 c4 10                    add esp, 16
c0109f82: bb 03 00 00 00              mov ebx, 3
c0109f87: eb 42                       jmp 0xc0109fcb <RemoveVfsMount+0x98>
c0109f89: 83 ec 0c                    sub esp, 12
c0109f8c: 8b 00                       mov eax, dword ptr [eax]
c0109f8e: ff 70 30                    push dword ptr [eax + 48]
c0109f91: e8 b9 06 00 00              call 0xc010a64f <DereferenceVnode>
c0109f96: 59                          pop ecx
c0109f97: ff 36                       push dword ptr [esi]
c0109f99: e8 39 f4 ff ff              call 0xc01093d7 <DereferenceFile>
c0109f9e: 58                          pop eax
c0109f9f: 5a                          pop edx
c0109fa0: 56                          push esi
c0109fa1: ff 35 18 b3 13 c0           push dword ptr [-1072450792]
c0109fa7: e8 e8 7b ff ff              call 0xc0101b94 <ListDeleteData>
c0109fac: 59                          pop ecx
c0109fad: ff 76 04                    push dword ptr [esi + 4]
c0109fb0: e8 be 99 ff ff              call 0xc0103973 <FreeHeap>
c0109fb5: c7 04 24 1c b3 13 c0        mov dword ptr [esp], 3222516508
c0109fbc: e8 e9 c9 ff ff              call 0xc01069aa <ReleaseSpinlock>
c0109fc1: 83 c4 10                    add esp, 16
c0109fc4: eb 05                       jmp 0xc0109fcb <RemoveVfsMount+0x98>
c0109fc6: bb 07 00 00 00              mov ebx, 7
c0109fcb: 89 d8                       mov eax, ebx
c0109fcd: 5a                          pop edx
c0109fce: 5b                          pop ebx
c0109fcf: 5e                          pop esi
c0109fd0: c3                          ret

c0109fd1 <RemoveFileOrDirectory>:
c0109fd1: 56                          push esi
c0109fd2: 53                          push ebx
c0109fd3: 83 ec 24                    sub esp, 36
c0109fd6: 8b 74 24 34                 mov esi, dword ptr [esp + 52]
c0109fda: 31 c9                       xor ecx, ecx
c0109fdc: 8d 54 24 1c                 lea edx, [esp + 28]
c0109fe0: 8b 44 24 30                 mov eax, dword ptr [esp + 48]
c0109fe4: e8 1c fd ff ff              call 0xc0109d05 <GetVnodeFromPath>
c0109fe9: 85 c0                       test eax, eax
c0109feb: 75 5a                       jne 0xc010a047 <RemoveFileOrDirectory+0x76>
c0109fed: 8b 5c 24 1c                 mov ebx, dword ptr [esp + 28]
```

```
c010a04a: 5b                            pop ebx
c010a04b: 5e                            pop esi
c010a04c: c3                            ret

c010a04d <OpenFile>:
c010a04d: 55                            push ebp
c010a04e: 57                            push edi
c010a04f: 56                            push esi
c010a050: 53                            push ebx
c010a051: 81 ec b4 00 00 00             sub esp, 180
c010a057: 8b bc 24 c8 00 00 00          mov edi, dword ptr [esp + 200]
c010a05e: 8b b4 24 cc 00 00 00          mov esi, dword ptr [esp + 204]
c010a065: 57                            push edi
c010a066: 68 3c 18 11 c0                push 3222345788
c010a06b: e8 55 ea ff ff                call 0xc0108ac5 <LogWriteSerial>
c010a070: 83 c4 10                      add esp, 16
c010a073: 83 bc 24 cc 00 00 00 00       cmp dword ptr [esp + 204], 0
c010a07b: 74 04                         je 0xc010a081 <OpenFile+0x34>
c010a07d: 85 ff                         test edi, edi
c010a07f: 75 16                         jne 0xc010a097 <OpenFile+0x4a>
c010a081: 53                            push ebx
c010a082: 53                            push ebx
c010a083: 6a 00                         push 0
c010a085: 68 4b 18 11 c0                push 3222345803
c010a08a: e8 36 ea ff ff                call 0xc0108ac5 <LogWriteSerial>
c010a08f: 83 c4 10                      add esp, 16
c010a092: e9 ca 01 00 00                jmp 0xc010a261 <OpenFile+0x214>
c010a097: 83 ec 0c                      sub esp, 12
c010a09a: 57                            push edi
c010a09b: e8 37 71 ff ff                call 0xc01011d7 <strlen>
c010a0a0: 83 c4 10                      add esp, 16
c010a0a3: 85 c0                         test eax, eax
c010a0a5: 74 da                         je 0xc010a081 <OpenFile+0x34>
c010a0a7: 31 c9                         xor ecx, ecx
c010a0a9: 8d 54 24 14                   lea edx, [esp + 20]
c010a0ad: 89 f8                         mov eax, edi
c010a0af: e8 51 fc ff ff                call 0xc0109d05 <GetVnodeFromPath>
c010a0b4: 89 c3                         mov ebx, eax
c010a0b6: f7 c6 04 00 00 00             test esi, 4
c010a0bc: 0f 84 2e 01 00 00             je 0xc010a1f0 <OpenFile+0x1a3>
c010a0c2: 83 f8 09                      cmp eax, 9
c010a0c5: 0f 85 18 01 00 00             jne 0xc010a1e3 <OpenFile+0x196>
c010a0cb: b9 01 00 00 00                mov ecx, 1
c010a0d0: 8d 54 24 14                   lea edx, [esp + 20]
c010a0d4: 89 f8                         mov eax, edi
c010a0d6: e8 2a fc ff ff                call 0xc0109d05 <GetVnodeFromPath>
c010a0db: 89 c3                         mov ebx, eax
c010a0dd: 85 c0                         test eax, eax
c010a0df: 0f 85 d9 01 00 00             jne 0xc010a2be <OpenFile+0x271>
c010a0e5: 83 ec 0c                      sub esp, 12
c010a0e8: 68 55 18 11 c0                push 3222345813
c010a0ed: e8 eb e9 ff ff                call 0xc0108add <LogDeveloperWarning>
c010a0f2: 31 c9                         xor ecx, ecx
c010a0f4: 89 4c 24 28                   mov dword ptr [esp + 40], ecx
c010a0f8: 89 f8                         mov eax, edi
c010a0fa: 83 c4 10                      add esp, 16
c010a0fd: 8a 10                         mov dl, byte ptr [eax]
c010a0ff: 84 d2                         test dl, dl
c010a101: 74 08                         je 0xc010a10b <OpenFile+0xbe>
c010a103: 40                            inc eax
c010a104: 80 fa 3a                      cmp dl, 58
c010a107: 75 f4                         jne 0xc010a0fd <OpenFile+0xb0>
c010a109: eb 43                         jmp 0xc010a14e <OpenFile+0x101>
c010a10b: 83 ec 0c                      sub esp, 12
c010a10e: 57                            push edi
c010a10f: e8 c3 70 ff ff                call 0xc01011d7 <strlen>
c010a114: 83 c4 10                      add esp, 16
c010a117: 3b 44 24 18                   cmp eax, dword ptr [esp + 24]
c010a11b: 7e 64                         jle 0xc010a181 <OpenFile+0x134>
c010a11d: 83 ec 0c                      sub esp, 12
c010a120: 6a 2f                         push 47
```

```
c010a170: 68 86 18 11 c0              push 3222345862
c010a175: e8 4b e9 ff ff              call 0xc0108ac5 <LogWriteSerial>
c010a17a: 83 c4 10                    add esp, 16
c010a17d: 8b 5c 24 0c                 mov ebx, dword ptr [esp + 12]
c010a181: 57                          push edi
c010a182: 57                          push edi
c010a183: 8d 6c 24 27                 lea ebp, [esp + 39]
c010a187: 55                          push ebp
c010a188: 68 9c 18 11 c0              push 3222345884
c010a18d: e8 33 e9 ff ff              call 0xc0108ac5 <LogWriteSerial>
c010a192: 83 c4 10                    add esp, 16
c010a195: 85 db                       test ebx, ebx
c010a197: 74 0f                       je 0xc010a1a8 <OpenFile+0x15b>
c010a199: 51                          push ecx
c010a19a: 51                          push ecx
c010a19b: 53                          push ebx
c010a19c: 68 bf 18 11 c0              push 3222345919
c010a1a1: e8 1f e9 ff ff              call 0xc0108ac5 <LogWriteSerial>
c010a1a6: eb 76                       jmp 0xc010a21e <OpenFile+0x1d1>
c010a1a8: 8b 7c 24 14                 mov edi, dword ptr [esp + 20]
c010a1ac: 83 ec 0c                    sub esp, 12
c010a1af: ff b4 24 d4 00 00 00        push dword ptr [esp + 212]
c010a1b6: 56                          push esi
c010a1b7: 55                          push ebp
c010a1b8: 8d 44 24 30                 lea eax, [esp + 48]
c010a1bc: 50                          push eax
c010a1bd: 57                          push edi
c010a1be: e8 6c 03 00 00              call 0xc010a52f <VnodeOpCreate>
c010a1c3: 89 c3                       mov ebx, eax
c010a1c5: 83 c4 14                    add esp, 20
c010a1c8: 57                          push edi
c010a1c9: e8 81 04 00 00              call 0xc010a64f <DereferenceVnode>
c010a1ce: 83 c4 10                    add esp, 16
c010a1d1: 85 db                       test ebx, ebx
c010a1d3: 0f 85 e5 00 00 00           jne 0xc010a2be <OpenFile+0x271>
c010a1d9: 8b 44 24 18                 mov eax, dword ptr [esp + 24]
c010a1dd: 89 44 24 14                 mov dword ptr [esp + 20], eax
c010a1e1: eb 15                       jmp 0xc010a1f8 <OpenFile+0x1ab>
c010a1e3: bb 08 00 00 00              mov ebx, 8
c010a1e8: f7 c6 08 00 00 00           test esi, 8
c010a1ee: eb 02                       jmp 0xc010a1f2 <OpenFile+0x1a5>
c010a1f0: 85 c0                       test eax, eax
c010a1f2: 0f 85 c6 00 00 00           jne 0xc010a2be <OpenFile+0x271>
c010a1f8: 8b 7c 24 14                 mov edi, dword ptr [esp + 20]
c010a1fc: 52                          push edx
c010a1fd: 52                          push edx
c010a1fe: 89 f0                       mov eax, esi
c010a200: 25 83 00 00 00              and eax, 131
c010a205: 50                          push eax
c010a206: 57                          push edi
c010a207: e8 25 02 00 00              call 0xc010a431 <VnodeOpCheckOpen>
c010a20c: 89 c3                       mov ebx, eax
c010a20e: 83 c4 10                    add esp, 16
c010a211: 85 c0                       test eax, eax
c010a213: 74 11                       je 0xc010a226 <OpenFile+0x1d9>
c010a215: 83 ec 0c                    sub esp, 12
c010a218: 57                          push edi
c010a219: e8 31 04 00 00              call 0xc010a64f <DereferenceVnode>
c010a21e: 83 c4 10                    add esp, 16
c010a221: e9 98 00 00 00              jmp 0xc010a2be <OpenFile+0x271>
c010a226: 89 f1                       mov ecx, esi
c010a228: 83 e1 03                    and ecx, 3
c010a22b: 0f 95 c0                    setne al
c010a22e: 8b 57 58                    mov edx, dword ptr [edi + 88]
c010a231: c1 ea 0f                    shr edx, 15
c010a234: 83 fa 05                    cmp edx, 5
c010a237: 75 17                       jne 0xc010a250 <OpenFile+0x203>
c010a239: 84 c0                       test al, al
c010a23b: 74 13                       je 0xc010a250 <OpenFile+0x203>
c010a23d: 83 ec 0c                    sub esp, 12
c010a240: 57                          push edi
```

```
c010a297: 31 c0                         xor eax, eax
c010a299: 49                            dec ecx
c010a29a: 0f 95 c0                      setne al
c010a29d: 50                            push eax
c010a29e: 81 e6 00 01 00 00             and esi, 256
c010a2a4: 56                            push esi
c010a2a5: ff b4 24 e0 00 00 00          push dword ptr [esp + 224]
c010a2ac: 57                            push edi
c010a2ad: e8 9b f0 ff ff                call 0xc010934d <CreateFile>
c010a2b2: 8b b4 24 ec 00 00 00          mov esi, dword ptr [esp + 236]
c010a2b9: 89 06                         mov dword ptr [esi], eax
c010a2bb: 83 c4 20                      add esp, 32
c010a2be: 89 d8                         mov eax, ebx
c010a2c0: 81 c4 ac 00 00 00             add esp, 172
c010a2c6: 5b                            pop ebx
c010a2c7: 5e                            pop esi
c010a2c8: 5f                            pop edi
c010a2c9: 5d                            pop ebp
c010a2ca: c3                            ret

c010a2cb <ReadFile>:
c010a2cb: 31 c9                         xor ecx, ecx
c010a2cd: 8b 54 24 08                   mov edx, dword ptr [esp + 8]
c010a2d1: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c010a2d5: e9 bf f5 ff ff                jmp 0xc0109899 <FileAccess>

c010a2da <WriteFile>:
c010a2da: b9 01 00 00 00                mov ecx, 1
c010a2df: 8b 54 24 08                   mov edx, dword ptr [esp + 8]
c010a2e3: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c010a2e7: e9 ad f5 ff ff                jmp 0xc0109899 <FileAccess>

c010a2ec <CloseFile>:
c010a2ec: 53                            push ebx
c010a2ed: 83 ec 08                      sub esp, 8
c010a2f0: 8b 5c 24 10                   mov ebx, dword ptr [esp + 16]
c010a2f4: b8 07 00 00 00                mov eax, 7
c010a2f9: 85 db                         test ebx, ebx
c010a2fb: 74 1d                         je 0xc010a31a <CloseFile+0x2e>
c010a2fd: 8b 53 30                      mov edx, dword ptr [ebx + 48]
c010a300: 85 d2                         test edx, edx
c010a302: 74 16                         je 0xc010a31a <CloseFile+0x2e>
c010a304: 83 ec 0c                      sub esp, 12
c010a307: 52                            push edx
c010a308: e8 42 03 00 00                call 0xc010a64f <DereferenceVnode>
c010a30d: 89 1c 24                      mov dword ptr [esp], ebx
c010a310: e8 c2 f0 ff ff                call 0xc01093d7 <DereferenceFile>
c010a315: 83 c4 10                      add esp, 16
c010a318: 31 c0                         xor eax, eax
c010a31a: 83 c4 08                      add esp, 8
c010a31d: 5b                            pop ebx
c010a31e: c3                            ret

c010a31f <SetWorkingDirectory>:
c010a31f: 57                            push edi
c010a320: 56                            push esi
c010a321: 53                            push ebx
c010a322: 8b 74 24 10                   mov esi, dword ptr [esp + 16]
c010a326: e8 5a c9 ff ff                call 0xc0106c85 <GetProcess>
c010a32b: 85 f6                         test esi, esi
c010a32d: 74 4e                         je 0xc010a37d <SetWorkingDirectory+0x5e>
c010a32f: 89 c3                         mov ebx, eax
c010a331: 85 c0                         test eax, eax
c010a333: 74 48                         je 0xc010a37d <SetWorkingDirectory+0x5e>
c010a335: 8b 56 58                      mov edx, dword ptr [esi + 88]
c010a338: 81 e2 00 80 03 00             and edx, 229376
c010a33e: b8 0e 00 00 00                mov eax, 14
c010a343: 81 fa 00 80 02 00             cmp edx, 163840
c010a349: 75 37                         jne 0xc010a382 <SetWorkingDirectory+0x63>
c010a34b: e8 f7 d2 ff ff                call 0xc0107647 <LockScheduler>
c010a350: 8b 7b 28                      mov edi, dword ptr [ebx + 40]
```

```
c010a398: 75 14                         jne 0xc010a3ae <CheckVnode+0x28>
c010a39a: 83 ec 0c                      sub esp, 12
c010a39d: 53                            push ebx
c010a39e: e8 b7 c5 ff ff                call 0xc010695a <AcquireSpinlock>
c010a3a3: 89 1c 24                      mov dword ptr [esp], ebx
c010a3a6: e8 ff c5 ff ff                call 0xc01069aa <ReleaseSpinlock>
c010a3ab: 83 c4 10                      add esp, 16
c010a3ae: 83 c4 08                      add esp, 8
c010a3b1: 5b                            pop ebx
c010a3b2: c3                            ret

c010a3b3 <CreateVnode>:
c010a3b3: 57                            push edi
c010a3b4: 56                            push esi
c010a3b5: 53                            push ebx
c010a3b6: 83 ec 0c                      sub esp, 12
c010a3b9: 68 98 00 00 00                push 152
c010a3be: e8 8c 95 ff ff                call 0xc010394f <AllocHeap>
c010a3c3: 89 c3                         mov ebx, eax
c010a3c5: b9 26 00 00 00                mov ecx, 38
c010a3ca: 31 c0                         xor eax, eax
c010a3cc: 89 df                         mov edi, ebx
c010a3ce: f3 ab                         rep  stosd dword ptr es:[edi], eax
c010a3d0: b9 0a 00 00 00                mov ecx, 10
c010a3d5: 89 df                         mov edi, ebx
c010a3d7: 8d 74 24 20                   lea esi, [esp + 32]
c010a3db: f3 a5                         rep  movsd dword ptr es:[edi], dword ptr [esi
c010a3dd: c7 43 2c 01 00 00 00          mov dword ptr [ebx + 44], 1
c010a3e4: 8d 7b 4c                      lea edi, [ebx + 76]
c010a3e7: 8d 74 24 48                   lea esi, [esp + 72]
c010a3eb: b9 12 00 00 00                mov ecx, 18
c010a3f0: f3 a5                         rep  movsd dword ptr es:[edi], dword ptr [esi
c010a3f2: 83 c4 0c                      add esp, 12
c010a3f5: 6a 03                         push 3
c010a3f7: 68 c9 18 11 c0                push 3222345929
c010a3fc: 8d 43 30                      lea eax, [ebx + 48]
c010a3ff: 50                            push eax
c010a400: e8 3a c5 ff ff                call 0xc010693f <InitSpinlock>
c010a405: 83 c4 10                      add esp, 16
c010a408: 89 d8                         mov eax, ebx
c010a40a: 5b                            pop ebx
c010a40b: 5e                            pop esi
c010a40c: 5f                            pop edi
c010a40d: c3                            ret

c010a40e <ReferenceVnode>:
c010a40e: 56                            push esi
c010a40f: 53                            push ebx
c010a410: 83 ec 10                      sub esp, 16
c010a413: 8b 5c 24 1c                   mov ebx, dword ptr [esp + 28]
c010a417: 8d 73 30                      lea esi, [ebx + 48]
c010a41a: 56                            push esi
c010a41b: e8 3a c5 ff ff                call 0xc010695a <AcquireSpinlock>
c010a420: ff 43 2c                      inc dword ptr [ebx + 44]
c010a423: 89 74 24 20                   mov dword ptr [esp + 32], esi
c010a427: 83 c4 14                      add esp, 20
c010a42a: 5b                            pop ebx
c010a42b: 5e                            pop esi
c010a42c: e9 79 c5 ff ff                jmp 0xc01069aa <ReleaseSpinlock>

c010a431 <VnodeOpCheckOpen>:
c010a431: 56                            push esi
c010a432: 53                            push ebx
c010a433: 53                            push ebx
c010a434: 8b 5c 24 10                   mov ebx, dword ptr [esp + 16]
c010a438: 8b 74 24 14                   mov esi, dword ptr [esp + 20]
c010a43c: 89 d8                         mov eax, ebx
c010a43e: e8 43 ff ff ff                call 0xc010a386 <CheckVnode>
c010a443: 8b 03                         mov eax, dword ptr [ebx]
c010a445: 85 c0                         test eax, eax
c010a447: 74 0d                         je 0xc010a456 <VnodeOpCheckOpen+0x25>
```

```
c010a485: 5e                            pop esi
c010a486: ff e0                         jmp eax
c010a488: b8 07 00 00 00                mov eax, 7
c010a48d: 5a                            pop edx
c010a48e: 5b                            pop ebx
c010a48f: 5e                            pop esi
c010a490: c3                            ret

c010a491 <VnodeOpWrite>:
c010a491: 56                            push esi
c010a492: 53                            push ebx
c010a493: 53                            push ebx
c010a494: 8b 5c 24 10                   mov ebx, dword ptr [esp + 16]
c010a498: 8b 74 24 14                   mov esi, dword ptr [esp + 20]
c010a49c: 89 d8                         mov eax, ebx
c010a49e: e8 e3 fe ff ff                call 0xc010a386 <CheckVnode>
c010a4a3: 8b 43 08                      mov eax, dword ptr [ebx + 8]
c010a4a6: 85 c0                         test eax, eax
c010a4a8: 74 13                         je 0xc010a4bd <VnodeOpWrite+0x2c>
c010a4aa: 83 7e 14 01                   cmp dword ptr [esi + 20], 1
c010a4ae: 75 0d                         jne 0xc010a4bd <VnodeOpWrite+0x2c>
c010a4b0: 89 74 24 14                   mov dword ptr [esp + 20], esi
c010a4b4: 89 5c 24 10                   mov dword ptr [esp + 16], ebx
c010a4b8: 59                            pop ecx
c010a4b9: 5b                            pop ebx
c010a4ba: 5e                            pop esi
c010a4bb: ff e0                         jmp eax
c010a4bd: b8 07 00 00 00                mov eax, 7
c010a4c2: 5a                            pop edx
c010a4c3: 5b                            pop ebx
c010a4c4: 5e                            pop esi
c010a4c5: c3                            ret

c010a4c6 <VnodeOpIoctl>:
c010a4c6: 57                            push edi
c010a4c7: 56                            push esi
c010a4c8: 53                            push ebx
c010a4c9: 8b 5c 24 10                   mov ebx, dword ptr [esp + 16]
c010a4cd: 8b 74 24 14                   mov esi, dword ptr [esp + 20]
c010a4d1: 8b 7c 24 18                   mov edi, dword ptr [esp + 24]
c010a4d5: 89 d8                         mov eax, ebx
c010a4d7: e8 aa fe ff ff                call 0xc010a386 <CheckVnode>
c010a4dc: 83 7b 0c 00                   cmp dword ptr [ebx + 12], 0
c010a4e0: 74 24                         je 0xc010a506 <VnodeOpIoctl+0x40>
c010a4e2: 50                            push eax
c010a4e3: 50                            push eax
c010a4e4: 56                            push esi
c010a4e5: 68 d5 18 11 c0                push 3222345941
c010a4ea: e8 d6 e5 ff ff                call 0xc0108ac5 <LogWriteSerial>
c010a4ef: 83 c4 10                      add esp, 16
c010a4f2: 89 7c 24 18                   mov dword ptr [esp + 24], edi
c010a4f6: 89 74 24 14                   mov dword ptr [esp + 20], esi
c010a4fa: 89 5c 24 10                   mov dword ptr [esp + 16], ebx
c010a4fe: 8b 43 0c                      mov eax, dword ptr [ebx + 12]
c010a501: 5b                            pop ebx
c010a502: 5e                            pop esi
c010a503: 5f                            pop edi
c010a504: ff e0                         jmp eax
c010a506: 83 fe 04                      cmp esi, 4
c010a509: 19 c0                         sbb eax, eax
c010a50b: 83 e0 0e                      and eax, 14
c010a50e: 83 c0 07                      add eax, 7
c010a511: 5b                            pop ebx
c010a512: 5e                            pop esi
c010a513: 5f                            pop edi
c010a514: c3                            ret

c010a515 <VnodeOpClose>:
c010a515: 8b 54 24 04                   mov edx, dword ptr [esp + 4]
c010a519: 8b 42 2c                      mov eax, dword ptr [edx + 44]
c010a51c: 85 c0                         test eax, eax
```

```
c010a56c: 89 74 24 34                  mov dword ptr [esp + 52], esi
c010a570: 89 5c 24 30                  mov dword ptr [esp + 48], ebx
c010a574: 83 c4 1c                     add esp, 28
c010a577: 5b                           pop ebx
c010a578: 5e                           pop esi
c010a579: 5f                           pop edi
c010a57a: 5d                           pop ebp
c010a57b: ff e0                        jmp eax
c010a57d: b8 07 00 00 00               mov eax, 7
c010a582: 83 c4 1c                     add esp, 28
c010a585: 5b                           pop ebx
c010a586: 5e                           pop esi
c010a587: 5f                           pop edi
c010a588: 5d                           pop ebp
c010a589: c3                           ret

c010a58a <VnodeOpTruncate>:
c010a58a: 56                           push esi
c010a58b: 53                           push ebx
c010a58c: 53                           push ebx
c010a58d: 8b 5c 24 10                  mov ebx, dword ptr [esp + 16]
c010a591: 8b 74 24 14                  mov esi, dword ptr [esp + 20]
c010a595: 89 d8                        mov eax, ebx
c010a597: e8 ea fd ff ff               call 0xc010a386 <CheckVnode>
c010a59c: 8b 43 14                     mov eax, dword ptr [ebx + 20]
c010a59f: 85 c0                        test eax, eax
c010a5a1: 74 0d                        je 0xc010a5b0 <VnodeOpTruncate+0x26>
c010a5a3: 89 74 24 14                  mov dword ptr [esp + 20], esi
c010a5a7: 89 5c 24 10                  mov dword ptr [esp + 16], ebx
c010a5ab: 59                           pop ecx
c010a5ac: 5b                           pop ebx
c010a5ad: 5e                           pop esi
c010a5ae: ff e0                        jmp eax
c010a5b0: b8 07 00 00 00               mov eax, 7
c010a5b5: 5a                           pop edx
c010a5b6: 5b                           pop ebx
c010a5b7: 5e                           pop esi
c010a5b8: c3                           ret

c010a5b9 <VnodeOpFollow>:
c010a5b9: 57                           push edi
c010a5ba: 56                           push esi
c010a5bb: 53                           push ebx
c010a5bc: 8b 5c 24 10                  mov ebx, dword ptr [esp + 16]
c010a5c0: 8b 74 24 14                  mov esi, dword ptr [esp + 20]
c010a5c4: 8b 7c 24 18                  mov edi, dword ptr [esp + 24]
c010a5c8: 89 d8                        mov eax, ebx
c010a5ca: e8 b7 fd ff ff               call 0xc010a386 <CheckVnode>
c010a5cf: 8b 43 1c                     mov eax, dword ptr [ebx + 28]
c010a5d2: 85 c0                        test eax, eax
c010a5d4: 74 11                        je 0xc010a5e7 <VnodeOpFollow+0x2e>
c010a5d6: 89 7c 24 18                  mov dword ptr [esp + 24], edi
c010a5da: 89 74 24 14                  mov dword ptr [esp + 20], esi
c010a5de: 89 5c 24 10                  mov dword ptr [esp + 16], ebx
c010a5e2: 5b                           pop ebx
c010a5e3: 5e                           pop esi
c010a5e4: 5f                           pop edi
c010a5e5: ff e0                        jmp eax
c010a5e7: b8 0e 00 00 00               mov eax, 14
c010a5ec: 5b                           pop ebx
c010a5ed: 5e                           pop esi
c010a5ee: 5f                           pop edi
c010a5ef: c3                           ret

c010a5f0 <VnodeOpDirentType>:
c010a5f0: 8b 44 24 04                  mov eax, dword ptr [esp + 4]
c010a5f4: 8b 40 58                     mov eax, dword ptr [eax + 88]
c010a5f7: c1 e8 0f                     shr eax, 15
c010a5fa: c3                           ret

c010a5fb <VnodeOpUnlink>:
```

```
c010a643: ff e0                         jmp eax
c010a645: b8 07 00 00 00                mov eax, 7
c010a64a: 83 c4 08                      add esp, 8
c010a64d: 5b                            pop ebx
c010a64e: c3                            ret

c010a64f <DereferenceVnode>:
c010a64f: 56                            push esi
c010a650: 53                            push ebx
c010a651: 51                            push ecx
c010a652: 8b 5c 24 10                   mov ebx, dword ptr [esp + 16]
c010a656: 89 d8                         mov eax, ebx
c010a658: e8 29 fd ff ff                call 0xc010a386 <CheckVnode>
c010a65d: 8d 73 30                      lea esi, [ebx + 48]
c010a660: 83 ec 0c                      sub esp, 12
c010a663: 56                            push esi
c010a664: e8 f1 c2 ff ff                call 0xc010695a <AcquireSpinlock>
c010a669: 8b 43 2c                      mov eax, dword ptr [ebx + 44]
c010a66c: 48                            dec eax
c010a66d: 89 43 2c                      mov dword ptr [ebx + 44], eax
c010a670: 83 c4 10                      add esp, 16
c010a673: 85 c0                         test eax, eax
c010a675: 75 32                         jne 0xc010a6a9 <DereferenceVnode+0x5a>
c010a677: 83 ec 0c                      sub esp, 12
c010a67a: 53                            push ebx
c010a67b: e8 95 fe ff ff                call 0xc010a515 <VnodeOpClose>
c010a680: 89 34 24                      mov dword ptr [esp], esi
c010a683: e8 22 c3 ff ff                call 0xc01069aa <ReleaseSpinlock>
c010a688: 83 c4 10                      add esp, 16
c010a68b: 83 7b 5c 00                   cmp dword ptr [ebx + 92], 0
c010a68f: 75 0c                         jne 0xc010a69d <DereferenceVnode+0x4e>
c010a691: 83 ec 0c                      sub esp, 12
c010a694: 53                            push ebx
c010a695: e8 8b ff ff ff                call 0xc010a625 <VnodeOpDelete>
c010a69a: 83 c4 10                      add esp, 16
c010a69d: 89 5c 24 10                   mov dword ptr [esp + 16], ebx
c010a6a1: 5a                            pop edx
c010a6a2: 5b                            pop ebx
c010a6a3: 5e                            pop esi
c010a6a4: e9 ca 92 ff ff                jmp 0xc0103973 <FreeHeap>
c010a6a9: 89 74 24 10                   mov dword ptr [esp + 16], esi
c010a6ad: 58                            pop eax
c010a6ae: 5b                            pop ebx
c010a6af: 5e                            pop esi
c010a6b0: e9 f5 c2 ff ff                jmp 0xc01069aa <ReleaseSpinlock>

c010a6b5 <demofs_read_inode>:
c010a6b5: 53                            push ebx
c010a6b6: 83 ec 28                      sub esp, 40
c010a6b9: 89 e3                         mov ebx, esp
c010a6bb: 50                            push eax
c010a6bc: 6a 00                         push 0
c010a6be: 8b 44 24 3c                   mov eax, dword ptr [esp + 60]
c010a6c2: c1 e0 09                      shl eax, 9
c010a6c5: 31 d2                         xor edx, edx
c010a6c7: 52                            push edx
c010a6c8: 50                            push eax
c010a6c9: 6a 00                         push 0
c010a6cb: 68 00 02 00 00                push 512
c010a6d0: ff 74 24 50                   push dword ptr [esp + 80]
c010a6d4: 53                            push ebx
c010a6d5: e8 d6 f0 ff ff                call 0xc01097b0 <CreateKernelTransfer>
c010a6da: 89 1c 24                      mov dword ptr [esp], ebx
c010a6dd: 8b 44 24 4c                   mov eax, dword ptr [esp + 76]
c010a6e1: ff 30                         push dword ptr [eax]
c010a6e3: e8 e3 fb ff ff                call 0xc010a2cb <ReadFile>
c010a6e8: 83 c4 48                      add esp, 72
c010a6eb: 5b                            pop ebx
c010a6ec: c3                            ret

c010a6ed <demofs_read_file>:
```

```
c010a743: 89 ef                         mov edi, ebp
c010a745: 0f ac fe 09                   shrd esi, edi, 9
c010a749: c1 ef 09                      shr edi, 9
c010a74c: 03 b4 24 64 02 00 00          add esi, dword ptr [esp + 612]
c010a753: c1 e6 09                      shl esi, 9
c010a756: 8b 44 24 10                   mov eax, dword ptr [esp + 16]
c010a75a: 25 ff 01 00 00                and eax, 511
c010a75f: 0f 94 44 24 18                sete byte ptr [esp + 24]
c010a764: b8 ff 01 00 00                mov eax, 511
c010a769: 39 d0                         cmp eax, edx
c010a76b: b8 00 00 00 00                mov eax, 0
c010a770: 19 c8                         sbb eax, ecx
c010a772: 0f 92 c0                      setb al
c010a775: 84 44 24 18                   test byte ptr [esp + 24], al
c010a779: 0f 84 88 00 00 00             je 0xc010a807 <demofs_read_file+0x11a>
c010a77f: 81 7c 24 0c ff 01 00 00       cmp dword ptr [esp + 12], 511
c010a787: 76 7e                         jbe 0xc010a807 <demofs_read_file+0x11a>
c010a789: 89 d0                         mov eax, edx
c010a78b: 25 ff 01 00 00                and eax, 511
c010a790: 89 44 24 18                   mov dword ptr [esp + 24], eax
c010a794: c1 f8 1f                      sar eax, 31
c010a797: 89 44 24 1c                   mov dword ptr [esp + 28], eax
c010a79b: 89 d0                         mov eax, edx
c010a79d: 89 ca                         mov edx, ecx
c010a79f: 2b 44 24 18                   sub eax, dword ptr [esp + 24]
c010a7a3: 1b 54 24 1c                   sbb edx, dword ptr [esp + 28]
c010a7a7: 89 43 04                      mov dword ptr [ebx + 4], eax
c010a7aa: 89 53 08                      mov dword ptr [ebx + 8], edx
c010a7ad: 8b 44 24 10                   mov eax, dword ptr [esp + 16]
c010a7b1: 29 c6                         sub esi, eax
c010a7b3: 89 f7                         mov edi, esi
c010a7b5: c1 ff 1f                      sar edi, 31
c010a7b8: 8b 44 24 10                   mov eax, dword ptr [esp + 16]
c010a7bc: 8b 54 24 14                   mov edx, dword ptr [esp + 20]
c010a7c0: 01 f0                         add eax, esi
c010a7c2: 11 fa                         adc edx, edi
c010a7c4: 89 43 0c                      mov dword ptr [ebx + 12], eax
c010a7c7: 89 53 10                      mov dword ptr [ebx + 16], edx
c010a7ca: 52                            push edx
c010a7cb: 52                            push edx
c010a7cc: 53                            push ebx
c010a7cd: 8b 84 24 6c 02 00 00          mov eax, dword ptr [esp + 620]
c010a7d4: ff 30                         push dword ptr [eax]
c010a7d6: e8 f0 fa ff ff                call 0xc010a2cb <ReadFile>
c010a7db: 83 c4 10                      add esp, 16
c010a7de: 85 c0                         test eax, eax
c010a7e0: 0f 85 c8 00 00 00             jne 0xc010a8ae <demofs_read_file+0x1c1>
c010a7e6: 29 73 0c                      sub dword ptr [ebx + 12], esi
c010a7e9: 19 7b 10                      sbb dword ptr [ebx + 16], edi
c010a7ec: 8b 44 24 18                   mov eax, dword ptr [esp + 24]
c010a7f0: 8b 54 24 1c                   mov edx, dword ptr [esp + 28]
c010a7f4: 89 43 04                      mov dword ptr [ebx + 4], eax
c010a7f7: 89 53 08                      mov dword ptr [ebx + 8], edx
c010a7fa: 81 6c 24 0c 00 02 00 00       sub dword ptr [esp + 12], 512
c010a802: e9 19 ff ff ff                jmp 0xc010a720 <demofs_read_file+0x33>
c010a807: 8d 6c 24 20                   lea ebp, [esp + 32]
c010a80b: 50                            push eax
c010a80c: 6a 00                         push 0
c010a80e: 89 f7                         mov edi, esi
c010a810: c1 ff 1f                      sar edi, 31
c010a813: 57                            push edi
c010a814: 56                            push esi
c010a815: 6a 00                         push 0
c010a817: 68 00 02 00 00                push 512
c010a81c: 8d 44 24 58                   lea eax, [esp + 88]
c010a820: 50                            push eax
c010a821: 55                            push ebp
c010a822: e8 89 ef ff ff                call 0xc01097b0 <CreateKernelTransfer>
c010a827: 89 2c 24                      mov dword ptr [esp], ebp
c010a82a: 8b 84 24 7c 02 00 00          mov eax, dword ptr [esp + 636]
c010a831: ff 30                         push dword ptr [eax]
```

```
c010a884: 19 f9                         sbb ecx, edi
c010a886: 73 04                         jae 0xc010a88c <demofs_read_file+0x19f>
c010a888: 89 c6                         mov esi, eax
c010a88a: 89 d7                         mov edi, edx
c010a88c: 57                            push edi
c010a88d: 56                            push esi
c010a88e: 53                            push ebx
c010a88f: 8b 44 24 1c                   mov eax, dword ptr [esp + 28]
c010a893: 25 ff 01 00 00                and eax, 511
c010a898: 8d 44 04 4c                   lea eax, [esp + eax + 76]
c010a89c: 50                            push eax
c010a89d: e8 51 ec ff ff                call 0xc01094f3 <PerformTransfer>
c010a8a2: 29 74 24 1c                   sub dword ptr [esp + 28], esi
c010a8a6: 83 c4 10                      add esp, 16
c010a8a9: e9 72 fe ff ff                jmp 0xc010a720 <demofs_read_file+0x33>
c010a8ae: 81 c4 4c 02 00 00             add esp, 588
c010a8b4: 5b                            pop ebx
c010a8b5: 5e                            pop esi
c010a8b6: 5f                            pop edi
c010a8b7: 5d                            pop ebp
c010a8b8: c3                            ret

c010a8b9 <demofs_follow>:
c010a8b9: 57                            push edi
c010a8ba: 56                            push esi
c010a8bb: 53                            push ebx
c010a8bc: 81 ec 0c 02 00 00             sub esp, 524
c010a8c2: 8b 9c 24 20 02 00 00          mov ebx, dword ptr [esp + 544]
c010a8c9: 8b b4 24 28 02 00 00          mov esi, dword ptr [esp + 552]
c010a8d0: 56                            push esi
c010a8d1: e8 01 69 ff ff                call 0xc01011d7 <strlen>
c010a8d6: 89 c2                         mov edx, eax
c010a8d8: 83 c4 10                      add esp, 16
c010a8db: b8 0d 00 00 00                mov eax, 13
c010a8e0: 83 fa 18                      cmp edx, 24
c010a8e3: 0f 87 0a 01 00 00             ja 0xc010a9f3 <demofs_follow+0x13a>
c010a8e9: b8 0e 00 00 00                mov eax, 14
c010a8ee: 85 db                         test ebx, ebx
c010a8f0: 0f 89 fd 00 00 00             jns 0xc010a9f3 <demofs_follow+0x13a>
c010a8f6: 52                            push edx
c010a8f7: 8d 7c 24 04                   lea edi, [esp + 4]
c010a8fb: 57                            push edi
c010a8fc: 53                            push ebx
c010a8fd: ff b4 24 1c 02 00 00          push dword ptr [esp + 540]
c010a904: e8 ac fd ff ff                call 0xc010a6b5 <demofs_read_inode>
c010a909: 89 fc                         mov esp, edi
c010a90b: 85 c0                         test eax, eax
c010a90d: 0f 85 e0 00 00 00             jne 0xc010a9f3 <demofs_follow+0x13a>
c010a913: 80 3c 24 fd                   cmp byte ptr [esp], -3
c010a917: 77 0a                         ja 0xc010a923 <demofs_follow+0x6a>
c010a919: b8 0a 00 00 00                mov eax, 10
c010a91e: e9 d0 00 00 00                jmp 0xc010a9f3 <demofs_follow+0x13a>
c010a923: bb 20 00 00 00                mov ebx, 32
c010a928: 80 3c 1f 00                   cmp byte ptr [edi + ebx], 0
c010a92c: 75 0a                         jne 0xc010a938 <demofs_follow+0x7f>
c010a92e: b8 09 00 00 00                mov eax, 9
c010a933: e9 bb 00 00 00                jmp 0xc010a9f3 <demofs_follow+0x13a>
c010a938: 50                            push eax
c010a939: 6a 18                         push 24
c010a93b: 8d 04 1f                      lea eax, [edi + ebx]
c010a93e: 50                            push eax
c010a93f: 56                            push esi
c010a940: e8 f1 68 ff ff                call 0xc0101236 <strncmp>
c010a945: 83 c4 10                      add esp, 16
c010a948: 85 c0                         test eax, eax
c010a94a: 75 61                         jne 0xc010a9ad <demofs_follow+0xf4>
c010a94c: 0f b6 74 1c 1c                movzx esi, byte ptr [esp + ebx + 28]
c010a951: 0f b6 54 1c 1d                movzx edx, byte ptr [esp + ebx + 29]
c010a956: c1 e2 08                      shl edx, 8
c010a959: 0f b6 4c 1c 1e                movzx ecx, byte ptr [esp + ebx + 30]
c010a95e: c1 e1 10                      shl ecx, 16
```

