```
                                CCF Lab Assignment:
                                 Memory and Filesystems
```

1 Memory

1. First download and extract the file evidence.tar.gz from https://software.os3.nl/CCF/. Make sure you check the tar-ball and included files. Keep in mind that the extracted files will be around 5GB

Answer:

Download:

```
root@caine:/local# wget https://software.os3.nl/CCF/evidence.tar.gz
```

Check the tar-ball:

Download sha 256 then compare with tar sha 256:

```
root@caine:/local# wget https://software.os3.nl/CCF/evidence.tar.gz.sha256

root@caine:/local# cat evidence.tar.gz.sha256
4713a1fc5e1e44a98d3dd2a3482d784c22525c83ca71c507cb31e5fbb752c6a4
evidence.tar.gz
root@caine:/local# shasum -a 256 evidence.tar.gz
4713a1fc5e1e44a98d3dd2a3482d784c22525c83ca71c507cb31e5fbb752c6a4
evidence.tar.gz
```

I checked them successfully.

Extract then check memory.raw and disk.img sha256 hashes:

```
root@caine:/local# tar -xvf evidence.tar.gz

root@caine:/local# cat memory.sha256
aa39ac826bc49a2c35dd63b2c6dfd694e86541c664bdfd31c8c3dbe59b6cb06c  memory.raw
root@caine:/local# shasum -a 256 memory.raw
aa39ac826bc49a2c35dd63b2c6dfd694e86541c664bdfd31c8c3dbe59b6cb06c  memory.raw
root@caine:/local# cat disk.sha256
65c894d5cd690f923b38f0ad4fc7e59e7713a2cd97bd7d10add58822db330dde  disk.img
root@caine:/local# shasum -a 256 disk.img
65c894d5cd690f923b38f0ad4fc7e59e7713a2cd97bd7d10add58822db330dde  disk.img
```

Everything is pretty good .

2. Read about Volatility and its features

(a) What does Volatility do?

Answer:

Volatility is an open source memory forensics framework for incident response and malware analysis. It is written in Python and supports Microsoft Windows, Mac OS X, and Linux The Volatility framework is an excellent open source tool to analyze memory in 32bit and 64 bit systems and it's our memory forensics platform of choice here at Horangi. Volatility comes with many useful plugins such as Pslist, Kdbgscan, Kpcrscan, and Dllist.

(b) Would Volatility be useful in the acquiring stage?

Answer:

Volatility is useful to analyze raw dumps, .img files, VMware dumps (.vmem) and many others. In other words, (After the acquiring stage). It only works on samples. So its not useful in the acquiring stage.

© What parts of Volatility would you use in your investigation on the acquired memory?

Answer:

Profile part: In order to detect and select the appropriate profile. This help with finding specific artifacts in the specific memory places.pslist plugin: to gather a list of running processes. I would use the plugin malfind to detect malware. Finally, memdump plugin in order to dump specific parts of the memory to a file.

Sources:

1- https://en.wikipedia.org/wiki/Volatility_(memory_forensics)

3. Identify the operating system that is running. Note down the steps you take to detect this.

Answer:

```
root@caine:/local# vol.py imageinfo -f memory.raw
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with
WinXPSP2x86)
                     AS Layer1 : IA32PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/local/memory.raw)
                      PAE type : No PAE
                           DTB : 0x39000L
                          KDBG : 0x8054cf60L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2017-02-12 13:37:02 UTC+0000
     Image local date and time : 2017-02-12 14:37:02 +0100
```

```
root@caine:/local# vol.py kdbgscan -f memory.raw
Volatility Foundation Volatility Framework 2.6
**************************************************
Instantiating KDBG using: Kernel AS WinXPSP2x86 (5.1.0 32bit)
Offset (V)                    : 0x8054cf60
Offset (P)                    : 0x54cf60
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): WinXPSP3x86
Version64                     : 0x8054cf38 (Major: 15, Minor: 2600)
Service Pack (CmNtCSDVersion) : 3
Build string (NtBuildLab)     : 2600.xpsp_sp3_qfe.130704-0421
PsActiveProcessHead           : 0x805614d8 (34 processes)
PsLoadedModuleList            : 0x8055b340 (117 modules)
KernelBase                    : 0x804d7000 (Matches MZ: True)
Major (OptionalHeader)        : 5
Minor (OptionalHeader)        : 1
KPCR                          : 0xffdff000 (CPU 0)

**************************************************
Instantiating KDBG using: Kernel AS WinXPSP2x86 (5.1.0 32bit)
Offset (V)                    : 0x8054cf60
Offset (P)                    : 0x54cf60
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): WinXPSP2x86
Version64                     : 0x8054cf38 (Major: 15, Minor: 2600)
Service Pack (CmNtCSDVersion) : 3
Build string (NtBuildLab)     : 2600.xpsp_sp3_qfe.130704-0421
PsActiveProcessHead           : 0x805614d8 (34 processes)
PsLoadedModuleList            : 0x8055b340 (117 modules)
KernelBase                    : 0x804d7000 (Matches MZ: True)
Major (OptionalHeader)        : 5
Minor (OptionalHeader)        : 1
KPCR                          : 0xffdff000 (CPU 0)
```

OSs are Windows XP Service Pack 2 x86 and Windows XP Service Pack 3 x86.