```
c010a9c9: 0f 85 4a ff ff ff           jne 0xc010a919 <demofs_follow+0x60>
c010a9cf: 0f b6 54 24 01              movzx edx, byte ptr [esp + 1]
c010a9d4: 0f b6 5c 24 02              movzx ebx, byte ptr [esp + 2]
c010a9d9: c1 e3 08                    shl ebx, 8
c010a9dc: 0f b6 44 24 03              movzx eax, byte ptr [esp + 3]
c010a9e1: c1 e0 10                    shl eax, 16
c010a9e4: 09 c3                       or ebx, eax
c010a9e6: 09 d3                       or ebx, edx
c010a9e8: 81 cb 00 00 00 80           or ebx, 2147483648
c010a9ee: e9 03 ff ff ff              jmp 0xc010a8f6 <demofs_follow+0x3d>
c010a9f3: 81 c4 00 02 00 00           add esp, 512
c010a9f9: 5b                          pop ebx
c010a9fa: 5e                          pop esi
c010a9fb: 5f                          pop edi
c010a9fc: c3                          ret

c010a9fd <demofs_read_directory_entry>:
c010a9fd: 55                          push ebp
c010a9fe: 57                          push edi
c010a9ff: 56                          push esi
c010aa00: 53                          push ebx
c010aa01: 81 ec 5c 03 00 00           sub esp, 860
c010aa07: 8b bc 24 74 03 00 00        mov edi, dword ptr [esp + 884]
c010aa0e: b9 0e 00 00 00              mov ecx, 14
c010aa13: 85 ff                       test edi, edi
c010aa15: 0f 89 32 02 00 00           jns 0xc010ac4d <demofs_read_directory_entry+0
c010aa1b: 8d 44 24 18                 lea eax, [esp + 24]
c010aa1f: 83 ec 0c                    sub esp, 12
c010aa22: 50                          push eax
c010aa23: 6a 00                       push 0
c010aa25: 68 0c 01 00 00              push 268
c010aa2a: 8b 84 24 90 03 00 00        mov eax, dword ptr [esp + 912]
c010aa31: ff 70 10                    push dword ptr [eax + 16]
c010aa34: ff 70 0c                    push dword ptr [eax + 12]
c010aa37: e8 3c 46 00 00              call 0xc010f078 <__udivmoddi4>
c010aa3c: 83 c4 20                    add esp, 32
c010aa3f: 8b 54 24 18                 mov edx, dword ptr [esp + 24]
c010aa43: 83 7c 24 1c 00              cmp dword ptr [esp + 28], 0
c010aa48: 0f 85 f3 01 00 00           jne 0xc010ac41 <demofs_read_directory_entry+0
c010aa4e: 85 d2                       test edx, edx
c010aa50: 0f 85 eb 01 00 00           jne 0xc010ac41 <demofs_read_directory_entry+0
c010aa56: 85 c0                       test eax, eax
c010aa58: 75 63                       jne 0xc010aabd <demofs_read_directory_entry+0
c010aa5a: 50                          push eax
c010aa5b: 50                          push eax
c010aa5c: 68 6f 17 11 c0              push 3222345583
c010aa61: 8d 5c 24 50                 lea ebx, [esp + 80]
c010aa65: 8d 44 24 54                 lea eax, [esp + 84]
c010aa69: 50                          push eax
c010aa6a: e8 50 67 ff ff              call 0xc01011bf <strcpy>
c010aa6f: c6 84 24 58 01 00 00 01     mov byte ptr [esp + 344], 1
c010aa77: 81 e7 ff ff ff 7f           and edi, 2147483647
c010aa7d: 89 7c 24 54                 mov dword ptr [esp + 84], edi
c010aa81: 8b 84 24 80 03 00 00        mov eax, dword ptr [esp + 896]
c010aa88: 8b 00                       mov eax, dword ptr [eax]
c010aa8a: 8b 40 30                    mov eax, dword ptr [eax + 48]
c010aa8d: 8b 40 4c                    mov eax, dword ptr [eax + 76]
c010aa90: 89 84 24 5c 01 00 00        mov dword ptr [esp + 348], eax
c010aa97: c6 84 24 59 01 00 00 05     mov byte ptr [esp + 345], 5
c010aa9f: 6a 00                       push 0
c010aaa1: 68 0c 01 00 00              push 268
c010aaa6: ff b4 24 90 03 00 00        push dword ptr [esp + 912]
c010aaad: 53                          push ebx
c010aaae: e8 40 ea ff ff              call 0xc01094f3 <PerformTransfer>
c010aab3: 89 c1                       mov ecx, eax
c010aab5: 83 c4 20                    add esp, 32
c010aab8: e9 90 01 00 00              jmp 0xc010ac4d <demofs_read_directory_entry+0
c010aabd: 48                          dec eax
c010aabe: 89 44 24 0c                 mov dword ptr [esp + 12], eax
c010aac2: b9 0f 00 00 00              mov ecx, 15
c010aac7: 99                          cdq
```

```
c010ab34: c1 e2 10                      shl edx, 16
c010ab37: 09 d7                         or edi, edx
c010ab39: 09 c7                         or edi, eax
c010ab3b: 45                            inc ebp
c010ab3c: eb 92                         jmp 0xc010aad0 <demofs_read_directory_entry+0
c010ab3e: 56                            push esi
c010ab3f: 53                            push ebx
c010ab40: 57                            push edi
c010ab41: ff b4 24 7c 03 00 00          push dword ptr [esp + 892]
c010ab48: e8 68 fb ff ff                call 0xc010a6b5 <demofs_read_inode>
c010ab4d: 89 c1                         mov ecx, eax
c010ab4f: 83 c4 10                      add esp, 16
c010ab52: 85 c0                         test eax, eax
c010ab54: 0f 85 f3 00 00 00             jne 0xc010ac4d <demofs_read_directory_entry+0
c010ab5a: bf 0f 00 00 00                mov edi, 15
c010ab5f: 8b 44 24 0c                   mov eax, dword ptr [esp + 12]
c010ab63: 99                            cdq
c010ab64: f7 ff                         idiv edi
c010ab66: 42                            inc edx
c010ab67: 89 d6                         mov esi, edx
c010ab69: 89 54 24 14                   mov dword ptr [esp + 20], edx
c010ab6d: c1 e6 05                      shl esi, 5
c010ab70: 80 bc 34 50 01 00 00 00       cmp byte ptr [esp + esi + 336], 0
c010ab78: 0f 84 cf 00 00 00             je 0xc010ac4d <demofs_read_directory_entry+0x
c010ab7e: 8d 6c 24 2a                   lea ebp, [esp + 42]
c010ab82: b9 1a 00 00 00                mov ecx, 26
c010ab87: 31 c0                         xor eax, eax
c010ab89: 89 ef                         mov edi, ebp
c010ab8b: f3 aa                         rep  stosb byte ptr es:[edi], al
c010ab8d: 50                            push eax
c010ab8e: 6a 18                         push 24
c010ab90: 01 f3                         add ebx, esi
c010ab92: 53                            push ebx
c010ab93: 55                            push ebp
c010ab94: e8 1f 67 ff ff                call 0xc01012b8 <strncpy>
c010ab99: 5a                            pop edx
c010ab9a: 59                            pop ecx
c010ab9b: 55                            push ebp
c010ab9c: 8d 7c 24 50                   lea edi, [esp + 80]
c010aba0: 8d 44 24 54                   lea eax, [esp + 84]
c010aba4: 50                            push eax
c010aba5: e8 15 66 ff ff                call 0xc01011bf <strcpy>
c010abaa: 89 2c 24                      mov dword ptr [esp], ebp
c010abad: e8 25 66 ff ff                call 0xc01011d7 <strlen>
c010abb2: 88 84 24 58 01 00 00          mov byte ptr [esp + 344], al
c010abb9: 0f b6 8c 34 7c 01 00 00       movzx ecx, byte ptr [esp + esi + 380]
c010abc1: 0f b6 9c 34 7d 01 00 00       movzx ebx, byte ptr [esp + esi + 381]
c010abc9: c1 e3 08                      shl ebx, 8
c010abcc: 0f b6 84 34 7e 01 00 00       movzx eax, byte ptr [esp + esi + 382]
c010abd4: c1 e0 10                      shl eax, 16
c010abd7: 09 c3                         or ebx, eax
c010abd9: 09 cb                         or ebx, ecx
c010abdb: 89 2c 24                      mov dword ptr [esp], ebp
c010abde: ff 74 24 20                   push dword ptr [esp + 32]
c010abe2: 8b 54 24 28                   mov edx, dword ptr [esp + 40]
c010abe6: 52                            push edx
c010abe7: ff 74 24 24                   push dword ptr [esp + 36]
c010abeb: 68 ed 18 11 c0                push 3222345965
c010abf0: e8 d0 de ff ff                call 0xc0108ac5 <LogWriteSerial>
c010abf5: 89 5c 24 64                   mov dword ptr [esp + 100], ebx
c010abf9: 8b 84 24 90 03 00 00          mov eax, dword ptr [esp + 912]
c010ac00: 8b 00                         mov eax, dword ptr [eax]
c010ac02: 8b 40 30                      mov eax, dword ptr [eax + 48]
c010ac05: 8b 40 4c                      mov eax, dword ptr [eax + 76]
c010ac08: 89 84 24 6c 01 00 00          mov dword ptr [esp + 364], eax
c010ac0f: 8a 84 34 8f 01 00 00          mov al, byte ptr [esp + esi + 399]
c010ac16: 83 e0 01                      and eax, 1
c010ac19: 83 c0 04                      add eax, 4
c010ac1c: 88 84 24 69 01 00 00          mov byte ptr [esp + 361], al
c010ac23: 83 c4 20                      add esp, 32
c010ac26: 6a 00                         push 0
```

```
c010ac70: c3                            ret

c010ac71 <Write>:
c010ac71: b8 11 00 00 00                mov eax, 17
c010ac76: c3                            ret

c010ac77 <Close>:
c010ac77: 83 ec 18                      sub esp, 24
c010ac7a: 8b 44 24 1c                   mov eax, dword ptr [esp + 28]
c010ac7e: ff 70 28                      push dword ptr [eax + 40]
c010ac81: e8 ed 8c ff ff                call 0xc0103973 <FreeHeap>
c010ac86: 31 c0                         xor eax, eax
c010ac88: 83 c4 1c                      add esp, 28
c010ac8b: c3                            ret

c010ac8c <CreateDemoFsVnode>:
c010ac8c: 57                            push edi
c010ac8d: 56                            push esi
c010ac8e: 53                            push ebx
c010ac8f: 83 ec 50                      sub esp, 80
c010ac92: 89 c3                         mov ebx, eax
c010ac94: 89 d6                         mov esi, edx
c010ac96: 8d 7c 24 1c                   lea edi, [esp + 28]
c010ac9a: b9 0c 00 00 00                mov ecx, 12
c010ac9f: 31 c0                         xor eax, eax
c010aca1: f3 ab                         rep  stosd dword ptr es:[edi], eax
c010aca3: e8 24 ee ff ff                call 0xc0109acc <NextDevId>
c010aca8: 89 44 24 08                   mov dword ptr [esp + 8], eax
c010acac: 99                            cdq
c010acad: 89 54 24 0c                   mov dword ptr [esp + 12], edx
c010acb1: 89 d8                         mov eax, ebx
c010acb3: 25 ff ff ff 7f                and eax, 2147483647
c010acb8: 89 44 24 10                   mov dword ptr [esp + 16], eax
c010acbc: 89 d8                         mov eax, ebx
c010acbe: c1 f8 1f                      sar eax, 31
c010acc1: 25 00 80 00 00                and eax, 32768
c010acc6: 05 ff 01 02 00                add eax, 131583
c010accb: 89 44 24 14                   mov dword ptr [esp + 20], eax
c010accf: c7 44 24 18 01 00 00 00       mov dword ptr [esp + 24], 1
c010acd7: 89 74 24 2c                   mov dword ptr [esp + 44], esi
c010acdb: c7 44 24 4c 00 02 00 00       mov dword ptr [esp + 76], 512
c010ace3: 83 ec 48                      sub esp, 72
c010ace6: 8d 74 24 50                   lea esi, [esp + 80]
c010acea: b9 12 00 00 00                mov ecx, 18
c010acef: 89 e7                         mov edi, esp
c010acf1: f3 a5                         rep  movsd dword ptr es:[edi], dword ptr [esi
c010acf3: 83 ec 28                      sub esp, 40
c010acf6: be 60 03 11 c0                mov esi, 3222340448
c010acfb: b9 0a 00 00 00                mov ecx, 10
c010ad00: 89 e7                         mov edi, esp
c010ad02: f3 a5                         rep  movsd dword ptr es:[edi], dword ptr [esi
c010ad04: e8 aa f6 ff ff                call 0xc010a3b3 <CreateVnode>
c010ad09: 81 c4 c0 00 00 00             add esp, 192
c010ad0f: 5b                            pop ebx
c010ad10: 5e                            pop esi
c010ad11: 5f                            pop edi
c010ad12: c3                            ret

c010ad13 <Follow>:
c010ad13: 55                            push ebp
c010ad14: 57                            push edi
c010ad15: 56                            push esi
c010ad16: 53                            push ebx
c010ad17: 83 ec 1c                      sub esp, 28
c010ad1a: 8b 44 24 30                   mov eax, dword ptr [esp + 48]
c010ad1e: 8b 78 28                      mov edi, dword ptr [eax + 40]
c010ad21: bb 0e 00 00 00                mov ebx, 14
c010ad26: 80 7f 10 00                   cmp byte ptr [edi + 16], 0
c010ad2a: 74 6d                         je 0xc010ad99 <Follow+0x86>
c010ad2c: 83 ec 0c                      sub esp, 12
c010ad2f: 8d 44 24 18                   lea eax, [esp + 24]
```

```
c010ad89: 80 60 10 01                and byte ptr [eax + 16], 1
c010ad8d: 89 46 28                   mov dword ptr [esi + 40], eax
c010ad90: 8b 44 24 44                mov eax, dword ptr [esp + 68]
c010ad94: 89 30                      mov dword ptr [eax], esi
c010ad96: 83 c4 10                   add esp, 16
c010ad99: 89 d8                      mov eax, ebx
c010ad9b: 83 c4 1c                   add esp, 28
c010ad9e: 5b                         pop ebx
c010ad9f: 5e                         pop esi
c010ada0: 5f                         pop edi
c010ada1: 5d                         pop ebp
c010ada2: c3                         ret

c010ada3 <Read>:
c010ada3: 53                         push ebx
c010ada4: 83 ec 08                   sub esp, 8
c010ada7: 8b 5c 24 14                mov ebx, dword ptr [esp + 20]
c010adab: 8b 44 24 10                mov eax, dword ptr [esp + 16]
c010adaf: 8b 40 28                   mov eax, dword ptr [eax + 40]
c010adb2: 8b 08                      mov ecx, dword ptr [eax]
c010adb4: 80 78 10 00                cmp byte ptr [eax + 16], 0
c010adb8: 8d 50 04                   lea edx, [eax + 4]
c010adbb: 74 0b                      je 0xc010adc8 <Read+0x25>
c010adbd: 50                         push eax
c010adbe: 53                         push ebx
c010adbf: 51                         push ecx
c010adc0: 52                         push edx
c010adc1: e8 37 fc ff ff             call 0xc010a9fd <demofs_read_directory_entry>
c010adc6: eb 0b                      jmp 0xc010add3 <Read+0x30>
c010adc8: 53                         push ebx
c010adc9: ff 70 0c                   push dword ptr [eax + 12]
c010adcc: 51                         push ecx
c010adcd: 52                         push edx
c010adce: e8 1a f9 ff ff             call 0xc010a6ed <demofs_read_file>
c010add3: 83 c4 10                   add esp, 16
c010add6: 83 c4 08                   add esp, 8
c010add9: 5b                         pop ebx
c010adda: c3                         ret

c010addb <DemofsMountCreator>:
c010addb: 55                         push ebp
c010addc: 57                         push edi
c010addd: 56                         push esi
c010adde: 53                         push ebx
c010addf: 83 ec 38                   sub esp, 56
c010ade2: 8b 74 24 4c                mov esi, dword ptr [esp + 76]
c010ade6: 8b 46 30                   mov eax, dword ptr [esi + 48]
c010ade9: 8b a8 90 00 00 00          mov ebp, dword ptr [eax + 144]
c010adef: 55                         push ebp
c010adf0: e8 5a 8b ff ff             call 0xc010394f <AllocHeap>
c010adf5: 89 c3                      mov ebx, eax
c010adf7: 8d 7c 24 10                lea edi, [esp + 16]
c010adfb: 83 c4 0c                   add esp, 12
c010adfe: 6a 00                      push 0
c010ae00: 8d 04 ed 00 00 00 00       lea eax, [8*ebp]
c010ae07: 31 d2                      xor edx, edx
c010ae09: 52                         push edx
c010ae0a: 50                         push eax
c010ae0b: 31 d2                      xor edx, edx
c010ae0d: 52                         push edx
c010ae0e: 55                         push ebp
c010ae0f: 53                         push ebx
c010ae10: 57                         push edi
c010ae11: e8 9a e9 ff ff             call 0xc01097b0 <CreateKernelTransfer>
c010ae16: 89 3c 24                   mov dword ptr [esp], edi
c010ae19: 56                         push esi
c010ae1a: e8 ac f4 ff ff             call 0xc010a2cb <ReadFile>
c010ae1f: 83 c4 20                   add esp, 32
c010ae22: 85 c0                      test eax, eax
c010ae24: 74 13                      je 0xc010ae39 <DemofsMountCreator+0x5e>
c010ae26: 83 ec 0c                   sub esp, 12
```

```
c010ae89: 31 d2                         xor edx, edx
c010ae8b: 89 50 0c                      mov dword ptr [eax + 12], edx
c010ae8e: c6 40 10 01                   mov byte ptr [eax + 16], 1
c010ae92: 89 43 28                      mov dword ptr [ebx + 40], eax
c010ae95: 31 c9                         xor ecx, ecx
c010ae97: 89 0c 24                      mov dword ptr [esp], ecx
c010ae9a: 6a 01                         push 1
c010ae9c: 6a 00                         push 0
c010ae9e: 6a 00                         push 0
c010aea0: 53                            push ebx
c010aea1: e8 a7 e4 ff ff                call 0xc010934d <CreateFile>
c010aea6: 8b 54 24 64                   mov edx, dword ptr [esp + 100]
c010aeaa: 89 02                         mov dword ptr [edx], eax
c010aeac: 83 c4 20                      add esp, 32
c010aeaf: 89 f8                         mov eax, edi
c010aeb1: 83 c4 2c                      add esp, 44
c010aeb4: 5b                            pop ebx
c010aeb5: 5e                            pop esi
c010aeb6: 5f                            pop edi
c010aeb7: 5d                            pop ebp
c010aeb8: c3                            ret

c010aeb9 <foo>:
c010aeb9: 83 ec 18                      sub esp, 24
c010aebc: 68 21 19 11 c0                push 3222346017
c010aec1: e8 ff db ff ff                call 0xc0108ac5 <LogWriteSerial>
c010aec6: 83 c4 1c                      add esp, 28
c010aec9: c3                            ret

c010aeca <ArchCallGlobalConstructors>:
c010aeca: 53                            push ebx
c010aecb: 83 ec 08                      sub esp, 8
c010aece: bb 08 f2 10 c0                mov ebx, 3222336008
c010aed3: 81 fb 0c f2 10 c0             cmp ebx, 3222336012
c010aed9: 74 25                         je 0xc010af00 <ArchCallGlobalConstructors+0x3
c010aedb: 50                            push eax
c010aedc: 50                            push eax
c010aedd: 53                            push ebx
c010aede: 68 3c 19 11 c0                push 3222346044
c010aee3: e8 dd db ff ff                call 0xc0108ac5 <LogWriteSerial>
c010aee8: 5a                            pop edx
c010aee9: 59                            pop ecx
c010aeea: ff 33                         push dword ptr [ebx]
c010aeec: 68 50 19 11 c0                push 3222346064
c010aef1: e8 cf db ff ff                call 0xc0108ac5 <LogWriteSerial>
c010aef6: ff 13                         call dword ptr [ebx]
c010aef8: 83 c3 04                      add ebx, 4
c010aefb: 83 c4 10                      add esp, 16
c010aefe: eb d3                         jmp 0xc010aed3 <ArchCallGlobalConstructors+0x
c010af00: 83 ec 0c                      sub esp, 12
c010af03: 68 62 19 11 c0                push 3222346082
c010af08: e8 b8 db ff ff                call 0xc0108ac5 <LogWriteSerial>
c010af0d: 83 c4 18                      add esp, 24
c010af10: 5b                            pop ebx
c010af11: c3                            ret

c010af12 <ArchInitBootstrapCpu>:
c010af12: 83 ec 0c                      sub esp, 12
c010af15: e8 b0 00 00 00                call 0xc010afca <x86InitGdt>
c010af1a: e8 4f 01 00 00                call 0xc010b06e <x86InitIdt>
c010af1f: e8 63 03 00 00                call 0xc010b287 <x86InitTss>
c010af24: e8 6a 16 00 00                call 0xc010c593 <InitPic>
c010af29: 83 ec 0c                      sub esp, 12
c010af2c: 6a 32                         push 50
c010af2e: e8 b7 16 00 00                call 0xc010c5ea <InitPit>
c010af33: fb                            sti
c010af34: e8 e7 02 00 00                call 0xc010b220 <x86MakeReadyForIrqs>
c010af39: 83 c4 1c                      add esp, 28
c010af3c: e9 27 04 00 00                jmp 0xc010b368 <InitCmos>

c010af41 <ArchSetPowerState>:
```

```
c010af96: b8 34 00 00 00                mov eax, 52
c010af9b: ba 00 06 00 00                mov edx, 1536
c010afa0: 66 ef                         out dx, ax
c010afa2: eb 16                         jmp 0xc010afba <ArchSetPowerState+0x79>
c010afa4: 83 ec 0c                      sub esp, 12
c010afa7: 68 94 19 11 c0                push 3222346132
c010afac: e8 57 d5 ff ff                call 0xc0108508 <GetSymbolAddress>
c010afb1: 83 c4 10                      add esp, 16
c010afb4: 85 c0                         test eax, eax
c010afb6: 74 02                         je 0xc010afba <ArchSetPowerState+0x79>
c010afb8: ff d0                         call eax
c010afba: e8 f4 35 00 00                call 0xc010e5b3 <ArchStallProcessor>
c010afbf: eb f9                         jmp 0xc010afba <ArchSetPowerState+0x79>
c010afc1: b8 07 00 00 00                mov eax, 7
c010afc6: 83 c4 0c                      add esp, 12
c010afc9: c3                            ret

c010afca <x86InitGdt>:
c010afca: 83 ec 18                      sub esp, 24
c010afcd: 0f 21 d8                      mov eax, dr3
c010afd0: c1 e0 06                      shl eax, 6
c010afd3: 8b 80 c8 40 11 c0             mov eax, dword ptr [eax - 1072611128]
c010afd9: 31 d2                         xor edx, edx
c010afdb: 89 50 04                      mov dword ptr [eax + 4], edx
c010afde: 89 50 08                      mov dword ptr [eax + 8], edx
c010afe1: c7 40 0c ff ff 00 00          mov dword ptr [eax + 12], 65535
c010afe8: c7 40 10 00 9a cf 00          mov dword ptr [eax + 16], 13605376
c010afef: c7 40 14 ff ff 00 00          mov dword ptr [eax + 20], 65535
c010aff6: c7 40 18 00 92 cf 00          mov dword ptr [eax + 24], 13603328
c010affd: c7 40 1c ff ff 00 00          mov dword ptr [eax + 28], 65535
c010b004: c7 40 20 00 fa cf 00          mov dword ptr [eax + 32], 13629952
c010b00b: c7 40 24 ff ff 00 00          mov dword ptr [eax + 36], 65535
c010b012: c7 40 28 00 f2 cf 00          mov dword ptr [eax + 40], 13627904
c010b019: 66 c7 80 84 08 00 00 7f 00    mov word ptr [eax + 2180], 127
c010b022: 8d 50 04                      lea edx, [eax + 4]
c010b025: 89 90 86 08 00 00             mov dword ptr [eax + 2182], edx
c010b02b: 05 84 08 00 00                add eax, 2180
c010b030: 50                            push eax
c010b031: e8 1a 35 00 00                call 0xc010e550 <x86LoadGdt>
c010b036: 83 c4 1c                      add esp, 28
c010b039: c3                            ret

c010b03a <x86AddTssToGdt>:
c010b03a: 8b 54 24 04                   mov edx, dword ptr [esp + 4]
c010b03e: 0f 21 d8                      mov eax, dr3
c010b041: c1 e0 06                      shl eax, 6
c010b044: 8b 80 c8 40 11 c0             mov eax, dword ptr [eax - 1072611128]
c010b04a: 66 c7 40 2c 68 00             mov word ptr [eax + 44], 104
c010b050: 66 89 50 2e                   mov word ptr [eax + 46], dx
c010b054: 89 d1                         mov ecx, edx
c010b056: c1 e9 10                      shr ecx, 16
c010b059: 88 48 30                      mov byte ptr [eax + 48], cl
c010b05c: 66 c7 40 31 89 00             mov word ptr [eax + 49], 137
c010b062: c1 ea 18                      shr edx, 24
c010b065: 88 50 33                      mov byte ptr [eax + 51], dl
c010b068: b8 28 00 00 00                mov eax, 40
c010b06d: c3                            ret

c010b06e <x86InitIdt>:
c010b06e: 56                            push esi
c010b06f: 53                            push ebx
c010b070: 50                            push eax
c010b071: 0f 21 d8                      mov eax, dr3
c010b074: c1 e0 06                      shl eax, 6
c010b077: 8b 90 c8 40 11 c0             mov edx, dword ptr [eax - 1072611128]
c010b07d: 31 c9                         xor ecx, ecx
c010b07f: b8 8e 00 00 00                mov eax, 142
c010b084: 8b 34 8d 30 31 11 c0          mov esi, dword ptr [4*ecx - 1072615120]
c010b08b: 0f 21 db                      mov ebx, dr3
c010b08e: c1 e3 06                      shl ebx, 6
c010b091: 8b 9b c8 40 11 c0             mov ebx, dword ptr [ebx - 1072611128]
```

```
c010b107 <x86HandleInterrupt>:
c010b107: 56                            push esi
c010b108: 53                            push ebx
c010b109: 50                            push eax
c010b10a: 8b 5c 24 10                   mov ebx, dword ptr [esp + 16]
c010b10e: 8b 43 30                      mov eax, dword ptr [ebx + 48]
c010b111: 8d 50 e0                      lea edx, [eax - 32]
c010b114: 83 fa 0f                      cmp edx, 15
c010b117: 77 18                         ja 0xc010b131 <x86HandleInterrupt+0x2a>
c010b119: ba 28 00 00 00                mov edx, 40
c010b11e: 83 f8 20                      cmp eax, 32
c010b121: 74 03                         je 0xc010b126 <x86HandleInterrupt+0x1f>
c010b123: 8d 50 e4                      lea edx, [eax - 28]
c010b126: 56                            push esi
c010b127: 53                            push ebx
c010b128: 52                            push edx
c010b129: 50                            push eax
c010b12a: e8 24 81 ff ff                call 0xc0103253 <RespondToIrq>
c010b12f: eb 49                         jmp 0xc010b17a <x86HandleInterrupt+0x73>
c010b131: 83 f8 0e                      cmp eax, 14
c010b134: 75 49                         jne 0xc010b17f <x86HandleInterrupt+0x78>
c010b136: 8b 43 34                      mov eax, dword ptr [ebx + 52]
c010b139: 89 c2                         mov edx, eax
c010b13b: 83 e2 01                      and edx, 1
c010b13e: a8 02                         test al, 2
c010b140: 74 03                         je 0xc010b145 <x86HandleInterrupt+0x3e>
c010b142: 83 ca 02                      or edx, 2
c010b145: 89 d6                         mov esi, edx
c010b147: 83 ce 04                      or esi, 4
c010b14a: a8 04                         test al, 4
c010b14c: 75 02                         jne 0xc010b150 <x86HandleInterrupt+0x49>
c010b14e: 89 d6                         mov esi, edx
c010b150: a8 10                         test al, 16
c010b152: 74 03                         je 0xc010b157 <x86HandleInterrupt+0x50>
c010b154: 83 ce 08                      or esi, 8
c010b157: 8b 5b 38                      mov ebx, dword ptr [ebx + 56]
c010b15a: e8 11 35 00 00                call 0xc010e670 <x86GetCr2>
c010b15f: 56                            push esi
c010b160: 53                            push ebx
c010b161: 50                            push eax
c010b162: 68 a0 19 11 c0                push 3222346144
c010b167: e8 59 d9 ff ff                call 0xc0108ac5 <LogWriteSerial>
c010b16c: e8 ff 34 00 00                call 0xc010e670 <x86GetCr2>
c010b171: 5a                            pop edx
c010b172: 59                            pop ecx
c010b173: 56                            push esi
c010b174: 50                            push eax
c010b175: e8 65 a8 ff ff                call 0xc01059df <HandleVirtFault>
c010b17a: 83 c4 10                      add esp, 16
c010b17d: eb 4c                         jmp 0xc010b1cb <x86HandleInterrupt+0xc4>
c010b17f: 83 f8 02                      cmp eax, 2
c010b182: 75 08                         jne 0xc010b18c <x86HandleInterrupt+0x85>
c010b184: 5b                            pop ebx
c010b185: 5b                            pop ebx
c010b186: 5e                            pop esi
c010b187: e9 b8 00 00 00                jmp 0xc010b244 <HandleNmi>
c010b18c: 83 f8 60                      cmp eax, 96
c010b18f: 75 21                         jne 0xc010b1b2 <x86HandleInterrupt+0xab>
c010b191: 51                            push ecx
c010b192: 51                            push ecx
c010b193: ff 73 10                      push dword ptr [ebx + 16]
c010b196: ff 73 14                      push dword ptr [ebx + 20]
c010b199: ff 73 24                      push dword ptr [ebx + 36]
c010b19c: ff 73 28                      push dword ptr [ebx + 40]
c010b19f: ff 73 20                      push dword ptr [ebx + 32]
c010b1a2: ff 73 2c                      push dword ptr [ebx + 44]
c010b1a5: e8 3e b8 ff ff                call 0xc01069e8 <HandleSystemCall>
c010b1aa: 89 43 2c                      mov dword ptr [ebx + 44], eax
c010b1ad: 83 c4 20                      add esp, 32
c010b1b0: eb 19                         jmp 0xc010b1cb <x86HandleInterrupt+0xc4>
c010b1b2: 52                            push edx
```

```
c010b1fc: d3 e0                         shl eax, cl
c010b1fe: f7 d8                         neg eax
c010b200: 25 fb ff 00 00                and eax, 65531
c010b205: 50                            push eax
c010b206: eb 05                         jmp 0xc010b20d <ArchSetIrql+0x39>
c010b208: 83 ec 0c                      sub esp, 12
c010b20b: 6a 00                         push 0
c010b20d: e8 62 13 00 00                call 0xc010c574 <DisablePicLines>
c010b212: 83 c4 10                      add esp, 16
c010b215: fb                            sti
c010b216: 83 c4 0c                      add esp, 12
c010b219: c3                            ret

c010b21a <x86IsReadyForIrqs>:
c010b21a: a0 38 b3 13 c0                mov al, byte ptr [3222516536]
c010b21f: c3                            ret

c010b220 <x86MakeReadyForIrqs>:
c010b220: 83 ec 0c                      sub esp, 12
c010b223: c6 05 38 b3 13 c0 01          mov byte ptr [-1072450760], 1
c010b22a: e8 40 81 ff ff                call 0xc010336f <GetIrql>
c010b22f: 83 ec 0c                      sub esp, 12
c010b232: 50                            push eax
c010b233: e8 44 81 ff ff                call 0xc010337c <RaiseIrql>
c010b238: 83 c4 1c                      add esp, 28
c010b23b: c3                            ret

c010b23c <ArchDisableInterrupts>:
c010b23c: fa                            cli
c010b23d: c3                            ret

c010b23e <ArchEnableInterrupts>:
c010b23e: fb                            sti
c010b23f: c3                            ret

c010b240 <ArchGetCurrentCpuIndex>:
c010b240: 0f 21 d8                      mov eax, dr3
c010b243: c3                            ret

c010b244 <HandleNmi>:
c010b244: 83 ec 18                      sub esp, 24
c010b247: 6a 00                         push 0
c010b249: e8 04 01 00 00                call 0xc010b352 <SetNmiEnable>
c010b24e: fa                            cli
c010b24f: c7 04 24 f3 19 11 c0          mov dword ptr [esp], 3222346227
c010b256: e8 82 d8 ff ff                call 0xc0108add <LogDeveloperWarning>
c010b25b: e4 61                         in al, 97
c010b25d: 83 c4 10                      add esp, 16
c010b260: a8 40                         test al, 64
c010b262: 74 07                         je 0xc010b26b <HandleNmi+0x27>
c010b264: 83 ec 0c                      sub esp, 12
c010b267: 6a 28                         push 40
c010b269: eb 09                         jmp 0xc010b274 <HandleNmi+0x30>
c010b26b: 84 c0                         test al, al
c010b26d: 79 0a                         jns 0xc010b279 <HandleNmi+0x35>
c010b26f: 83 ec 0c                      sub esp, 12
c010b272: 6a 29                         push 41
c010b274: e8 26 d9 ff ff                call 0xc0108b9f <Panic>
c010b279: 50                            push eax
c010b27a: 50                            push eax
c010b27b: 68 1b 1a 11 c0                push 3222346267
c010b280: 6a 28                         push 40
c010b282: e8 c7 d8 ff ff                call 0xc0108b4e <PanicEx>

c010b287 <x86InitTss>:
c010b287: 53                            push ebx
c010b288: 83 ec 14                      sub esp, 20
c010b28b: 0f 21 d8                      mov eax, dr3
c010b28e: c1 e0 06                      shl eax, 6
c010b291: 8b 98 c8 40 11 c0             mov ebx, dword ptr [eax - 1072611128]
c010b297: 6a 68                         push 104
```

```
c010b2f1: 83 e3 7f                      and ebx, 127
c010b2f4: 09 d8                         or eax, ebx
c010b2f6: e6 70                         out 112, al
c010b2f8: 90                            nop
c010b2f9: e4 71                         in al, 113
c010b2fb: 88 c3                         mov bl, al
c010b2fd: 90                            nop
c010b2fe: c7 04 24 3c b3 13 c0          mov dword ptr [esp], 3222516540
c010b305: e8 a0 b6 ff ff                call 0xc01069aa <ReleaseSpinlock>
c010b30a: 88 d8                         mov al, bl
c010b30c: 83 c4 18                      add esp, 24
c010b30f: 5b                            pop ebx
c010b310: c3                            ret

c010b311 <WriteCmos>:
c010b311: 56                            push esi
c010b312: 53                            push ebx
c010b313: 83 ec 10                      sub esp, 16
c010b316: 8b 74 24 1c                   mov esi, dword ptr [esp + 28]
c010b31a: 8a 5c 24 20                   mov bl, byte ptr [esp + 32]
c010b31e: 68 3c b3 13 c0                push 3222516540
c010b323: e8 32 b6 ff ff                call 0xc010695a <AcquireSpinlock>
c010b328: a0 1c 31 11 c0                mov al, byte ptr [3222352156]
c010b32d: 83 f0 01                      xor eax, 1
c010b330: c1 e0 07                      shl eax, 7
c010b333: 83 e6 7f                      and esi, 127
c010b336: 09 f0                         or eax, esi
c010b338: e6 70                         out 112, al
c010b33a: 90                            nop
c010b33b: 88 d8                         mov al, bl
c010b33d: e6 71                         out 113, al
c010b33f: 90                            nop
c010b340: c7 44 24 20 3c b3 13 c0       mov dword ptr [esp + 32], 3222516540
c010b348: 83 c4 14                      add esp, 20
c010b34b: 5b                            pop ebx
c010b34c: 5e                            pop esi
c010b34d: e9 58 b6 ff ff                jmp 0xc01069aa <ReleaseSpinlock>

c010b352 <SetNmiEnable>:
c010b352: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c010b356: a2 1c 31 11 c0                mov byte ptr [3222352156], al
c010b35b: c7 44 24 04 10 00 00 00       mov dword ptr [esp + 4], 16
c010b363: e9 6c ff ff ff                jmp 0xc010b2d4 <ReadCmos>

c010b368 <InitCmos>:
c010b368: 83 ec 10                      sub esp, 16
c010b36b: 6a 29                         push 41
c010b36d: 68 27 1a 11 c0                push 3222346279
c010b372: 68 3c b3 13 c0                push 3222516540
c010b377: e8 c3 b5 ff ff                call 0xc010693f <InitSpinlock>
c010b37c: c7 04 24 01 00 00 00          mov dword ptr [esp], 1
c010b383: e8 ca ff ff ff                call 0xc010b352 <SetNmiEnable>
c010b388: 83 c4 1c                      add esp, 28
c010b38b: c3                            ret

c010b38c <FloppyIrqHandler>:
c010b38c: c6 05 5c b3 13 c0 01          mov byte ptr [-1072450724], 1
c010b393: 31 c0                         xor eax, eax
c010b395: c3                            ret

c010b396 <Follow>:
c010b396: 83 ec 24                      sub esp, 36
c010b399: 6a ff                         push -1
c010b39b: ff 35 58 b3 13 c0             push dword ptr [-1072450728]
c010b3a1: e8 93 b3 ff ff                call 0xc0106739 <AcquireSemaphore>
c010b3a6: 83 c4 0c                      add esp, 12
c010b3a9: ff 74 24 2c                   push dword ptr [esp + 44]
c010b3ad: ff 74 24 2c                   push dword ptr [esp + 44]
c010b3b1: 8b 44 24 2c                   mov eax, dword ptr [esp + 44]
c010b3b5: 8b 40 28                      mov eax, dword ptr [eax + 40]
c010b3b8: 83 c0 10                      add eax, 16
```

```
c010b41b: c3                            ret

c010b41c <FloppyMotorControlThread>:
c010b41c: 83 ec 0c                      sub esp, 12
c010b41f: 83 ec 0c                      sub esp, 12
c010b422: 6a 32                         push 50
c010b424: e8 67 ca ff ff                call 0xc0107e90 <SleepMilli>
c010b429: a1 64 b3 13 c0                mov eax, dword ptr [3222516580]
c010b42e: 83 c4 10                      add esp, 16
c010b431: 83 f8 02                      cmp eax, 2
c010b434: 75 e9                         jne 0xc010b41f <FloppyMotorControlThread+0x3>
c010b436: a1 60 b3 13 c0                mov eax, dword ptr [3222516576]
c010b43b: 83 e8 32                      sub eax, 50
c010b43e: a3 60 b3 13 c0                mov dword ptr [3222516576], eax
c010b443: a1 60 b3 13 c0                mov eax, dword ptr [3222516576]
c010b448: 85 c0                         test eax, eax
c010b44a: 7f d3                         jg 0xc010b41f <FloppyMotorControlThread+0x3>
c010b44c: b0 0c                         mov al, 12
c010b44e: ba f2 03 00 00                mov edx, 1010
c010b453: ee                            out dx, al
c010b454: 31 c0                         xor eax, eax
c010b456: a3 64 b3 13 c0                mov dword ptr [3222516580], eax
c010b45b: eb c2                         jmp 0xc010b41f <FloppyMotorControlThread+0x3>

c010b45d <FloppyMotor>:
c010b45d: 84 d2                         test dl, dl
c010b45f: 74 2e                         je 0xc010b48f <FloppyMotor+0x32>
c010b461: 8b 15 64 b3 13 c0             mov edx, dword ptr [-1072450716]
c010b467: 85 d2                         test edx, edx
c010b469: 75 39                         jne 0xc010b4a4 <FloppyMotor+0x47>
c010b46b: 83 ec 18                      sub esp, 24
c010b46e: 8b 50 0c                      mov edx, dword ptr [eax + 12]
c010b471: 83 c2 02                      add edx, 2
c010b474: b0 1c                         mov al, 28
c010b476: ee                            out dx, al
c010b477: 68 96 00 00 00                push 150
c010b47c: e8 0f ca ff ff                call 0xc0107e90 <SleepMilli>
c010b481: c7 05 64 b3 13 c0 01 00 00 00 mov dword ptr [-1072450716], 1
c010b48b: 83 c4 1c                      add esp, 28
c010b48e: c3                            ret
c010b48f: c7 05 64 b3 13 c0 02 00 00 00 mov dword ptr [-1072450716], 2
c010b499: c7 05 60 b3 13 c0 e8 03 00 00 mov dword ptr [-1072450720], 1000
c010b4a3: c3                            ret
c010b4a4: c7 05 64 b3 13 c0 01 00 00 00 mov dword ptr [-1072450716], 1
c010b4ae: c3                            ret

c010b4af <FloppyIrqWait.constprop.0.isra.0>:
c010b4af: 53                            push ebx
c010b4b0: 83 ec 08                      sub esp, 8
c010b4b3: bb c9 00 00 00                mov ebx, 201
c010b4b8: a0 5c b3 13 c0                mov al, byte ptr [3222516572]
c010b4bd: 84 c0                         test al, al
c010b4bf: 75 22                         jne 0xc010b4e3 <FloppyIrqWait.constprop.0.isr
c010b4c1: 83 ec 0c                      sub esp, 12
c010b4c4: 6a 0a                         push 10
c010b4c6: e8 c5 c9 ff ff                call 0xc0107e90 <SleepMilli>
c010b4cb: 83 c4 10                      add esp, 16
c010b4ce: 4b                            dec ebx
c010b4cf: 75 e7                         jne 0xc010b4b8 <FloppyIrqWait.constprop.0.isr
c010b4d1: 83 ec 0c                      sub esp, 12
c010b4d4: 68 2c 1a 11 c0                push 3222346284
c010b4d9: e8 e7 d5 ff ff                call 0xc0108ac5 <LogWriteSerial>
c010b4de: 83 c4 10                      add esp, 16
c010b4e1: eb 07                         jmp 0xc010b4ea <FloppyIrqWait.constprop.0.isr
c010b4e3: c6 05 5c b3 13 c0 00          mov byte ptr [-1072450724], 0
c010b4ea: 83 c4 08                      add esp, 8
c010b4ed: 5b                            pop ebx
c010b4ee: c3                            ret

c010b4ef <FloppyReadData.isra.0>:
c010b4ef: 56                            push esi
```

```
c010b524: be 3c 00 00 00                mov esi, 60
c010b529: 83 ec 0c                      sub esp, 12
c010b52c: 6a 0a                         push 10
c010b52e: e8 5d c9 ff ff                call 0xc0107e90 <SleepMilli>
c010b533: 8d 53 04                      lea edx, [ebx + 4]
c010b536: ec                            in al, dx
c010b537: 83 c4 10                      add esp, 16
c010b53a: 84 c0                         test al, al
c010b53c: 79 08                         jns 0xc010b546 <FloppyWriteCommand.isra.0+0x2
c010b53e: 8d 53 05                      lea edx, [ebx + 5]
c010b541: 89 f8                         mov eax, edi
c010b543: ee                            out dx, al
c010b544: eb 03                         jmp 0xc010b549 <FloppyWriteCommand.isra.0+0x2
c010b546: 4e                            dec esi
c010b547: 75 e0                         jne 0xc010b529 <FloppyWriteCommand.isra.0+0xc
c010b549: 5b                            pop ebx
c010b54a: 5e                            pop esi
c010b54b: 5f                            pop edi
c010b54c: c3                            ret

c010b54d <FloppyCheckInterrupt>:
c010b54d: 57                            push edi
c010b54e: 56                            push esi
c010b54f: 53                            push ebx
c010b550: 89 c3                         mov ebx, eax
c010b552: 89 d7                         mov edi, edx
c010b554: 89 ce                         mov esi, ecx
c010b556: 8b 40 0c                      mov eax, dword ptr [eax + 12]
c010b559: ba 08 00 00 00                mov edx, 8
c010b55e: e8 ba ff ff ff                call 0xc010b51d <FloppyWriteCommand.isra.0>
c010b563: 8b 43 0c                      mov eax, dword ptr [ebx + 12]
c010b566: e8 84 ff ff ff                call 0xc010b4ef <FloppyReadData.isra.0>
c010b56b: 0f b6 c0                      movzx eax, al
c010b56e: 89 07                         mov dword ptr [edi], eax
c010b570: 8b 43 0c                      mov eax, dword ptr [ebx + 12]
c010b573: e8 77 ff ff ff                call 0xc010b4ef <FloppyReadData.isra.0>
c010b578: 0f b6 c0                      movzx eax, al
c010b57b: 89 06                         mov dword ptr [esi], eax
c010b57d: 5b                            pop ebx
c010b57e: 5e                            pop esi
c010b57f: 5f                            pop edi
c010b580: c3                            ret

c010b581 <FloppyCalibrate.isra.0>:
c010b581: 56                            push esi
c010b582: 53                            push ebx
c010b583: 83 ec 20                      sub esp, 32
c010b586: 89 c3                         mov ebx, eax
c010b588: 68 41 1a 11 c0                push 3222346305
c010b58d: e8 33 d5 ff ff                call 0xc0108ac5 <LogWriteSerial>
c010b592: c7 44 24 18 ff ff ff ff       mov dword ptr [esp + 24], 4294967295
c010b59a: c7 44 24 1c ff ff ff ff       mov dword ptr [esp + 28], 4294967295
c010b5a2: ba 01 00 00 00                mov edx, 1
c010b5a7: 89 d8                         mov eax, ebx
c010b5a9: e8 af fe ff ff                call 0xc010b45d <FloppyMotor>
c010b5ae: 83 c4 10                      add esp, 16
c010b5b1: be 0a 00 00 00                mov esi, 10
c010b5b6: 8b 43 0c                      mov eax, dword ptr [ebx + 12]
c010b5b9: ba 07 00 00 00                mov edx, 7
c010b5be: e8 5a ff ff ff                call 0xc010b51d <FloppyWriteCommand.isra.0>
c010b5c3: 8b 43 0c                      mov eax, dword ptr [ebx + 12]
c010b5c6: 31 d2                         xor edx, edx
c010b5c8: e8 50 ff ff ff                call 0xc010b51d <FloppyWriteCommand.isra.0>
c010b5cd: e8 dd fe ff ff                call 0xc010b4af <FloppyIrqWait.constprop.0.is
c010b5d2: 8d 4c 24 0c                   lea ecx, [esp + 12]
c010b5d6: 8d 54 24 08                   lea edx, [esp + 8]
c010b5da: 89 d8                         mov eax, ebx
c010b5dc: e8 6c ff ff ff                call 0xc010b54d <FloppyCheckInterrupt>
c010b5e1: 8b 44 24 08                   mov eax, dword ptr [esp + 8]
c010b5e5: 25 c0 00 00 00                and eax, 192
c010b5ea: 0b 44 24 0c                   or eax, dword ptr [esp + 12]
```

```
c010b62c: e8 1c ff ff ff              call 0xc010b54d <FloppyCheckInterrupt>
c010b631: 4f                          dec edi
c010b632: 75 ee                       jne 0xc010b622 <FloppyReset.isra.0+0x1e>
c010b634: 8d 56 07                    lea edx, [esi + 7]
c010b637: 31 c0                       xor eax, eax
c010b639: ee                          out dx, al
c010b63a: ba 01 00 00 00              mov edx, 1
c010b63f: 89 d8                       mov eax, ebx
c010b641: e8 17 fe ff ff              call 0xc010b45d <FloppyMotor>
c010b646: 8b 43 0c                    mov eax, dword ptr [ebx + 12]
c010b649: ba 03 00 00 00              mov edx, 3
c010b64e: e8 ca fe ff ff              call 0xc010b51d <FloppyWriteCommand.isra.0>
c010b653: 8b 43 0c                    mov eax, dword ptr [ebx + 12]
c010b656: ba df 00 00 00              mov edx, 223
c010b65b: e8 bd fe ff ff              call 0xc010b51d <FloppyWriteCommand.isra.0>
c010b660: 8b 43 0c                    mov eax, dword ptr [ebx + 12]
c010b663: ba 02 00 00 00              mov edx, 2
c010b668: e8 b0 fe ff ff              call 0xc010b51d <FloppyWriteCommand.isra.0>
c010b66d: 83 ec 0c                    sub esp, 12
c010b670: 68 2c 01 00 00              push 300
c010b675: e8 16 c8 ff ff              call 0xc0107e90 <SleepMilli>
c010b67a: 8b 43 0c                    mov eax, dword ptr [ebx + 12]
c010b67d: ba 13 00 00 00              mov edx, 19
c010b682: e8 96 fe ff ff              call 0xc010b51d <FloppyWriteCommand.isra.0>
c010b687: 8b 43 0c                    mov eax, dword ptr [ebx + 12]
c010b68a: 31 d2                       xor edx, edx
c010b68c: e8 8c fe ff ff              call 0xc010b51d <FloppyWriteCommand.isra.0>
c010b691: 8b 43 0c                    mov eax, dword ptr [ebx + 12]
c010b694: ba 08 00 00 00              mov edx, 8
c010b699: e8 7f fe ff ff              call 0xc010b51d <FloppyWriteCommand.isra.0>
c010b69e: 8b 43 0c                    mov eax, dword ptr [ebx + 12]
c010b6a1: 31 d2                       xor edx, edx
c010b6a3: e8 75 fe ff ff              call 0xc010b51d <FloppyWriteCommand.isra.0>
c010b6a8: c7 04 24 2c 01 00 00        mov dword ptr [esp], 300
c010b6af: e8 dc c7 ff ff              call 0xc0107e90 <SleepMilli>
c010b6b4: 31 d2                       xor edx, edx
c010b6b6: 89 d8                       mov eax, ebx
c010b6b8: e8 a0 fd ff ff              call 0xc010b45d <FloppyMotor>
c010b6bd: 89 d8                       mov eax, ebx
c010b6bf: 83 c4 20                    add esp, 32
c010b6c2: 5b                          pop ebx
c010b6c3: 5e                          pop esi
c010b6c4: 5f                          pop edi
c010b6c5: e9 b7 fe ff ff              jmp 0xc010b581 <FloppyCalibrate.isra.0>

c010b6ca <FloppySeek>:
c010b6ca: 55                          push ebp
c010b6cb: 57                          push edi
c010b6cc: 56                          push esi
c010b6cd: 53                          push ebx
c010b6ce: 83 ec 2c                    sub esp, 44
c010b6d1: 89 c3                       mov ebx, eax
c010b6d3: 89 d7                       mov edi, edx
c010b6d5: 89 ce                       mov esi, ecx
c010b6d7: ba 01 00 00 00              mov edx, 1
c010b6dc: e8 7c fd ff ff              call 0xc010b45d <FloppyMotor>
c010b6e1: 8d 04 b5 00 00 00 00        lea eax, [4*esi]
c010b6e8: 89 44 24 0c                 mov dword ptr [esp + 12], eax
c010b6ec: bd 0a 00 00 00              mov ebp, 10
c010b6f1: 8b 43 0c                    mov eax, dword ptr [ebx + 12]
c010b6f4: ba 0f 00 00 00              mov edx, 15
c010b6f9: e8 1f fe ff ff              call 0xc010b51d <FloppyWriteCommand.isra.0>
c010b6fe: 8b 43 0c                    mov eax, dword ptr [ebx + 12]
c010b701: 8b 54 24 0c                 mov edx, dword ptr [esp + 12]
c010b705: e8 13 fe ff ff              call 0xc010b51d <FloppyWriteCommand.isra.0>
c010b70a: 8b 43 0c                    mov eax, dword ptr [ebx + 12]
c010b70d: 89 fa                       mov edx, edi
c010b70f: e8 09 fe ff ff              call 0xc010b51d <FloppyWriteCommand.isra.0>
c010b714: e8 96 fd ff ff              call 0xc010b4af <FloppyIrqWait.constprop.0.is
c010b719: 8d 4c 24 1c                 lea ecx, [esp + 28]
c010b71d: 8d 54 24 18                 lea edx, [esp + 24]
```

```
c010b763: 53                            push ebx
c010b764: 83 ec 1c                      sub esp, 28
c010b767: 89 c3                         mov ebx, eax
c010b769: 89 54 24 08                   mov dword ptr [esp + 8], edx
c010b76d: 31 c9                         xor ecx, ecx
c010b76f: e8 56 ff ff ff                call 0xc010b6ca <FloppySeek>
c010b774: 85 c0                         test eax, eax
c010b776: 0f 85 f9 01 00 00             jne 0xc010b975 <FloppyDoCylinder+0x215>
c010b77c: b9 01 00 00 00                mov ecx, 1
c010b781: 8b 54 24 08                   mov edx, dword ptr [esp + 8]
c010b785: 89 d8                         mov eax, ebx
c010b787: e8 3e ff ff ff                call 0xc010b6ca <FloppySeek>
c010b78c: 89 c5                         mov ebp, eax
c010b78e: 85 c0                         test eax, eax
c010b790: 0f 85 df 01 00 00             jne 0xc010b975 <FloppyDoCylinder+0x215>
c010b796: 31 f6                         xor esi, esi
c010b798: ba 01 00 00 00                mov edx, 1
c010b79d: 89 d8                         mov eax, ebx
c010b79f: e8 b9 fc ff ff                call 0xc010b45d <FloppyMotor>
c010b7a4: b9 05 00 00 00                mov ecx, 5
c010b7a9: 89 f0                         mov eax, esi
c010b7ab: 99                            cdq
c010b7ac: f7 f9                         idiv ecx
c010b7ae: 83 fa 03                      cmp edx, 3
c010b7b1: 0f 84 13 01 00 00             je 0xc010b8ca <FloppyDoCylinder+0x16a>
c010b7b7: 8b 53 5c                      mov edx, dword ptr [ebx + 92]
c010b7ba: b0 06                         mov al, 6
c010b7bc: e6 0a                         out 10, al
c010b7be: b1 ff                         mov cl, -1
c010b7c0: 88 c8                         mov al, cl
c010b7c2: e6 0c                         out 12, al
c010b7c4: 88 d0                         mov al, dl
c010b7c6: e6 04                         out 4, al
c010b7c8: 89 d0                         mov eax, edx
c010b7ca: c1 e8 08                      shr eax, 8
c010b7cd: e6 04                         out 4, al
c010b7cf: 89 d0                         mov eax, edx
c010b7d1: c1 e8 10                      shr eax, 16
c010b7d4: e6 81                         out 129, al
c010b7d6: 88 c8                         mov al, cl
c010b7d8: e6 0c                         out 12, al
c010b7da: e6 05                         out 5, al
c010b7dc: b0 47                         mov al, 71
c010b7de: e6 05                         out 5, al
c010b7e0: b0 46                         mov al, 70
c010b7e2: e6 0b                         out 11, al
c010b7e4: b0 02                         mov al, 2
c010b7e6: e6 0a                         out 10, al
c010b7e8: 83 ec 0c                      sub esp, 12
c010b7eb: 6a 64                         push 100
c010b7ed: e8 9e c6 ff ff                call 0xc0107e90 <SleepMilli>
c010b7f2: 8b 43 0c                      mov eax, dword ptr [ebx + 12]
c010b7f5: ba c6 00 00 00                mov edx, 198
c010b7fa: e8 1e fd ff ff                call 0xc010b51d <FloppyWriteCommand.isra.0>
c010b7ff: 8b 43 0c                      mov eax, dword ptr [ebx + 12]
c010b802: 31 d2                         xor edx, edx
c010b804: e8 14 fd ff ff                call 0xc010b51d <FloppyWriteCommand.isra.0>
c010b809: 8b 43 0c                      mov eax, dword ptr [ebx + 12]
c010b80c: 8b 54 24 18                   mov edx, dword ptr [esp + 24]
c010b810: e8 08 fd ff ff                call 0xc010b51d <FloppyWriteCommand.isra.0>
c010b815: 8b 43 0c                      mov eax, dword ptr [ebx + 12]
c010b818: 31 d2                         xor edx, edx
c010b81a: e8 fe fc ff ff                call 0xc010b51d <FloppyWriteCommand.isra.0>
c010b81f: 8b 43 0c                      mov eax, dword ptr [ebx + 12]
c010b822: ba 01 00 00 00                mov edx, 1
c010b827: e8 f1 fc ff ff                call 0xc010b51d <FloppyWriteCommand.isra.0>
c010b82c: 8b 43 0c                      mov eax, dword ptr [ebx + 12]
c010b82f: ba 02 00 00 00                mov edx, 2
c010b834: e8 e4 fc ff ff                call 0xc010b51d <FloppyWriteCommand.isra.0>
c010b839: 8b 43 0c                      mov eax, dword ptr [ebx + 12]
c010b83c: ba 12 00 00 00                mov edx, 18
```

```
c010b8be: 80 7c 24 0f 3f             cmp byte ptr [esp + 15], 63
c010b8c3: 76 59                      jbe 0xc010b91e <FloppyDoCylinder+0x1be>
c010b8c5: e9 98 00 00 00             jmp 0xc010b962 <FloppyDoCylinder+0x202>
c010b8ca: b9 0a 00 00 00             mov ecx, 10
c010b8cf: 89 f0                      mov eax, esi
c010b8d1: 99                         cdq
c010b8d2: f7 f9                      idiv ecx
c010b8d4: 83 fa 08                   cmp edx, 8
c010b8d7: 75 13                      jne 0xc010b8ec <FloppyDoCylinder+0x18c>
c010b8d9: 89 d8                      mov eax, ebx
c010b8db: e8 24 fd ff ff             call 0xc010b604 <FloppyReset.isra.0>
c010b8e0: ba 01 00 00 00             mov edx, 1
c010b8e5: 89 d8                      mov eax, ebx
c010b8e7: e8 71 fb ff ff             call 0xc010b45d <FloppyMotor>
c010b8ec: 89 d8                      mov eax, ebx
c010b8ee: e8 8e fc ff ff             call 0xc010b581 <FloppyCalibrate.isra.0>
c010b8f3: 31 c9                      xor ecx, ecx
c010b8f5: 8b 54 24 08                mov edx, dword ptr [esp + 8]
c010b8f9: 89 d8                      mov eax, ebx
c010b8fb: e8 ca fd ff ff             call 0xc010b6ca <FloppySeek>
c010b900: 85 c0                      test eax, eax
c010b902: 75 71                      jne 0xc010b975 <FloppyDoCylinder+0x215>
c010b904: b9 01 00 00 00             mov ecx, 1
c010b909: 8b 54 24 08                mov edx, dword ptr [esp + 8]
c010b90d: 89 d8                      mov eax, ebx
c010b90f: e8 b6 fd ff ff             call 0xc010b6ca <FloppySeek>
c010b914: 85 c0                      test eax, eax
c010b916: 0f 84 9b fe ff ff          je 0xc010b7b7 <FloppyDoCylinder+0x57>
c010b91c: eb 57                      jmp 0xc010b975 <FloppyDoCylinder+0x215>
c010b91e: 89 f9                      mov ecx, edi
c010b920: 84 c9                      test cl, cl
c010b922: 78 3e                      js 0xc010b962 <FloppyDoCylinder+0x202>
c010b924: 83 e7 30                   and edi, 48
c010b927: 8a 54 24 0f                mov dl, byte ptr [esp + 15]
c010b92b: 83 e2 08                   and edx, 8
c010b92e: 89 f9                      mov ecx, edi
c010b930: 08 d1                      or cl, dl
c010b932: 75 2e                      jne 0xc010b962 <FloppyDoCylinder+0x202>
c010b934: 3c 02                      cmp al, 2
c010b936: 75 2a                      jne 0xc010b962 <FloppyDoCylinder+0x202>
c010b938: 31 d2                      xor edx, edx
c010b93a: 89 d8                      mov eax, ebx
c010b93c: e8 1c fb ff ff             call 0xc010b45d <FloppyMotor>
c010b941: 8b 43 04                   mov eax, dword ptr [ebx + 4]
c010b944: 8b 73 60                   mov esi, dword ptr [ebx + 96]
c010b947: b9 00 12 00 00             mov ecx, 4608
c010b94c: 89 c7                      mov edi, eax
c010b94e: f3 a5                      rep  movsd dword ptr es:[edi], dword ptr [esi
c010b950: 83 ec 0c                   sub esp, 12
c010b953: 68 87 1a 11 c0             push 3222346375
c010b958: e8 68 d1 ff ff             call 0xc0108ac5 <LogWriteSerial>
c010b95d: 83 c4 10                   add esp, 16
c010b960: eb 18                      jmp 0xc010b97a <FloppyDoCylinder+0x21a>
c010b962: 46                         inc esi
c010b963: 83 fe 14                   cmp esi, 20
c010b966: 0f 85 2c fe ff ff          jne 0xc010b798 <FloppyDoCylinder+0x38>
c010b96c: 31 d2                      xor edx, edx
c010b96e: 89 d8                      mov eax, ebx
c010b970: e8 e8 fa ff ff             call 0xc010b45d <FloppyMotor>
c010b975: bd 0a 00 00 00             mov ebp, 10
c010b97a: 89 e8                      mov eax, ebp
c010b97c: 83 c4 1c                   add esp, 28
c010b97f: 5b                         pop ebx
c010b980: 5e                         pop esi
c010b981: 5f                         pop edi
c010b982: 5d                         pop ebp
c010b983: c3                         ret

c010b984 <ReadWrite>:
c010b984: 55                         push ebp
c010b985: 57                         push edi
```

```
c010b9e9: 0f ac fe 09                  shrd esi, edi, 9
c010b9ed: c1 ef 09                     shr edi, 9
c010b9f0: 89 74 24 10                  mov dword ptr [esp + 16], esi
c010b9f4: 89 7c 24 14                  mov dword ptr [esp + 20], edi
c010b9f8: 8b 34 24                     mov esi, dword ptr [esp]
c010b9fb: 81 e6 ff 01 00 00            and esi, 511
c010ba01: 31 ff                        xor edi, edi
c010ba03: 85 ff                        test edi, edi
c010ba05: 75 04                        jne 0xc010ba0b <ReadWrite+0x87>
c010ba07: 85 f6                        test esi, esi
c010ba09: 74 0a                        je 0xc010ba15 <ReadWrite+0x91>
c010ba0b: 83 ec 0c                     sub esp, 12
c010ba0e: 68 bc 1a 11 c0               push 3222346428
c010ba13: eb 17                        jmp 0xc010ba2c <ReadWrite+0xa8>
c010ba15: 25 ff 01 00 00               and eax, 511
c010ba1a: 31 d2                        xor edx, edx
c010ba1c: 85 d2                        test edx, edx
c010ba1e: 75 04                        jne 0xc010ba24 <ReadWrite+0xa0>
c010ba20: 85 c0                        test eax, eax
c010ba22: 74 1a                        je 0xc010ba3e <ReadWrite+0xba>
c010ba24: 83 ec 0c                     sub esp, 12
c010ba27: 68 d2 1a 11 c0               push 3222346450
c010ba2c: e8 94 d0 ff ff               call 0xc0108ac5 <LogWriteSerial>
c010ba31: 83 c4 10                     add esp, 16
c010ba34: bf 07 00 00 00               mov edi, 7
c010ba39: e9 72 01 00 00               jmp 0xc010bbb0 <ReadWrite+0x22c>
c010ba3e: 8b 44 24 10                  mov eax, dword ptr [esp + 16]
c010ba42: 48                           dec eax
c010ba43: 3d fe 00 00 00               cmp eax, 254
c010ba48: 77 0a                        ja 0xc010ba54 <ReadWrite+0xd0>
c010ba4a: 81 7c 24 08 3f 0b 00 00      cmp dword ptr [esp + 8], 2879
c010ba52: 76 0a                        jbe 0xc010ba5e <ReadWrite+0xda>
c010ba54: 83 ec 0c                     sub esp, 12
c010ba57: 68 e8 1a 11 c0               push 3222346472
c010ba5c: eb ce                        jmp 0xc010ba2c <ReadWrite+0xa8>
c010ba5e: 8b 44 24 08                  mov eax, dword ptr [esp + 8]
c010ba62: 89 04 24                     mov dword ptr [esp], eax
c010ba65: 8b 44 24 10                  mov eax, dword ptr [esp + 16]
c010ba69: 89 44 24 08                  mov dword ptr [esp + 8], eax
c010ba6d: 52                           push edx
c010ba6e: 52                           push edx
c010ba6f: 6a ff                        push -1
c010ba71: ff 35 58 b3 13 c0            push dword ptr [-1072450728]
c010ba77: e8 bd ac ff ff               call 0xc0106739 <AcquireSemaphore>
c010ba7c: 83 c4 10                     add esp, 16
c010ba7f: b9 24 00 00 00               mov ecx, 36
c010ba84: 8b 04 24                     mov eax, dword ptr [esp]
c010ba87: 99                           cdq
c010ba88: f7 f9                        idiv ecx
c010ba8a: 89 c6                        mov esi, eax
c010ba8c: b9 12 00 00 00               mov ecx, 18
c010ba91: 89 d0                        mov eax, edx
c010ba93: 99                           cdq
c010ba94: f7 f9                        idiv ecx
c010ba96: 89 44 24 10                  mov dword ptr [esp + 16], eax
c010ba9a: 8b 04 24                     mov eax, dword ptr [esp]
c010ba9d: 99                           cdq
c010ba9e: f7 f9                        idiv ecx
c010baa0: 89 54 24 1c                  mov dword ptr [esp + 28], edx
c010baa4: 85 f6                        test esi, esi
c010baa6: 75 6d                        jne 0xc010bb15 <ReadWrite+0x191>
c010baa8: 80 7b 58 00                  cmp byte ptr [ebx + 88], 0
c010baac: 75 35                        jne 0xc010bae3 <ReadWrite+0x15f>
c010baae: c6 43 58 01                  mov byte ptr [ebx + 88], 1
c010bab2: 31 d2                        xor edx, edx
c010bab4: 89 d8                        mov eax, ebx
c010bab6: e8 a5 fc ff ff               call 0xc010b760 <FloppyDoCylinder>
c010babb: 89 c7                        mov edi, eax
c010babd: 85 c0                        test eax, eax
c010babf: 75 68                        jne 0xc010bb29 <ReadWrite+0x1a5>
c010bac1: 83 ec 0c                     sub esp, 12
```

```
c010bb1e: e8 3d fc ff ff              call 0xc010b760 <FloppyDoCylinder>
c010bb23: 89 c7                       mov edi, eax
c010bb25: 85 c0                       test eax, eax
c010bb27: 74 1f                       je 0xc010bb48 <ReadWrite+0x1c4>
c010bb29: 83 ec 0c                    sub esp, 12
c010bb2c: ff 35 58 b3 13 c0           push dword ptr [-1072450728]
c010bb32: e8 7c ad ff ff              call 0xc01068b3 <ReleaseSemaphore>
c010bb37: c7 04 24 04 1b 11 c0        mov dword ptr [esp], 3222346500
c010bb3e: e8 82 cf ff ff              call 0xc0108ac5 <LogWriteSerial>
c010bb43: 83 c4 10                    add esp, 16
c010bb46: eb 68                       jmp 0xc010bbb0 <ReadWrite+0x22c>
c010bb48: 83 ec 0c                    sub esp, 12
c010bb4b: 68 77 1b 11 c0              push 3222346615
c010bb50: e8 70 cf ff ff              call 0xc0108ac5 <LogWriteSerial>
c010bb55: 6a 00                       push 0
c010bb57: 68 00 02 00 00              push 512
c010bb5c: 55                          push ebp
c010bb5d: 8b 44 24 2c                 mov eax, dword ptr [esp + 44]
c010bb61: f7 d8                       neg eax
c010bb63: 83 e0 12                    and eax, 18
c010bb66: 8b 4c 24 38                 mov ecx, dword ptr [esp + 56]
c010bb6a: 01 c8                       add eax, ecx
c010bb6c: c1 e0 09                    shl eax, 9
c010bb6f: 03 43 04                    add eax, dword ptr [ebx + 4]
c010bb72: 50                          push eax
c010bb73: e8 7b d9 ff ff              call 0xc01094f3 <PerformTransfer>
c010bb78: 89 73 54                    mov dword ptr [ebx + 84], esi
c010bb7b: 83 c4 20                    add esp, 32
c010bb7e: 83 7c 24 08 00              cmp dword ptr [esp + 8], 0
c010bb83: 74 0c                       je 0xc010bb91 <ReadWrite+0x20d>
c010bb85: ff 04 24                    inc dword ptr [esp]
c010bb88: ff 4c 24 08                 dec dword ptr [esp + 8]
c010bb8c: e9 ee fe ff ff              jmp 0xc010ba7f <ReadWrite+0xfb>
c010bb91: 83 ec 0c                    sub esp, 12
c010bb94: ff 35 58 b3 13 c0           push dword ptr [-1072450728]
c010bb9a: e8 14 ad ff ff              call 0xc01068b3 <ReleaseSemaphore>
c010bb9f: c7 04 24 a3 1b 11 c0        mov dword ptr [esp], 3222346659
c010bba6: e8 1a cf ff ff              call 0xc0108ac5 <LogWriteSerial>
c010bbab: 83 c4 10                    add esp, 16
c010bbae: 31 ff                       xor edi, edi
c010bbb0: 89 f8                       mov eax, edi
c010bbb2: 83 c4 2c                    add esp, 44
c010bbb5: 5b                          pop ebx
c010bbb6: 5e                          pop esi
c010bbb7: 5f                          pop edi
c010bbb8: 5d                          pop ebp
c010bbb9: c3                          ret

c010bbba <InitFloppy>:
c010bbba: 55                          push ebp
c010bbbb: 57                          push edi
c010bbbc: 56                          push esi
c010bbbd: 53                          push ebx
c010bbbe: 83 ec 70                    sub esp, 112
c010bbc1: 6a 00                       push 0
c010bbc3: 6a 01                       push 1
c010bbc5: 68 b3 1b 11 c0              push 3222346675
c010bbca: e8 0a ab ff ff              call 0xc01066d9 <CreateSemaphore>
c010bbcf: a3 58 b3 13 c0              mov dword ptr [3222516568], eax
c010bbd4: e8 a0 8a ff ff              call 0xc0104679 <GetVas>
c010bbd9: 68 ba 1b 11 c0              push 3222346682
c010bbde: 50                          push eax
c010bbdf: 6a 00                       push 0
c010bbe1: 68 1c b4 10 c0              push 3222320156
c010bbe6: e8 5d bd ff ff              call 0xc0107948 <CreateThread>
c010bbeb: 8d 7c 24 40                 lea edi, [esp + 64]
c010bbef: b9 0e 00 00 00              mov ecx, 14
c010bbf4: 31 c0                       xor eax, eax
c010bbf6: f3 ab                       rep  stosd dword ptr es:[edi], eax
c010bbf8: 83 c4 20                    add esp, 32
c010bbfb: e8 cc de ff ff              call 0xc0109acc <NextDevId>
```

```
c010bc79: 83 ec 0c                   sub esp, 12
c010bc7c: 68 c3 1b 11 c0             push 3222346691
c010bc81: e8 57 ce ff ff             call 0xc0108add <LogDeveloperWarning>
c010bc86: e9 df 00 00 00             jmp 0xc010bd6a <InitFloppy+0x1b0>
c010bc8b: 89 c5                      mov ebp, eax
c010bc8d: 50                         push eax
c010bc8e: 50                         push eax
c010bc8f: 6a 00                      push 0
c010bc91: 6a 00                      push 0
c010bc93: 68 93 00 00 00             push 147
c010bc98: 68 00 48 00 00             push 18432
c010bc9d: 6a 00                      push 0
c010bc9f: 55                         push ebp
c010bca0: e8 a3 96 ff ff             call 0xc0105348 <MapVirt>
c010bca5: 89 44 24 2c                mov dword ptr [esp + 44], eax
c010bca9: 83 c4 14                   add esp, 20
c010bcac: 6a 64                      push 100
c010bcae: e8 9c 7c ff ff             call 0xc010394f <AllocHeap>
c010bcb3: 89 c3                      mov ebx, eax
c010bcb5: 5a                         pop edx
c010bcb6: 59                         pop ecx
c010bcb7: 6a 00                      push 0
c010bcb9: 6a 00                      push 0
c010bcbb: 6a 13                      push 19
c010bcbd: 68 00 48 00 00             push 18432
c010bcc2: 6a 00                      push 0
c010bcc4: 6a 00                      push 0
c010bcc6: e8 7d 96 ff ff             call 0xc0105348 <MapVirt>
c010bccb: 89 44 24 28                mov dword ptr [esp + 40], eax
c010bccf: 83 c4 18                   add esp, 24
c010bcd2: 6a 00                      push 0
c010bcd4: 6a 00                      push 0
c010bcd6: 6a 13                      push 19
c010bcd8: 68 00 48 00 00             push 18432
c010bcdd: 6a 00                      push 0
c010bcdf: 6a 00                      push 0
c010bce1: e8 62 96 ff ff             call 0xc0105348 <MapVirt>
c010bce6: 89 c2                      mov edx, eax
c010bce8: b9 19 00 00 00             mov ecx, 25
c010bced: 89 df                      mov edi, ebx
c010bcef: 31 c0                      xor eax, eax
c010bcf1: f3 ab                      rep  stosd dword ptr es:[edi], eax
c010bcf3: 8b 44 24 28                mov eax, dword ptr [esp + 40]
c010bcf7: 89 43 04                   mov dword ptr [ebx + 4], eax
c010bcfa: 89 53 08                   mov dword ptr [ebx + 8], edx
c010bcfd: c7 43 0c f0 03 00 00       mov dword ptr [ebx + 12], 1008
c010bd04: c7 43 54 ff ff ff ff       mov dword ptr [ebx + 84], 4294967295
c010bd0b: 89 6b 5c                   mov dword ptr [ebx + 92], ebp
c010bd0e: 8b 44 24 2c                mov eax, dword ptr [esp + 44]
c010bd12: 89 43 60                   mov dword ptr [ebx + 96], eax
c010bd15: 89 5e 28                   mov dword ptr [esi + 40], ebx
c010bd18: 83 c4 18                   add esp, 24
c010bd1b: 68 8c b3 10 c0             push 3222320012
c010bd20: 6a 26                      push 38
c010bd22: e8 e0 74 ff ff             call 0xc0103207 <RegisterIrqHandler>
c010bd27: 89 d8                      mov eax, ebx
c010bd29: e8 d6 f8 ff ff             call 0xc010b604 <FloppyReset.isra.0>
c010bd2e: 83 c3 10                   add ebx, 16
c010bd31: 89 1c 24                   mov dword ptr [esp], ebx
c010bd34: e8 8f d1 ff ff             call 0xc0108ec8 <InitDiskPartitionHelper>
c010bd39: c7 04 24 01 00 00 00       mov dword ptr [esp], 1
c010bd40: e8 38 d0 ff ff             call 0xc0108d7d <GenerateNewRawDiskName>
c010bd45: 5b                         pop ebx
c010bd46: 5f                         pop edi
c010bd47: 50                         push eax
c010bd48: 56                         push esi
c010bd49: e8 7b e0 ff ff             call 0xc0109dc9 <AddVfsMount>
c010bd4e: c7 04 24 01 00 00 00       mov dword ptr [esp], 1
c010bd55: 6a 01                      push 1
c010bd57: 6a 00                      push 0
c010bd59: 6a 00                      push 0
```

```
c010bdab: e8 03 ab ff ff              call 0xc01068b3 <ReleaseSemaphore>
c010bdb0: 8b 44 24 1c                 mov eax, dword ptr [esp + 28]
c010bdb4: 83 c4 2c                    add esp, 44
c010bdb7: c3                          ret

c010bdb8 <Create>:
c010bdb8: 83 ec 24                    sub esp, 36
c010bdbb: 6a ff                       push -1
c010bdbd: ff 35 68 b3 13 c0           push dword ptr [-1072450712]
c010bdc3: e8 71 a9 ff ff              call 0xc0106739 <AcquireSemaphore>
c010bdc8: 83 c4 0c                    add esp, 12
c010bdcb: ff 74 24 2c                 push dword ptr [esp + 44]
c010bdcf: ff 74 24 2c                 push dword ptr [esp + 44]
c010bdd3: 8b 44 24 2c                 mov eax, dword ptr [esp + 44]
c010bdd7: 8b 40 28                    mov eax, dword ptr [eax + 40]
c010bdda: 83 c0 28                    add eax, 40
c010bddd: 50                          push eax
c010bdde: e8 2c d1 ff ff              call 0xc0108f0f <DiskCreateHelper>
c010bde3: 89 44 24 1c                 mov dword ptr [esp + 28], eax
c010bde7: 58                          pop eax
c010bde8: ff 35 68 b3 13 c0           push dword ptr [-1072450712]
c010bdee: e8 c0 aa ff ff              call 0xc01068b3 <ReleaseSemaphore>
c010bdf3: 8b 44 24 1c                 mov eax, dword ptr [esp + 28]
c010bdf7: 83 c4 2c                    add esp, 44
c010bdfa: c3                          ret

c010bdfb <IdeCheckError>:
c010bdfb: 8b 44 24 04                 mov eax, dword ptr [esp + 4]
c010bdff: 83 38 01                    cmp dword ptr [eax], 1
c010be02: 7e 05                       jle 0xc010be09 <IdeCheckError+0xe>
c010be04: 8b 50 1c                    mov edx, dword ptr [eax + 28]
c010be07: eb 03                       jmp 0xc010be0c <IdeCheckError+0x11>
c010be09: 8b 50 14                    mov edx, dword ptr [eax + 20]
c010be0c: 83 c2 07                    add edx, 7
c010be0f: 0f b7 d2                    movzx edx, dx
c010be12: ec                          in al, dx
c010be13: ba 0a 00 00 00              mov edx, 10
c010be18: a8 21                       test al, 33
c010be1a: 75 0a                       jne 0xc010be26 <IdeCheckError+0x2b>
c010be1c: 83 e0 08                    and eax, 8
c010be1f: 3c 01                       cmp al, 1
c010be21: 19 d2                       sbb edx, edx
c010be23: 83 e2 0a                    and edx, 10
c010be26: 89 d0                       mov eax, edx
c010be28: c3                          ret

c010be29 <IdePoll>:
c010be29: 56                          push esi
c010be2a: 53                          push ebx
c010be2b: 51                          push ecx
c010be2c: 8b 44 24 10                 mov eax, dword ptr [esp + 16]
c010be30: 83 38 01                    cmp dword ptr [eax], 1
c010be33: 7e 08                       jle 0xc010be3d <IdePoll+0x14>
c010be35: 8b 70 1c                    mov esi, dword ptr [eax + 28]
c010be38: 8b 50 20                    mov edx, dword ptr [eax + 32]
c010be3b: eb 06                       jmp 0xc010be43 <IdePoll+0x1a>
c010be3d: 8b 70 14                    mov esi, dword ptr [eax + 20]
c010be40: 8b 50 18                    mov edx, dword ptr [eax + 24]
c010be43: ec                          in al, dx
c010be44: ec                          in al, dx
c010be45: ec                          in al, dx
c010be46: ec                          in al, dx
c010be47: 31 db                       xor ebx, ebx
c010be49: 8d 56 07                    lea edx, [esi + 7]
c010be4c: ec                          in al, dx
c010be4d: 84 c0                       test al, al
c010be4f: 79 30                       jns 0xc010be81 <IdePoll+0x58>
c010be51: e8 79 b7 ff ff              call 0xc01075cf <HasBeenSignalled>
c010be56: 84 c0                       test al, al
c010be58: 75 2b                       jne 0xc010be85 <IdePoll+0x5c>
c010be5a: 81 fb cf 03 00 00           cmp ebx, 975
```

```
c010bea7: 31 ff                   xor edi, edi
c010bea9: 8d 4c 24 38             lea ecx, [esp + 56]
c010bead: 83 ec 0c                sub esp, 12
c010beb0: 51                      push ecx
c010beb1: 57                      push edi
c010beb2: 56                      push esi
c010beb3: 8b 44 24 7c             mov eax, dword ptr [esp + 124]
c010beb7: ff 70 10                push dword ptr [eax + 16]
c010beba: ff 70 0c                push dword ptr [eax + 12]
c010bebd: e8 b6 31 00 00          call 0xc010f078 <__udivmoddi4>
c010bec2: 83 c4 14                add esp, 20
c010bec5: 89 c3                   mov ebx, eax
c010bec7: 8b 44 24 44             mov eax, dword ptr [esp + 68]
c010becb: 89 44 24 24             mov dword ptr [esp + 36], eax
c010becf: 8b 44 24 48             mov eax, dword ptr [esp + 72]
c010bed3: 89 44 24 28             mov dword ptr [esp + 40], eax
c010bed7: 89 5c 24 1c             mov dword ptr [esp + 28], ebx
c010bedb: 8d 4c 24 44             lea ecx, [esp + 68]
c010bedf: 51                      push ecx
c010bee0: 57                      push edi
c010bee1: 56                      push esi
c010bee2: 8b 44 24 7c             mov eax, dword ptr [esp + 124]
c010bee6: ff 70 08                push dword ptr [eax + 8]
c010bee9: ff 70 04                push dword ptr [eax + 4]
c010beec: e8 87 31 00 00          call 0xc010f078 <__udivmoddi4>
c010bef1: 83 c4 20                add esp, 32
c010bef4: 89 c7                   mov edi, eax
c010bef6: 8b 44 24 38             mov eax, dword ptr [esp + 56]
c010befa: 8b 74 24 3c             mov esi, dword ptr [esp + 60]
c010befe: 8b 4c 24 18             mov ecx, dword ptr [esp + 24]
c010bf02: 89 4c 24 24             mov dword ptr [esp + 36], ecx
c010bf06: 8b 4c 24 1c             mov ecx, dword ptr [esp + 28]
c010bf0a: 89 4c 24 30             mov dword ptr [esp + 48], ecx
c010bf0e: 85 c9                   test ecx, ecx
c010bf10: 0f 85 ea 02 00 00       jne 0xc010c200 <ReadWrite+0x372>
c010bf16: 83 7c 24 24 00          cmp dword ptr [esp + 36], 0
c010bf1b: 0f 85 df 02 00 00       jne 0xc010c200 <ReadWrite+0x372>
c010bf21: 85 ff                   test edi, edi
c010bf23: 0f 9e c1                setle cl
c010bf26: 81 7c 24 10 ff ff ff 0f cmp dword ptr [esp + 16], 268435455
c010bf2e: 0f 97 c2                seta dl
c010bf31: 08 ca                   or dl, cl
c010bf33: 0f 85 c7 02 00 00       jne 0xc010c200 <ReadWrite+0x372>
c010bf39: 09 f0                   or eax, esi
c010bf3b: 0f 85 bf 02 00 00       jne 0xc010c200 <ReadWrite+0x372>
c010bf41: 89 5c 24 18             mov dword ptr [esp + 24], ebx
c010bf45: 89 d8                   mov eax, ebx
c010bf47: 99                      cdq
c010bf48: 89 fb                   mov ebx, edi
c010bf4a: c1 fb 1f                sar ebx, 31
c010bf4d: 01 f8                   add eax, edi
c010bf4f: 11 da                   adc edx, ebx
c010bf51: 3b 45 08                cmp eax, dword ptr [ebp + 8]
c010bf54: 89 d0                   mov eax, edx
c010bf56: 1b 45 0c                sbb eax, dword ptr [ebp + 12]
c010bf59: bb 07 00 00 00          mov ebx, 7
c010bf5e: 0f 83 a1 02 00 00       jae 0xc010c205 <ReadWrite+0x377>
c010bf64: 8b 5d 00                mov ebx, dword ptr [ebp]
c010bf67: 83 fb 01                cmp ebx, 1
c010bf6a: 7e 08                   jle 0xc010bf74 <ReadWrite+0xe6>
c010bf6c: 8b 75 1c                mov esi, dword ptr [ebp + 28]
c010bf6f: 8b 45 20                mov eax, dword ptr [ebp + 32]
c010bf72: eb 06                   jmp 0xc010bf7a <ReadWrite+0xec>
c010bf74: 8b 75 14                mov esi, dword ptr [ebp + 20]
c010bf77: 8b 45 18                mov eax, dword ptr [ebp + 24]
c010bf7a: 66 89 44 24 34          mov word ptr [esp + 52], ax
c010bf7f: 8b 45 10                mov eax, dword ptr [ebp + 16]
c010bf82: 89 44 24 1c             mov dword ptr [esp + 28], eax
c010bf86: b8 00 40 00 00          mov eax, 16384
c010bf8b: 31 d2                   xor edx, edx
c010bf8d: f7 74 24 0c             div dword ptr [esp + 12]
```

```
c010bffa: 83 78 14 01                cmp dword ptr [eax + 20], 1
c010bffe: 75 17                      jne 0xc010c017 <ReadWrite+0x189>
c010c000: 8b 45 04                   mov eax, dword ptr [ebp + 4]
c010c003: 31 d2                      xor edx, edx
c010c005: 52                         push edx
c010c006: 50                         push eax
c010c007: ff 74 24 6c                push dword ptr [esp + 108]
c010c00b: ff 74 24 28                push dword ptr [esp + 40]
c010c00f: e8 df d4 ff ff             call 0xc01094f3 <PerformTransfer>
c010c014: 83 c4 10                   add esp, 16
c010c017: 8b 44 24 18                mov eax, dword ptr [esp + 24]
c010c01b: c1 f8 18                   sar eax, 24
c010c01e: 83 e0 0f                   and eax, 15
c010c021: 0a 44 24 37                or al, byte ptr [esp + 55]
c010c025: 83 c8 e0                   or eax, -32
c010c028: 8d 56 06                   lea edx, [esi + 6]
c010c02b: ee                         out dx, al
c010c02c: b0 02                      mov al, 2
c010c02e: 8b 54 24 34                mov edx, dword ptr [esp + 52]
c010c032: ee                         out dx, al
c010c033: 8d 56 01                   lea edx, [esi + 1]
c010c036: 31 c0                      xor eax, eax
c010c038: ee                         out dx, al
c010c039: 8d 56 02                   lea edx, [esi + 2]
c010c03c: 8a 44 24 0c                mov al, byte ptr [esp + 12]
c010c040: ee                         out dx, al
c010c041: 8d 56 03                   lea edx, [esi + 3]
c010c044: 8a 44 24 18                mov al, byte ptr [esp + 24]
c010c048: ee                         out dx, al
c010c049: 8b 44 24 18                mov eax, dword ptr [esp + 24]
c010c04d: c1 f8 08                   sar eax, 8
c010c050: 8d 56 04                   lea edx, [esi + 4]
c010c053: ee                         out dx, al
c010c054: 8b 44 24 18                mov eax, dword ptr [esp + 24]
c010c058: c1 f8 10                   sar eax, 16
c010c05b: 8d 56 05                   lea edx, [esi + 5]
c010c05e: ee                         out dx, al
c010c05f: 8b 44 24 64                mov eax, dword ptr [esp + 100]
c010c063: 83 78 14 01                cmp dword ptr [eax + 20], 1
c010c067: 0f 94 c0                   sete al
c010c06a: 0f b6 c0                   movzx eax, al
c010c06d: 48                         dec eax
c010c06e: 83 e0 f0                   and eax, -16
c010c071: 83 c0 30                   add eax, 48
c010c074: 8d 56 07                   lea edx, [esi + 7]
c010c077: ee                         out dx, al
c010c078: 83 ec 0c                   sub esp, 12
c010c07b: 55                         push ebp
c010c07c: e8 a8 fd ff ff             call 0xc010be29 <IdePoll>
c010c081: 83 c4 10                   add esp, 16
c010c084: 31 db                      xor ebx, ebx
c010c086: 89 5c 24 10                mov dword ptr [esp + 16], ebx
c010c08a: 8b 44 24 64                mov eax, dword ptr [esp + 100]
c010c08e: 83 78 14 01                cmp dword ptr [eax + 20], 1
c010c092: 0f 85 a3 00 00 00          jne 0xc010c13b <ReadWrite+0x2ad>
c010c098: 8b 5c 24 10                mov ebx, dword ptr [esp + 16]
c010c09c: 39 5c 24 0c                cmp dword ptr [esp + 12], ebx
c010c0a0: 74 65                      je 0xc010c107 <ReadWrite+0x279>
c010c0a2: 83 7c 24 10 00             cmp dword ptr [esp + 16], 0
c010c0a7: 74 1f                      je 0xc010c0c8 <ReadWrite+0x23a>
c010c0a9: 8b 45 04                   mov eax, dword ptr [ebp + 4]
c010c0ac: 31 d2                      xor edx, edx
c010c0ae: 52                         push edx
c010c0af: 50                         push eax
c010c0b0: ff 74 24 6c                push dword ptr [esp + 108]
c010c0b4: ff 74 24 28                push dword ptr [esp + 40]
c010c0b8: e8 36 d4 ff ff             call 0xc01094f3 <PerformTransfer>
c010c0bd: 89 2c 24                   mov dword ptr [esp], ebp
c010c0c0: e8 64 fd ff ff             call 0xc010be29 <IdePoll>
c010c0c5: 83 c4 10                   add esp, 16
c010c0c8: 8b 45 04                   mov eax, dword ptr [ebp + 4]
```