You need to be exact as Volatility takes a profile as input. Or show that both SP2 and SP3 profiles give the same result.

Since two different versions are exists. I will use the kdbgscan for vol.py I was able to identify the build number of Windows which is 130704-0421. This means that the build number of SP3 of Windows XP 32-bit according to https://www.lifewire.com/windows-version-numbers-2625171.

4. Find out if there is any malware running on the computer

Answer:

For this task I will use malfind plugin to detect any injected code in processes.

```
root@caine:/local# vol.py --profile=WinXPSP3x86 -f memory.raw malfind --
dump-dir malwareResults/
Volatility Foundation Volatility Framework 2.6
Process: csrss.exe Pid: 560 Address: 0x7f6f0000
Vad Tag: Vad  Protection: PAGE_EXECUTE_READWRITE
Flags: Protection: 6

0x7f6f0000  c8 00 00 00 8d 01 00 00 ff ee ff ee 08 70 00 00
.............p..
0x7f6f0010  08 00 00 00 00 fe 00 00 00 00 10 00 00 20 00 00
.................
0x7f6f0020  00 02 00 00 00 20 00 00 8d 01 00 00 ff ef fd 7f
.................
0x7f6f0030  03 00 08 06 00 00 00 00 00 00 00 00 00 00 00 00
.................

0x7f6f0000 c8000000         ENTER 0x0, 0x0
0x7f6f0004 8d01             LEA EAX, [ECX]
0x7f6f0006 0000             ADD [EAX], AL
0x7f6f0008 ff               DB 0xff
0x7f6f0009 ee               OUT DX, AL
0x7f6f000a ff               DB 0xff
0x7f6f000b ee               OUT DX, AL
0x7f6f000c 087000           OR [EAX+0x0], DH
0x7f6f000f 0008             ADD [EAX], CL
0x7f6f0011 0000             ADD [EAX], AL
0x7f6f0013 0000             ADD [EAX], AL
0x7f6f0015 fe00             INC BYTE [EAX]
0x7f6f0017 0000             ADD [EAX], AL
```

```
0x7f6f0019 0010             ADD [EAX], DL
0x7f6f001b 0000             ADD [EAX], AL
0x7f6f001d 2000             AND [EAX], AL
0x7f6f001f 0000             ADD [EAX], AL
0x7f6f0021 0200             ADD AL, [EAX]
0x7f6f0023 0000             ADD [EAX], AL
0x7f6f0025 2000             AND [EAX], AL
0x7f6f0027 008d010000ff     ADD [EBP-0xffffff], CL
0x7f6f002d ef               OUT DX, EAX
0x7f6f002e fd               STD
0x7f6f002f 7f03             JG 0x7f6f0034
0x7f6f0031 0008             ADD [EAX], CL
0x7f6f0033 06               PUSH ES
0x7f6f0034 0000             ADD [EAX], AL
0x7f6f0036 0000             ADD [EAX], AL
0x7f6f0038 0000             ADD [EAX], AL
0x7f6f003a 0000             ADD [EAX], AL
0x7f6f003c 0000             ADD [EAX], AL
0x7f6f003e 0000             ADD [EAX], AL

Process: IEXPLORE.EXE Pid: 552 Address: 0x5fff0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 16, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x5fff0000  64 74 72 52 00 00 00 00 20 03 ff 5f 00 00 00 00
dtrR....... ...._....
0x5fff0010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
................
0x5fff0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
................
0x5fff0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
................

0x5fff0000 647472           JZ 0x5fff0075
0x5fff0003 52               PUSH EDX
0x5fff0004 0000             ADD [EAX], AL
0x5fff0006 0000             ADD [EAX], AL
0x5fff0008 2003             AND [EBX], AL
0x5fff000a ff5f00           CALL FAR DWORD [EDI+0x0]
0x5fff000d 0000             ADD [EAX], AL
0x5fff000f 0000             ADD [EAX], AL
0x5fff0011 0000             ADD [EAX], AL
0x5fff0013 0000             ADD [EAX], AL
0x5fff0015 0000             ADD [EAX], AL
0x5fff0017 0000             ADD [EAX], AL
0x5fff0019 0000             ADD [EAX], AL
0x5fff001b 0000             ADD [EAX], AL
0x5fff001d 0000             ADD [EAX], AL
0x5fff001f 0000             ADD [EAX], AL
0x5fff0021 0000             ADD [EAX], AL
0x5fff0023 0000             ADD [EAX], AL
```

```
0x5fff0025 0000             ADD [EAX], AL
0x5fff0027 0000             ADD [EAX], AL
0x5fff0029 0000             ADD [EAX], AL
0x5fff002b 0000             ADD [EAX], AL
0x5fff002d 0000             ADD [EAX], AL
0x5fff002f 0000             ADD [EAX], AL
0x5fff0031 0000             ADD [EAX], AL