```
c010c121: 8d 50 07                   lea edx, [eax + 7]
c010c124: 0f b7 d2                   movzx edx, dx
c010c127: b0 e7                      mov al, -25
c010c129: ee                         out dx, al
c010c12a: 83 ec 0c                   sub esp, 12
c010c12d: 55                         push ebp
c010c12e: e8 f6 fc ff ff             call 0xc010be29 <IdePoll>
c010c133: 83 c4 10                   add esp, 16
c010c136: e9 9e 00 00 00             jmp 0xc010c1d9 <ReadWrite+0x34b>
c010c13b: 83 ec 0c                   sub esp, 12
c010c13e: 55                         push ebp
c010c13f: e8 b7 fc ff ff             call 0xc010bdfb <IdeCheckError>
c010c144: 89 c3                      mov ebx, eax
c010c146: 83 c4 10                   add esp, 16
c010c149: 85 c0                      test eax, eax
c010c14b: 74 2b                      je 0xc010c178 <ReadWrite+0x2ea>
c010c14d: 83 ec 0c                   sub esp, 12
c010c150: ff 35 68 b3 13 c0          push dword ptr [-1072450712]
c010c156: e8 58 a7 ff ff             call 0xc01068b3 <ReleaseSemaphore>
c010c15b: 83 c4 10                   add esp, 16
c010c15e: e9 a2 00 00 00             jmp 0xc010c205 <ReadWrite+0x377>
c010c163: 31 d2                      xor edx, edx
c010c165: 52                         push edx
c010c166: 51                         push ecx
c010c167: ff 74 24 6c                push dword ptr [esp + 108]
c010c16b: ff 74 24 28                push dword ptr [esp + 40]
c010c16f: e8 7f d3 ff ff             call 0xc01094f3 <PerformTransfer>
c010c174: 43                         inc ebx
c010c175: 83 c4 10                   add esp, 16
c010c178: 39 5c 24 0c                cmp dword ptr [esp + 12], ebx
c010c17c: 74 5b                      je 0xc010c1d9 <ReadWrite+0x34b>
c010c17e: 85 db                      test ebx, ebx
c010c180: 74 0c                      je 0xc010c18e <ReadWrite+0x300>
c010c182: 83 ec 0c                   sub esp, 12
c010c185: 55                         push ebp
c010c186: e8 9e fc ff ff             call 0xc010be29 <IdePoll>
c010c18b: 83 c4 10                   add esp, 16
c010c18e: 8b 44 24 24                mov eax, dword ptr [esp + 36]
c010c192: 89 44 24 10                mov dword ptr [esp + 16], eax
c010c196: 8b 44 24 30                mov eax, dword ptr [esp + 48]
c010c19a: 89 44 24 14                mov dword ptr [esp + 20], eax
c010c19e: 8b 4d 04                   mov ecx, dword ptr [ebp + 4]
c010c1a1: 89 c8                      mov eax, ecx
c010c1a3: d1 e8                      shr eax
c010c1a5: 89 44 24 28                mov dword ptr [esp + 40], eax
c010c1a9: 31 d2                      xor edx, edx
c010c1ab: 89 54 24 2c                mov dword ptr [esp + 44], edx
c010c1af: 39 44 24 10                cmp dword ptr [esp + 16], eax
c010c1b3: 8b 44 24 14                mov eax, dword ptr [esp + 20]
c010c1b7: 1b 44 24 2c                sbb eax, dword ptr [esp + 44]
c010c1bb: 73 a6                      jae 0xc010c163 <ReadWrite+0x2d5>
c010c1bd: 89 f2                      mov edx, esi
c010c1bf: 66 ed                      in ax, dx
c010c1c1: 8b 54 24 10                mov edx, dword ptr [esp + 16]
c010c1c5: 8b 4c 24 1c                mov ecx, dword ptr [esp + 28]
c010c1c9: 66 89 04 51                mov word ptr [ecx + 2*edx], ax
c010c1cd: 83 44 24 10 01             add dword ptr [esp + 16], 1
c010c1d2: 83 54 24 14 00             adc dword ptr [esp + 20], 0
c010c1d7: eb c5                      jmp 0xc010c19e <ReadWrite+0x310>
c010c1d9: 8b 44 24 0c                mov eax, dword ptr [esp + 12]
c010c1dd: 29 c7                      sub edi, eax
c010c1df: 01 44 24 18                add dword ptr [esp + 24], eax
c010c1e3: 85 ff                      test edi, edi
c010c1e5: 0f 8f d7 fd ff ff          jg 0xc010bfc2 <ReadWrite+0x134>
c010c1eb: 83 ec 0c                   sub esp, 12
c010c1ee: ff 35 68 b3 13 c0          push dword ptr [-1072450712]
c010c1f4: e8 ba a6 ff ff             call 0xc01068b3 <ReleaseSemaphore>
c010c1f9: 83 c4 10                   add esp, 16
c010c1fc: 31 db                      xor ebx, ebx
c010c1fe: eb 05                      jmp 0xc010c205 <ReadWrite+0x377>
c010c200: bb 07 00 00 00             mov ebx, 7
```

```
c010c246: 6a 00                     push 0
c010c248: e8 fb 90 ff ff            call 0xc0105348 <MapVirt>
c010c24d: 89 c2                     mov edx, eax
c010c24f: 31 f6                     xor esi, esi
c010c251: b9 1b 00 00 00            mov ecx, 27
c010c256: 89 df                     mov edi, ebx
c010c258: 89 f0                     mov eax, esi
c010c25a: f3 ab                     rep  stosd dword ptr es:[edi], eax
c010c25c: c7 43 04 00 02 00 00      mov dword ptr [ebx + 4], 512
c010c263: 89 53 10                  mov dword ptr [ebx + 16], edx
c010c266: c7 43 14 f0 01 00 00      mov dword ptr [ebx + 20], 496
c010c26d: c7 43 18 f6 03 00 00      mov dword ptr [ebx + 24], 1014
c010c274: c7 43 1c 70 01 00 00      mov dword ptr [ebx + 28], 368
c010c27b: c7 43 20 76 03 00 00      mov dword ptr [ebx + 32], 886
c010c282: 83 c4 18                  add esp, 24
c010c285: 6a ff                     push -1
c010c287: ff 35 68 b3 13 c0         push dword ptr [-1072450712]
c010c28d: e8 a7 a4 ff ff            call 0xc0106739 <AcquireSemaphore>
c010c292: 8a 03                     mov al, byte ptr [ebx]
c010c294: c1 e0 04                  shl eax, 4
c010c297: 83 e0 10                  and eax, 16
c010c29a: 83 c8 e0                  or eax, -32
c010c29d: bf f6 01 00 00            mov edi, 502
c010c2a2: 89 fa                     mov edx, edi
c010c2a4: ee                        out dx, al
c010c2a5: b0 f8                     mov al, -8
c010c2a7: ba f7 01 00 00            mov edx, 503
c010c2ac: ee                        out dx, al
c010c2ad: 89 1c 24                  mov dword ptr [esp], ebx
c010c2b0: e8 74 fb ff ff            call 0xc010be29 <IdePoll>
c010c2b5: ba f3 01 00 00            mov edx, 499
c010c2ba: ec                        in al, dx
c010c2bb: 0f b6 e8                  movzx ebp, al
c010c2be: ba f4 01 00 00            mov edx, 500
c010c2c3: ec                        in al, dx
c010c2c4: 0f b6 c8                  movzx ecx, al
c010c2c7: ba f5 01 00 00            mov edx, 501
c010c2cc: ec                        in al, dx
c010c2cd: c1 e1 08                  shl ecx, 8
c010c2d0: 0f b6 c0                  movzx eax, al
c010c2d3: c1 e0 10                  shl eax, 16
c010c2d6: 09 c1                     or ecx, eax
c010c2d8: 09 e9                     or ecx, ebp
c010c2da: 89 fa                     mov edx, edi
c010c2dc: ec                        in al, dx
c010c2dd: 89 c7                     mov edi, eax
c010c2df: c1 e7 18                  shl edi, 24
c010c2e2: 81 e7 00 00 00 0f         and edi, 251658240
c010c2e8: 09 cf                     or edi, ecx
c010c2ea: 59                        pop ecx
c010c2eb: ff 35 68 b3 13 c0         push dword ptr [-1072450712]
c010c2f1: e8 bd a5 ff ff            call 0xc01068b3 <ReleaseSemaphore>
c010c2f6: 89 7b 08                  mov dword ptr [ebx + 8], edi
c010c2f9: c1 ff 1f                  sar edi, 31
c010c2fc: 89 7b 0c                  mov dword ptr [ebx + 12], edi
c010c2ff: 8d 7c 24 20               lea edi, [esp + 32]
c010c303: b9 0e 00 00 00            mov ecx, 14
c010c308: 89 f0                     mov eax, esi
c010c30a: f3 ab                     rep  stosd dword ptr es:[edi], eax
c010c30c: e8 bb d7 ff ff            call 0xc0109acc <NextDevId>
c010c311: 89 44 24 18               mov dword ptr [esp + 24], eax
c010c315: c1 f8 1f                  sar eax, 31
c010c318: 89 44 24 1c               mov dword ptr [esp + 28], eax
c010c31c: c7 44 24 24 ff 81 00 00   mov dword ptr [esp + 36], 33279
c010c324: c7 44 24 28 01 00 00 00   mov dword ptr [esp + 40], 1
c010c32c: 8b 53 08                  mov edx, dword ptr [ebx + 8]
c010c32f: 8b 43 04                  mov eax, dword ptr [ebx + 4]
c010c332: 89 d1                     mov ecx, edx
c010c334: 0f af c8                  imul ecx, eax
c010c337: 89 4c 24 3c               mov dword ptr [esp + 60], ecx
c010c33b: 89 54 24 58               mov dword ptr [esp + 88], edx
```

```
c010c398: 6a 00                         push 0
c010c39a: 56                            push esi
c010c39b: e8 ad cf ff ff                call 0xc010934d <CreateFile>
c010c3a0: 83 c4 14                      add esp, 20
c010c3a3: 50                            push eax
c010c3a4: e8 28 5f ff ff                call 0xc01022d1 <CreateDiskCache>
c010c3a9: 89 04 24                      mov dword ptr [esp], eax
c010c3ac: e8 55 ca ff ff                call 0xc0108e06 <CreateDiskPartitions>
c010c3b1: 83 c4 6c                      add esp, 108
c010c3b4: 5b                            pop ebx
c010c3b5: 5e                            pop esi
c010c3b6: 5f                            pop edi
c010c3b7: 5d                            pop ebp
c010c3b8: c3                            ret

c010c3b9 <Loadx86Driver>:
c010c3b9: 56                            push esi
c010c3ba: 53                            push ebx
c010c3bb: 83 ec 10                      sub esp, 16
c010c3be: 89 c3                         mov ebx, eax
c010c3c0: 89 d6                         mov esi, edx
c010c3c2: 50                            push eax
c010c3c3: e8 90 c1 ff ff                call 0xc0108558 <RequireDriver>
c010c3c8: 83 c4 10                      add esp, 16
c010c3cb: 85 c0                         test eax, eax
c010c3cd: 74 0a                         je 0xc010c3d9 <Loadx86Driver+0x20>
c010c3cf: 51                            push ecx
c010c3d0: 51                            push ecx
c010c3d1: 53                            push ebx
c010c3d2: 6a 1e                         push 30
c010c3d4: e8 75 c7 ff ff                call 0xc0108b4e <PanicEx>
c010c3d9: 83 ec 0c                      sub esp, 12
c010c3dc: 56                            push esi
c010c3dd: e8 26 c1 ff ff                call 0xc0108508 <GetSymbolAddress>
c010c3e2: 83 c4 10                      add esp, 16
c010c3e5: 85 c0                         test eax, eax
c010c3e7: 75 0c                         jne 0xc010c3f5 <Loadx86Driver+0x3c>
c010c3e9: 83 ec 0c                      sub esp, 12
c010c3ec: 53                            push ebx
c010c3ed: e8 af bf ff ff                call 0xc01083a1 <GetDriverAddress>
c010c3f2: 83 c4 10                      add esp, 16
c010c3f5: 5a                            pop edx
c010c3f6: 5b                            pop ebx
c010c3f7: 5e                            pop esi
c010c3f8: c3                            ret

c010c3f9 <LoadSlowDriversInBackground>:
c010c3f9: 83 ec 0c                      sub esp, 12
c010c3fc: ba f2 1b 11 c0                mov edx, 3222346738
c010c401: b8 fd 1b 11 c0                mov eax, 3222346749
c010c406: e8 ae ff ff ff                call 0xc010c3b9 <Loadx86Driver>
c010c40b: 83 c4 0c                      add esp, 12
c010c40e: ff e0                         jmp eax

c010c410 <ArchInitDev>:
c010c410: 55                            push ebp
c010c411: 57                            push edi
c010c412: 56                            push esi
c010c413: 83 ec 50                      sub esp, 80
c010c416: 80 7c 24 60 00                cmp byte ptr [esp + 96], 0
c010c41b: 0f 85 b6 00 00 00             jne 0xc010c4d7 <ArchInitDev+0xc7>
c010c421: 8d 44 24 1f                   lea eax, [esp + 31]
c010c425: 83 ec 0c                      sub esp, 12
c010c428: 50                            push eax
c010c429: e8 0d 6c ff ff                call 0xc010303b <GetBootInformation>
c010c42e: 83 c4 0c                      add esp, 12
c010c431: e8 d9 fd ff ff                call 0xc010c20f <InitIde>
c010c436: 80 7c 24 4f 00                cmp byte ptr [esp + 79], 0
c010c43b: 74 05                         je 0xc010c442 <ArchInitDev+0x32>
c010c43d: e8 78 f7 ff ff                call 0xc010bbba <InitFloppy>
c010c442: 50                            push eax
```

```
c010c487: ff 74 24 28                   push dword ptr [esp + 40]
c010c48b: 0f b6 44 24 28                movzx eax, byte ptr [esp + 40]
c010c490: 50                            push eax
c010c491: 0f b6 44 24 2b                movzx eax, byte ptr [esp + 43]
c010c496: 50                            push eax
c010c497: 0f b6 44 24 2c                movzx eax, byte ptr [esp + 44]
c010c49c: 50                            push eax
c010c49d: 0f b6 44 24 31                movzx eax, byte ptr [esp + 49]
c010c4a2: 50                            push eax
c010c4a3: 0f b6 44 24 36                movzx eax, byte ptr [esp + 54]
c010c4a8: 50                            push eax
c010c4a9: 68 2e 1c 11 c0                push 3222346798
c010c4ae: e8 12 c6 ff ff                call 0xc0108ac5 <LogWriteSerial>
c010c4b3: 83 c4 20                      add esp, 32
c010c4b6: b9 04 00 00 00                mov ecx, 4
c010c4bb: 89 e7                         mov edi, esp
c010c4bd: 89 ee                         mov esi, ebp
c010c4bf: f3 a5                         rep  movsd dword ptr es:[edi], dword ptr [esi
c010c4c1: e8 8e 4e ff ff                call 0xc0101354 <TimeStructToValue>
c010c4c6: 83 c4 0c                      add esp, 12
c010c4c9: 52                            push edx
c010c4ca: 50                            push eax
c010c4cb: 68 40 1c 11 c0                push 3222346816
c010c4d0: e8 f0 c5 ff ff                call 0xc0108ac5 <LogWriteSerial>
c010c4d5: eb 39                         jmp 0xc010c510 <ArchInitDev+0x100>
c010c4d7: ba 5e 1c 11 c0                mov edx, 3222346846
c010c4dc: b8 66 1c 11 c0                mov eax, 3222346854
c010c4e1: e8 d3 fe ff ff                call 0xc010c3b9 <Loadx86Driver>
c010c4e6: ff d0                         call eax
c010c4e8: ba 73 1c 11 c0                mov edx, 3222346867
c010c4ed: b8 7b 1c 11 c0                mov eax, 3222346875
c010c4f2: e8 c2 fe ff ff                call 0xc010c3b9 <Loadx86Driver>
c010c4f7: ff d0                         call eax
c010c4f9: e8 7b 81 ff ff                call 0xc0104679 <GetVas>
c010c4fe: 68 88 1c 11 c0                push 3222346888
c010c503: 50                            push eax
c010c504: 6a 00                         push 0
c010c506: 68 f9 c3 10 c0                push 3222324217
c010c50b: e8 38 b4 ff ff                call 0xc0107948 <CreateThread>
c010c510: 83 c4 10                      add esp, 16
c010c513: 83 c4 50                      add esp, 80
c010c516: 5e                            pop esi
c010c517: 5f                            pop edi
c010c518: 5d                            pop ebp
c010c519: c3                            ret

c010c51a <IsPicIrqSpurious>:
c010c51a: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c010c51e: 83 f8 27                      cmp eax, 39
c010c521: 75 20                         jne 0xc010c543 <IsPicIrqSpurious+0x29>
c010c523: b0 0b                         mov al, 11
c010c525: e6 20                         out 32, al
c010c527: e6 a0                         out 160, al
c010c529: e4 a0                         in al, 160
c010c52b: 88 c2                         mov dl, al
c010c52d: e4 20                         in al, 32
c010c52f: c1 e2 08                      shl edx, 8
c010c532: 0f b6 c0                      movzx eax, al
c010c535: 09 c2                         or edx, eax
c010c537: 66 c1 ea 07                   shr dx, 7
c010c53b: 83 f2 01                      xor edx, 1
c010c53e: 83 e2 01                      and edx, 1
c010c541: eb 1e                         jmp 0xc010c561 <IsPicIrqSpurious+0x47>
c010c543: 31 d2                         xor edx, edx
c010c545: 83 f8 2f                      cmp eax, 47
c010c548: 75 17                         jne 0xc010c561 <IsPicIrqSpurious+0x47>
c010c54a: b0 0b                         mov al, 11
c010c54c: e6 20                         out 32, al
c010c54e: e6 a0                         out 160, al
c010c550: e4 a0                         in al, 160
c010c552: 88 c1                         mov cl, al
```

```
c010c593 <InitPic>:
c010c593: e4 21                         in al, 33
c010c595: 88 c1                         mov cl, al
c010c597: e4 a1                         in al, 161
c010c599: 88 c2                         mov dl, al
c010c59b: b0 11                         mov al, 17
c010c59d: e6 20                         out 32, al
c010c59f: 90                            nop
c010c5a0: e6 a0                         out 160, al
c010c5a2: 90                            nop
c010c5a3: b0 20                         mov al, 32
c010c5a5: e6 21                         out 33, al
c010c5a7: 90                            nop
c010c5a8: b0 28                         mov al, 40
c010c5aa: e6 a1                         out 161, al
c010c5ac: 90                            nop
c010c5ad: b0 04                         mov al, 4
c010c5af: e6 21                         out 33, al
c010c5b1: 90                            nop
c010c5b2: b0 02                         mov al, 2
c010c5b4: e6 a1                         out 161, al
c010c5b6: 90                            nop
c010c5b7: b0 01                         mov al, 1
c010c5b9: e6 21                         out 33, al
c010c5bb: 90                            nop
c010c5bc: e6 a1                         out 161, al
c010c5be: 90                            nop
c010c5bf: 88 c8                         mov al, cl
c010c5c1: e6 21                         out 33, al
c010c5c3: 88 d0                         mov al, dl
c010c5c5: e6 a1                         out 161, al
c010c5c7: 6a 00                         push 0
c010c5c9: e8 a6 ff ff ff                call 0xc010c574 <DisablePicLines>
c010c5ce: 58                            pop eax
c010c5cf: c3                            ret

c010c5d0 <HandlePit>:
c010c5d0: 83 ec 14                      sub esp, 20
c010c5d3: ff 35 74 b3 13 c0             push dword ptr [-1072450700]
c010c5d9: ff 35 70 b3 13 c0             push dword ptr [-1072450704]
c010c5df: e8 d4 b6 ff ff                call 0xc0107cb8 <ReceivedTimer>
c010c5e4: 31 c0                         xor eax, eax
c010c5e6: 83 c4 1c                      add esp, 28
c010c5e9: c3                            ret

c010c5ea <InitPit>:
c010c5ea: 53                            push ebx
c010c5eb: 83 ec 08                      sub esp, 8
c010c5ee: 8b 5c 24 10                   mov ebx, dword ptr [esp + 16]
c010c5f2: b8 dc 34 12 00                mov eax, 1193180
c010c5f7: 99                            cdq
c010c5f8: f7 fb                         idiv ebx
c010c5fa: 89 c1                         mov ecx, eax
c010c5fc: b0 36                         mov al, 54
c010c5fe: e6 43                         out 67, al
c010c600: 88 c8                         mov al, cl
c010c602: e6 40                         out 64, al
c010c604: 89 c8                         mov eax, ecx
c010c606: c1 f8 08                      sar eax, 8
c010c609: e6 40                         out 64, al
c010c60b: 89 d8                         mov eax, ebx
c010c60d: 99                            cdq
c010c60e: 52                            push edx
c010c60f: 53                            push ebx
c010c610: 6a 00                         push 0
c010c612: 68 00 ca 9a 3b                push 1000000000
c010c617: e8 34 28 00 00                call 0xc010ee50 <__udivdi3>
c010c61c: 59                            pop ecx
c010c61d: 5b                            pop ebx
c010c61e: a3 70 b3 13 c0                mov dword ptr [3222516592], eax
c010c623: 89 15 74 b3 13 c0             mov dword ptr [-1072450700], edx
```

```
c010c689: 88 46 04                      mov byte ptr [esi + 4], al
c010c68c: c7 04 24 09 00 00 00          mov dword ptr [esp], 9
c010c693: e8 3c ec ff ff                call 0xc010b2d4 <ReadCmos>
c010c698: 0f b6 c0                      movzx eax, al
c010c69b: 89 46 08                      mov dword ptr [esi + 8], eax
c010c69e: c7 04 24 0b 00 00 00          mov dword ptr [esp], 11
c010c6a5: e8 2a ec ff ff                call 0xc010b2d4 <ReadCmos>
c010c6aa: 88 c3                         mov bl, al
c010c6ac: 89 c7                         mov edi, eax
c010c6ae: 83 e7 02                      and edi, 2
c010c6b1: 83 c4 10                      add esp, 16
c010c6b4: 80 e3 04                      and bl, 4
c010c6b7: 75 72                         jne 0xc010c72b <ReadTimeState+0xf1>
c010c6b9: 8a 0e                         mov cl, byte ptr [esi]
c010c6bb: 88 c8                         mov al, cl
c010c6bd: c0 e8 04                      shr al, 4
c010c6c0: b2 0a                         mov dl, 10
c010c6c2: f6 e2                         mul dl
c010c6c4: 83 e1 0f                      and ecx, 15
c010c6c7: 01 c8                         add eax, ecx
c010c6c9: 88 06                         mov byte ptr [esi], al
c010c6cb: 8a 4e 01                      mov cl, byte ptr [esi + 1]
c010c6ce: 88 c8                         mov al, cl
c010c6d0: c0 e8 04                      shr al, 4
c010c6d3: f6 e2                         mul dl
c010c6d5: 83 e1 0f                      and ecx, 15
c010c6d8: 01 c8                         add eax, ecx
c010c6da: 88 46 01                      mov byte ptr [esi + 1], al
c010c6dd: 8a 4e 02                      mov cl, byte ptr [esi + 2]
c010c6e0: 88 c8                         mov al, cl
c010c6e2: c0 e8 04                      shr al, 4
c010c6e5: 83 e0 07                      and eax, 7
c010c6e8: f6 e2                         mul dl
c010c6ea: 83 e1 0f                      and ecx, 15
c010c6ed: 01 c8                         add eax, ecx
c010c6ef: 88 46 02                      mov byte ptr [esi + 2], al
c010c6f2: 8a 4e 03                      mov cl, byte ptr [esi + 3]
c010c6f5: 88 c8                         mov al, cl
c010c6f7: c0 e8 04                      shr al, 4
c010c6fa: f6 e2                         mul dl
c010c6fc: 83 e1 0f                      and ecx, 15
c010c6ff: 01 c8                         add eax, ecx
c010c701: 88 46 03                      mov byte ptr [esi + 3], al
c010c704: 8a 4e 04                      mov cl, byte ptr [esi + 4]
c010c707: 88 c8                         mov al, cl
c010c709: c0 e8 04                      shr al, 4
c010c70c: f6 e2                         mul dl
c010c70e: 83 e1 0f                      and ecx, 15
c010c711: 01 c8                         add eax, ecx
c010c713: 88 46 04                      mov byte ptr [esi + 4], al
c010c716: 8b 4e 08                      mov ecx, dword ptr [esi + 8]
c010c719: 88 c8                         mov al, cl
c010c71b: c0 e8 04                      shr al, 4
c010c71e: f6 e2                         mul dl
c010c720: 83 e1 0f                      and ecx, 15
c010c723: 01 c8                         add eax, ecx
c010c725: 0f b6 c0                      movzx eax, al
c010c728: 89 46 08                      mov dword ptr [esi + 8], eax
c010c72b: 89 f8                         mov eax, edi
c010c72d: 84 c0                         test al, al
c010c72f: 75 16                         jne 0xc010c747 <ReadTimeState+0x10d>
c010c731: 0f b6 46 02                   movzx eax, byte ptr [esi + 2]
c010c735: 3c 0c                         cmp al, 12
c010c737: 74 09                         je 0xc010c742 <ReadTimeState+0x108>
c010c739: 84 c0                         test al, al
c010c73b: 79 07                         jns 0xc010c744 <ReadTimeState+0x10a>
c010c73d: 83 c0 0c                      add eax, 12
c010c740: eb 02                         jmp 0xc010c744 <ReadTimeState+0x10a>
c010c742: 31 c0                         xor eax, eax
c010c744: 88 46 02                      mov byte ptr [esi + 2], al
c010c747: 8b 56 08                      mov edx, dword ptr [esi + 8]
```

```
c010c79e: 68 92 1c 11 c0                push 3222346898
c010c7a3: e8 35 c3 ff ff                call 0xc0108add <LogDeveloperWarning>
c010c7a8: 83 c4 10                      add esp, 16
c010c7ab: 89 da                         mov edx, ebx
c010c7ad: 6b d2 64                      imul edx, edx, 100
c010c7b0: 01 56 08                      add dword ptr [esi + 8], edx
c010c7b3: 5b                            pop ebx
c010c7b4: 5e                            pop esi
c010c7b5: 5f                            pop edi
c010c7b6: c3                            ret

c010c7b7 <ArchGetUtcTime>:
c010c7b7: 55                            push ebp
c010c7b8: 57                            push edi
c010c7b9: 56                            push esi
c010c7ba: 53                            push ebx
c010c7bb: 83 ec 5c                      sub esp, 92
c010c7be: 8b 44 24 70                   mov eax, dword ptr [esp + 112]
c010c7c2: 8b 54 24 74                   mov edx, dword ptr [esp + 116]
c010c7c6: 89 04 24                      mov dword ptr [esp], eax
c010c7c9: 89 54 24 04                   mov dword ptr [esp + 4], edx
c010c7cd: 83 ec 0c                      sub esp, 12
c010c7d0: 6a 0a                         push 10
c010c7d2: e8 fd ea ff ff                call 0xc010b2d4 <ReadCmos>
c010c7d7: 83 c4 10                      add esp, 16
c010c7da: 84 c0                         test al, al
c010c7dc: 78 ef                         js 0xc010c7cd <ArchGetUtcTime+0x16>
c010c7de: 8d 44 24 10                   lea eax, [esp + 16]
c010c7e2: e8 53 fe ff ff                call 0xc010c63a <ReadTimeState>
c010c7e7: 8d 7c 24 20                   lea edi, [esp + 32]
c010c7eb: 8d 74 24 10                   lea esi, [esp + 16]
c010c7ef: b9 04 00 00 00                mov ecx, 4
c010c7f4: f3 a5                         rep  movsd dword ptr es:[edi], dword ptr [esi
c010c7f6: 8a 5c 24 14                   mov bl, byte ptr [esp + 20]
c010c7fa: 8b 6c 24 18                   mov ebp, dword ptr [esp + 24]
c010c7fe: 83 ec 0c                      sub esp, 12
c010c801: 6a 0a                         push 10
c010c803: e8 cc ea ff ff                call 0xc010b2d4 <ReadCmos>
c010c808: 83 c4 10                      add esp, 16
c010c80b: 84 c0                         test al, al
c010c80d: 78 ef                         js 0xc010c7fe <ArchGetUtcTime+0x47>
c010c80f: 8d 44 24 10                   lea eax, [esp + 16]
c010c813: e8 22 fe ff ff                call 0xc010c63a <ReadTimeState>
c010c818: 8d 7c 24 30                   lea edi, [esp + 48]
c010c81c: b9 04 00 00 00                mov ecx, 4
c010c821: 8d 74 24 10                   lea esi, [esp + 16]
c010c825: f3 a5                         rep  movsd dword ptr es:[edi], dword ptr [esi
c010c827: 0f b6 44 24 14                movzx eax, byte ptr [esp + 20]
c010c82c: 8b 54 24 18                   mov edx, dword ptr [esp + 24]
c010c830: 8d 7c 24 40                   lea edi, [esp + 64]
c010c834: 8d 74 24 20                   lea esi, [esp + 32]
c010c838: b9 04 00 00 00                mov ecx, 4
c010c83d: f3 a5                         rep  movsd dword ptr es:[edi], dword ptr [esi
c010c83f: 8b 74 24 40                   mov esi, dword ptr [esp + 64]
c010c843: 39 74 24 30                   cmp dword ptr [esp + 48], esi
c010c847: 0f 94 44 24 0f                sete byte ptr [esp + 15]
c010c84c: 38 d8                         cmp al, bl
c010c84e: 0f 94 c1                      sete cl
c010c851: 84 4c 24 0f                   test byte ptr [esp + 15], cl
c010c855: 74 90                         je 0xc010c7e7 <ArchGetUtcTime+0x30>
c010c857: 39 ea                         cmp edx, ebp
c010c859: 75 8c                         jne 0xc010c7e7 <ArchGetUtcTime+0x30>
c010c85b: 51                            push ecx
c010c85c: 52                            push edx
c010c85d: 50                            push eax
c010c85e: 0f b6 44 24 1f                movzx eax, byte ptr [esp + 31]
c010c863: 50                            push eax
c010c864: 0f b6 44 24 20                movzx eax, byte ptr [esp + 32]
c010c869: 50                            push eax
c010c86a: 0f b6 44 24 25                movzx eax, byte ptr [esp + 37]
c010c86f: 50                            push eax
```

```
c010c8cb: 89 44 24 08                mov dword ptr [esp + 8], eax
c010c8cf: 89 54 24 0c                mov dword ptr [esp + 12], edx
c010c8d3: 8d 44 24 40                lea eax, [esp + 64]
c010c8d7: 52                         push edx
c010c8d8: ff 74 24 10                push dword ptr [esp + 16]
c010c8dc: ff 74 24 10                push dword ptr [esp + 16]
c010c8e0: 50                         push eax
c010c8e1: e8 90 4b ff ff             call 0xc0101476 <TimeValueToStruct>
c010c8e6: 8a 44 24 4c                mov al, byte ptr [esp + 76]
c010c8ea: 88 44 24 35                mov byte ptr [esp + 53], al
c010c8ee: 8a 44 24 4d                mov al, byte ptr [esp + 77]
c010c8f2: 88 44 24 34                mov byte ptr [esp + 52], al
c010c8f6: 8a 44 24 4e                mov al, byte ptr [esp + 78]
c010c8fa: 88 44 24 2a                mov byte ptr [esp + 42], al
c010c8fe: 8a 44 24 4f                mov al, byte ptr [esp + 79]
c010c902: 88 44 24 2b                mov byte ptr [esp + 43], al
c010c906: 8a 44 24 50                mov al, byte ptr [esp + 80]
c010c90a: 88 44 24 1f                mov byte ptr [esp + 31], al
c010c90e: 8b 44 24 4c                mov eax, dword ptr [esp + 76]
c010c912: 89 44 24 44                mov dword ptr [esp + 68], eax
c010c916: 8b 44 24 54                mov eax, dword ptr [esp + 84]
c010c91a: 89 44 24 20                mov dword ptr [esp + 32], eax
c010c91e: 0f b6 44 24 2a             movzx eax, byte ptr [esp + 42]
c010c923: 89 44 24 24                mov dword ptr [esp + 36], eax
c010c927: 83 c4 0c                   add esp, 12
c010c92a: b9 0c 00 00 00             mov ecx, 12
c010c92f: 99                         cdq
c010c930: f7 f9                      idiv ecx
c010c932: 85 d2                      test edx, edx
c010c934: 75 05                      jne 0xc010c93b <ArchSetUtcTime+0x96>
c010c936: ba 0c 00 00 00             mov edx, 12
c010c93b: 88 54 24 2b                mov byte ptr [esp + 43], dl
c010c93f: bf 64 00 00 00             mov edi, 100
c010c944: 8b 44 24 14                mov eax, dword ptr [esp + 20]
c010c948: 99                         cdq
c010c949: f7 ff                      idiv edi
c010c94b: 89 54 24 24                mov dword ptr [esp + 36], edx
c010c94f: 89 44 24 20                mov dword ptr [esp + 32], eax
c010c953: b2 0a                      mov dl, 10
c010c955: 0f b6 44 24 20             movzx eax, byte ptr [esp + 32]
c010c95a: f6 f2                      div dl
c010c95c: 88 c1                      mov cl, al
c010c95e: c1 e1 04                   shl ecx, 4
c010c961: 00 e1                      add cl, ah
c010c963: 0f b6 c1                   movzx eax, cl
c010c966: 89 44 24 30                mov dword ptr [esp + 48], eax
c010c96a: 0f b6 44 24 29             movzx eax, byte ptr [esp + 41]
c010c96f: f6 f2                      div dl
c010c971: 88 c1                      mov cl, al
c010c973: c1 e1 04                   shl ecx, 4
c010c976: 00 e1                      add cl, ah
c010c978: 88 4c 24 37                mov byte ptr [esp + 55], cl
c010c97c: 0f b6 44 24 28             movzx eax, byte ptr [esp + 40]
c010c981: f6 f2                      div dl
c010c983: 88 c1                      mov cl, al
c010c985: c1 e1 04                   shl ecx, 4
c010c988: 00 e1                      add cl, ah
c010c98a: 88 4c 24 36                mov byte ptr [esp + 54], cl
c010c98e: 0f b6 44 24 1f             movzx eax, byte ptr [esp + 31]
c010c993: f6 f2                      div dl
c010c995: 88 c1                      mov cl, al
c010c997: c1 e1 04                   shl ecx, 4
c010c99a: 00 e1                      add cl, ah
c010c99c: 88 4c 24 35                mov byte ptr [esp + 53], cl
c010c9a0: 0f b6 44 24 13             movzx eax, byte ptr [esp + 19]
c010c9a5: f6 f2                      div dl
c010c9a7: 88 c1                      mov cl, al
c010c9a9: c1 e1 04                   shl ecx, 4
c010c9ac: 00 e1                      add cl, ah
c010c9ae: 88 4c 24 34                mov byte ptr [esp + 52], cl
c010c9b2: 0f b6 44 24 24             movzx eax, byte ptr [esp + 36]
```

```
c010ca0f: 55                    push ebp
c010ca10: 0f b6 d2              movzx edx, dl
c010ca13: 52                    push edx
c010ca14: 0f b6 c0              movzx eax, al
c010ca17: 50                    push eax
c010ca18: e8 f4 e8 ff ff        call 0xc010b311 <WriteCmos>
c010ca1d: 83 c4 10              add esp, 16
c010ca20: 89 f0                 mov eax, esi
c010ca22: 84 c0                 test al, al
c010ca24: 75 27                 jne 0xc010ca4d <ArchSetUtcTime+0x1a8>
c010ca26: b2 0a                 mov dl, 10
c010ca28: 0f b6 c3              movzx eax, bl
c010ca2b: f6 f2                 div dl
c010ca2d: 88 c3                 mov bl, al
c010ca2f: c1 e3 04              shl ebx, 4
c010ca32: 00 e3                 add bl, ah
c010ca34: 8b 44 24 2c           mov eax, dword ptr [esp + 44]
c010ca38: 8b 74 24 34           mov esi, dword ptr [esp + 52]
c010ca3c: 0f b6 7c 24 35        movzx edi, byte ptr [esp + 53]
c010ca41: 0f b6 6c 24 36        movzx ebp, byte ptr [esp + 54]
c010ca46: 0f b6 54 24 37        movzx edx, byte ptr [esp + 55]
c010ca4b: eb 17                 jmp 0xc010ca64 <ArchSetUtcTime+0x1bf>
c010ca4d: 8b 44 24 24           mov eax, dword ptr [esp + 36]
c010ca51: 0f b6 74 24 13        movzx esi, byte ptr [esp + 19]
c010ca56: 0f b6 7c 24 1f        movzx edi, byte ptr [esp + 31]
c010ca5b: 8b 6c 24 28           mov ebp, dword ptr [esp + 40]
c010ca5f: 0f b6 54 24 29        movzx edx, byte ptr [esp + 41]
c010ca64: 89 44 24 3c           mov dword ptr [esp + 60], eax
c010ca68: 8a 4c 24 2a           mov cl, byte ptr [esp + 42]
c010ca6c: c1 e1 07              shl ecx, 7
c010ca6f: 09 cb                 or ebx, ecx
c010ca71: 50                    push eax
c010ca72: 50                    push eax
c010ca73: 52                    push edx
c010ca74: 6a 00                 push 0
c010ca76: e8 96 e8 ff ff        call 0xc010b311 <WriteCmos>
c010ca7b: 58                    pop eax
c010ca7c: 5a                    pop edx
c010ca7d: 89 e8                 mov eax, ebp
c010ca7f: 0f b6 e8              movzx ebp, al
c010ca82: 55                    push ebp
c010ca83: 6a 02                 push 2
c010ca85: e8 87 e8 ff ff        call 0xc010b311 <WriteCmos>
c010ca8a: 59                    pop ecx
c010ca8b: 5d                    pop ebp
c010ca8c: 0f b6 db              movzx ebx, bl
c010ca8f: 53                    push ebx
c010ca90: 6a 04                 push 4
c010ca92: e8 7a e8 ff ff        call 0xc010b311 <WriteCmos>
c010ca97: 58                    pop eax
c010ca98: 5a                    pop edx
c010ca99: 89 f8                 mov eax, edi
c010ca9b: 0f b6 f8              movzx edi, al
c010ca9e: 57                    push edi
c010ca9f: 6a 07                 push 7
c010caa1: e8 6b e8 ff ff        call 0xc010b311 <WriteCmos>
c010caa6: 59                    pop ecx
c010caa7: 5b                    pop ebx
c010caa8: 89 f0                 mov eax, esi
c010caaa: 0f b6 f0              movzx esi, al
c010caad: 56                    push esi
c010caae: 6a 08                 push 8
c010cab0: e8 5c e8 ff ff        call 0xc010b311 <WriteCmos>
c010cab5: 5e                    pop esi
c010cab6: 5f                    pop edi
c010cab7: 8b 44 24 44           mov eax, dword ptr [esp + 68]
c010cabb: 0f b6 c0              movzx eax, al
c010cabe: 50                    push eax
c010cabf: 6a 09                 push 9
c010cac1: e8 4b e8 ff ff        call 0xc010b311 <WriteCmos>
c010cac6: 8d 5c 24 60           lea ebx, [esp + 96]
```

```
c010cb38: 50                    push eax
c010cb39: ff 74 24 14           push dword ptr [esp + 20]
c010cb3d: ff 74 24 14           push dword ptr [esp + 20]
c010cb41: e8 98 4a ff ff        call 0xc01015de <GetWeekday>
c010cb46: 5a                    pop edx
c010cb47: 59                    pop ecx
c010cb48: 0f b6 c0              movzx eax, al
c010cb4b: 50                    push eax
c010cb4c: 6a 06                 push 6
c010cb4e: e8 be e7 ff ff        call 0xc010b311 <WriteCmos>
c010cb53: 5b                    pop ebx
c010cb54: 5e                    pop esi
c010cb55: ff 74 24 14           push dword ptr [esp + 20]
c010cb59: ff 74 24 14           push dword ptr [esp + 20]
c010cb5d: e8 7c 4a ff ff        call 0xc01015de <GetWeekday>
c010cb62: 5f                    pop edi
c010cb63: 5d                    pop ebp
c010cb64: 50                    push eax
c010cb65: 68 e8 1c 11 c0        push 3222346984
c010cb6a: e8 56 bf ff ff        call 0xc0108ac5 <LogWriteSerial>
c010cb6f: 31 c0                 xor eax, eax
c010cb71: 81 c4 9c 00 00 00     add esp, 156
c010cb77: 5b                    pop ebx
c010cb78: 5e                    pop esi
c010cb79: 5f                    pop edi
c010cb7a: 5d                    pop ebp
c010cb7b: c3                    ret

c010cb7c <ArchLoadDriver>:
c010cb7c: 55                    push ebp
c010cb7d: 57                    push edi
c010cb7e: 56                    push esi
c010cb7f: 53                    push ebx
c010cb80: 83 ec 44              sub esp, 68
c010cb83: 8b 44 24 5c           mov eax, dword ptr [esp + 92]
c010cb87: 8b 40 30              mov eax, dword ptr [eax + 48]
c010cb8a: 8b 40 70              mov eax, dword ptr [eax + 112]
c010cb8d: 89 44 24 24           mov dword ptr [esp + 36], eax
c010cb91: 6a 00                 push 0
c010cb93: ff 74 24 60           push dword ptr [esp + 96]
c010cb97: 6a 21                 push 33
c010cb99: ff 74 24 30           push dword ptr [esp + 48]
c010cb9d: 6a 00                 push 0
c010cb9f: 6a 00                 push 0
c010cba1: e8 a2 87 ff ff        call 0xc0105348 <MapVirt>
c010cba6: 89 c5                 mov ebp, eax
c010cba8: 83 c4 20              add esp, 32
c010cbab: 83 7c 24 5c 00        cmp dword ptr [esp + 92], 0
c010cbb0: 74 0f                 je 0xc010cbc1 <ArchLoadDriver+0x45>
c010cbb2: 8b 44 24 50           mov eax, dword ptr [esp + 80]
c010cbb6: 8b 00                 mov eax, dword ptr [eax]
c010cbb8: 03 45 18              add eax, dword ptr [ebp + 24]
c010cbbb: 8b 4c 24 5c           mov ecx, dword ptr [esp + 92]
c010cbbf: 89 01                 mov dword ptr [ecx], eax
c010cbc1: 80 7d 00 7f           cmp byte ptr [ebp], 127
c010cbc5: 75 06                 jne 0xc010cbcd <ArchLoadDriver+0x51>
c010cbc7: 80 7d 01 45           cmp byte ptr [ebp + 1], 69
c010cbcb: 74 0a                 je 0xc010cbd7 <ArchLoadDriver+0x5b>
c010cbcd: b8 07 00 00 00        mov eax, 7
c010cbd2: e9 cd 05 00 00        jmp 0xc010d1a4 <ArchLoadDriver+0x628>
c010cbd7: 80 7d 02 4c           cmp byte ptr [ebp + 2], 76
c010cbdb: 75 f0                 jne 0xc010cbcd <ArchLoadDriver+0x51>
c010cbdd: 80 7d 03 46           cmp byte ptr [ebp + 3], 70
c010cbe1: 75 ea                 jne 0xc010cbcd <ArchLoadDriver+0x51>
c010cbe3: 66 83 7d 30 00        cmp word ptr [ebp + 48], 0
c010cbe8: 74 e3                 je 0xc010cbcd <ArchLoadDriver+0x51>
c010cbea: 0f b7 45 2c           movzx eax, word ptr [ebp + 44]
c010cbee: 66 85 c0              test ax, ax
c010cbf1: 74 da                 je 0xc010cbcd <ArchLoadDriver+0x51>
c010cbf3: 8b 4d 1c              mov ecx, dword ptr [ebp + 28]
c010cbf6: 01 e9                 add ecx, ebp
```

```
c010cc47: e8 fc 86 ff ff              call 0xc0105348 <MapVirt>
c010cc4c: 89 44 24 28                 mov dword ptr [esp + 40], eax
c010cc50: 8b 44 24 70                 mov eax, dword ptr [esp + 112]
c010cc54: 8b 4c 24 28                 mov ecx, dword ptr [esp + 40]
c010cc58: 89 08                       mov dword ptr [eax], ecx
c010cc5a: 83 c4 20                    add esp, 32
c010cc5d: 83 7c 24 5c 00              cmp dword ptr [esp + 92], 0
c010cc62: 0f 95 44 24 20              setne byte ptr [esp + 32]
c010cc67: 0f 95 c0                    setne al
c010cc6a: 0f b6 c0                    movzx eax, al
c010cc6d: 01 c0                       add eax, eax
c010cc6f: 89 44 24 24                 mov dword ptr [esp + 36], eax
c010cc73: 8b 45 1c                    mov eax, dword ptr [ebp + 28]
c010cc76: 01 e8                       add eax, ebp
c010cc78: 89 44 24 04                 mov dword ptr [esp + 4], eax
c010cc7c: 31 db                       xor ebx, ebx
c010cc7e: 89 5c 24 14                 mov dword ptr [esp + 20], ebx
c010cc82: 0f b7 45 2c                 movzx eax, word ptr [ebp + 44]
c010cc86: 39 44 24 14                 cmp dword ptr [esp + 20], eax
c010cc8a: 0f 8d 97 01 00 00           jge 0xc010ce27 <ArchLoadDriver+0x2ab>
c010cc90: 8b 44 24 04                 mov eax, dword ptr [esp + 4]
c010cc94: 83 38 01                    cmp dword ptr [eax], 1
c010cc97: 0f 85 7c 01 00 00           jne 0xc010ce19 <ArchLoadDriver+0x29d>
c010cc9d: 8b 40 04                    mov eax, dword ptr [eax + 4]
c010cca0: 89 44 24 0c                 mov dword ptr [esp + 12], eax
c010cca4: 8b 44 24 04                 mov eax, dword ptr [esp + 4]
c010cca8: 8b 40 10                    mov eax, dword ptr [eax + 16]
c010ccab: 89 44 24 10                 mov dword ptr [esp + 16], eax
c010ccaf: 8b 44 24 04                 mov eax, dword ptr [esp + 4]
c010ccb3: 8b 50 18                    mov edx, dword ptr [eax + 24]
c010ccb6: 8b 40 14                    mov eax, dword ptr [eax + 20]
c010ccb9: 8b 4c 24 04                 mov ecx, dword ptr [esp + 4]
c010ccbd: 8b 5c 24 08                 mov ebx, dword ptr [esp + 8]
c010ccc1: 03 59 08                    add ebx, dword ptr [ecx + 8]
c010ccc4: 8d 34 d5 00 00 00 00        lea esi, [8*edx]
c010cccb: 83 e6 08                    and esi, 8
c010ccce: 89 d1                       mov ecx, edx
c010ccd0: 83 e1 02                    and ecx, 2
c010ccd3: 74 03                       je 0xc010ccd8 <ArchLoadDriver+0x15c>
c010ccd5: 83 ce 02                    or esi, 2
c010ccd8: 80 e2 04                    and dl, 4
c010ccdb: 74 03                       je 0xc010cce0 <ArchLoadDriver+0x164>
c010ccdd: 83 ce 01                    or esi, 1
c010cce0: 85 c9                       test ecx, ecx
c010cce2: 0f 94 44 24 18              sete byte ptr [esp + 24]
c010cce7: 0b 4c 24 5c                 or ecx, dword ptr [esp + 92]
c010cceb: 0f 84 80 00 00 00           je 0xc010cd71 <ArchLoadDriver+0x1f5>
c010ccf1: 8b 4c 24 24                 mov ecx, dword ptr [esp + 36]
c010ccf5: 09 ce                       or esi, ecx
c010ccf7: 05 ff 0f 00 00              add eax, 4095
c010ccfc: 25 00 f0 ff ff              and eax, 4294963200
c010cd01: 8d 3c 18                    lea edi, [eax + ebx]
c010cd04: 89 da                       mov edx, ebx
c010cd06: 39 d7                       cmp edi, edx
c010cd08: 74 1d                       je 0xc010cd27 <ArchLoadDriver+0x1ab>
c010cd0a: 50                          push eax
c010cd0b: 6a 0b                       push 11
c010cd0d: 56                          push esi
c010cd0e: 52                          push edx
c010cd0f: 89 54 24 38                 mov dword ptr [esp + 56], edx
c010cd13: e8 45 7c ff ff              call 0xc010495d <SetVirtPermissions>
c010cd18: 8b 54 24 38                 mov edx, dword ptr [esp + 56]
c010cd1c: 81 c2 00 10 00 00           add edx, 4096
c010cd22: 83 c4 10                    add esp, 16
c010cd25: eb df                       jmp 0xc010cd06 <ArchLoadDriver+0x18a>
c010cd27: 8b 74 24 0c                 mov esi, dword ptr [esp + 12]
c010cd2b: 01 ee                       add esi, ebp
c010cd2d: 89 df                       mov edi, ebx
c010cd2f: 8b 4c 24 10                 mov ecx, dword ptr [esp + 16]
c010cd33: f3 a4                       rep  movsb byte ptr es:[edi], byte ptr [esi]
c010cd35: 80 7c 24 20 00              cmp byte ptr [esp + 32], 0
```

```
c010cdad: 50                            push eax
c010cdae: 6a 09                         push 9
c010cdb0: 83 ce 02                      or esi, 2
c010cdb3: 56                            push esi
c010cdb4: 53                            push ebx
c010cdb5: e8 a3 7b ff ff                call 0xc010495d <SetVirtPermissions>
c010cdba: 8b 74 24 1c                   mov esi, dword ptr [esp + 28]
c010cdbe: 01 fe                         add esi, edi
c010cdc0: 01 ee                         add esi, ebp
c010cdc2: 89 df                         mov edi, ebx
c010cdc4: 8b 4c 24 28                   mov ecx, dword ptr [esp + 40]
c010cdc8: f3 a4                         rep  movsb byte ptr es:[edi], byte ptr [esi]
c010cdca: 83 c4 0c                      add esp, 12
c010cdcd: 6a 02                         push 2
c010cdcf: 6a 00                         push 0
c010cdd1: 53                            push ebx
c010cdd2: e8 86 7b ff ff                call 0xc010495d <SetVirtPermissions>
c010cdd7: 83 c4 10                      add esp, 16
c010cdda: eb 3d                         jmp 0xc010ce19 <ArchLoadDriver+0x29d>
c010cddc: 89 d7                         mov edi, edx
c010cdde: 89 54 24 10                   mov dword ptr [esp + 16], edx
c010cde2: 81 e7 00 f0 ff ff             and edi, 4294963200
c010cde8: 50                            push eax
c010cde9: 50                            push eax
c010cdea: 57                            push edi
c010cdeb: 53                            push ebx
c010cdec: e8 07 87 ff ff                call 0xc01054f8 <UnmapVirt>
c010cdf1: 58                            pop eax
c010cdf2: 5a                            pop edx
c010cdf3: ff 74 24 14                   push dword ptr [esp + 20]
c010cdf7: ff 74 24 60                   push dword ptr [esp + 96]
c010cdfb: 89 f0                         mov eax, esi
c010cdfd: 0d 20 04 00 00                or eax, 1056
c010ce02: 50                            push eax
c010ce03: 57                            push edi
c010ce04: 53                            push ebx
c010ce05: ff 74 24 24                   push dword ptr [esp + 36]
c010ce09: e8 3a 85 ff ff                call 0xc0105348 <MapVirt>
c010ce0e: 83 c4 20                      add esp, 32
c010ce11: 39 c3                         cmp ebx, eax
c010ce13: 8b 54 24 10                   mov edx, dword ptr [esp + 16]
c010ce17: 74 83                         je 0xc010cd9c <ArchLoadDriver+0x220>
c010ce19: ff 44 24 14                   inc dword ptr [esp + 20]
c010ce1d: 83 44 24 04 20                add dword ptr [esp + 4], 32
c010ce22: e9 5b fe ff ff                jmp 0xc010cc82 <ArchLoadDriver+0x106>
c010ce27: 8b 44 24 50                   mov eax, dword ptr [esp + 80]
c010ce2b: 8b 00                         mov eax, dword ptr [eax]
c010ce2d: 89 44 24 10                   mov dword ptr [esp + 16], eax
c010ce31: 8b 45 20                      mov eax, dword ptr [ebp + 32]
c010ce34: 01 e8                         add eax, ebp
c010ce36: 89 44 24 04                   mov dword ptr [esp + 4], eax
c010ce3a: 31 c0                         xor eax, eax
c010ce3c: 89 44 24 20                   mov dword ptr [esp + 32], eax
c010ce40: 0f b7 45 30                   movzx eax, word ptr [ebp + 48]
c010ce44: 39 44 24 20                   cmp dword ptr [esp + 32], eax
c010ce48: 0f 8d 9f 02 00 00             jge 0xc010d0ed <ArchLoadDriver+0x571>
c010ce4e: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c010ce52: 8b 40 04                      mov eax, dword ptr [eax + 4]
c010ce55: 83 f8 09                      cmp eax, 9
c010ce58: 0f 85 67 02 00 00             jne 0xc010d0c5 <ArchLoadDriver+0x549>
c010ce5e: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c010ce62: 8b 78 10                      mov edi, dword ptr [eax + 16]
c010ce65: 8b 70 14                      mov esi, dword ptr [eax + 20]
c010ce68: 8b 58 24                      mov ebx, dword ptr [eax + 36]
c010ce6b: 8b 10                         mov edx, dword ptr [eax]
c010ce6d: 0f b7 45 32                   movzx eax, word ptr [ebp + 50]
c010ce71: 31 c9                         xor ecx, ecx
c010ce73: 66 85 c0                      test ax, ax
c010ce76: 74 0f                         je 0xc010ce87 <ArchLoadDriver+0x30b>
c010ce78: 6b c0 28                      imul eax, eax, 40
c010ce7b: 01 e8                         add eax, ebp
```

```
c010ced8: 0f 8e cd 01 00 00           jle 0xc010d0ab <ArchLoadDriver+0x52f>
c010cede: 31 c9                       xor ecx, ecx
c010cee0: 89 4c 24 18                 mov dword ptr [esp + 24], ecx
c010cee4: 83 7c 24 58 00              cmp dword ptr [esp + 88], 0
c010cee9: 74 0a                       je 0xc010cef5 <ArchLoadDriver+0x379>
c010ceeb: 8b 44 24 58                 mov eax, dword ptr [esp + 88]
c010ceef: 8b 00                       mov eax, dword ptr [eax]
c010cef1: 89 44 24 18                 mov dword ptr [esp + 24], eax
c010cef5: 8b 44 24 0c                 mov eax, dword ptr [esp + 12]
c010cef9: 8b 7c 24 10                 mov edi, dword ptr [esp + 16]
c010cefd: 03 38                       add edi, dword ptr [eax]
c010ceff: 8b 40 04                    mov eax, dword ptr [eax + 4]
c010cf02: 89 44 24 08                 mov dword ptr [esp + 8], eax
c010cf06: 89 c1                       mov ecx, eax
c010cf08: c1 e9 08                    shr ecx, 8
c010cf0b: 75 07                       jne 0xc010cf14 <ArchLoadDriver+0x398>
c010cf0d: 31 db                       xor ebx, ebx
c010cf0f: e9 aa 00 00 00              jmp 0xc010cfbe <ArchLoadDriver+0x442>
c010cf14: 8b 44 24 04                 mov eax, dword ptr [esp + 4]
c010cf18: 8b 58 18                    mov ebx, dword ptr [eax + 24]
c010cf1b: 85 db                       test ebx, ebx
c010cf1d: 75 15                       jne 0xc010cf34 <ArchLoadDriver+0x3b8>
c010cf1f: 52                          push edx
c010cf20: 52                          push edx
c010cf21: ff 74 24 1c                 push dword ptr [esp + 28]
c010cf25: 68 15 1d 11 c0              push 3222347029
c010cf2a: e8 96 bb ff ff              call 0xc0108ac5 <LogWriteSerial>
c010cf2f: e9 a3 01 00 00              jmp 0xc010d0d7 <ArchLoadDriver+0x55b>
c010cf34: 8b 45 20                    mov eax, dword ptr [ebp + 32]
c010cf37: 01 e8                       add eax, ebp
c010cf39: 89 44 24 08                 mov dword ptr [esp + 8], eax
c010cf3d: 6b db 28                    imul ebx, ebx, 40
c010cf40: 01 c3                       add ebx, eax
c010cf42: 8b 73 18                    mov esi, dword ptr [ebx + 24]
c010cf45: 8b 43 14                    mov eax, dword ptr [ebx + 20]
c010cf48: 31 d2                       xor edx, edx
c010cf4a: f7 73 24                    div dword ptr [ebx + 36]
c010cf4d: 39 c1                       cmp ecx, eax
c010cf4f: 73 ce                       jae 0xc010cf1f <ArchLoadDriver+0x3a3>
c010cf51: c1 e1 04                    shl ecx, 4
c010cf54: 03 4b 10                    add ecx, dword ptr [ebx + 16]
c010cf57: 8d 5c 0d 00                 lea ebx, [ebp + ecx]
c010cf5b: 66 8b 43 0e                 mov ax, word ptr [ebx + 14]
c010cf5f: 66 85 c0                    test ax, ax
c010cf62: 75 44                       jne 0xc010cfa8 <ArchLoadDriver+0x42c>
c010cf64: 6b f6 28                    imul esi, esi, 40
c010cf67: 8b 03                       mov eax, dword ptr [ebx]
c010cf69: 8b 54 24 08                 mov edx, dword ptr [esp + 8]
c010cf6d: 03 44 32 10                 add eax, dword ptr [edx + esi + 16]
c010cf71: 8d 74 05 00                 lea esi, [ebp + eax]
c010cf75: 83 ec 0c                    sub esp, 12
c010cf78: 56                          push esi
c010cf79: e8 8a b5 ff ff              call 0xc0108508 <GetSymbolAddress>
c010cf7e: 83 c4 10                    add esp, 16
c010cf81: 85 c0                       test eax, eax
c010cf83: 75 37                       jne 0xc010cfbc <ArchLoadDriver+0x440>
c010cf85: 8a 5b 0c                    mov bl, byte ptr [ebx + 12]
c010cf88: 83 e3 20                    and ebx, 32
c010cf8b: 50                          push eax
c010cf8c: 50                          push eax
c010cf8d: 56                          push esi
c010cf8e: 68 37 1d 11 c0              push 3222347063
c010cf93: e8 2d bb ff ff              call 0xc0108ac5 <LogWriteSerial>
c010cf98: 83 c4 10                    add esp, 16
c010cf9b: 84 db                       test bl, bl
c010cf9d: 0f 85 6a ff ff ff           jne 0xc010cf0d <ArchLoadDriver+0x391>
c010cfa3: e9 77 ff ff ff              jmp 0xc010cf1f <ArchLoadDriver+0x3a3>
c010cfa8: 8b 53 04                    mov edx, dword ptr [ebx + 4]
c010cfab: 8b 4c 24 10                 mov ecx, dword ptr [esp + 16]
c010cfaf: 8d 1c 11                    lea ebx, [ecx + edx]
c010cfb2: 66 83 f8 f1                 cmp ax, -15
```

```
c010d005: e8 53 79 ff ff             call 0xc010495d <SetVirtPermissions>
c010d00a: 83 c4 10                   add esp, 16
c010d00d: 8b 44 24 0c                mov eax, dword ptr [esp + 12]
c010d011: 0f b6 40 04                movzx eax, byte ptr [eax + 4]
c010d015: 83 f8 01                   cmp eax, 1
c010d018: 74 1b                      je 0xc010d035 <ArchLoadDriver+0x4b9>
c010d01a: 83 f8 02                   cmp eax, 2
c010d01d: 75 0d                      jne 0xc010d02c <ArchLoadDriver+0x4b0>
c010d01f: 8b 07                      mov eax, dword ptr [edi]
c010d021: 29 f8                      sub eax, edi
c010d023: 01 c3                      add ebx, eax
c010d025: c6 44 24 08 01             mov byte ptr [esp + 8], 1
c010d02a: eb 24                      jmp 0xc010d050 <ArchLoadDriver+0x4d4>
c010d02c: 83 f8 08                   cmp eax, 8
c010d02f: 75 08                      jne 0xc010d039 <ArchLoadDriver+0x4bd>
c010d031: 8b 5c 24 10                mov ebx, dword ptr [esp + 16]
c010d035: 03 1f                      add ebx, dword ptr [edi]
c010d037: eb ec                      jmp 0xc010d025 <ArchLoadDriver+0x4a9>
c010d039: 83 ec 0c                   sub esp, 12
c010d03c: 68 4d 1d 11 c0             push 3222347085
c010d041: e8 7f ba ff ff             call 0xc0108ac5 <LogWriteSerial>
c010d046: 83 c4 10                   add esp, 16
c010d049: 31 db                      xor ebx, ebx
c010d04b: c6 44 24 08 00             mov byte ptr [esp + 8], 0
c010d050: 89 1f                      mov dword ptr [edi], ebx
c010d052: 83 7c 24 18 00             cmp dword ptr [esp + 24], 0
c010d057: 74 0f                      je 0xc010d068 <ArchLoadDriver+0x4ec>
c010d059: 50                         push eax
c010d05a: 53                         push ebx
c010d05b: 57                         push edi
c010d05c: ff 74 24 24                push dword ptr [esp + 36]
c010d060: e8 f4 b5 ff ff             call 0xc0108659 <AddToRelocationTable>
c010d065: 83 c4 10                   add esp, 16
c010d068: 83 7c 24 24 00             cmp dword ptr [esp + 36], 0
c010d06d: 75 0e                      jne 0xc010d07d <ArchLoadDriver+0x501>
c010d06f: 50                         push eax
c010d070: 6a 02                      push 2
c010d072: 6a 00                      push 0
c010d074: 57                         push edi
c010d075: e8 e3 78 ff ff             call 0xc010495d <SetVirtPermissions>
c010d07a: 83 c4 10                   add esp, 16
c010d07d: 83 7c 24 28 00             cmp dword ptr [esp + 40], 0
c010d082: 75 0e                      jne 0xc010d092 <ArchLoadDriver+0x516>
c010d084: 57                         push edi
c010d085: 6a 02                      push 2
c010d087: 6a 00                      push 0
c010d089: 56                         push esi
c010d08a: e8 ce 78 ff ff             call 0xc010495d <SetVirtPermissions>
c010d08f: 83 c4 10                   add esp, 16
c010d092: 83 44 24 0c 08             add dword ptr [esp + 12], 8
c010d097: 80 7c 24 08 00             cmp byte ptr [esp + 8], 0
c010d09c: 0f 84 7d fe ff ff          je 0xc010cf1f <ArchLoadDriver+0x3a3>
c010d0a2: ff 44 24 14                inc dword ptr [esp + 20]
c010d0a6: e9 25 fe ff ff             jmp 0xc010ced0 <ArchLoadDriver+0x354>
c010d0ab: 83 7c 24 58 00             cmp dword ptr [esp + 88], 0
c010d0b0: 74 2d                      je 0xc010d0df <ArchLoadDriver+0x563>
c010d0b2: 83 ec 0c                   sub esp, 12
c010d0b5: 8b 44 24 64                mov eax, dword ptr [esp + 100]
c010d0b9: ff 30                      push dword ptr [eax]
c010d0bb: e8 7c b5 ff ff             call 0xc010863c <SortRelocationTable>
c010d0c0: 83 c4 10                   add esp, 16
c010d0c3: eb 1a                      jmp 0xc010d0df <ArchLoadDriver+0x563>
c010d0c5: 83 f8 04                   cmp eax, 4
c010d0c8: 75 15                      jne 0xc010d0df <ArchLoadDriver+0x563>
c010d0ca: 83 ec 0c                   sub esp, 12
c010d0cd: 68 62 1d 11 c0             push 3222347106
c010d0d2: e8 06 ba ff ff             call 0xc0108add <LogDeveloperWarning>
c010d0d7: 83 c4 10                   add esp, 16
c010d0da: e9 ee fa ff ff             jmp 0xc010cbcd <ArchLoadDriver+0x51>
c010d0df: ff 44 24 20                inc dword ptr [esp + 32]
c010d0e3: 83 44 24 04 28             add dword ptr [esp + 4], 40
```

```
c010d13b: 03 50 10                   add edx, dword ptr [eax + 16]
c010d13e: 8d 7c 15 00                lea edi, [ebp + edx]
c010d142: 52                         push edx
c010d143: 52                         push edx
c010d144: 68 9f 1d 11 c0             push 3222347167
c010d149: 57                         push edi
c010d14a: e8 52 40 ff ff             call 0xc01011a1 <strcmp>
c010d14f: 83 c4 10                   add esp, 16
c010d152: 85 c0                      test eax, eax
c010d154: 75 1e                      jne 0xc010d174 <ArchLoadDriver+0x5f8>
c010d156: 8b 44 24 50                mov eax, dword ptr [esp + 80]
c010d15a: 8b 00                      mov eax, dword ptr [eax]
c010d15c: 03 43 0c                   add eax, dword ptr [ebx + 12]
c010d15f: 25 00 f0 ff ff             and eax, 4294963200
c010d164: 89 c7                      mov edi, eax
c010d166: 8b 5b 14                   mov ebx, dword ptr [ebx + 20]
c010d169: 81 c3 ff 0f 00 00          add ebx, 4095
c010d16f: c1 eb 0c                   shr ebx, 12
c010d172: eb 17                      jmp 0xc010d18b <ArchLoadDriver+0x60f>
c010d174: 50                         push eax
c010d175: 50                         push eax
c010d176: 68 ab 1d 11 c0             push 3222347179
c010d17b: 57                         push edi
c010d17c: e8 20 40 ff ff             call 0xc01011a1 <strcmp>
c010d181: 83 c4 10                   add esp, 16
c010d184: 85 c0                      test eax, eax
c010d186: 74 ce                      je 0xc010d156 <ArchLoadDriver+0x5da>
c010d188: 46                         inc esi
c010d189: eb 8a                      jmp 0xc010d115 <ArchLoadDriver+0x599>
c010d18b: 83 eb 01                   sub ebx, 1
c010d18e: 72 f8                      jb 0xc010d188 <ArchLoadDriver+0x60c>
c010d190: 83 ec 0c                   sub esp, 12
c010d193: 57                         push edi
c010d194: e8 5c 7b ff ff             call 0xc0104cf5 <LockVirt>
c010d199: 81 c7 00 10 00 00          add edi, 4096
c010d19f: 83 c4 10                   add esp, 16
c010d1a2: eb e7                      jmp 0xc010d18b <ArchLoadDriver+0x60f>
c010d1a4: 83 c4 3c                   add esp, 60
c010d1a7: 5b                         pop ebx
c010d1a8: 5e                         pop esi
c010d1a9: 5f                         pop edi
c010d1aa: 5d                         pop ebp
c010d1ab: c3                         ret

c010d1ac <ArchLoadSymbols>:
c010d1ac: 55                         push ebp
c010d1ad: 57                         push edi
c010d1ae: 56                         push esi
c010d1af: 53                         push ebx
c010d1b0: 83 ec 34                   sub esp, 52
c010d1b3: 8b 44 24 48                mov eax, dword ptr [esp + 72]
c010d1b7: 8b 7c 24 4c                mov edi, dword ptr [esp + 76]
c010d1bb: 89 7c 24 20                mov dword ptr [esp + 32], edi
c010d1bf: 8b 50 30                   mov edx, dword ptr [eax + 48]
c010d1c2: 8b 52 70                   mov edx, dword ptr [edx + 112]
c010d1c5: 89 54 24 18                mov dword ptr [esp + 24], edx
c010d1c9: 6a 00                      push 0
c010d1cb: 50                         push eax
c010d1cc: 6a 21                      push 33
c010d1ce: ff 74 24 24                push dword ptr [esp + 36]
c010d1d2: 6a 00                      push 0
c010d1d4: 6a 00                      push 0
c010d1d6: e8 6d 81 ff ff             call 0xc0105348 <MapVirt>
c010d1db: 83 c4 20                   add esp, 32
c010d1de: 80 38 7f                   cmp byte ptr [eax], 127
c010d1e1: 75 1b                      jne 0xc010d1fe <ArchLoadSymbols+0x52>
c010d1e3: 89 c3                      mov ebx, eax
c010d1e5: 80 78 01 45                cmp byte ptr [eax + 1], 69
c010d1e9: 75 13                      jne 0xc010d1fe <ArchLoadSymbols+0x52>
c010d1eb: 80 78 02 4c                cmp byte ptr [eax + 2], 76
c010d1ef: 75 0d                      jne 0xc010d1fe <ArchLoadSymbols+0x52>
```

```
c010d24b: 8b 4c 02 10                mov ecx, dword ptr [edx + eax + 16]
c010d24f: 01 d9                      add ecx, ebx
c010d251: 03 0e                      add ecx, dword ptr [esi]
c010d253: 50                         push eax
c010d254: 50                         push eax
c010d255: 68 b7 1d 11 c0             push 3222347191
c010d25a: 51                         push ecx
c010d25b: 89 4c 24 2c                mov dword ptr [esp + 44], ecx
c010d25f: e8 3d 3f ff ff             call 0xc01011a1 <strcmp>
c010d264: 83 c4 10                   add esp, 16
c010d267: 85 c0                      test eax, eax
c010d269: 8b 4c 24 1c                mov ecx, dword ptr [esp + 28]
c010d26d: 75 0c                      jne 0xc010d27b <ArchLoadSymbols+0xcf>
c010d26f: 8b 6e 14                   mov ebp, dword ptr [esi + 20]
c010d272: 8b 44 24 14                mov eax, dword ptr [esp + 20]
c010d276: 89 04 24                   mov dword ptr [esp], eax
c010d279: eb 1f                      jmp 0xc010d29a <ArchLoadSymbols+0xee>
c010d27b: 50                         push eax
c010d27c: 50                         push eax
c010d27d: 68 bf 1d 11 c0             push 3222347199
c010d282: 51                         push ecx
c010d283: e8 19 3f ff ff             call 0xc01011a1 <strcmp>
c010d288: 83 c4 10                   add esp, 16
c010d28b: 85 c0                      test eax, eax
c010d28d: 75 0b                      jne 0xc010d29a <ArchLoadSymbols+0xee>
c010d28f: 8b 46 14                   mov eax, dword ptr [esi + 20]
c010d292: 89 44 24 0c                mov dword ptr [esp + 12], eax
c010d296: 8b 7c 24 14                mov edi, dword ptr [esp + 20]
c010d29a: ff 44 24 04                inc dword ptr [esp + 4]
c010d29e: eb 81                      jmp 0xc010d221 <ArchLoadSymbols+0x75>
c010d2a0: 83 3c 24 00                cmp dword ptr [esp], 0
c010d2a4: 0f 94 c0                   sete al
c010d2a7: 85 ff                      test edi, edi
c010d2a9: 0f 94 c2                   sete dl
c010d2ac: 09 d0                      or eax, edx
c010d2ae: 85 ed                      test ebp, ebp
c010d2b0: 0f 94 c2                   sete dl
c010d2b3: 08 d0                      or al, dl
c010d2b5: 0f 85 43 ff ff ff          jne 0xc010d1fe <ArchLoadSymbols+0x52>
c010d2bb: 83 7c 24 0c 00             cmp dword ptr [esp + 12], 0
c010d2c0: 0f 84 38 ff ff ff          je 0xc010d1fe <ArchLoadSymbols+0x52>
c010d2c6: 8b 34 24                   mov esi, dword ptr [esp]
c010d2c9: 01 de                      add esi, ebx
c010d2cb: 01 df                      add edi, ebx
c010d2cd: 83 e5 f0                   and ebp, -16
c010d2d0: 01 f5                      add ebp, esi
c010d2d2: 39 f5                      cmp ebp, esi
c010d2d4: 74 28                      je 0xc010d2fe <ArchLoadSymbols+0x152>
c010d2d6: 8b 46 04                   mov eax, dword ptr [esi + 4]
c010d2d9: 85 c0                      test eax, eax
c010d2db: 74 1c                      je 0xc010d2f9 <ArchLoadSymbols+0x14d>
c010d2dd: f6 46 0d 03                test byte ptr [esi + 13], 3
c010d2e1: 75 16                      jne 0xc010d2f9 <ArchLoadSymbols+0x14d>
c010d2e3: 52                         push edx
c010d2e4: 52                         push edx
c010d2e5: 8b 54 24 20                mov edx, dword ptr [esp + 32]
c010d2e9: 01 d0                      add eax, edx
c010d2eb: 50                         push eax
c010d2ec: 8b 06                      mov eax, dword ptr [esi]
c010d2ee: 01 f8                      add eax, edi
c010d2f0: 50                         push eax
c010d2f1: e8 68 b1 ff ff             call 0xc010845e <AddSymbol>
c010d2f6: 83 c4 10                   add esp, 16
c010d2f9: 83 c6 10                   add esi, 16
c010d2fc: eb d4                      jmp 0xc010d2d2 <ArchLoadSymbols+0x126>
c010d2fe: 8b 44 24 10                mov eax, dword ptr [esp + 16]
c010d302: 89 44 24 44                mov dword ptr [esp + 68], eax
c010d306: 89 5c 24 40                mov dword ptr [esp + 64], ebx
c010d30a: 83 c4 2c                   add esp, 44
c010d30d: 5b                         pop ebx
c010d30e: 5e                         pop esi
```

```
c010d355: 19 c0                         sbb eax, eax
c010d357: 83 e0 f8                      and eax, -8
c010d35a: 05 4e 01 00 00                add eax, 334
c010d35f: f6 04 24 04                   test byte ptr [esp], 4
c010d363: 74 03                         je 0xc010d368 <ArchLoadProgramLoader+0x52>
c010d365: 83 c8 01                      or eax, 1
c010d368: 89 4c 24 0c                   mov dword ptr [esp + 12], ecx
c010d36c: 51                            push ecx
c010d36d: 51                            push ecx
c010d36e: 6a 00                         push 0
c010d370: 6a 00                         push 0
c010d372: 50                            push eax
c010d373: 57                            push edi
c010d374: 52                            push edx
c010d375: 89 54 24 24                   mov dword ptr [esp + 36], edx
c010d379: 6a 00                         push 0
c010d37b: e8 c8 7f ff ff                call 0xc0105348 <MapVirt>
c010d380: 83 c4 20                      add esp, 32
c010d383: 8b 54 24 08                   mov edx, dword ptr [esp + 8]
c010d387: 39 c2                         cmp edx, eax
c010d389: 75 37                         jne 0xc010d3c2 <ArchLoadProgramLoader+0xac>
c010d38b: 01 ee                         add esi, ebp
c010d38d: 89 d7                         mov edi, edx
c010d38f: 8b 4c 24 0c                   mov ecx, dword ptr [esp + 12]
c010d393: f3 a4                         rep  movsb byte ptr es:[edi], byte ptr [esi]
c010d395: f6 04 24 02                   test byte ptr [esp], 2
c010d399: 75 0e                         jne 0xc010d3a9 <ArchLoadProgramLoader+0x93>
c010d39b: 50                            push eax
c010d39c: 6a 02                         push 2
c010d39e: 6a 00                         push 0
c010d3a0: 52                            push edx
c010d3a1: e8 b7 75 ff ff                call 0xc010495d <SetVirtPermissions>
c010d3a6: 83 c4 10                      add esp, 16
c010d3a9: ff 44 24 04                   inc dword ptr [esp + 4]
c010d3ad: 83 c3 20                      add ebx, 32
c010d3b0: e9 77 ff ff ff                jmp 0xc010d32c <ArchLoadProgramLoader+0x16>
c010d3b5: 8b 55 18                      mov edx, dword ptr [ebp + 24]
c010d3b8: 8b 44 24 34                   mov eax, dword ptr [esp + 52]
c010d3bc: 89 10                         mov dword ptr [eax], edx
c010d3be: 31 c0                         xor eax, eax
c010d3c0: eb 05                         jmp 0xc010d3c7 <ArchLoadProgramLoader+0xb1>
c010d3c2: b8 02 00 00 00                mov eax, 2
c010d3c7: 83 c4 1c                      add esp, 28
c010d3ca: 5b                            pop ebx
c010d3cb: 5e                            pop esi
c010d3cc: 5f                            pop edi
c010d3cd: 5d                            pop ebp
c010d3ce: c3                            ret

c010d3cf <ArchGetMemory>:
c010d3cf: 55                            push ebp
c010d3d0: 57                            push edi
c010d3d1: 56                            push esi
c010d3d2: 53                            push ebx
c010d3d3: 83 ec 1c                      sub esp, 28
c010d3d6: 8b 44 24 30                   mov eax, dword ptr [esp + 48]
c010d3da: ba ff 2f 14 00                mov edx, 1323007
c010d3df: 81 e2 00 f0 ff ff             and edx, 4294963200
c010d3e5: 89 d5                         mov ebp, edx
c010d3e7: 8b 78 08                      mov edi, dword ptr [eax + 8]
c010d3ea: 81 ef 00 00 00 40             sub edi, 1073741824
c010d3f0: 89 7c 24 08                   mov dword ptr [esp + 8], edi
c010d3f4: 8b 00                         mov eax, dword ptr [eax]
c010d3f6: 89 44 24 0c                   mov dword ptr [esp + 12], eax
c010d3fa: 89 14 24                      mov dword ptr [esp], edx
c010d3fd: 31 d2                         xor edx, edx
c010d3ff: 89 54 24 04                   mov dword ptr [esp + 4], edx
c010d403: 8b 1d 78 b3 13 c0             mov ebx, dword ptr [-1072450696]
c010d409: 8b 44 24 0c                   mov eax, dword ptr [esp + 12]
c010d40d: 39 c3                         cmp ebx, eax
c010d40f: 0f 8d fb 00 00 00             jge 0xc010d510 <ArchGetMemory+0x141>
```

```
c010d468: 8b 03                         mov eax, dword ptr [ebx]
c010d46a: 8b 53 04                      mov edx, dword ptr [ebx + 4]
c010d46d: 89 c6                         mov esi, eax
c010d46f: 89 d7                         mov edi, edx
c010d471: 03 73 08                      add esi, dword ptr [ebx + 8]
c010d474: 13 7b 0c                      adc edi, dword ptr [ebx + 12]
c010d477: b9 ff ff 07 00                mov ecx, 524287
c010d47c: 39 f1                         cmp ecx, esi
c010d47e: b9 00 00 00 00                mov ecx, 0
c010d483: 19 f9                         sbb ecx, edi
c010d485: 73 11                         jae 0xc010d498 <ArchGetMemory+0xc9>
c010d487: be 00 00 08 00                mov esi, 524288
c010d48c: 31 ff                         xor edi, edi
c010d48e: 29 c6                         sub esi, eax
c010d490: 19 d7                         sbb edi, edx
c010d492: 89 73 08                      mov dword ptr [ebx + 8], esi
c010d495: 89 7b 0c                      mov dword ptr [ebx + 12], edi
c010d498: 89 c6                         mov esi, eax
c010d49a: 89 d7                         mov edi, edx
c010d49c: 03 73 08                      add esi, dword ptr [ebx + 8]
c010d49f: 13 7b 0c                      adc edi, dword ptr [ebx + 12]
c010d4a2: 39 ee                         cmp esi, ebp
c010d4a4: 89 f9                         mov ecx, edi
c010d4a6: 1b 4c 24 04                   sbb ecx, dword ptr [esp + 4]
c010d4aa: 72 52                         jb 0xc010d4fe <ArchGetMemory+0x12f>
c010d4ac: 83 ec 0c                      sub esp, 12
c010d4af: 57                            push edi
c010d4b0: 56                            push esi
c010d4b1: 52                            push edx
c010d4b2: 50                            push eax
c010d4b3: 68 c7 1d 11 c0                push 3222347207
c010d4b8: e8 20 b6 ff ff                call 0xc0108add <LogDeveloperWarning>
c010d4bd: 83 c4 20                      add esp, 32
c010d4c0: eb 3c                         jmp 0xc010d4fe <ArchGetMemory+0x12f>
c010d4c2: be ff ff 0f 00                mov esi, 1048575
c010d4c7: 39 c6                         cmp esi, eax
c010d4c9: 19 d1                         sbb ecx, edx
c010d4cb: 0f 83 32 ff ff ff             jae 0xc010d403 <ArchGetMemory+0x34>
c010d4d1: 8b 73 08                      mov esi, dword ptr [ebx + 8]
c010d4d4: 8b 7b 0c                      mov edi, dword ptr [ebx + 12]
c010d4d7: 39 e8                         cmp eax, ebp
c010d4d9: 89 d1                         mov ecx, edx
c010d4db: 1b 4c 24 04                   sbb ecx, dword ptr [esp + 4]
c010d4df: 73 1d                         jae 0xc010d4fe <ArchGetMemory+0x12f>
c010d4e1: 01 f0                         add eax, esi
c010d4e3: 11 fa                         adc edx, edi
c010d4e5: 2b 04 24                      sub eax, dword ptr [esp]
c010d4e8: 1b 54 24 04                   sbb edx, dword ptr [esp + 4]
c010d4ec: 89 43 08                      mov dword ptr [ebx + 8], eax
c010d4ef: 89 53 0c                      mov dword ptr [ebx + 12], edx
c010d4f2: 8b 04 24                      mov eax, dword ptr [esp]
c010d4f5: 8b 54 24 04                   mov edx, dword ptr [esp + 4]
c010d4f9: 89 03                         mov dword ptr [ebx], eax
c010d4fb: 89 53 04                      mov dword ptr [ebx + 4], edx
c010d4fe: 83 7b 0c 00                   cmp dword ptr [ebx + 12], 0
c010d502: 75 0e                         jne 0xc010d512 <ArchGetMemory+0x143>
c010d504: 83 7b 08 00                   cmp dword ptr [ebx + 8], 0
c010d508: 0f 84 f5 fe ff ff             je 0xc010d403 <ArchGetMemory+0x34>
c010d50e: eb 02                         jmp 0xc010d512 <ArchGetMemory+0x143>
c010d510: 31 db                         xor ebx, ebx
c010d512: 89 d8                         mov eax, ebx
c010d514: 83 c4 1c                      add esp, 28
c010d517: 5b                            pop ebx
c010d518: 5e                            pop esi
c010d519: 5f                            pop edi
c010d51a: 5d                            pop ebp
c010d51b: c3                            ret

c010d51c <x86KernelMemoryToPhysical>:
c010d51c: 8d 81 00 00 00 c0             lea eax, [ecx - 1073741824]
c010d522: c3                            ret
```

```
c010d578: 89 44 24 04                  mov dword ptr [esp + 4], eax
c010d57c: e9 f3 10 00 00               jmp 0xc010e674 <x86SetCr3>

c010d581 <x86AllocatePageTable>:
c010d581: 57                           push edi
c010d582: 56                           push esi
c010d583: 53                           push ebx
c010d584: 89 c6                        mov esi, eax
c010d586: 89 d3                        mov ebx, edx
c010d588: 8b 40 04                     mov eax, dword ptr [eax + 4]
c010d58b: 8b 78 04                     mov edi, dword ptr [eax + 4]
c010d58e: e8 d6 65 ff ff               call 0xc0103b69 <AllocPhys>
c010d593: 83 c8 07                     or eax, 7
c010d596: 89 04 9f                     mov dword ptr [edi + 4*ebx], eax
c010d599: 83 ec 0c                     sub esp, 12
c010d59c: 56                           push esi
c010d59d: e8 cd ff ff ff               call 0xc010d56f <ArchSetVas>
c010d5a2: 8d 93 00 fc 0f 00            lea edx, [ebx + 1047552]
c010d5a8: c1 e2 0c                     shl edx, 12
c010d5ab: b9 00 04 00 00               mov ecx, 1024
c010d5b0: 31 c0                        xor eax, eax
c010d5b2: 89 d7                        mov edi, edx
c010d5b4: f3 ab                        rep  stosd dword ptr es:[edi], eax
c010d5b6: 83 c4 10                     add esp, 16
c010d5b9: 5b                           pop ebx
c010d5ba: 5e                           pop esi
c010d5bb: 5f                           pop edi
c010d5bc: c3                           ret

c010d5bd <x86GetPageEntry>:
c010d5bd: 57                           push edi
c010d5be: 56                           push esi
c010d5bf: 53                           push ebx
c010d5c0: 8b 7c 24 10                  mov edi, dword ptr [esp + 16]
c010d5c4: 8b 74 24 14                  mov esi, dword ptr [esp + 20]
c010d5c8: e8 ac 70 ff ff               call 0xc0104679 <GetVas>
c010d5cd: 39 c7                        cmp edi, eax
c010d5cf: 74 10                        je 0xc010d5e1 <x86GetPageEntry+0x24>
c010d5d1: 83 ec 0c                     sub esp, 12
c010d5d4: 68 f1 1d 11 c0               push 3222347249
c010d5d9: e8 ff b4 ff ff               call 0xc0108add <LogDeveloperWarning>
c010d5de: 83 c4 10                     add esp, 16
c010d5e1: 89 f3                        mov ebx, esi
c010d5e3: c1 eb 16                     shr ebx, 22
c010d5e6: c1 ee 0c                     shr esi, 12
c010d5e9: 81 e6 ff 03 00 00            and esi, 1023
c010d5ef: 8b 47 04                     mov eax, dword ptr [edi + 4]
c010d5f2: 8b 40 04                     mov eax, dword ptr [eax + 4]
c010d5f5: f6 04 98 01                  test byte ptr [eax + 4*ebx], 1
c010d5f9: 75 09                        jne 0xc010d604 <x86GetPageEntry+0x47>
c010d5fb: 89 da                        mov edx, ebx
c010d5fd: 89 f8                        mov eax, edi
c010d5ff: e8 7d ff ff ff               call 0xc010d581 <x86AllocatePageTable>
c010d604: c1 e3 0a                     shl ebx, 10
c010d607: 8d 84 1e 00 00 f0 3f         lea eax, [esi + ebx + 1072693248]
c010d60e: c1 e0 02                     shl eax, 2
c010d611: 5b                           pop ebx
c010d612: 5e                           pop esi
c010d613: 5f                           pop edi
c010d614: c3                           ret

c010d615 <ArchSetPageUsageBits>:
c010d615: 56                           push esi
c010d616: 53                           push ebx
c010d617: 83 ec 0c                     sub esp, 12
c010d61a: 8b 74 24 20                  mov esi, dword ptr [esp + 32]
c010d61e: 8b 5c 24 24                  mov ebx, dword ptr [esp + 36]
c010d622: 8b 44 24 1c                  mov eax, dword ptr [esp + 28]
c010d626: ff 30                        push dword ptr [eax]
c010d628: ff 74 24 1c                  push dword ptr [esp + 28]
c010d62c: e8 8c ff ff ff               call 0xc010d5bd <x86GetPageEntry>
```

```
c010d671: 83 e2 01                  and edx, 1
c010d674: 8b 4c 24 28               mov ecx, dword ptr [esp + 40]
c010d678: 88 11                     mov byte ptr [ecx], dl
c010d67a: c1 e8 06                  shr eax, 6
c010d67d: 83 e0 01                  and eax, 1
c010d680: 8b 54 24 2c               mov edx, dword ptr [esp + 44]
c010d684: 88 02                     mov byte ptr [edx], al
c010d686: 83 c4 1c                  add esp, 28
c010d689: c3                        ret

c010d68a <x86MapPage>:
c010d68a: 57                        push edi
c010d68b: 56                        push esi
c010d68c: 53                        push ebx
c010d68d: 89 c6                     mov esi, eax
c010d68f: 89 d3                     mov ebx, edx
c010d691: 89 cf                     mov edi, ecx
c010d693: e8 e1 6f ff ff            call 0xc0104679 <GetVas>
c010d698: 39 c6                     cmp esi, eax
c010d69a: 74 10                     je 0xc010d6ac <x86MapPage+0x22>
c010d69c: 83 ec 0c                  sub esp, 12
c010d69f: 68 33 1e 11 c0            push 3222347315
c010d6a4: e8 34 b4 ff ff            call 0xc0108add <LogDeveloperWarning>
c010d6a9: 83 c4 10                  add esp, 16
c010d6ac: 50                        push eax
c010d6ad: 50                        push eax
c010d6ae: 57                        push edi
c010d6af: 56                        push esi
c010d6b0: e8 08 ff ff ff            call 0xc010d5bd <x86GetPageEntry>
c010d6b5: 0b 5c 24 20               or ebx, dword ptr [esp + 32]
c010d6b9: 89 18                     mov dword ptr [eax], ebx
c010d6bb: 83 c4 10                  add esp, 16
c010d6be: 5b                        pop ebx
c010d6bf: 5e                        pop esi
c010d6c0: 5f                        pop edi
c010d6c1: c3                        ret

c010d6c2 <ArchUnmap>:
c010d6c2: 8b 44 24 04               mov eax, dword ptr [esp + 4]
c010d6c6: 31 d2                     xor edx, edx
c010d6c8: 89 54 24 04               mov dword ptr [esp + 4], edx
c010d6cc: 8b 54 24 08               mov edx, dword ptr [esp + 8]
c010d6d0: 8b 0a                     mov ecx, dword ptr [edx]
c010d6d2: 31 d2                     xor edx, edx
c010d6d4: e9 b1 ff ff ff            jmp 0xc010d68a <x86MapPage>

c010d6d9 <ArchUpdateMapping>:
c010d6d9: 55                        push ebp
c010d6da: 57                        push edi
c010d6db: 56                        push esi
c010d6dc: 53                        push ebx
c010d6dd: 83 ec 0c                  sub esp, 12
c010d6e0: 8b 7c 24 20               mov edi, dword ptr [esp + 32]
c010d6e4: 8b 74 24 24               mov esi, dword ptr [esp + 36]
c010d6e8: 8a 5e 04                  mov bl, byte ptr [esi + 4]
c010d6eb: 8a 56 05                  mov dl, byte ptr [esi + 5]
c010d6ee: 88 d9                     mov cl, bl
c010d6f0: 83 e1 88                  and ecx, -120
c010d6f3: b8 02 00 00 00            mov eax, 2
c010d6f8: 80 f9 80                  cmp cl, -128
c010d6fb: 74 0a                     je 0xc010d707 <ArchUpdateMapping+0x2e>
c010d6fd: 88 d0                     mov al, dl
c010d6ff: c0 e8 03                  shr al, 3
c010d702: 83 e0 01                  and eax, 1
c010d705: 01 c0                     add eax, eax
c010d707: 83 e3 01                  and ebx, 1
c010d70a: 09 c3                     or ebx, eax
c010d70c: 80 e2 02                  and dl, 2
c010d70f: 74 03                     je 0xc010d714 <ArchUpdateMapping+0x3b>
c010d711: 83 cb 04                  or ebx, 4
c010d714: 31 ed                     xor ebp, ebp
```

```
c010d75b: 83 c4 0c                  add esp, 12
c010d75e: 5b                        pop ebx
c010d75f: 5e                        pop esi
c010d760: 5f                        pop edi
c010d761: 5d                        pop ebp
c010d762: c3                        ret

c010d763 <ArchAddMapping>:
c010d763: e9 71 ff ff ff            jmp 0xc010d6d9 <ArchUpdateMapping>

c010d768 <ArchFlushTlb>:
c010d768: e9 02 fe ff ff            jmp 0xc010d56f <ArchSetVas>

c010d76d <ArchInitVas>:
c010d76d: 57                        push edi
c010d76e: 56                        push esi
c010d76f: 53                        push ebx
c010d770: 8b 74 24 10               mov esi, dword ptr [esp + 16]
c010d774: 50                        push eax
c010d775: 50                        push eax
c010d776: 6a 00                     push 0
c010d778: 6a 00                     push 0
c010d77a: 6a 17                     push 23
c010d77c: 68 00 10 00 00            push 4096
c010d781: 6a 00                     push 0
c010d783: 6a 00                     push 0
c010d785: e8 be 7b ff ff            call 0xc0105348 <MapVirt>
c010d78a: 89 c7                     mov edi, eax
c010d78c: 83 c4 14                  add esp, 20
c010d78f: 50                        push eax
c010d790: e8 94 75 ff ff            call 0xc0104d29 <GetPhysFromVirt>
c010d795: 89 c3                     mov ebx, eax
c010d797: c7 04 24 08 00 00 00      mov dword ptr [esp], 8
c010d79e: e8 ac 61 ff ff            call 0xc010394f <AllocHeap>
c010d7a3: 89 46 04                  mov dword ptr [esi + 4], eax
c010d7a6: 89 18                     mov dword ptr [eax], ebx
c010d7a8: 8b 46 04                  mov eax, dword ptr [esi + 4]
c010d7ab: 89 78 04                  mov dword ptr [eax + 4], edi
c010d7ae: 8b 46 04                  mov eax, dword ptr [esi + 4]
c010d7b1: 8b 40 04                  mov eax, dword ptr [eax + 4]
c010d7b4: 83 cb 03                  or ebx, 3
c010d7b7: 89 98 fc 0f 00 00         mov dword ptr [eax + 4092], ebx
c010d7bd: 83 c4 10                  add esp, 16
c010d7c0: b8 00 0c 00 00            mov eax, 3072
c010d7c5: 8b 88 00 d0 13 c0         mov ecx, dword ptr [eax - 1072443392]
c010d7cb: 8b 56 04                  mov edx, dword ptr [esi + 4]
c010d7ce: 8b 52 04                  mov edx, dword ptr [edx + 4]
c010d7d1: 89 0c 02                  mov dword ptr [edx + eax], ecx
c010d7d4: 83 c0 04                  add eax, 4
c010d7d7: 3d fc 0f 00 00            cmp eax, 4092
c010d7dc: 75 e7                     jne 0xc010d7c5 <ArchInitVas+0x58>
c010d7de: 5b                        pop ebx
c010d7df: 5e                        pop esi
c010d7e0: 5f                        pop edi
c010d7e1: c3                        ret

c010d7e2 <ArchInitVirt>:
c010d7e2: 57                        push edi
c010d7e3: 56                        push esi
c010d7e4: 53                        push ebx
c010d7e5: c7 05 84 e0 13 c0 00 e0 13 c0 mov dword ptr [-1072439164], 3222528000
c010d7ef: 52                        push edx
c010d7f0: 52                        push edx
c010d7f1: 6a 01                     push 1
c010d7f3: 68 80 e0 13 c0            push 3222528128
c010d7f8: e8 e7 6a ff ff            call 0xc01042e4 <CreateVasEx>
c010d7fd: ba 00 d0 13 c0            mov edx, 3222523904
c010d802: 31 c0                     xor eax, eax
c010d804: b9 00 04 00 00            mov ecx, 1024
c010d809: 89 d7                     mov edi, edx
c010d80b: f3 ab                     rep  stosd dword ptr es:[edi], eax
```

```
c010d87c: 68 80 e0 13 c0              push 3222528128
c010d881: e8 f6 80 ff ff              call 0xc010597c <SetVas>
c010d886: 83 c4 10                    add esp, 16
c010d889: 31 db                       xor ebx, ebx
c010d88b: 8d b3 10 03 00 00           lea esi, [ebx + 784]
c010d891: 81 fe 2f 03 00 00           cmp esi, 815
c010d897: 77 17                       ja 0xc010d8b0 <ArchInitVirt+0xce>
c010d899: 43                          inc ebx
c010d89a: 89 f2                       mov edx, esi
c010d89c: b8 80 e0 13 c0              mov eax, 3222528128
c010d8a1: e8 db fc ff ff              call 0xc010d581 <x86AllocatePageTable>
c010d8a6: 81 fb ef 00 00 00           cmp ebx, 239
c010d8ac: 75 dd                       jne 0xc010d88b <ArchInitVirt+0xa9>
c010d8ae: eb 10                       jmp 0xc010d8c0 <ArchInitVirt+0xde>
c010d8b0: e8 ab 65 ff ff              call 0xc0103e60 <GetTotalPhysKilobytes>
c010d8b5: 89 c2                       mov edx, eax
c010d8b7: 89 d8                       mov eax, ebx
c010d8b9: c1 e0 04                    shl eax, 4
c010d8bc: 39 c2                       cmp edx, eax
c010d8be: 73 d9                       jae 0xc010d899 <ArchInitVirt+0xb7>
c010d8c0: 50                          push eax
c010d8c1: 50                          push eax
c010d8c2: c1 e3 02                    shl ebx, 2
c010d8c5: 53                          push ebx
c010d8c6: 68 70 1e 11 c0              push 3222347376
c010d8cb: e8 f5 b1 ff ff              call 0xc0108ac5 <LogWriteSerial>
c010d8d0: c7 04 24 00 00 14 c0        mov dword ptr [esp], 3222536192
c010d8d7: e8 47 fc ff ff              call 0xc010d523 <ArchVirtualToPhysical>
c010d8dc: 89 04 24                    mov dword ptr [esp], eax
c010d8df: e8 e3 61 ff ff              call 0xc0103ac7 <DeallocPhys>
c010d8e4: c7 04 24 00 10 14 c0        mov dword ptr [esp], 3222540288
c010d8eb: e8 33 fc ff ff              call 0xc010d523 <ArchVirtualToPhysical>
c010d8f0: 89 04 24                    mov dword ptr [esp], eax
c010d8f3: e8 cf 61 ff ff              call 0xc0103ac7 <DeallocPhys>
c010d8f8: 83 c4 10                    add esp, 16
c010d8fb: 5b                          pop ebx
c010d8fc: 5e                          pop esi
c010d8fd: 5f                          pop edi
c010d8fe: c3                          ret

c010d8ff <SysChdir>:
c010d8ff: 83 ec 1c                    sub esp, 28
c010d902: e8 7e 93 ff ff              call 0xc0106c85 <GetProcess>
c010d907: 83 ec 0c                    sub esp, 12
c010d90a: 50                          push eax
c010d90b: e8 d2 93 ff ff              call 0xc0106ce2 <GetFdTable>
c010d910: 83 c4 0c                    add esp, 12
c010d913: 8d 54 24 10                 lea edx, [esp + 16]
c010d917: 52                          push edx
c010d918: ff 74 24 28                 push dword ptr [esp + 40]
c010d91c: 50                          push eax
c010d91d: e8 08 b8 ff ff              call 0xc010912a <GetFileFromFd>
c010d922: 83 c4 10                    add esp, 16
c010d925: 85 c0                       test eax, eax
c010d927: 75 12                       jne 0xc010d93b <SysChdir+0x3c>
c010d929: 83 ec 0c                    sub esp, 12
c010d92c: 8b 44 24 18                 mov eax, dword ptr [esp + 24]
c010d930: ff 70 30                    push dword ptr [eax + 48]
c010d933: e8 e7 c9 ff ff              call 0xc010a31f <SetWorkingDirectory>
c010d938: 83 c4 10                    add esp, 16
c010d93b: 83 c4 1c                    add esp, 28
c010d93e: c3                          ret

c010d93f <SysClose>:
c010d93f: 53                          push ebx
c010d940: 83 ec 18                    sub esp, 24
c010d943: e8 3d 93 ff ff              call 0xc0106c85 <GetProcess>
c010d948: 83 ec 0c                    sub esp, 12
c010d94b: 50                          push eax
c010d94c: e8 91 93 ff ff              call 0xc0106ce2 <GetFdTable>
c010d951: 89 c3                       mov ebx, eax
```

```
c010d995: 8b 74 24 34                  mov esi, dword ptr [esp + 52]
c010d999: 8b 5c 24 38                  mov ebx, dword ptr [esp + 56]
c010d99d: 8b 7c 24 3c                  mov edi, dword ptr [esp + 60]
c010d9a1: e8 df 92 ff ff               call 0xc0106c85 <GetProcess>
c010d9a6: 83 ec 0c                     sub esp, 12
c010d9a9: 50                           push eax
c010d9aa: e8 33 93 ff ff               call 0xc0106ce2 <GetFdTable>
c010d9af: 83 c4 10                     add esp, 16
c010d9b2: f7 c7 ff fe ff ff            test edi, 4294967039
c010d9b8: 75 52                        jne 0xc010da0c <SysDup+0x82>
c010d9ba: 89 c2                        mov edx, eax
c010d9bc: 83 fd 01                     cmp ebp, 1
c010d9bf: 75 25                        jne 0xc010d9e6 <SysDup+0x5c>
c010d9c1: 51                           push ecx
c010d9c2: 8d 44 24 10                  lea eax, [esp + 16]
c010d9c6: 50                           push eax
c010d9c7: 56                           push esi
c010d9c8: 52                           push edx
c010d9c9: e8 27 b8 ff ff               call 0xc01091f5 <DupFd>
c010d9ce: 83 c4 10                     add esp, 16
c010d9d1: 85 c0                        test eax, eax
c010d9d3: 75 3c                        jne 0xc010da11 <SysDup+0x87>
c010d9d5: 50                           push eax
c010d9d6: 50                           push eax
c010d9d7: ff 74 24 14                  push dword ptr [esp + 20]
c010d9db: 53                           push ebx
c010d9dc: e8 10 bd ff ff               call 0xc01096f1 <WriteWordToUsermode>
c010d9e1: 83 c4 10                     add esp, 16
c010d9e4: eb 2b                        jmp 0xc010da11 <SysDup+0x87>
c010d9e6: b8 07 00 00 00               mov eax, 7
c010d9eb: 83 fd 02                     cmp ebp, 2
c010d9ee: 75 21                        jne 0xc010da11 <SysDup+0x87>
c010d9f0: 89 7c 24 3c                  mov dword ptr [esp + 60], edi
c010d9f4: 89 5c 24 38                  mov dword ptr [esp + 56], ebx
c010d9f8: 89 74 24 34                  mov dword ptr [esp + 52], esi
c010d9fc: 89 54 24 30                  mov dword ptr [esp + 48], edx
c010da00: 83 c4 1c                     add esp, 28
c010da03: 5b                           pop ebx
c010da04: 5e                           pop esi
c010da05: 5f                           pop edi
c010da06: 5d                           pop ebp
c010da07: e9 84 b8 ff ff               jmp 0xc0109290 <DupFd2>
c010da0c: b8 07 00 00 00               mov eax, 7
c010da11: 83 c4 1c                     add esp, 28
c010da14: 5b                           pop ebx
c010da15: 5e                           pop esi
c010da16: 5f                           pop edi
c010da17: 5d                           pop ebp
c010da18: c3                           ret

c010da19 <SysExit>:
c010da19: 83 ec 18                     sub esp, 24
c010da1c: ff 74 24 1c                  push dword ptr [esp + 28]
c010da20: e8 74 92 ff ff               call 0xc0106c99 <KillProcess>
c010da25: b8 20 00 00 00               mov eax, 32
c010da2a: 83 c4 1c                     add esp, 28
c010da2d: c3                           ret

c010da2e <SysFork>:
c010da2e: 83 ec 18                     sub esp, 24
c010da31: 68 9b 1e 11 c0               push 3222347419
c010da36: e8 8a b0 ff ff               call 0xc0108ac5 <LogWriteSerial>
c010da3b: e8 c7 96 ff ff               call 0xc0107107 <ForkProcess>
c010da40: c7 04 24 b4 1e 11 c0         mov dword ptr [esp], 3222347444
c010da47: e8 79 b0 ff ff               call 0xc0108ac5 <LogWriteSerial>
c010da4c: 31 c0                        xor eax, eax
c010da4e: 83 c4 1c                     add esp, 28
c010da51: c3                           ret

c010da52 <SysGetPid>:
c010da52: 57                           push edi
```

```
c010daa0: 8d 44 24 38                  lea eax, [esp + 56]
c010daa4: 50                           push eax
c010daa5: 8d 44 24 38                  lea eax, [esp + 56]
c010daa9: 50                           push eax
c010daaa: e8 44 ba ff ff               call 0xc01094f3 <PerformTransfer>
c010daaf: 31 c0                        xor eax, eax
c010dab1: 83 c4 64                     add esp, 100
c010dab4: 5e                           pop esi
c010dab5: 5f                           pop edi
c010dab6: c3                           ret

c010dab7 <SysGetTid>:
c010dab7: 0f 21 d8                     mov eax, dr3
c010daba: c1 e0 06                     shl eax, 6
c010dabd: 8b 80 c4 40 11 c0            mov eax, dword ptr [eax - 1072611132]
c010dac3: 8b 40 20                     mov eax, dword ptr [eax + 32]
c010dac6: c3                           ret

c010dac7 <SysInfo>:
c010dac7: 53                           push ebx
c010dac8: 83 ec 08                     sub esp, 8
c010dacb: 8b 54 24 10                  mov edx, dword ptr [esp + 16]
c010dacf: 8b 5c 24 14                  mov ebx, dword ptr [esp + 20]
c010dad3: 8b 4c 24 18                  mov ecx, dword ptr [esp + 24]
c010dad7: 8b 44 24 1c                  mov eax, dword ptr [esp + 28]
c010dadb: 83 fa 02                     cmp edx, 2
c010dade: 74 24                        je 0xc010db04 <SysInfo+0x3d>
c010dae0: 77 0b                        ja 0xc010daed <SysInfo+0x26>
c010dae2: 85 d2                        test edx, edx
c010dae4: 75 13                        jne 0xc010daf9 <SysInfo+0x32>
c010dae6: e8 7e 63 ff ff               call 0xc0103e69 <GetFreePhysKilobytes>
c010daeb: eb 11                        jmp 0xc010dafe <SysInfo+0x37>
c010daed: 83 fa 03                     cmp edx, 3
c010daf0: 74 4a                        je 0xc010db3c <SysInfo+0x75>
c010daf2: b8 01 00 00 00               mov eax, 1
c010daf7: eb 4c                        jmp 0xc010db45 <SysInfo+0x7e>
c010daf9: e8 62 63 ff ff               call 0xc0103e60 <GetTotalPhysKilobytes>
c010dafe: 89 44 24 14                  mov dword ptr [esp + 20], eax
c010db02: eb 2b                        jmp 0xc010db2f <SysInfo+0x68>
c010db04: 3d ff 00 00 00               cmp eax, 255
c010db09: 76 05                        jbe 0xc010db10 <SysInfo+0x49>
c010db0b: b8 ff 00 00 00               mov eax, 255
c010db10: 40                           inc eax
c010db11: 31 d2                        xor edx, edx
c010db13: 52                           push edx
c010db14: 50                           push eax
c010db15: 51                           push ecx
c010db16: 68 cd 1e 11 c0               push 3222347469
c010db1b: e8 a3 ba ff ff               call 0xc01095c3 <WriteStringToUsermode>
c010db20: 83 c4 10                     add esp, 16
c010db23: 85 c0                        test eax, eax
c010db25: 75 1e                        jne 0xc010db45 <SysInfo+0x7e>
c010db27: c7 44 24 14 01 00 00 00      mov dword ptr [esp + 20], 1
c010db2f: 89 5c 24 10                  mov dword ptr [esp + 16], ebx
c010db33: 83 c4 08                     add esp, 8
c010db36: 5b                           pop ebx
c010db37: e9 b5 bb ff ff               jmp 0xc01096f1 <WriteWordToUsermode>
c010db3c: 83 f8 03                     cmp eax, 3
c010db3f: 0f 97 c0                     seta al
c010db42: 0f b6 c0                     movzx eax, al
c010db45: 83 c4 08                     add esp, 8
c010db48: 5b                           pop ebx
c010db49: c3                           ret

c010db4a <SysIoctl>:
c010db4a: 57                           push edi
c010db4b: 56                           push esi
c010db4c: 53                           push ebx
c010db4d: 83 ec 10                     sub esp, 16
c010db50: 8b 7c 24 20                  mov edi, dword ptr [esp + 32]
c010db54: 8b 5c 24 24                  mov ebx, dword ptr [esp + 36]
```

```
c010dba3: e8 1e c9 ff ff              call 0xc010a4c6 <VnodeOpIoctl>
c010dba8: 83 c4 10                    add esp, 16
c010dbab: 85 c0                       test eax, eax
c010dbad: 75 10                       jne 0xc010dbbf <SysIoctl+0x75>
c010dbaf: 50                          push eax
c010dbb0: 50                          push eax
c010dbb1: 6a 00                       push 0
c010dbb3: ff 74 24 3c                 push dword ptr [esp + 60]
c010dbb7: e8 35 bb ff ff              call 0xc01096f1 <WriteWordToUsermode>
c010dbbc: 83 c4 10                    add esp, 16
c010dbbf: 83 c4 10                    add esp, 16
c010dbc2: 5b                          pop ebx
c010dbc3: 5e                          pop esi
c010dbc4: 5f                          pop edi
c010dbc5: c3                          ret

c010dbc6 <SysMapVirt>:
c010dbc6: 55                          push ebp
c010dbc7: 57                          push edi
c010dbc8: 56                          push esi
c010dbc9: 53                          push ebx
c010dbca: 83 ec 1c                    sub esp, 28
c010dbcd: 8b 5c 24 30                 mov ebx, dword ptr [esp + 48]
c010dbd1: 8b 74 24 34                 mov esi, dword ptr [esp + 52]
c010dbd5: f7 c3 94 ef ff ff           test ebx, 4294963092
c010dbdb: 74 0a                       je 0xc010dbe7 <SysMapVirt+0x21>
c010dbdd: b8 07 00 00 00              mov eax, 7
c010dbe2: e9 d9 00 00 00              jmp 0xc010dcc0 <SysMapVirt+0xfa>
c010dbe7: 57                          push edi
c010dbe8: 57                          push edi
c010dbe9: 8d 44 24 0c                 lea eax, [esp + 12]
c010dbed: 50                          push eax
c010dbee: ff 74 24 4c                 push dword ptr [esp + 76]
c010dbf2: e8 58 bb ff ff              call 0xc010974f <ReadWordFromUsermode>
c010dbf7: 83 c4 10                    add esp, 16
c010dbfa: 85 c0                       test eax, eax
c010dbfc: 0f 85 be 00 00 00           jne 0xc010dcc0 <SysMapVirt+0xfa>
c010dc02: 8b 44 24 04                 mov eax, dword ptr [esp + 4]
c010dc06: 8d 50 ff                    lea edx, [eax - 1]
c010dc09: 81 fa fe ff ff 07           cmp edx, 134217726
c010dc0f: 76 cc                       jbe 0xc010dbdd <SysMapVirt+0x17>
c010dc11: 85 c0                       test eax, eax
c010dc13: 74 12                       je 0xc010dc27 <SysMapVirt+0x61>
c010dc15: 31 d2                       xor edx, edx
c010dc17: 01 f0                       add eax, esi
c010dc19: 0f 92 c2                    setb dl
c010dc1c: 3d ff ff ff bf              cmp eax, 3221225471
c010dc21: 77 ba                       ja 0xc010dbdd <SysMapVirt+0x17>
c010dc23: 85 d2                       test edx, edx
c010dc25: 75 b6                       jne 0xc010dbdd <SysMapVirt+0x17>
c010dc27: 31 c9                       xor ecx, ecx
c010dc29: 89 4c 24 08                 mov dword ptr [esp + 8], ecx
c010dc2d: f6 c3 20                    test bl, 32
c010dc30: 75 4f                       jne 0xc010dc81 <SysMapVirt+0xbb>
c010dc32: 81 cb 04 01 00 00           or ebx, 260
c010dc38: ff 74 24 04                 push dword ptr [esp + 4]
c010dc3c: 53                          push ebx
c010dc3d: 56                          push esi
c010dc3e: 68 f9 1e 11 c0              push 3222347513
c010dc43: e8 7d ae ff ff              call 0xc0108ac5 <LogWriteSerial>
c010dc48: 8b 6c 24 18                 mov ebp, dword ptr [esp + 24]
c010dc4c: 89 34 24                    mov dword ptr [esp], esi
c010dc4f: e8 6b 7e ff ff              call 0xc0105abf <BytesToPages>
c010dc54: 89 c6                       mov esi, eax
c010dc56: 8b 7c 24 14                 mov edi, dword ptr [esp + 20]
c010dc5a: e8 1a 6a ff ff              call 0xc0104679 <GetVas>
c010dc5f: 8d 4c 24 1c                 lea ecx, [esp + 28]
c010dc63: 51                          push ecx
c010dc64: ff 74 24 50                 push dword ptr [esp + 80]
c010dc68: 55                          push ebp
c010dc69: 53                          push ebx
```

```
c010dcb4: ff 74 24 4c                  push dword ptr [esp + 76]
c010dcb8: e8 34 ba ff ff               call 0xc01096f1 <WriteWordToUsermode>
c010dcbd: 83 c4 10                     add esp, 16
c010dcc0: 83 c4 1c                     add esp, 28
c010dcc3: 5b                           pop ebx
c010dcc4: 5e                           pop esi
c010dcc5: 5f                           pop edi
c010dcc6: 5d                           pop ebp
c010dcc7: c3                           ret

c010dcc8 <SysMprotect>:
c010dcc8: 55                           push ebp
c010dcc9: 57                           push edi
c010dcca: 56                           push esi
c010dccb: 53                           push ebx
c010dccc: 83 ec 0c                     sub esp, 12
c010dccf: 8b 5c 24 20                  mov ebx, dword ptr [esp + 32]
c010dcd3: 8b 54 24 24                  mov edx, dword ptr [esp + 36]
c010dcd7: 8b 7c 24 28                  mov edi, dword ptr [esp + 40]
c010dcdb: b8 07 00 00 00               mov eax, 7
c010dce0: f7 c3 ff 0f 00 00            test ebx, 4095
c010dce6: 75 64                        jne 0xc010dd4c <SysMprotect+0x84>
c010dce8: b8 02 00 00 00               mov eax, 2
c010dced: 81 fb ff ff ff 07            cmp ebx, 134217727
c010dcf3: 76 57                        jbe 0xc010dd4c <SysMprotect+0x84>
c010dcf5: 89 d9                        mov ecx, ebx
c010dcf7: 31 c0                        xor eax, eax
c010dcf9: 01 d1                        add ecx, edx
c010dcfb: 0f 92 c0                     setb al
c010dcfe: 81 f9 ff ff ff bf            cmp ecx, 3221225471
c010dd04: 77 41                        ja 0xc010dd47 <SysMprotect+0x7f>
c010dd06: 85 c0                        test eax, eax
c010dd08: 75 3d                        jne 0xc010dd47 <SysMprotect+0x7f>
c010dd0a: b8 07 00 00 00               mov eax, 7
c010dd0f: 89 fe                        mov esi, edi
c010dd11: 83 e6 f4                     and esi, -12
c010dd14: 75 36                        jne 0xc010dd4c <SysMprotect+0x84>
c010dd16: 83 ec 0c                     sub esp, 12
c010dd19: 52                           push edx
c010dd1a: e8 a0 7d ff ff               call 0xc0105abf <BytesToPages>
c010dd1f: 89 c5                        mov ebp, eax
c010dd21: 83 c4 10                     add esp, 16
c010dd24: 39 ee                        cmp esi, ebp
c010dd26: 74 1b                        je 0xc010dd43 <SysMprotect+0x7b>
c010dd28: 50                           push eax
c010dd29: 6a 0b                        push 11
c010dd2b: 57                           push edi
c010dd2c: 89 f0                        mov eax, esi
c010dd2e: c1 e0 0c                     shl eax, 12
c010dd31: 01 d8                        add eax, ebx
c010dd33: 50                           push eax
c010dd34: e8 24 6c ff ff               call 0xc010495d <SetVirtPermissions>
c010dd39: 83 c4 10                     add esp, 16
c010dd3c: 85 c0                        test eax, eax
c010dd3e: 75 0c                        jne 0xc010dd4c <SysMprotect+0x84>
c010dd40: 46                           inc esi
c010dd41: eb e1                        jmp 0xc010dd24 <SysMprotect+0x5c>
c010dd43: 31 c0                        xor eax, eax
c010dd45: eb 05                        jmp 0xc010dd4c <SysMprotect+0x84>
c010dd47: b8 02 00 00 00               mov eax, 2
c010dd4c: 83 c4 0c                     add esp, 12
c010dd4f: 5b                           pop ebx
c010dd50: 5e                           pop esi
c010dd51: 5f                           pop edi
c010dd52: 5d                           pop ebp
c010dd53: c3                           ret

c010dd54 <SysNanosleep>:
c010dd54: 55                           push ebp
c010dd55: 57                           push edi
c010dd56: 56                           push esi
```

```
c010dda7: e8 9c 9f ff ff              call 0xc0107d48 <GetSystemTimer>
c010ddac: 89 c6                       mov esi, eax
c010ddae: 89 d7                       mov edi, edx
c010ddb0: 52                          push edx
c010ddb1: ff 74 24 28                 push dword ptr [esp + 40]
c010ddb5: ff 74 24 28                 push dword ptr [esp + 40]
c010ddb9: 68 36 1f 11 c0              push 3222347574
c010ddbe: e8 02 ad ff ff              call 0xc0108ac5 <LogWriteSerial>
c010ddc3: 59                          pop ecx
c010ddc4: 5d                          pop ebp
c010ddc5: ff 74 24 2c                 push dword ptr [esp + 44]
c010ddc9: ff 74 24 2c                 push dword ptr [esp + 44]
c010ddcd: e8 9a a0 ff ff              call 0xc0107e6c <SleepNano>
c010ddd2: 89 c5                       mov ebp, eax
c010ddd4: e8 6f 9f ff ff              call 0xc0107d48 <GetSystemTimer>
c010ddd9: 29 f0                       sub eax, esi
c010dddb: 19 fa                       sbb edx, edi
c010dddd: 89 44 24 38                 mov dword ptr [esp + 56], eax
c010dde1: 89 54 24 3c                 mov dword ptr [esp + 60], edx
c010dde5: 8b 54 24 3c                 mov edx, dword ptr [esp + 60]
c010dde9: 89 dc                       mov esp, ebx
c010ddeb: 85 d2                       test edx, edx
c010dded: 79 04                       jns 0xc010ddf3 <SysNanosleep+0x9f>
c010ddef: 31 c0                       xor eax, eax
c010ddf1: 31 d2                       xor edx, edx
c010ddf3: 89 44 24 28                 mov dword ptr [esp + 40], eax
c010ddf7: 89 54 24 2c                 mov dword ptr [esp + 44], edx
c010ddfb: 50                          push eax
c010ddfc: 50                          push eax
c010ddfd: 6a 00                       push 0
c010ddff: 6a 00                       push 0
c010de01: 6a 00                       push 0
c010de03: 6a 08                       push 8
c010de05: ff b4 24 8c 00 00 00        push dword ptr [esp + 140]
c010de0c: 53                          push ebx
c010de0d: e8 d7 b9 ff ff              call 0xc01097e9 <CreateTransferWritingToUser>
c010de12: 8d 7c 24 4c                 lea edi, [esp + 76]
c010de16: b9 08 00 00 00              mov ecx, 8
c010de1b: 89 de                       mov esi, ebx
c010de1d: f3 a5                       rep  movsd dword ptr es:[edi], dword ptr [esi
c010de1f: 83 c4 1c                    add esp, 28
c010de22: 6a 00                       push 0
c010de24: 6a 08                       push 8
c010de26: 8d 44 24 38                 lea eax, [esp + 56]
c010de2a: 50                          push eax
c010de2b: 8d 44 24 34                 lea eax, [esp + 52]
c010de2f: 50                          push eax
c010de30: e8 be b6 ff ff              call 0xc01094f3 <PerformTransfer>
c010de35: 83 c4 10                    add esp, 16
c010de38: 85 c0                       test eax, eax
c010de3a: 75 02                       jne 0xc010de3e <SysNanosleep+0xea>
c010de3c: 89 e8                       mov eax, ebp
c010de3e: 83 c4 5c                    add esp, 92
c010de41: 5b                          pop ebx
c010de42: 5e                          pop esi
c010de43: 5f                          pop edi
c010de44: 5d                          pop ebp
c010de45: c3                          ret

c010de46 <SysOpen>:
c010de46: 57                          push edi
c010de47: 56                          push esi
c010de48: 53                          push ebx
c010de49: 81 ec a0 01 00 00           sub esp, 416
c010de4f: 8b bc 24 b4 01 00 00        mov edi, dword ptr [esp + 436]
c010de56: bb 07 00 00 00              mov ebx, 7
c010de5b: 81 ff ff 03 00 00           cmp edi, 1023
c010de61: 0f 87 b4 00 00 00           ja 0xc010df1b <SysOpen+0xd5>
c010de67: 6a 00                       push 0
c010de69: 68 8f 01 00 00              push 399
c010de6e: ff b4 24 b8 01 00 00        push dword ptr [esp + 440]
```

```
c010dece: 89 c3                         mov ebx, eax
c010ded0: 83 c4 20                      add esp, 32
c010ded3: 85 c0                         test eax, eax
c010ded5: 74 0e                         je 0xc010dee5 <SysOpen+0x9f>
c010ded7: 83 ec 0c                      sub esp, 12
c010deda: ff 74 24 18                   push dword ptr [esp + 24]
c010dede: e8 09 c4 ff ff                call 0xc010a2ec <CloseFile>
c010dee3: eb 33                         jmp 0xc010df18 <SysOpen+0xd2>
c010dee5: 51                            push ecx
c010dee6: 51                            push ecx
c010dee7: ff 74 24 10                   push dword ptr [esp + 16]
c010deeb: ff b4 24 c8 01 00 00          push dword ptr [esp + 456]
c010def2: e8 fa b7 ff ff                call 0xc01096f1 <WriteWordToUsermode>
c010def7: 89 c3                         mov ebx, eax
c010def9: 83 c4 10                      add esp, 16
c010defc: 85 c0                         test eax, eax
c010defe: 74 1b                         je 0xc010df1b <SysOpen+0xd5>
c010df00: 83 ec 0c                      sub esp, 12
c010df03: ff 74 24 18                   push dword ptr [esp + 24]
c010df07: e8 e0 c3 ff ff                call 0xc010a2ec <CloseFile>
c010df0c: 58                            pop eax
c010df0d: 5a                            pop edx
c010df0e: ff 74 24 14                   push dword ptr [esp + 20]
c010df12: 56                            push esi
c010df13: e8 ad b1 ff ff                call 0xc01090c5 <RemoveFd>
c010df18: 83 c4 10                      add esp, 16
c010df1b: 89 d8                         mov eax, ebx
c010df1d: 81 c4 a0 01 00 00             add esp, 416
c010df23: 5b                            pop ebx
c010df24: 5e                            pop esi
c010df25: 5f                            pop edi
c010df26: c3                            ret

c010df27 <SysPrepExec>:
c010df27: 83 ec 0c                      sub esp, 12
c010df2a: e8 56 8d ff ff                call 0xc0106c85 <GetProcess>
c010df2f: 83 ec 0c                      sub esp, 12
c010df32: 50                            push eax
c010df33: e8 aa 8d ff ff                call 0xc0106ce2 <GetFdTable>
c010df38: 89 04 24                      mov dword ptr [esp], eax
c010df3b: e8 42 b2 ff ff                call 0xc0109182 <HandleExecFd>
c010df40: 89 c2                         mov edx, eax
c010df42: 83 c4 10                      add esp, 16
c010df45: b8 07 00 00 00                mov eax, 7
c010df4a: 85 d2                         test edx, edx
c010df4c: 75 10                         jne 0xc010df5e <SysPrepExec+0x37>
c010df4e: e8 53 76 ff ff                call 0xc01055a6 <WipeUsermodePages>
c010df53: 85 c0                         test eax, eax
c010df55: 0f 95 c0                      setne al
c010df58: 0f b6 c0                      movzx eax, al
c010df5b: c1 e0 05                      shl eax, 5
c010df5e: 83 c4 0c                      add esp, 12
c010df61: c3                            ret

c010df62 <SysReadWrite>:
c010df62: 57                            push edi
c010df63: 56                            push esi
c010df64: 53                            push ebx
c010df65: 83 ec 30                      sub esp, 48
c010df68: 8b 5c 24 44                   mov ebx, dword ptr [esp + 68]
c010df6c: 8b 74 24 50                   mov esi, dword ptr [esp + 80]
c010df70: e8 10 8d ff ff                call 0xc0106c85 <GetProcess>
c010df75: 83 ec 0c                      sub esp, 12
c010df78: 50                            push eax
c010df79: e8 64 8d ff ff                call 0xc0106ce2 <GetFdTable>
c010df7e: 83 c4 0c                      add esp, 12
c010df81: 8d 54 24 10                   lea edx, [esp + 16]
c010df85: 52                            push edx
c010df86: ff 74 24 48                   push dword ptr [esp + 72]
c010df8a: 50                            push eax
c010df8b: e8 9a b1 ff ff                call 0xc010912a <GetFileFromFd>
```

```
c010dfd7: 85 f6                         test esi, esi
c010dfd9: 0f 95 c2                      setne dl
c010dfdc: 89 54 24 24                   mov dword ptr [esp + 36], edx
c010dfe0: 74 05                         je 0xc010dfe7 <SysReadWrite+0x85>
c010dfe2: b8 da a2 10 c0                mov eax, 3222315738
c010dfe7: 52                            push edx
c010dfe8: 52                            push edx
c010dfe9: 57                            push edi
c010dfea: ff 74 24 18                   push dword ptr [esp + 24]
c010dfee: ff d0                         call eax
c010dff0: 83 c4 10                      add esp, 16
c010dff3: 85 c0                         test eax, eax
c010dff5: 75 1a                         jne 0xc010e011 <SysReadWrite+0xaf>
c010dff7: 2b 5c 24 14                   sub ebx, dword ptr [esp + 20]
c010dffb: 8b 44 24 0c                   mov eax, dword ptr [esp + 12]
c010dfff: 01 58 08                      add dword ptr [eax + 8], ebx
c010e002: 50                            push eax
c010e003: 50                            push eax
c010e004: 53                            push ebx
c010e005: ff 74 24 58                   push dword ptr [esp + 88]
c010e009: e8 e3 b6 ff ff                call 0xc01096f1 <WriteWordToUsermode>
c010e00e: 83 c4 10                      add esp, 16
c010e011: 83 c4 30                      add esp, 48
c010e014: 5b                            pop ebx
c010e015: 5e                            pop esi
c010e016: 5f                            pop edi
c010e017: c3                            ret

c010e018 <SysRemove>:
c010e018: 56                            push esi
c010e019: 53                            push ebx
c010e01a: 81 ec 94 01 00 00             sub esp, 404
c010e020: 8b b4 24 a4 01 00 00          mov esi, dword ptr [esp + 420]
c010e027: b8 07 00 00 00                mov eax, 7
c010e02c: 83 fe 01                      cmp esi, 1
c010e02f: 77 29                         ja 0xc010e05a <SysRemove+0x42>
c010e031: 6a 00                         push 0
c010e033: 68 8f 01 00 00                push 399
c010e038: ff b4 24 a8 01 00 00          push dword ptr [esp + 424]
c010e03f: 8d 5c 24 0c                   lea ebx, [esp + 12]
c010e043: 53                            push ebx
c010e044: e8 14 b6 ff ff                call 0xc010965d <ReadStringFromUsermode>
c010e049: 89 dc                         mov esp, ebx
c010e04b: 85 c0                         test eax, eax
c010e04d: 75 0b                         jne 0xc010e05a <SysRemove+0x42>
c010e04f: 50                            push eax
c010e050: 50                            push eax
c010e051: 56                            push esi
c010e052: 53                            push ebx
c010e053: e8 79 bf ff ff                call 0xc0109fd1 <RemoveFileOrDirectory>
c010e058: 89 dc                         mov esp, ebx
c010e05a: 81 c4 94 01 00 00             add esp, 404
c010e060: 5b                            pop ebx
c010e061: 5e                            pop esi
c010e062: c3                            ret

c010e063 <SysSeek>:
c010e063: 55                            push ebp
c010e064: 57                            push edi
c010e065: 56                            push esi
c010e066: 53                            push ebx
c010e067: 83 ec 5c                      sub esp, 92
c010e06a: 8b 7c 24 74                   mov edi, dword ptr [esp + 116]
c010e06e: 8b 74 24 78                   mov esi, dword ptr [esp + 120]
c010e072: e8 0e 8c ff ff                call 0xc0106c85 <GetProcess>
c010e077: 83 ec 0c                      sub esp, 12
c010e07a: 50                            push eax
c010e07b: e8 62 8c ff ff                call 0xc0106ce2 <GetFdTable>
c010e080: 83 c4 0c                      add esp, 12
c010e083: 8d 54 24 2c                   lea edx, [esp + 44]
c010e087: 52                            push edx
```

```
c010e0dd: 8b 44 24 34                mov eax, dword ptr [esp + 52]
c010e0e1: ff 70 30                   push dword ptr [eax + 48]
c010e0e4: e8 07 c5 ff ff             call 0xc010a5f0 <VnodeOpDirentType>
c010e0e9: 83 e0 fb                   and eax, -5
c010e0ec: 88 c2                      mov dl, al
c010e0ee: 83 c4 10                   add esp, 16
c010e0f1: b8 1b 00 00 00             mov eax, 27
c010e0f6: 80 fa 03                   cmp dl, 3
c010e0f9: 74 68                      je 0xc010e163 <SysSeek+0x100>
c010e0fb: 83 fe 01                   cmp esi, 1
c010e0fe: 75 09                      jne 0xc010e109 <SysSeek+0xa6>
c010e100: 8b 44 24 28                mov eax, dword ptr [esp + 40]
c010e104: 8b 40 08                   mov eax, dword ptr [eax + 8]
c010e107: eb 0f                      jmp 0xc010e118 <SysSeek+0xb5>
c010e109: 83 fe 02                   cmp esi, 2
c010e10c: 75 10                      jne 0xc010e11e <SysSeek+0xbb>
c010e10e: 8b 44 24 28                mov eax, dword ptr [esp + 40]
c010e112: 8b 40 30                   mov eax, dword ptr [eax + 48]
c010e115: 8b 40 70                   mov eax, dword ptr [eax + 112]
c010e118: 01 44 24 2c                add dword ptr [esp + 44], eax
c010e11c: eb 09                      jmp 0xc010e127 <SysSeek+0xc4>
c010e11e: b8 07 00 00 00             mov eax, 7
c010e123: 85 f6                      test esi, esi
c010e125: 75 3c                      jne 0xc010e163 <SysSeek+0x100>
c010e127: 8b 44 24 28                mov eax, dword ptr [esp + 40]
c010e12b: 8b 54 24 2c                mov edx, dword ptr [esp + 44]
c010e12f: 89 50 08                   mov dword ptr [eax + 8], edx
c010e132: 89 e6                      mov esi, esp
c010e134: 50                         push eax
c010e135: 50                         push eax
c010e136: 6a 00                      push 0
c010e138: 6a 00                      push 0
c010e13a: 6a 00                      push 0
c010e13c: 6a 04                      push 4
c010e13e: 57                         push edi
c010e13f: 56                         push esi
c010e140: e8 a4 b6 ff ff             call 0xc01097e9 <CreateTransferWritingToUser>
c010e145: b9 08 00 00 00             mov ecx, 8
c010e14a: 89 df                      mov edi, ebx
c010e14c: f3 a5                      rep  movsd dword ptr es:[edi], dword ptr [esi
c010e14e: 83 c4 1c                   add esp, 28
c010e151: 6a 00                      push 0
c010e153: 6a 04                      push 4
c010e155: 8d 44 24 38                lea eax, [esp + 56]
c010e159: 50                         push eax
c010e15a: 55                         push ebp
c010e15b: e8 93 b3 ff ff             call 0xc01094f3 <PerformTransfer>
c010e160: 83 c4 10                   add esp, 16
c010e163: 83 c4 5c                   add esp, 92
c010e166: 5b                         pop ebx
c010e167: 5e                         pop esi
c010e168: 5f                         pop edi
c010e169: 5d                         pop ebp
c010e16a: c3                         ret

c010e16b <SysStat>:
c010e16b: 57                         push edi
c010e16c: 56                         push esi
c010e16d: 53                         push ebx
c010e16e: 81 ec c0 01 00 00          sub esp, 448
c010e174: 8b b4 24 d4 01 00 00       mov esi, dword ptr [esp + 468]
c010e17b: 8b 84 24 e0 01 00 00       mov eax, dword ptr [esp + 480]
c010e182: 83 bc 24 d8 01 00 00 00    cmp dword ptr [esp + 472], 0
c010e18a: 74 7c                      je 0xc010e208 <SysStat+0x9d>
c010e18c: bb 07 00 00 00             mov ebx, 7
c010e191: 85 c0                      test eax, eax
c010e193: 0f 85 f5 00 00 00          jne 0xc010e28e <SysStat+0x123>
c010e199: e8 e7 8a ff ff             call 0xc0106c85 <GetProcess>
c010e19e: 83 ec 0c                   sub esp, 12
c010e1a1: 50                         push eax
c010e1a2: e8 3b 8b ff ff             call 0xc0106ce2 <GetFdTable>
```

```
c010e1fb: 50                            push eax
c010e1fc: e8 f2 b2 ff ff                call 0xc01094f3 <PerformTransfer>
c010e201: 89 c3                         mov ebx, eax
c010e203: e9 83 00 00 00                jmp 0xc010e28b <SysStat+0x120>
c010e208: bb 01 00 00 00                mov ebx, 1
c010e20d: 83 f8 01                      cmp eax, 1
c010e210: 74 7c                         je 0xc010e28e <SysStat+0x123>
c010e212: bb 07 00 00 00                mov ebx, 7
c010e217: 77 75                         ja 0xc010e28e <SysStat+0x123>
c010e219: 6a 00                         push 0
c010e21b: 68 8f 01 00 00                push 399
c010e220: ff b4 24 d8 01 00 00          push dword ptr [esp + 472]
c010e227: 8d 7c 24 3c                   lea edi, [esp + 60]
c010e22b: 57                            push edi
c010e22c: e8 2c b4 ff ff                call 0xc010965d <ReadStringFromUsermode>
c010e231: 89 c3                         mov ebx, eax
c010e233: 83 c4 10                      add esp, 16
c010e236: 85 c0                         test eax, eax
c010e238: 75 54                         jne 0xc010e28e <SysStat+0x123>
c010e23a: 8d 44 24 0c                   lea eax, [esp + 12]
c010e23e: 50                            push eax
c010e23f: 6a 00                         push 0
c010e241: 6a 00                         push 0
c010e243: 57                            push edi
c010e244: e8 04 be ff ff                call 0xc010a04d <OpenFile>
c010e249: 89 c3                         mov ebx, eax
c010e24b: 83 c4 10                      add esp, 16
c010e24e: 85 c0                         test eax, eax
c010e250: 75 3c                         jne 0xc010e28e <SysStat+0x123>
c010e252: 8d 5c 24 10                   lea ebx, [esp + 16]
c010e256: 50                            push eax
c010e257: 50                            push eax
c010e258: 6a 00                         push 0
c010e25a: 6a 00                         push 0
c010e25c: 6a 00                         push 0
c010e25e: 6a 48                         push 72
c010e260: 56                            push esi
c010e261: 53                            push ebx
c010e262: e8 82 b5 ff ff                call 0xc01097e9 <CreateTransferWritingToUser>
c010e267: 83 c4 1c                      add esp, 28
c010e26a: 6a 00                         push 0
c010e26c: 6a 48                         push 72
c010e26e: 53                            push ebx
c010e26f: 8b 44 24 18                   mov eax, dword ptr [esp + 24]
c010e273: 8b 40 30                      mov eax, dword ptr [eax + 48]
c010e276: 83 c0 4c                      add eax, 76
c010e279: 50                            push eax
c010e27a: e8 74 b2 ff ff                call 0xc01094f3 <PerformTransfer>
c010e27f: 89 c3                         mov ebx, eax
c010e281: 5a                            pop edx
c010e282: ff 74 24 18                   push dword ptr [esp + 24]
c010e286: e8 61 c0 ff ff                call 0xc010a2ec <CloseFile>
c010e28b: 83 c4 10                      add esp, 16
c010e28e: 89 d8                         mov eax, ebx
c010e290: 81 c4 c0 01 00 00             add esp, 448
c010e296: 5b                            pop ebx
c010e297: 5e                            pop esi
c010e298: 5f                            pop edi
c010e299: c3                            ret

c010e29a <SysTerminate>:
c010e29a: 83 ec 18                      sub esp, 24
c010e29d: 0f 21 d8                      mov eax, dr3
c010e2a0: c1 e0 06                      shl eax, 6
c010e2a3: ff b0 c4 40 11 c0             push dword ptr [eax - 1072611132]
c010e2a9: e8 c8 87 ff ff                call 0xc0106a76 <TerminateThread>
c010e2ae: b8 20 00 00 00                mov eax, 32
c010e2b3: 83 c4 1c                      add esp, 28
c010e2b6: c3                            ret

c010e2b7 <SysTime>:
```

```
c010e30c: 8d 7c 24 4c                lea edi, [esp + 76]
c010e310: b9 08 00 00 00             mov ecx, 8
c010e315: f3 a5                      rep  movsd dword ptr es:[edi], dword ptr [esi
c010e317: 83 c4 1c                   add esp, 28
c010e31a: 6a 00                      push 0
c010e31c: 6a 08                      push 8
c010e31e: 8d 44 24 38                lea eax, [esp + 56]
c010e322: 50                         push eax
c010e323: 8d 44 24 34                lea eax, [esp + 52]
c010e327: e9 e7 00 00 00             jmp 0xc010e413 <SysTime+0x15c>
c010e32c: 83 f8 01                   cmp eax, 1
c010e32f: 75 64                      jne 0xc010e395 <SysTime+0xde>
c010e331: 89 e6                      mov esi, esp
c010e333: 52                         push edx
c010e334: 52                         push edx
c010e335: 6a 00                      push 0
c010e337: 6a 00                      push 0
c010e339: 6a 00                      push 0
c010e33b: 6a 08                      push 8
c010e33d: 53                         push ebx
c010e33e: 56                         push esi
c010e33f: e8 de b4 ff ff             call 0xc0109822 <CreateTransferReadingFromUse
c010e344: 8d 7c 24 4c                lea edi, [esp + 76]
c010e348: b9 08 00 00 00             mov ecx, 8
c010e34d: f3 a5                      rep  movsd dword ptr es:[edi], dword ptr [esi
c010e34f: 83 c4 1c                   add esp, 28
c010e352: 6a 00                      push 0
c010e354: 6a 08                      push 8
c010e356: 8d 44 24 38                lea eax, [esp + 56]
c010e35a: 50                         push eax
c010e35b: 8d 44 24 34                lea eax, [esp + 52]
c010e35f: 50                         push eax
c010e360: e8 8e b1 ff ff             call 0xc01094f3 <PerformTransfer>
c010e365: 83 c4 10                   add esp, 16
c010e368: 85 c0                      test eax, eax
c010e36a: 0f 85 be 00 00 00          jne 0xc010e42e <SysTime+0x177>
c010e370: 8b 4c 24 20                mov ecx, dword ptr [esp + 32]
c010e374: 8b 5c 24 24                mov ebx, dword ptr [esp + 36]
c010e378: 53                         push ebx
c010e379: 51                         push ecx
c010e37a: 8b 44 24 30                mov eax, dword ptr [esp + 48]
c010e37e: 8b 54 24 34                mov edx, dword ptr [esp + 52]
c010e382: 29 c8                      sub eax, ecx
c010e384: 19 da                      sbb edx, ebx
c010e386: 52                         push edx
c010e387: 50                         push eax
c010e388: e8 18 e5 ff ff             call 0xc010c8a5 <ArchSetUtcTime>
c010e38d: 83 c4 10                   add esp, 16
c010e390: e9 99 00 00 00             jmp 0xc010e42e <SysTime+0x177>
c010e395: 83 f8 02                   cmp eax, 2
c010e398: 0f 85 80 00 00 00          jne 0xc010e41e <SysTime+0x167>
c010e39e: 83 ec 0c                   sub esp, 12
c010e3a1: 68 4f 1f 11 c0             push 3222347599
c010e3a6: e8 2c 2e ff ff             call 0xc01011d7 <strlen>
c010e3ab: 89 c2                      mov edx, eax
c010e3ad: 83 c4 10                   add esp, 16
c010e3b0: b8 0d 00 00 00             mov eax, 13
c010e3b5: 3b 54 24 68                cmp edx, dword ptr [esp + 104]
c010e3b9: 73 73                      jae 0xc010e42e <SysTime+0x177>
c010e3bb: 83 ec 0c                   sub esp, 12
c010e3be: 68 4f 1f 11 c0             push 3222347599
c010e3c3: e8 0f 2e ff ff             call 0xc01011d7 <strlen>
c010e3c8: 40                         inc eax
c010e3c9: 31 d2                      xor edx, edx
c010e3cb: 52                         push edx
c010e3cc: 50                         push eax
c010e3cd: 53                         push ebx
c010e3ce: 68 4f 1f 11 c0             push 3222347599
c010e3d3: e8 eb b1 ff ff             call 0xc01095c3 <WriteStringToUsermode>
c010e3d8: 83 c4 20                   add esp, 32
c010e3db: 85 c0                      test eax, eax
```

```
c010e42e: 83 c4 50                      add esp, 80
c010e431: 5b                            pop ebx
c010e432: 5e                            pop esi
c010e433: 5f                            pop edi
c010e434: c3                            ret

c010e435 <SysUnmapVirt>:
c010e435: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c010e439: 8b 54 24 08                   mov edx, dword ptr [esp + 8]
c010e43d: 3d ff ff ff 07                cmp eax, 134217727
c010e442: 76 18                         jbe 0xc010e45c <SysUnmapVirt+0x27>
c010e444: 01 d0                         add eax, edx
c010e446: 0f 92 c2                      setb dl
c010e449: 0f b6 d2                      movzx edx, dl
c010e44c: 3d ff ff ff bf                cmp eax, 3221225471
c010e451: 77 09                         ja 0xc010e45c <SysUnmapVirt+0x27>
c010e453: 85 d2                         test edx, edx
c010e455: 75 05                         jne 0xc010e45c <SysUnmapVirt+0x27>
c010e457: e9 9c 70 ff ff                jmp 0xc01054f8 <UnmapVirt>
c010e45c: b8 07 00 00 00                mov eax, 7
c010e461: c3                            ret

c010e462 <SysWaitpid>:
c010e462: 55                            push ebp
c010e463: 57                            push edi
c010e464: 56                            push esi
c010e465: 53                            push ebx
c010e466: 83 ec 60                      sub esp, 96
c010e469: ff b4 24 80 00 00 00          push dword ptr [esp + 128]
c010e470: 8d 6c 24 30                   lea ebp, [esp + 48]
c010e474: 55                            push ebp
c010e475: ff 74 24 7c                   push dword ptr [esp + 124]
c010e479: e8 56 8d ff ff                call 0xc01071d4 <WaitProcess>
c010e47e: 89 44 24 3c                   mov dword ptr [esp + 60], eax
c010e482: 8d 5c 24 40                   lea ebx, [esp + 64]
c010e486: 5a                            pop edx
c010e487: 59                            pop ecx
c010e488: 6a 00                         push 0
c010e48a: 6a 00                         push 0
c010e48c: 6a 00                         push 0
c010e48e: 6a 04                         push 4
c010e490: ff b4 24 8c 00 00 00          push dword ptr [esp + 140]
c010e497: 53                            push ebx
c010e498: e8 4c b3 ff ff                call 0xc01097e9 <CreateTransferWritingToUser>
c010e49d: 83 c4 1c                      add esp, 28
c010e4a0: 6a 00                         push 0
c010e4a2: 6a 04                         push 4
c010e4a4: 53                            push ebx
c010e4a5: 8d 44 24 38                   lea eax, [esp + 56]
c010e4a9: 50                            push eax
c010e4aa: e8 44 b0 ff ff                call 0xc01094f3 <PerformTransfer>
c010e4af: 83 c4 10                      add esp, 16
c010e4b2: 83 7c 24 38 00                cmp dword ptr [esp + 56], 0
c010e4b7: 75 07                         jne 0xc010e4c0 <SysWaitpid+0x5e>
c010e4b9: 83 7c 24 34 00                cmp dword ptr [esp + 52], 0
c010e4be: 74 07                         je 0xc010e4c7 <SysWaitpid+0x65>
c010e4c0: b8 07 00 00 00                mov eax, 7
c010e4c5: eb 43                         jmp 0xc010e50a <SysWaitpid+0xa8>
c010e4c7: 89 e6                         mov esi, esp
c010e4c9: 50                            push eax
c010e4ca: 50                            push eax
c010e4cb: 6a 00                         push 0
c010e4cd: 6a 00                         push 0
c010e4cf: 6a 00                         push 0
c010e4d1: 6a 04                         push 4
c010e4d3: ff b4 24 90 00 00 00          push dword ptr [esp + 144]
c010e4da: 56                            push esi
c010e4db: e8 09 b3 ff ff                call 0xc01097e9 <CreateTransferWritingToUser>
c010e4e0: b9 08 00 00 00                mov ecx, 8
c010e4e5: 89 df                         mov edi, ebx
c010e4e7: f3 a5                         rep  movsd dword ptr es:[edi], dword ptr [esi
```

```
c010e52d: 0f 22 d9                      mov cr3, ecx
c010e530: 31 c0                         xor eax, eax
c010e532: 0f 23 d8                      mov dr3, eax
c010e535: bc 00 00 14 c0                mov esp, 3222536192
c010e53a: 53                            push ebx
c010e53b: e8 14 4b ff ff                call 0xc0103054 <KernelMain>
c010e540: fa                            cli
c010e541: f4                            hlt
c010e542: eb fe                         jmp 0xc010e542 <KernelEntryPoint+0x22>
  ...

c010e550 <x86LoadGdt>:
c010e550: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c010e554: 0f 01 10                      lgdtd [eax]
c010e557: ea 5e e5 10 c0 08 00          ljmp 8, 3222332766

c010e55e <x86LoadGdt.reload>:
c010e55e: 66 b8 10 00                   mov ax, 16
c010e562: 8e d8                         mov ds, eax
c010e564: 8e c0                         mov es, eax
c010e566: 8e d0                         mov ss, eax
c010e568: c3                            ret
c010e569: 00 00                         add byte ptr [eax], al
c010e56b: 00 00                         add byte ptr [eax], al
c010e56d: 00 00                         add byte ptr [eax], al
c010e56f: 00 8b 44 24 04 0f             add byte ptr [ebx + 251929668], cl

c010e570 <x86LoadIdt>:
c010e570: 8b 44 24 04                   mov eax, dword ptr [esp + 4]
c010e574: 0f 01 18                      lidtd [eax]
c010e577: c3                            ret
  ...

c010e580 <InterruptCommonHandler>:
c010e580: 60                            pushal
c010e581: 1e                            push ds
c010e582: 06                            push es
c010e583: 0f a0                         push fs
c010e585: 0f a8                         push gs
c010e587: 66 b8 10 00                   mov ax, 16
c010e58b: 8e d8                         mov ds, eax
c010e58d: 8e c0                         mov es, eax
c010e58f: 54                            push esp
c010e590: fc                            cld
c010e591: e8 71 cb ff ff                call 0xc010b107 <x86HandleInterrupt>
c010e596: 83 c4 04                      add esp, 4
c010e599: 0f a9                         pop gs
c010e59b: 0f a1                         pop fs
c010e59d: 07                            pop es
c010e59e: 1f                            pop ds
c010e59f: 61                            popal
c010e5a0: 83 c4 08                      add esp, 8
c010e5a3: cf                            iretd
  ...

c010e5b0 <ArchReadTimestamp>:
c010e5b0: 0f 31                         rdtsc
c010e5b2: c3                            ret

c010e5b3 <ArchStallProcessor>:
c010e5b3: f4                            hlt
c010e5b4: c3                            ret
  ...
c010e5bd: 00 00                         add byte ptr [eax], al
c010e5bf: 00 8b 44 24 04 f0             add byte ptr [ebx - 268164028], cl

c010e5c0 <ArchSpinlockAcquire>:
c010e5c0: 8b 44 24 04                   mov eax, dword ptr [esp + 4]

c010e5c4 <ArchSpinlockAcquire.try_acquire>:
c010e5c4: f0                            lock
```

```
c010e603: 8b 7c 24 14                 mov edi, dword ptr [esp + 20]
c010e607: 8b 74 24 18                 mov esi, dword ptr [esp + 24]
c010e60b: 89 67 04                    mov dword ptr [edi + 4], esp
c010e60e: 8b 66 04                    mov esp, dword ptr [esi + 4]
c010e611: e8 e5 4b ff ff              call 0xc01031fb <GetCpu>
c010e616: 8b 1e                       mov ebx, dword ptr [esi]
c010e618: 8b 48 08                    mov ecx, dword ptr [eax + 8]
c010e61b: 8b 11                       mov edx, dword ptr [ecx]
c010e61d: 89 5a 04                    mov dword ptr [edx + 4], ebx
c010e620: 5d                          pop ebp
c010e621: 5f                          pop edi
c010e622: 5e                          pop esi
c010e623: 5b                          pop ebx
c010e624: c3                          ret
  ...
c010e62d: 00 00                       add byte ptr [eax], al
c010e62f: 00 8b 44 24 04 0f           add byte ptr [ebx + 251929668], cl

c010e630 <x86LoadTss>:
c010e630: 8b 44 24 04                 mov eax, dword ptr [esp + 4]
c010e634: 0f 00 d8                    ltr ax
c010e637: c3                          ret
  ...

c010e640 <ArchSwitchToUsermode>:
c010e640: 8b 5c 24 04                 mov ebx, dword ptr [esp + 4]
c010e644: 8b 4c 24 08                 mov ecx, dword ptr [esp + 8]
c010e648: 8b 54 24 0c                 mov edx, dword ptr [esp + 12]
c010e64c: 66 b8 23 00                 mov ax, 35
c010e650: 8e d8                       mov ds, eax
c010e652: 8e c0                       mov es, eax
c010e654: 8e e0                       mov fs, eax
c010e656: 8e e8                       mov gs, eax
c010e658: 6a 23                       push 35
c010e65a: 51                          push ecx
c010e65b: 68 02 02 00 00              push 514
c010e660: 6a 1b                       push 27
c010e662: 53                          push ebx
c010e663: cf                          iretd
  ...

c010e670 <x86GetCr2>:
c010e670: 0f 20 d0                    mov eax, cr2
c010e673: c3                          ret

c010e674 <x86SetCr3>:
c010e674: 8b 44 24 04                 mov eax, dword ptr [esp + 4]
c010e678: 0f 22 d8                    mov cr3, eax
c010e67b: c3                          ret
c010e67c: 00 00                       add byte ptr [eax], al
c010e67e: 00 00                       add byte ptr [eax], al

c010e680 <isrx0>:
c010e680: 6a 00                       push 0
c010e682: 6a 00                       push 0
c010e684: eb 4e                       jmp 0xc010e6d4 <thunk0>

c010e686 <isrx1>:
c010e686: 6a 00                       push 0
c010e688: 6a 01                       push 1
c010e68a: eb 48                       jmp 0xc010e6d4 <thunk0>

c010e68c <isrx2>:
c010e68c: 6a 00                       push 0
c010e68e: 6a 02                       push 2
c010e690: eb 42                       jmp 0xc010e6d4 <thunk0>

c010e692 <isrx3>:
c010e692: 6a 00                       push 0
c010e694: 6a 03                       push 3
c010e696: eb 3c                       jmp 0xc010e6d4 <thunk0>
```

```
c010e6ba <isrx10>:
c010e6ba: 6a 0a                         push 10
c010e6bc: eb 16                         jmp 0xc010e6d4 <thunk0>

c010e6be <isrx11>:
c010e6be: 6a 0b                         push 11
c010e6c0: eb 12                         jmp 0xc010e6d4 <thunk0>

c010e6c2 <isrx12>:
c010e6c2: 6a 0c                         push 12
c010e6c4: eb 0e                         jmp 0xc010e6d4 <thunk0>

c010e6c6 <isrx13>:
c010e6c6: 6a 0d                         push 13
c010e6c8: eb 0a                         jmp 0xc010e6d4 <thunk0>

c010e6ca <isrx14>:
c010e6ca: 6a 0e                         push 14
c010e6cc: eb 06                         jmp 0xc010e6d4 <thunk0>

c010e6ce <isrx15>:
c010e6ce: 6a 00                         push 0
c010e6d0: 6a 0f                         push 15
c010e6d2: eb 00                         jmp 0xc010e6d4 <thunk0>

c010e6d4 <thunk0>:
c010e6d4: e9 a7 fe ff ff                jmp 0xc010e580 <InterruptCommonHandler>

c010e6d9 <isrx16>:
c010e6d9: 6a 00                         push 0
c010e6db: 6a 10                         push 16
c010e6dd: eb f5                         jmp 0xc010e6d4 <thunk0>

c010e6df <isrx17>:
c010e6df: 6a 11                         push 17
c010e6e1: eb f1                         jmp 0xc010e6d4 <thunk0>

c010e6e3 <isrx18>:
c010e6e3: 6a 00                         push 0
c010e6e5: 6a 12                         push 18
c010e6e7: eb eb                         jmp 0xc010e6d4 <thunk0>

c010e6e9 <isrx19>:
c010e6e9: 6a 00                         push 0
c010e6eb: 6a 13                         push 19
c010e6ed: eb e5                         jmp 0xc010e6d4 <thunk0>

c010e6ef <isrx20>:
c010e6ef: 6a 00                         push 0
c010e6f1: 6a 14                         push 20
c010e6f3: eb df                         jmp 0xc010e6d4 <thunk0>

c010e6f5 <isrx21>:
c010e6f5: 6a 00                         push 0
c010e6f7: 6a 15                         push 21
c010e6f9: eb d9                         jmp 0xc010e6d4 <thunk0>

c010e6fb <isrx22>:
c010e6fb: 6a 00                         push 0
c010e6fd: 6a 16                         push 22
c010e6ff: eb d3                         jmp 0xc010e6d4 <thunk0>

c010e701 <isrx23>:
c010e701: 6a 00                         push 0
c010e703: 6a 17                         push 23
c010e705: eb cd                         jmp 0xc010e6d4 <thunk0>

c010e707 <isrx24>:
c010e707: 6a 00                         push 0
c010e709: 6a 18                         push 24
```

```
c010e72d: 6a 1e                          push 30
c010e72f: eb a3                          jmp 0xc010e6d4 <thunk0>

c010e731 <isrx31>:
c010e731: 6a 00                          push 0
c010e733: 6a 1f                          push 31
c010e735: eb 9d                          jmp 0xc010e6d4 <thunk0>

c010e737 <isrx32>:
c010e737: 6a 00                          push 0
c010e739: 6a 20                          push 32
c010e73b: eb 5a                          jmp 0xc010e797 <thunk1>

c010e73d <isrx33>:
c010e73d: 6a 00                          push 0
c010e73f: 6a 21                          push 33
c010e741: eb 54                          jmp 0xc010e797 <thunk1>

c010e743 <isrx34>:
c010e743: 6a 00                          push 0
c010e745: 6a 22                          push 34
c010e747: eb 4e                          jmp 0xc010e797 <thunk1>

c010e749 <isrx35>:
c010e749: 6a 00                          push 0
c010e74b: 6a 23                          push 35
c010e74d: eb 48                          jmp 0xc010e797 <thunk1>

c010e74f <isrx36>:
c010e74f: 6a 00                          push 0
c010e751: 6a 24                          push 36
c010e753: eb 42                          jmp 0xc010e797 <thunk1>

c010e755 <isrx37>:
c010e755: 6a 00                          push 0
c010e757: 6a 25                          push 37
c010e759: eb 3c                          jmp 0xc010e797 <thunk1>

c010e75b <isrx38>:
c010e75b: 6a 00                          push 0
c010e75d: 6a 26                          push 38
c010e75f: eb 36                          jmp 0xc010e797 <thunk1>

c010e761 <isrx39>:
c010e761: 6a 00                          push 0
c010e763: 6a 27                          push 39
c010e765: eb 30                          jmp 0xc010e797 <thunk1>

c010e767 <isrx40>:
c010e767: 6a 00                          push 0
c010e769: 6a 28                          push 40
c010e76b: eb 2a                          jmp 0xc010e797 <thunk1>

c010e76d <isrx41>:
c010e76d: 6a 00                          push 0
c010e76f: 6a 29                          push 41
c010e771: eb 24                          jmp 0xc010e797 <thunk1>

c010e773 <isrx42>:
c010e773: 6a 00                          push 0
c010e775: 6a 2a                          push 42
c010e777: eb 1e                          jmp 0xc010e797 <thunk1>

c010e779 <isrx43>:
c010e779: 6a 00                          push 0
c010e77b: 6a 2b                          push 43
c010e77d: eb 18                          jmp 0xc010e797 <thunk1>

c010e77f <isrx44>:
c010e77f: 6a 00                          push 0
c010e781: 6a 2c                          push 44
```

```
c010e7a8 <isrx50>:
c010e7a8: 6a 00                         push 0
c010e7aa: 6a 32                         push 50
c010e7ac: eb e9                         jmp 0xc010e797 <thunk1>

c010e7ae <isrx51>:
c010e7ae: 6a 00                         push 0
c010e7b0: 6a 33                         push 51
c010e7b2: eb e3                         jmp 0xc010e797 <thunk1>

c010e7b4 <isrx52>:
c010e7b4: 6a 00                         push 0
c010e7b6: 6a 34                         push 52
c010e7b8: eb dd                         jmp 0xc010e797 <thunk1>

c010e7ba <isrx53>:
c010e7ba: 6a 00                         push 0
c010e7bc: 6a 35                         push 53
c010e7be: eb d7                         jmp 0xc010e797 <thunk1>

c010e7c0 <isrx54>:
c010e7c0: 6a 00                         push 0
c010e7c2: 6a 36                         push 54
c010e7c4: eb d1                         jmp 0xc010e797 <thunk1>

c010e7c6 <isrx55>:
c010e7c6: 6a 00                         push 0
c010e7c8: 6a 37                         push 55
c010e7ca: eb cb                         jmp 0xc010e797 <thunk1>

c010e7cc <isrx56>:
c010e7cc: 6a 00                         push 0
c010e7ce: 6a 38                         push 56
c010e7d0: eb c5                         jmp 0xc010e797 <thunk1>

c010e7d2 <isrx57>:
c010e7d2: 6a 00                         push 0
c010e7d4: 6a 39                         push 57
c010e7d6: eb bf                         jmp 0xc010e797 <thunk1>

c010e7d8 <isrx58>:
c010e7d8: 6a 00                         push 0
c010e7da: 6a 3a                         push 58
c010e7dc: eb b9                         jmp 0xc010e797 <thunk1>

c010e7de <isrx59>:
c010e7de: 6a 00                         push 0
c010e7e0: 6a 3b                         push 59
c010e7e2: eb b3                         jmp 0xc010e797 <thunk1>

c010e7e4 <isrx60>:
c010e7e4: 6a 00                         push 0
c010e7e6: 6a 3c                         push 60
c010e7e8: eb ad                         jmp 0xc010e797 <thunk1>

c010e7ea <isrx61>:
c010e7ea: 6a 00                         push 0
c010e7ec: 6a 3d                         push 61
c010e7ee: eb a7                         jmp 0xc010e797 <thunk1>

c010e7f0 <isrx62>:
c010e7f0: 6a 00                         push 0
c010e7f2: 6a 3e                         push 62
c010e7f4: eb a1                         jmp 0xc010e797 <thunk1>

c010e7f6 <isrx63>:
c010e7f6: 6a 00                         push 0
c010e7f8: 6a 3f                         push 63
c010e7fa: eb 9b                         jmp 0xc010e797 <thunk1>
```

```
c010e820 <isrx70>:
c010e820: 6a 00                         push 0
c010e822: 6a 46                         push 70
c010e824: eb 36                         jmp 0xc010e85c <thunk2>

c010e826 <isrx71>:
c010e826: 6a 00                         push 0
c010e828: 6a 47                         push 71
c010e82a: eb 30                         jmp 0xc010e85c <thunk2>

c010e82c <isrx72>:
c010e82c: 6a 00                         push 0
c010e82e: 6a 48                         push 72
c010e830: eb 2a                         jmp 0xc010e85c <thunk2>

c010e832 <isrx73>:
c010e832: 6a 00                         push 0
c010e834: 6a 49                         push 73
c010e836: eb 24                         jmp 0xc010e85c <thunk2>

c010e838 <isrx74>:
c010e838: 6a 00                         push 0
c010e83a: 6a 4a                         push 74
c010e83c: eb 1e                         jmp 0xc010e85c <thunk2>

c010e83e <isrx75>:
c010e83e: 6a 00                         push 0
c010e840: 6a 4b                         push 75
c010e842: eb 18                         jmp 0xc010e85c <thunk2>

c010e844 <isrx76>:
c010e844: 6a 00                         push 0
c010e846: 6a 4c                         push 76
c010e848: eb 12                         jmp 0xc010e85c <thunk2>

c010e84a <isrx77>:
c010e84a: 6a 00                         push 0
c010e84c: 6a 4d                         push 77
c010e84e: eb 0c                         jmp 0xc010e85c <thunk2>

c010e850 <isrx78>:
c010e850: 6a 00                         push 0
c010e852: 6a 4e                         push 78
c010e854: eb 06                         jmp 0xc010e85c <thunk2>

c010e856 <isrx79>:
c010e856: 6a 00                         push 0
c010e858: 6a 4f                         push 79
c010e85a: eb 00                         jmp 0xc010e85c <thunk2>

c010e85c <thunk2>:
c010e85c: e9 1f fd ff ff                jmp 0xc010e580 <InterruptCommonHandler>

c010e861 <isrx80>:
c010e861: 6a 00                         push 0
c010e863: 6a 50                         push 80
c010e865: eb f5                         jmp 0xc010e85c <thunk2>

c010e867 <isrx81>:
c010e867: 6a 00                         push 0
c010e869: 6a 51                         push 81
c010e86b: eb ef                         jmp 0xc010e85c <thunk2>

c010e86d <isrx82>:
c010e86d: 6a 00                         push 0
c010e86f: 6a 52                         push 82
c010e871: eb e9                         jmp 0xc010e85c <thunk2>

c010e873 <isrx83>:
c010e873: 6a 00                         push 0
```

```
c010e897: 6a 00                         push 0
c010e899: 6a 59                         push 89
c010e89b: eb bf                         jmp 0xc010e85c <thunk2>

c010e89d <isrx90>:
c010e89d: 6a 00                         push 0
c010e89f: 6a 5a                         push 90
c010e8a1: eb b9                         jmp 0xc010e85c <thunk2>

c010e8a3 <isrx91>:
c010e8a3: 6a 00                         push 0
c010e8a5: 6a 5b                         push 91
c010e8a7: eb b3                         jmp 0xc010e85c <thunk2>

c010e8a9 <isrx92>:
c010e8a9: 6a 00                         push 0
c010e8ab: 6a 5c                         push 92
c010e8ad: eb ad                         jmp 0xc010e85c <thunk2>

c010e8af <isrx93>:
c010e8af: 6a 00                         push 0
c010e8b1: 6a 5d                         push 93
c010e8b3: eb a7                         jmp 0xc010e85c <thunk2>

c010e8b5 <isrx94>:
c010e8b5: 6a 00                         push 0
c010e8b7: 6a 5e                         push 94
c010e8b9: eb a1                         jmp 0xc010e85c <thunk2>

c010e8bb <isrx95>:
c010e8bb: 6a 00                         push 0
c010e8bd: 6a 5f                         push 95
c010e8bf: eb 9b                         jmp 0xc010e85c <thunk2>

c010e8c1 <isrx96>:
c010e8c1: 6a 00                         push 0
c010e8c3: 6a 60                         push 96
c010e8c5: eb 5a                         jmp 0xc010e921 <thunk3>

c010e8c7 <isrx97>:
c010e8c7: 6a 00                         push 0
c010e8c9: 6a 61                         push 97
c010e8cb: eb 54                         jmp 0xc010e921 <thunk3>

c010e8cd <isrx98>:
c010e8cd: 6a 00                         push 0
c010e8cf: 6a 62                         push 98
c010e8d1: eb 4e                         jmp 0xc010e921 <thunk3>

c010e8d3 <isrx99>:
c010e8d3: 6a 00                         push 0
c010e8d5: 6a 63                         push 99
c010e8d7: eb 48                         jmp 0xc010e921 <thunk3>

c010e8d9 <isrx100>:
c010e8d9: 6a 00                         push 0
c010e8db: 6a 64                         push 100
c010e8dd: eb 42                         jmp 0xc010e921 <thunk3>

c010e8df <isrx101>:
c010e8df: 6a 00                         push 0
c010e8e1: 6a 65                         push 101
c010e8e3: eb 3c                         jmp 0xc010e921 <thunk3>

c010e8e5 <isrx102>:
c010e8e5: 6a 00                         push 0
c010e8e7: 6a 66                         push 102
c010e8e9: eb 36                         jmp 0xc010e921 <thunk3>

c010e8eb <isrx103>:
c010e8eb: 6a 00                         push 0
```

```
c010e90f: 6a 00                         push 0
c010e911: 6a 6d                         push 109
c010e913: eb 0c                         jmp 0xc010e921 <thunk3>

c010e915 <isrx110>:
c010e915: 6a 00                         push 0
c010e917: 6a 6e                         push 110
c010e919: eb 06                         jmp 0xc010e921 <thunk3>

c010e91b <isrx111>:
c010e91b: 6a 00                         push 0
c010e91d: 6a 6f                         push 111
c010e91f: eb 00                         jmp 0xc010e921 <thunk3>

c010e921 <thunk3>:
c010e921: e9 5a fc ff ff                jmp 0xc010e580 <InterruptCommonHandler>

c010e926 <isrx112>:
c010e926: 6a 00                         push 0
c010e928: 6a 70                         push 112
c010e92a: eb f5                         jmp 0xc010e921 <thunk3>

c010e92c <isrx113>:
c010e92c: 6a 00                         push 0
c010e92e: 6a 71                         push 113
c010e930: eb ef                         jmp 0xc010e921 <thunk3>

c010e932 <isrx114>:
c010e932: 6a 00                         push 0
c010e934: 6a 72                         push 114
c010e936: eb e9                         jmp 0xc010e921 <thunk3>

c010e938 <isrx115>:
c010e938: 6a 00                         push 0
c010e93a: 6a 73                         push 115
c010e93c: eb e3                         jmp 0xc010e921 <thunk3>

c010e93e <isrx116>:
c010e93e: 6a 00                         push 0
c010e940: 6a 74                         push 116
c010e942: eb dd                         jmp 0xc010e921 <thunk3>

c010e944 <isrx117>:
c010e944: 6a 00                         push 0
c010e946: 6a 75                         push 117
c010e948: eb d7                         jmp 0xc010e921 <thunk3>

c010e94a <isrx118>:
c010e94a: 6a 00                         push 0
c010e94c: 6a 76                         push 118
c010e94e: eb d1                         jmp 0xc010e921 <thunk3>

c010e950 <isrx119>:
c010e950: 6a 00                         push 0
c010e952: 6a 77                         push 119
c010e954: eb cb                         jmp 0xc010e921 <thunk3>

c010e956 <isrx120>:
c010e956: 6a 00                         push 0
c010e958: 6a 78                         push 120
c010e95a: eb c5                         jmp 0xc010e921 <thunk3>

c010e95c <isrx121>:
c010e95c: 6a 00                         push 0
c010e95e: 6a 79                         push 121
c010e960: eb bf                         jmp 0xc010e921 <thunk3>

c010e962 <isrx122>:
c010e962: 6a 00                         push 0
c010e964: 6a 7a                         push 122
c010e966: eb b9                         jmp 0xc010e921 <thunk3>
```

```
c010e98a: eb 5a                         jmp 0xc010e9e6 <thunk4>

c010e98c <isrx129>:
c010e98c: 6a 00                         push 0
c010e98e: 6a 81                         push -127
c010e990: eb 54                         jmp 0xc010e9e6 <thunk4>

c010e992 <isrx130>:
c010e992: 6a 00                         push 0
c010e994: 6a 82                         push -126
c010e996: eb 4e                         jmp 0xc010e9e6 <thunk4>

c010e998 <isrx131>:
c010e998: 6a 00                         push 0
c010e99a: 6a 83                         push -125
c010e99c: eb 48                         jmp 0xc010e9e6 <thunk4>

c010e99e <isrx132>:
c010e99e: 6a 00                         push 0
c010e9a0: 6a 84                         push -124
c010e9a2: eb 42                         jmp 0xc010e9e6 <thunk4>

c010e9a4 <isrx133>:
c010e9a4: 6a 00                         push 0
c010e9a6: 6a 85                         push -123
c010e9a8: eb 3c                         jmp 0xc010e9e6 <thunk4>

c010e9aa <isrx134>:
c010e9aa: 6a 00                         push 0
c010e9ac: 6a 86                         push -122
c010e9ae: eb 36                         jmp 0xc010e9e6 <thunk4>

c010e9b0 <isrx135>:
c010e9b0: 6a 00                         push 0
c010e9b2: 6a 87                         push -121
c010e9b4: eb 30                         jmp 0xc010e9e6 <thunk4>

c010e9b6 <isrx136>:
c010e9b6: 6a 00                         push 0
c010e9b8: 6a 88                         push -120
c010e9ba: eb 2a                         jmp 0xc010e9e6 <thunk4>

c010e9bc <isrx137>:
c010e9bc: 6a 00                         push 0
c010e9be: 6a 89                         push -119
c010e9c0: eb 24                         jmp 0xc010e9e6 <thunk4>

c010e9c2 <isrx138>:
c010e9c2: 6a 00                         push 0
c010e9c4: 6a 8a                         push -118
c010e9c6: eb 1e                         jmp 0xc010e9e6 <thunk4>

c010e9c8 <isrx139>:
c010e9c8: 6a 00                         push 0
c010e9ca: 6a 8b                         push -117
c010e9cc: eb 18                         jmp 0xc010e9e6 <thunk4>

c010e9ce <isrx140>:
c010e9ce: 6a 00                         push 0
c010e9d0: 6a 8c                         push -116
c010e9d2: eb 12                         jmp 0xc010e9e6 <thunk4>

c010e9d4 <isrx141>:
c010e9d4: 6a 00                         push 0
c010e9d6: 6a 8d                         push -115
c010e9d8: eb 0c                         jmp 0xc010e9e6 <thunk4>

c010e9da <isrx142>:
c010e9da: 6a 00                         push 0
c010e9dc: 6a 8e                         push -114
c010e9de: eb 06                         jmp 0xc010e9e6 <thunk4>
```

```
c010ea03 <isrx148>:
c010ea03: 6a 00                         push 0
c010ea05: 6a 94                         push -108
c010ea07: eb dd                         jmp 0xc010e9e6 <thunk4>

c010ea09 <isrx149>:
c010ea09: 6a 00                         push 0
c010ea0b: 6a 95                         push -107
c010ea0d: eb d7                         jmp 0xc010e9e6 <thunk4>

c010ea0f <isrx150>:
c010ea0f: 6a 00                         push 0
c010ea11: 6a 96                         push -106
c010ea13: eb d1                         jmp 0xc010e9e6 <thunk4>

c010ea15 <isrx151>:
c010ea15: 6a 00                         push 0
c010ea17: 6a 97                         push -105
c010ea19: eb cb                         jmp 0xc010e9e6 <thunk4>

c010ea1b <isrx152>:
c010ea1b: 6a 00                         push 0
c010ea1d: 6a 98                         push -104
c010ea1f: eb c5                         jmp 0xc010e9e6 <thunk4>

c010ea21 <isrx153>:
c010ea21: 6a 00                         push 0
c010ea23: 6a 99                         push -103
c010ea25: eb bf                         jmp 0xc010e9e6 <thunk4>

c010ea27 <isrx154>:
c010ea27: 6a 00                         push 0
c010ea29: 6a 9a                         push -102
c010ea2b: eb b9                         jmp 0xc010e9e6 <thunk4>

c010ea2d <isrx155>:
c010ea2d: 6a 00                         push 0
c010ea2f: 6a 9b                         push -101
c010ea31: eb b3                         jmp 0xc010e9e6 <thunk4>

c010ea33 <isrx156>:
c010ea33: 6a 00                         push 0
c010ea35: 6a 9c                         push -100
c010ea37: eb ad                         jmp 0xc010e9e6 <thunk4>

c010ea39 <isrx157>:
c010ea39: 6a 00                         push 0
c010ea3b: 6a 9d                         push -99
c010ea3d: eb a7                         jmp 0xc010e9e6 <thunk4>

c010ea3f <isrx158>:
c010ea3f: 6a 00                         push 0
c010ea41: 6a 9e                         push -98
c010ea43: eb a1                         jmp 0xc010e9e6 <thunk4>

c010ea45 <isrx159>:
c010ea45: 6a 00                         push 0
c010ea47: 6a 9f                         push -97
c010ea49: eb 9b                         jmp 0xc010e9e6 <thunk4>

c010ea4b <isrx160>:
c010ea4b: 6a 00                         push 0
c010ea4d: 6a a0                         push -96
c010ea4f: eb 5a                         jmp 0xc010eaab <thunk5>

c010ea51 <isrx161>:
c010ea51: 6a 00                         push 0
c010ea53: 6a a1                         push -95
c010ea55: eb 54                         jmp 0xc010eaab <thunk5>

c010ea57 <isrx162>:
```

```
c010ea7b <isrx168>:
c010ea7b: 6a 00                         push 0
c010ea7d: 6a a8                         push -88
c010ea7f: eb 2a                         jmp 0xc010eaab <thunk5>

c010ea81 <isrx169>:
c010ea81: 6a 00                         push 0
c010ea83: 6a a9                         push -87
c010ea85: eb 24                         jmp 0xc010eaab <thunk5>

c010ea87 <isrx170>:
c010ea87: 6a 00                         push 0
c010ea89: 6a aa                         push -86
c010ea8b: eb 1e                         jmp 0xc010eaab <thunk5>

c010ea8d <isrx171>:
c010ea8d: 6a 00                         push 0
c010ea8f: 6a ab                         push -85
c010ea91: eb 18                         jmp 0xc010eaab <thunk5>

c010ea93 <isrx172>:
c010ea93: 6a 00                         push 0
c010ea95: 6a ac                         push -84
c010ea97: eb 12                         jmp 0xc010eaab <thunk5>

c010ea99 <isrx173>:
c010ea99: 6a 00                         push 0
c010ea9b: 6a ad                         push -83
c010ea9d: eb 0c                         jmp 0xc010eaab <thunk5>

c010ea9f <isrx174>:
c010ea9f: 6a 00                         push 0
c010eaa1: 6a ae                         push -82
c010eaa3: eb 06                         jmp 0xc010eaab <thunk5>

c010eaa5 <isrx175>:
c010eaa5: 6a 00                         push 0
c010eaa7: 6a af                         push -81
c010eaa9: eb 00                         jmp 0xc010eaab <thunk5>

c010eaab <thunk5>:
c010eaab: e9 d0 fa ff ff                jmp 0xc010e580 <InterruptCommonHandler>

c010eab0 <isrx176>:
c010eab0: 6a 00                         push 0
c010eab2: 6a b0                         push -80
c010eab4: eb f5                         jmp 0xc010eaab <thunk5>

c010eab6 <isrx177>:
c010eab6: 6a 00                         push 0
c010eab8: 6a b1                         push -79
c010eaba: eb ef                         jmp 0xc010eaab <thunk5>

c010eabc <isrx178>:
c010eabc: 6a 00                         push 0
c010eabe: 6a b2                         push -78
c010eac0: eb e9                         jmp 0xc010eaab <thunk5>

c010eac2 <isrx179>:
c010eac2: 6a 00                         push 0
c010eac4: 6a b3                         push -77
c010eac6: eb e3                         jmp 0xc010eaab <thunk5>

c010eac8 <isrx180>:
c010eac8: 6a 00                         push 0
c010eaca: 6a b4                         push -76
c010eacc: eb dd                         jmp 0xc010eaab <thunk5>

c010eace <isrx181>:
c010eace: 6a 00                         push 0
c010ead0: 6a b5                         push -75
```

```
c010eaf4: 6a bb                         push -69
c010eaf6: eb b3                         jmp 0xc010eaab <thunk5>

c010eaf8 <isrx188>:
c010eaf8: 6a 00                         push 0
c010eafa: 6a bc                         push -68
c010eafc: eb ad                         jmp 0xc010eaab <thunk5>

c010eafe <isrx189>:
c010eafe: 6a 00                         push 0
c010eb00: 6a bd                         push -67
c010eb02: eb a7                         jmp 0xc010eaab <thunk5>

c010eb04 <isrx190>:
c010eb04: 6a 00                         push 0
c010eb06: 6a be                         push -66
c010eb08: eb a1                         jmp 0xc010eaab <thunk5>

c010eb0a <isrx191>:
c010eb0a: 6a 00                         push 0
c010eb0c: 6a bf                         push -65
c010eb0e: eb 9b                         jmp 0xc010eaab <thunk5>

c010eb10 <isrx192>:
c010eb10: 6a 00                         push 0
c010eb12: 6a c0                         push -64
c010eb14: eb 5a                         jmp 0xc010eb70 <thunk6>

c010eb16 <isrx193>:
c010eb16: 6a 00                         push 0
c010eb18: 6a c1                         push -63
c010eb1a: eb 54                         jmp 0xc010eb70 <thunk6>

c010eb1c <isrx194>:
c010eb1c: 6a 00                         push 0
c010eb1e: 6a c2                         push -62
c010eb20: eb 4e                         jmp 0xc010eb70 <thunk6>

c010eb22 <isrx195>:
c010eb22: 6a 00                         push 0
c010eb24: 6a c3                         push -61
c010eb26: eb 48                         jmp 0xc010eb70 <thunk6>

c010eb28 <isrx196>:
c010eb28: 6a 00                         push 0
c010eb2a: 6a c4                         push -60
c010eb2c: eb 42                         jmp 0xc010eb70 <thunk6>

c010eb2e <isrx197>:
c010eb2e: 6a 00                         push 0
c010eb30: 6a c5                         push -59
c010eb32: eb 3c                         jmp 0xc010eb70 <thunk6>

c010eb34 <isrx198>:
c010eb34: 6a 00                         push 0
c010eb36: 6a c6                         push -58
c010eb38: eb 36                         jmp 0xc010eb70 <thunk6>

c010eb3a <isrx199>:
c010eb3a: 6a 00                         push 0
c010eb3c: 6a c7                         push -57
c010eb3e: eb 30                         jmp 0xc010eb70 <thunk6>

c010eb40 <isrx200>:
c010eb40: 6a 00                         push 0
c010eb42: 6a c8                         push -56
c010eb44: eb 2a                         jmp 0xc010eb70 <thunk6>

c010eb46 <isrx201>:
c010eb46: 6a 00                         push 0
c010eb48: 6a c9                         push -55
```

```
c010eb6c: 6a cf                         push -49
c010eb6e: eb 00                         jmp 0xc010eb70 <thunk6>

c010eb70 <thunk6>:
c010eb70: e9 0b fa ff ff                jmp 0xc010e580 <InterruptCommonHandler>

c010eb75 <isrx208>:
c010eb75: 6a 00                         push 0
c010eb77: 6a d0                         push -48
c010eb79: eb f5                         jmp 0xc010eb70 <thunk6>

c010eb7b <isrx209>:
c010eb7b: 6a 00                         push 0
c010eb7d: 6a d1                         push -47
c010eb7f: eb ef                         jmp 0xc010eb70 <thunk6>

c010eb81 <isrx210>:
c010eb81: 6a 00                         push 0
c010eb83: 6a d2                         push -46
c010eb85: eb e9                         jmp 0xc010eb70 <thunk6>

c010eb87 <isrx211>:
c010eb87: 6a 00                         push 0
c010eb89: 6a d3                         push -45
c010eb8b: eb e3                         jmp 0xc010eb70 <thunk6>

c010eb8d <isrx212>:
c010eb8d: 6a 00                         push 0
c010eb8f: 6a d4                         push -44
c010eb91: eb dd                         jmp 0xc010eb70 <thunk6>

c010eb93 <isrx213>:
c010eb93: 6a 00                         push 0
c010eb95: 6a d5                         push -43
c010eb97: eb d7                         jmp 0xc010eb70 <thunk6>

c010eb99 <isrx214>:
c010eb99: 6a 00                         push 0
c010eb9b: 6a d6                         push -42
c010eb9d: eb d1                         jmp 0xc010eb70 <thunk6>

c010eb9f <isrx215>:
c010eb9f: 6a 00                         push 0
c010eba1: 6a d7                         push -41
c010eba3: eb cb                         jmp 0xc010eb70 <thunk6>

c010eba5 <isrx216>:
c010eba5: 6a 00                         push 0
c010eba7: 6a d8                         push -40
c010eba9: eb c5                         jmp 0xc010eb70 <thunk6>

c010ebab <isrx217>:
c010ebab: 6a 00                         push 0
c010ebad: 6a d9                         push -39
c010ebaf: eb bf                         jmp 0xc010eb70 <thunk6>

c010ebb1 <isrx218>:
c010ebb1: 6a 00                         push 0
c010ebb3: 6a da                         push -38
c010ebb5: eb b9                         jmp 0xc010eb70 <thunk6>

c010ebb7 <isrx219>:
c010ebb7: 6a 00                         push 0
c010ebb9: 6a db                         push -37
c010ebbb: eb b3                         jmp 0xc010eb70 <thunk6>

c010ebbd <isrx220>:
c010ebbd: 6a 00                         push 0
c010ebbf: 6a dc                         push -36
c010ebc1: eb ad                         jmp 0xc010eb70 <thunk6>
```

```
c010ebe7 <isrx227>:
c010ebe7: 6a 00                         push 0
c010ebe9: 6a e3                         push -29
c010ebeb: eb 48                         jmp 0xc010ec35 <thunk7>

c010ebed <isrx228>:
c010ebed: 6a 00                         push 0
c010ebef: 6a e4                         push -28
c010ebf1: eb 42                         jmp 0xc010ec35 <thunk7>

c010ebf3 <isrx229>:
c010ebf3: 6a 00                         push 0
c010ebf5: 6a e5                         push -27
c010ebf7: eb 3c                         jmp 0xc010ec35 <thunk7>

c010ebf9 <isrx230>:
c010ebf9: 6a 00                         push 0
c010ebfb: 6a e6                         push -26
c010ebfd: eb 36                         jmp 0xc010ec35 <thunk7>

c010ebff <isrx231>:
c010ebff: 6a 00                         push 0
c010ec01: 6a e7                         push -25
c010ec03: eb 30                         jmp 0xc010ec35 <thunk7>

c010ec05 <isrx232>:
c010ec05: 6a 00                         push 0
c010ec07: 6a e8                         push -24
c010ec09: eb 2a                         jmp 0xc010ec35 <thunk7>

c010ec0b <isrx233>:
c010ec0b: 6a 00                         push 0
c010ec0d: 6a e9                         push -23
c010ec0f: eb 24                         jmp 0xc010ec35 <thunk7>

c010ec11 <isrx234>:
c010ec11: 6a 00                         push 0
c010ec13: 6a ea                         push -22
c010ec15: eb 1e                         jmp 0xc010ec35 <thunk7>

c010ec17 <isrx235>:
c010ec17: 6a 00                         push 0
c010ec19: 6a eb                         push -21
c010ec1b: eb 18                         jmp 0xc010ec35 <thunk7>

c010ec1d <isrx236>:
c010ec1d: 6a 00                         push 0
c010ec1f: 6a ec                         push -20
c010ec21: eb 12                         jmp 0xc010ec35 <thunk7>

c010ec23 <isrx237>:
c010ec23: 6a 00                         push 0
c010ec25: 6a ed                         push -19
c010ec27: eb 0c                         jmp 0xc010ec35 <thunk7>

c010ec29 <isrx238>:
c010ec29: 6a 00                         push 0
c010ec2b: 6a ee                         push -18
c010ec2d: eb 06                         jmp 0xc010ec35 <thunk7>

c010ec2f <isrx239>:
c010ec2f: 6a 00                         push 0
c010ec31: 6a ef                         push -17
c010ec33: eb 00                         jmp 0xc010ec35 <thunk7>

c010ec35 <thunk7>:
c010ec35: e9 46 f9 ff ff                jmp 0xc010e580 <InterruptCommonHandler>

c010ec3a <isrx240>:
c010ec3a: 6a 00                         push 0
```

```
c010ec5e: 6a 00                         push 0
c010ec60: 6a f6                         push -10
c010ec62: eb d1                         jmp 0xc010ec35 <thunk7>

c010ec64 <isrx247>:
c010ec64: 6a 00                         push 0
c010ec66: 6a f7                         push -9
c010ec68: eb cb                         jmp 0xc010ec35 <thunk7>

c010ec6a <isrx248>:
c010ec6a: 6a 00                         push 0
c010ec6c: 6a f8                         push -8
c010ec6e: eb c5                         jmp 0xc010ec35 <thunk7>

c010ec70 <isrx249>:
c010ec70: 6a 00                         push 0
c010ec72: 6a f9                         push -7
c010ec74: eb bf                         jmp 0xc010ec35 <thunk7>

c010ec76 <isrx250>:
c010ec76: 6a 00                         push 0
c010ec78: 6a fa                         push -6
c010ec7a: eb b9                         jmp 0xc010ec35 <thunk7>

c010ec7c <isrx251>:
c010ec7c: 6a 00                         push 0
c010ec7e: 6a fb                         push -5
c010ec80: eb b3                         jmp 0xc010ec35 <thunk7>

c010ec82 <isrx252>:
c010ec82: 6a 00                         push 0
c010ec84: 6a fc                         push -4
c010ec86: eb ad                         jmp 0xc010ec35 <thunk7>

c010ec88 <isrx253>:
c010ec88: 6a 00                         push 0
c010ec8a: 6a fd                         push -3
c010ec8c: eb a7                         jmp 0xc010ec35 <thunk7>

c010ec8e <isrx254>:
c010ec8e: 6a 00                         push 0
c010ec90: 6a fe                         push -2
c010ec92: eb a1                         jmp 0xc010ec35 <thunk7>

c010ec94 <isrx255>:
c010ec94: 6a 00                         push 0
c010ec96: 6a ff                         push -1
c010ec98: eb 9b                         jmp 0xc010ec35 <thunk7>
c010ec9a: 00 00                         add byte ptr [eax], al

c010ec9c <__moddi3>:
c010ec9c: 55                            push ebp
c010ec9d: 89 e5                         mov ebp, esp
c010ec9f: 57                            push edi
c010eca0: 56                            push esi
c010eca1: 53                            push ebx
c010eca2: 83 ec 2c                      sub esp, 44
c010eca5: 8b 45 08                      mov eax, dword ptr [ebp + 8]
c010eca8: 8b 55 0c                      mov edx, dword ptr [ebp + 12]
c010ecab: 8b 4d 10                      mov ecx, dword ptr [ebp + 16]
c010ecae: 8b 5d 14                      mov ebx, dword ptr [ebp + 20]
c010ecb1: 85 d2                         test edx, edx
c010ecb3: 0f 88 5b 01 00 00             js 0xc010ee14 <__moddi3+0x178>
c010ecb9: 89 d6                         mov esi, edx
c010ecbb: c7 45 e4 00 00 00 00          mov dword ptr [ebp - 28], 0
c010ecc2: 89 df                         mov edi, ebx
c010ecc4: 85 db                         test ebx, ebx
c010ecc6: 0f 88 f0 00 00 00             js 0xc010edbc <__moddi3+0x120>
c010eccc: 89 cb                         mov ebx, ecx
c010ecce: 89 7d dc                      mov dword ptr [ebp - 36], edi
c010ecd1: 89 45 e0                      mov dword ptr [ebp - 32], eax
```

```
c010ed1e: 29 c7                   sub edi, eax
c010ed20: 89 7d cc                mov dword ptr [ebp - 52], edi
c010ed23: 8b 55 dc                mov edx, dword ptr [ebp - 36]
c010ed26: 88 c1                   mov cl, al
c010ed28: d3 e2                   shl edx, cl
c010ed2a: 89 d8                   mov eax, ebx
c010ed2c: 89 f9                   mov ecx, edi
c010ed2e: d3 e8                   shr eax, cl
c010ed30: 09 d0                   or eax, edx
c010ed32: 89 45 dc                mov dword ptr [ebp - 36], eax
c010ed35: 8b 55 d8                mov edx, dword ptr [ebp - 40]
c010ed38: 88 d1                   mov cl, dl
c010ed3a: d3 e3                   shl ebx, cl
c010ed3c: 89 5d d0                mov dword ptr [ebp - 48], ebx
c010ed3f: 89 f3                   mov ebx, esi
c010ed41: 89 f9                   mov ecx, edi
c010ed43: d3 eb                   shr ebx, cl
c010ed45: 88 d1                   mov cl, dl
c010ed47: d3 e6                   shl esi, cl
c010ed49: 8b 45 e0                mov eax, dword ptr [ebp - 32]
c010ed4c: 89 f9                   mov ecx, edi
c010ed4e: d3 e8                   shr eax, cl
c010ed50: 09 f0                   or eax, esi
c010ed52: 8b 7d e0                mov edi, dword ptr [ebp - 32]
c010ed55: 88 d1                   mov cl, dl
c010ed57: d3 e7                   shl edi, cl
c010ed59: 89 da                   mov edx, ebx
c010ed5b: f7 75 dc                div dword ptr [ebp - 36]
c010ed5e: 89 d3                   mov ebx, edx
c010ed60: f7 65 d0                mul dword ptr [ebp - 48]
c010ed63: 89 c1                   mov ecx, eax
c010ed65: 89 d6                   mov esi, edx
c010ed67: 39 d3                   cmp ebx, edx
c010ed69: 0f 82 d1 00 00 00       jb 0xc010ee40 <__moddi3+0x1a4>
c010ed6f: 0f 84 c3 00 00 00       je 0xc010ee38 <__moddi3+0x19c>
c010ed75: 89 f8                   mov eax, edi
c010ed77: 29 c8                   sub eax, ecx
c010ed79: 19 f3                   sbb ebx, esi
c010ed7b: 89 de                   mov esi, ebx
c010ed7d: 8a 4d cc                mov cl, byte ptr [ebp - 52]
c010ed80: d3 e6                   shl esi, cl
c010ed82: 8b 7d d8                mov edi, dword ptr [ebp - 40]
c010ed85: 89 f9                   mov ecx, edi
c010ed87: d3 e8                   shr eax, cl
c010ed89: 09 c6                   or esi, eax
c010ed8b: 89 f0                   mov eax, esi
c010ed8d: d3 eb                   shr ebx, cl
c010ed8f: 89 da                   mov edx, ebx
c010ed91: e9 55 ff ff ff          jmp 0xc010eceb <__moddi3+0x4f>
c010ed96: 66 90                   nop
c010ed98: 85 db                   test ebx, ebx
c010ed9a: 75 0b                   jne 0xc010eda7 <__moddi3+0x10b>
c010ed9c: b8 01 00 00 00          mov eax, 1
c010eda1: 31 d2                   xor edx, edx
c010eda3: f7 f3                   div ebx
c010eda5: 89 c3                   mov ebx, eax
c010eda7: 89 f0                   mov eax, esi
c010eda9: 31 d2                   xor edx, edx
c010edab: f7 f3                   div ebx
c010edad: 8b 45 e0                mov eax, dword ptr [ebp - 32]
c010edb0: f7 f3                   div ebx
c010edb2: 89 d1                   mov ecx, edx
c010edb4: e9 2e ff ff ff          jmp 0xc010ece7 <__moddi3+0x4b>
c010edb9: 8d 76 00                lea esi, [esi]
c010edbc: f7 d9                   neg ecx
c010edbe: 83 d3 00                adc ebx, 0
c010edc1: f7 db                   neg ebx
c010edc3: 89 4d d0                mov dword ptr [ebp - 48], ecx
c010edc6: 89 5d d4                mov dword ptr [ebp - 44], ebx
c010edc9: 89 cb                   mov ebx, ecx
c010edcb: 8b 7d d4                mov edi, dword ptr [ebp - 44]
```

```
c010ee24: e9 99 fe ff ff              jmp 0xc010ecc2 <__moddi3+0x26>
c010ee29: 8d 76 00                    lea esi, [esi]
c010ee2c: 89 c1                       mov ecx, eax
c010ee2e: 89 c8                       mov eax, ecx
c010ee30: 89 f2                       mov edx, esi
c010ee32: e9 b4 fe ff ff              jmp 0xc010eceb <__moddi3+0x4f>
c010ee37: 90                          nop
c010ee38: 39 c7                       cmp edi, eax
c010ee3a: 0f 83 35 ff ff ff           jae 0xc010ed75 <__moddi3+0xd9>
c010ee40: 2b 45 d0                    sub eax, dword ptr [ebp - 48]
c010ee43: 1b 55 dc                    sbb edx, dword ptr [ebp - 36]
c010ee46: 89 d6                       mov esi, edx
c010ee48: 89 c1                       mov ecx, eax
c010ee4a: e9 26 ff ff ff              jmp 0xc010ed75 <__moddi3+0xd9>
c010ee4f: 00 55 89                    add byte ptr [ebp - 119], dl

c010ee50 <__udivdi3>:
c010ee50: 55                          push ebp
c010ee51: 89 e5                       mov ebp, esp
c010ee53: 57                          push edi
c010ee54: 56                          push esi
c010ee55: 53                          push ebx
c010ee56: 83 ec 1c                    sub esp, 28
c010ee59: 8b 7d 08                    mov edi, dword ptr [ebp + 8]
c010ee5c: 89 7d e4                    mov dword ptr [ebp - 28], edi
c010ee5f: 8b 75 0c                    mov esi, dword ptr [ebp + 12]
c010ee62: 8b 5d 10                    mov ebx, dword ptr [ebp + 16]
c010ee65: 8b 45 14                    mov eax, dword ptr [ebp + 20]
c010ee68: 85 c0                       test eax, eax
c010ee6a: 75 18                       jne 0xc010ee84 <__udivdi3+0x34>
c010ee6c: 39 de                       cmp esi, ebx
c010ee6e: 73 44                       jae 0xc010eeb4 <__udivdi3+0x64>
c010ee70: 89 f8                       mov eax, edi
c010ee72: 89 f2                       mov edx, esi
c010ee74: f7 f3                       div ebx
c010ee76: 31 ff                       xor edi, edi
c010ee78: 89 fa                       mov edx, edi
c010ee7a: 83 c4 1c                    add esp, 28
c010ee7d: 5b                          pop ebx
c010ee7e: 5e                          pop esi
c010ee7f: 5f                          pop edi
c010ee80: 5d                          pop ebp
c010ee81: c3                          ret
c010ee82: 66 90                       nop
c010ee84: 39 c6                       cmp esi, eax
c010ee86: 73 10                       jae 0xc010ee98 <__udivdi3+0x48>
c010ee88: 31 ff                       xor edi, edi
c010ee8a: 31 c0                       xor eax, eax
c010ee8c: 89 fa                       mov edx, edi
c010ee8e: 83 c4 1c                    add esp, 28
c010ee91: 5b                          pop ebx
c010ee92: 5e                          pop esi
c010ee93: 5f                          pop edi
c010ee94: 5d                          pop ebp
c010ee95: c3                          ret
c010ee96: 66 90                       nop
c010ee98: 0f bd f8                    bsr edi, eax
c010ee9b: 83 f7 1f                    xor edi, 31
c010ee9e: 75 40                       jne 0xc010eee0 <__udivdi3+0x90>
c010eea0: 39 f0                       cmp eax, esi
c010eea2: 72 09                       jb 0xc010eead <__udivdi3+0x5d>
c010eea4: 39 5d e4                    cmp dword ptr [ebp - 28], ebx
c010eea7: 0f 82 a7 00 00 00           jb 0xc010ef54 <__udivdi3+0x104>
c010eead: b8 01 00 00 00              mov eax, 1
c010eeb2: eb d8                       jmp 0xc010ee8c <__udivdi3+0x3c>
c010eeb4: 89 d9                       mov ecx, ebx
c010eeb6: 85 db                       test ebx, ebx
c010eeb8: 75 0b                       jne 0xc010eec5 <__udivdi3+0x75>
c010eeba: b8 01 00 00 00              mov eax, 1
c010eebf: 31 d2                       xor edx, edx
c010eec1: f7 f3                       div ebx
```

```
c010ef00: d3 e3                         shl ebx, cl
c010ef02: 89 5d dc                      mov dword ptr [ebp - 36], ebx
c010ef05: 89 f0                         mov eax, esi
c010ef07: 88 d1                         mov cl, dl
c010ef09: d3 e8                         shr eax, cl
c010ef0b: 89 45 d8                      mov dword ptr [ebp - 40], eax
c010ef0e: 89 f9                         mov ecx, edi
c010ef10: d3 e6                         shl esi, cl
c010ef12: 8b 5d e4                      mov ebx, dword ptr [ebp - 28]
c010ef15: 88 d1                         mov cl, dl
c010ef17: d3 eb                         shr ebx, cl
c010ef19: 89 d8                         mov eax, ebx
c010ef1b: 09 f0                         or eax, esi
c010ef1d: 8b 55 d8                      mov edx, dword ptr [ebp - 40]
c010ef20: f7 75 e0                      div dword ptr [ebp - 32]
c010ef23: 89 d1                         mov ecx, edx
c010ef25: 89 c3                         mov ebx, eax
c010ef27: f7 65 dc                      mul dword ptr [ebp - 36]
c010ef2a: 39 d1                         cmp ecx, edx
c010ef2c: 72 1a                         jb 0xc010ef48 <__udivdi3+0xf8>
c010ef2e: 74 0c                         je 0xc010ef3c <__udivdi3+0xec>
c010ef30: 89 d8                         mov eax, ebx
c010ef32: 31 ff                         xor edi, edi
c010ef34: e9 53 ff ff ff                jmp 0xc010ee8c <__udivdi3+0x3c>
c010ef39: 8d 76 00                      lea esi, [esi]
c010ef3c: 8b 55 e4                      mov edx, dword ptr [ebp - 28]
c010ef3f: 89 f9                         mov ecx, edi
c010ef41: d3 e2                         shl edx, cl
c010ef43: 39 c2                         cmp edx, eax
c010ef45: 73 e9                         jae 0xc010ef30 <__udivdi3+0xe0>
c010ef47: 90                            nop
c010ef48: 8d 43 ff                      lea eax, [ebx - 1]
c010ef4b: 31 ff                         xor edi, edi
c010ef4d: e9 3a ff ff ff                jmp 0xc010ee8c <__udivdi3+0x3c>
c010ef52: 66 90                         nop
c010ef54: 31 c0                         xor eax, eax
c010ef56: e9 31 ff ff ff                jmp 0xc010ee8c <__udivdi3+0x3c>
c010ef5b: 00 55 89                      add byte ptr [ebp - 119], dl

c010ef5c <__umoddi3>:
c010ef5c: 55                            push ebp
c010ef5d: 89 e5                         mov ebp, esp
c010ef5f: 57                            push edi
c010ef60: 56                            push esi
c010ef61: 53                            push ebx
c010ef62: 83 ec 1c                      sub esp, 28
c010ef65: 8b 75 08                      mov esi, dword ptr [ebp + 8]
c010ef68: 8b 5d 0c                      mov ebx, dword ptr [ebp + 12]
c010ef6b: 8b 7d 10                      mov edi, dword ptr [ebp + 16]
c010ef6e: 8b 45 14                      mov eax, dword ptr [ebp + 20]
c010ef71: 89 da                         mov edx, ebx
c010ef73: 85 c0                         test eax, eax
c010ef75: 75 15                         jne 0xc010ef8c <__umoddi3+0x30>
c010ef77: 39 fb                         cmp ebx, edi
c010ef79: 73 4d                         jae 0xc010efc8 <__umoddi3+0x6c>
c010ef7b: 89 f0                         mov eax, esi
c010ef7d: f7 f7                         div edi
c010ef7f: 89 d0                         mov eax, edx
c010ef81: 31 d2                         xor edx, edx
c010ef83: 83 c4 1c                      add esp, 28
c010ef86: 5b                            pop ebx
c010ef87: 5e                            pop esi
c010ef88: 5f                            pop edi
c010ef89: 5d                            pop ebp
c010ef8a: c3                            ret
c010ef8b: 90                            nop
c010ef8c: 89 75 e0                      mov dword ptr [ebp - 32], esi
c010ef8f: 39 c3                         cmp ebx, eax
c010ef91: 73 0d                         jae 0xc010efa0 <__umoddi3+0x44>
c010ef93: 89 f0                         mov eax, esi
c010ef95: 83 c4 1c                      add esp, 28
```

```
c010efce: b8 01 00 00 00              mov eax, 1
c010efd3: 31 d2                       xor edx, edx
c010efd5: f7 f7                       div edi
c010efd7: 89 c1                       mov ecx, eax
c010efd9: 89 d8                       mov eax, ebx
c010efdb: 31 d2                       xor edx, edx
c010efdd: f7 f1                       div ecx
c010efdf: 89 f0                       mov eax, esi
c010efe1: f7 f1                       div ecx
c010efe3: eb 9a                       jmp 0xc010ef7f <__umoddi3+0x23>
c010efe5: 8d 76 00                    lea esi, [esi]
c010efe8: ba 20 00 00 00              mov edx, 32
c010efed: 8b 4d e4                    mov ecx, dword ptr [ebp - 28]
c010eff0: 29 ca                       sub edx, ecx
c010eff2: d3 e0                       shl eax, cl
c010eff4: 89 45 dc                    mov dword ptr [ebp - 36], eax
c010eff7: 89 f8                       mov eax, edi
c010eff9: 89 55 e0                    mov dword ptr [ebp - 32], edx
c010effc: 88 d1                       mov cl, dl
c010effe: d3 e8                       shr eax, cl
c010f000: 89 c2                       mov edx, eax
c010f002: 8b 45 dc                    mov eax, dword ptr [ebp - 36]
c010f005: 09 c2                       or edx, eax
c010f007: 89 55 dc                    mov dword ptr [ebp - 36], edx
c010f00a: 8b 45 e4                    mov eax, dword ptr [ebp - 28]
c010f00d: 88 c1                       mov cl, al
c010f00f: d3 e7                       shl edi, cl
c010f011: 89 da                       mov edx, ebx
c010f013: 8a 4d e0                    mov cl, byte ptr [ebp - 32]
c010f016: d3 ea                       shr edx, cl
c010f018: 88 c1                       mov cl, al
c010f01a: d3 e3                       shl ebx, cl
c010f01c: 89 f0                       mov eax, esi
c010f01e: 8a 4d e0                    mov cl, byte ptr [ebp - 32]
c010f021: d3 e8                       shr eax, cl
c010f023: 09 d8                       or eax, ebx
c010f025: 8a 4d e4                    mov cl, byte ptr [ebp - 28]
c010f028: d3 e6                       shl esi, cl
c010f02a: 89 75 d8                    mov dword ptr [ebp - 40], esi
c010f02d: f7 75 dc                    div dword ptr [ebp - 36]
c010f030: 89 d3                       mov ebx, edx
c010f032: f7 e7                       mul edi
c010f034: 89 c6                       mov esi, eax
c010f036: 89 d1                       mov ecx, edx
c010f038: 39 d3                       cmp ebx, edx
c010f03a: 72 30                       jb 0xc010f06c <__umoddi3+0x110>
c010f03c: 74 26                       je 0xc010f064 <__umoddi3+0x108>
c010f03e: 8b 45 d8                    mov eax, dword ptr [ebp - 40]
c010f041: 29 f0                       sub eax, esi
c010f043: 19 cb                       sbb ebx, ecx
c010f045: 89 da                       mov edx, ebx
c010f047: 8a 4d e0                    mov cl, byte ptr [ebp - 32]
c010f04a: d3 e2                       shl edx, cl
c010f04c: 8b 7d e4                    mov edi, dword ptr [ebp - 28]
c010f04f: 89 f9                       mov ecx, edi
c010f051: d3 e8                       shr eax, cl
c010f053: 09 d0                       or eax, edx
c010f055: d3 eb                       shr ebx, cl
c010f057: 89 da                       mov edx, ebx
c010f059: 83 c4 1c                    add esp, 28
c010f05c: 5b                          pop ebx
c010f05d: 5e                          pop esi
c010f05e: 5f                          pop edi
c010f05f: 5d                          pop ebp
c010f060: c3                          ret
c010f061: 8d 76 00                    lea esi, [esi]
c010f064: 39 45 d8                    cmp dword ptr [ebp - 40], eax
c010f067: 73 d5                       jae 0xc010f03e <__umoddi3+0xe2>
c010f069: 8d 76 00                    lea esi, [esi]
c010f06c: 29 f8                       sub eax, edi
c010f06e: 1b 55 dc                    sbb edx, dword ptr [ebp - 36]
```

```
c010f0b3: 89 10                   mov dword ptr [eax], edx
c010f0b5: c7 40 04 00 00 00 00    mov dword ptr [eax + 4], 0
c010f0bc: 89 d8                   mov eax, ebx
c010f0be: 8b 55 e4                mov edx, dword ptr [ebp - 28]
c010f0c1: 83 c4 2c                add esp, 44
c010f0c4: 5b                      pop ebx
c010f0c5: 5e                      pop esi
c010f0c6: 5f                      pop edi
c010f0c7: 5d                      pop ebp
c010f0c8: c3                      ret
c010f0c9: 8d 76 00                lea esi, [esi]
c010f0cc: 39 fb                   cmp ebx, edi
c010f0ce: 73 20                   jae 0xc010f0f0 <__udivmoddi4+0x78>
c010f0d0: 8b 75 18                mov esi, dword ptr [ebp + 24]
c010f0d3: 85 f6                   test esi, esi
c010f0d5: 74 0b                   je 0xc010f0e2 <__udivmoddi4+0x6a>
c010f0d7: 8b 45 18                mov eax, dword ptr [ebp + 24]
c010f0da: 8b 75 e0                mov esi, dword ptr [ebp - 32]
c010f0dd: 89 30                   mov dword ptr [eax], esi
c010f0df: 89 58 04                mov dword ptr [eax + 4], ebx
c010f0e2: c7 45 e4 00 00 00 00    mov dword ptr [ebp - 28], 0
c010f0e9: 31 db                   xor ebx, ebx
c010f0eb: eb cf                   jmp 0xc010f0bc <__udivmoddi4+0x44>
c010f0ed: 8d 76 00                lea esi, [esi]
c010f0f0: 0f bd cf                bsr ecx, edi
c010f0f3: 83 f1 1f                xor ecx, 31
c010f0f6: 89 4d e4                mov dword ptr [ebp - 28], ecx
c010f0f9: 75 55                   jne 0xc010f150 <__udivmoddi4+0xd8>
c010f0fb: 39 df                   cmp edi, ebx
c010f0fd: 72 08                   jb 0xc010f107 <__udivmoddi4+0x8f>
c010f0ff: 39 f0                   cmp eax, esi
c010f101: 0f 82 f5 00 00 00       jb 0xc010f1fc <__udivmoddi4+0x184>
c010f107: 89 da                   mov edx, ebx
c010f109: 8b 45 e0                mov eax, dword ptr [ebp - 32]
c010f10c: 29 f0                   sub eax, esi
c010f10e: 19 fa                   sbb edx, edi
c010f110: bb 01 00 00 00          mov ebx, 1
c010f115: 8b 4d 18                mov ecx, dword ptr [ebp + 24]
c010f118: 85 c9                   test ecx, ecx
c010f11a: 74 a0                   je 0xc010f0bc <__udivmoddi4+0x44>
c010f11c: 8b 75 18                mov esi, dword ptr [ebp + 24]
c010f11f: 89 06                   mov dword ptr [esi], eax
c010f121: 89 56 04                mov dword ptr [esi + 4], edx
c010f124: eb 96                   jmp 0xc010f0bc <__udivmoddi4+0x44>
c010f126: 66 90                   nop
c010f128: 89 f1                   mov ecx, esi
c010f12a: 85 f6                   test esi, esi
c010f12c: 75 0b                   jne 0xc010f139 <__udivmoddi4+0xc1>
c010f12e: b8 01 00 00 00          mov eax, 1
c010f133: 31 d2                   xor edx, edx
c010f135: f7 f6                   div esi
c010f137: 89 c1                   mov ecx, eax
c010f139: 31 d2                   xor edx, edx
c010f13b: 89 d8                   mov eax, ebx
c010f13d: f7 f1                   div ecx
c010f13f: 89 c3                   mov ebx, eax
c010f141: 8b 45 e0                mov eax, dword ptr [ebp - 32]
c010f144: f7 f1                   div ecx
c010f146: 89 5d e4                mov dword ptr [ebp - 28], ebx
c010f149: e9 59 ff ff ff          jmp 0xc010f0a7 <__udivmoddi4+0x2f>
c010f14e: 66 90                   nop
c010f150: ba 20 00 00 00          mov edx, 32
c010f155: 8b 45 e4                mov eax, dword ptr [ebp - 28]
c010f158: 29 c2                   sub edx, eax
c010f15a: 89 55 cc                mov dword ptr [ebp - 52], edx
c010f15d: 88 c1                   mov cl, al
c010f15f: d3 e7                   shl edi, cl
c010f161: 89 f0                   mov eax, esi
c010f163: 88 d1                   mov cl, dl
c010f165: d3 e8                   shr eax, cl
c010f167: 09 c7                   or edi, eax
```

```
c010f1ae: 8b 45 18                   mov eax, dword ptr [ebp + 24]
c010f1b1: 85 c0                      test eax, eax
c010f1b3: 74 26                      je 0xc010f1db <__udivmoddi4+0x163>
c010f1b5: 8b 45 e0                   mov eax, dword ptr [ebp - 32]
c010f1b8: 8b 55 d0                   mov edx, dword ptr [ebp - 48]
c010f1bb: 2b 55 d8                   sub edx, dword ptr [ebp - 40]
c010f1be: 1b 45 d4                   sbb eax, dword ptr [ebp - 44]
c010f1c1: 89 c6                      mov esi, eax
c010f1c3: 8a 4d cc                   mov cl, byte ptr [ebp - 52]
c010f1c6: d3 e6                      shl esi, cl
c010f1c8: 8b 7d e4                   mov edi, dword ptr [ebp - 28]
c010f1cb: 89 f9                      mov ecx, edi
c010f1cd: d3 ea                      shr edx, cl
c010f1cf: 09 f2                      or edx, esi
c010f1d1: d3 e8                      shr eax, cl
c010f1d3: 8b 75 18                   mov esi, dword ptr [ebp + 24]
c010f1d6: 89 16                      mov dword ptr [esi], edx
c010f1d8: 89 46 04                   mov dword ptr [esi + 4], eax
c010f1db: c7 45 e4 00 00 00 00       mov dword ptr [ebp - 28], 0
c010f1e2: e9 d5 fe ff ff             jmp 0xc010f0bc <__udivmoddi4+0x44>
c010f1e7: 90                         nop
c010f1e8: 39 c7                      cmp edi, eax
c010f1ea: 73 c2                      jae 0xc010f1ae <__udivmoddi4+0x136>
c010f1ec: 8d 59 ff                   lea ebx, [ecx - 1]
c010f1ef: 29 f0                      sub eax, esi
c010f1f1: 1b 55 dc                   sbb edx, dword ptr [ebp - 36]
c010f1f4: 89 55 d4                   mov dword ptr [ebp - 44], edx
c010f1f7: 89 45 d8                   mov dword ptr [ebp - 40], eax
c010f1fa: eb b2                      jmp 0xc010f1ae <__udivmoddi4+0x136>
c010f1fc: 31 db                      xor ebx, ebx
c010f1fe: e9 12 ff ff ff             jmp 0xc010f115 <__udivmoddi4+0x9d>
c010f203: 00 00                      add byte ptr [eax], al
c010f205: 00 00                      add byte ptr [eax], al
c010f207: 00 b9                      <unknown>

c010f208 <start_ctors>:
c010f208: b9                         <unknown>
c010f209: ae                         scasb al, byte ptr es:[edi]
c010f20a: 10 c0                      adc al, al
```