0x5fff0033 0000             ADD [EAX], AL
0x5fff0035 0000             ADD [EAX], AL
0x5fff0037 0000             ADD [EAX], AL
0x5fff0039 0000             ADD [EAX], AL
0x5fff003b 0000             ADD [EAX], AL
0x5fff003d 0000             ADD [EAX], AL
0x5fff003f 00               DB 0x0

Process: IEXPLORE.EXE Pid: 1996 Address: 0x3960000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x03960000  01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
................
0x03960010  0f b6 05 00 00 96 03 85 c0 74 05 e9 4d ff c6 ff
.........t..M...
0x03960020  e9 c9 88 98 3a 00 00 00 00 00 00 00 00 00 00 00
....:...........
0x03960030  0f b6 05 00 00 96 03 85 c0 74 05 e9 b5 e1 ba ff
.........t......

0x03960000 0100             ADD [EAX], EAX
0x03960002 0000             ADD [EAX], AL
0x03960004 0000             ADD [EAX], AL
0x03960006 0000             ADD [EAX], AL
0x03960008 0000             ADD [EAX], AL
0x0396000a 0000             ADD [EAX], AL
0x0396000c 0000             ADD [EAX], AL
0x0396000e 0000             ADD [EAX], AL
0x03960010 0fb60500009603   MOVZX EAX, BYTE [0x3960000]
0x03960017 85c0             TEST EAX, EAX
0x03960019 7405             JZ 0x3960020
0x0396001b e94dffc6ff       JMP 0x35cff6d
0x03960020 e9c988983a       JMP 0x3e2e88ee
0x03960025 0000             ADD [EAX], AL
0x03960027 0000             ADD [EAX], AL
0x03960029 0000             ADD [EAX], AL
0x0396002b 0000             ADD [EAX], AL
0x0396002d 0000             ADD [EAX], AL
0x0396002f 000f             ADD [EDI], CL
0x03960031 b605             MOV DH, 0x5
0x03960033 0000             ADD [EAX], AL
0x03960035 96               XCHG ESI, EAX
0x03960036 0385c07405e9     ADD EAX, [EBP-0x16fa8b40]
```

```
0x0396003c b5e1             MOV CH, 0xe1
0x0396003e ba               DB 0xba
0x0396003f ff               DB 0xff

Process: IEXPLORE.EXE Pid: 1996 Address: 0x38620000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 11, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x38620000  01 00 00 00 00 00 00 00 35 5c 91 7c 10 db 00 10
........5\.|....
0x38620010  d8 67 02 10 03 00 00 00 05 00 00 00 68 6c 02 00
.g..........hl..
0x38620020  00 e9 14 5c 2f 44 00 00 00 00 00 00 00 00 00 00
...\/D..........
0x38620030  05 00 00 00 68 6c 02 00 00 68 88 5d 91 7c e9 fc
....hl...h.].|..

0x38620000 0100             ADD [EAX], EAX
0x38620002 0000             ADD [EAX], AL
0x38620004 0000             ADD [EAX], AL
0x38620006 0000             ADD [EAX], AL
0x38620008 355c917c10       XOR EAX, 0x107c915c
0x3862000d db00             FILD DWORD [EAX]
0x3862000f 10d8             ADC AL, BL
0x38620011 670210           ADD DL, [BX+SI]
0x38620014 0300             ADD EAX, [EAX]
0x38620016 0000             ADD [EAX], AL
0x38620018 0500000068       ADD EAX, 0x68000000
0x3862001d 6c               INS BYTE [ES:EDI], DX
0x3862001e 0200             ADD AL, [EAX]
0x38620020 00e9             ADD CL, CH
0x38620022 145c             ADC AL, 0x5c
0x38620024 2f               DAS
0x38620025 44               INC ESP
0x38620026 0000             ADD [EAX], AL
0x38620028 0000             ADD [EAX], AL
0x3862002a 0000             ADD [EAX], AL
0x3862002c 0000             ADD [EAX], AL
0x3862002e 0000             ADD [EAX], AL
0x38620030 0500000068       ADD EAX, 0x68000000
0x38620035 6c               INS BYTE [ES:EDI], DX
0x38620036 0200             ADD AL, [EAX]
0x38620038 006888           ADD [EAX-0x78], CH
0x3862003b 5d               POP EBP
0x3862003c 91               XCHG ECX, EAX
0x3862003d 7ce9             JL 0x38620028
0x3862003f fc               CLD

Process: IEXPLORE.EXE Pid: 1996 Address: 0x5fff0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 16, MemCommit: 1, PrivateMemory: 1, Protection: 6
```

```
0x5fff0000  64 74 72 52 00 00 00 00 20 03 ff 5f 00 00 00 00
dtrR....... ...._....
0x5fff0010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
................
0x5fff0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
................
0x5fff0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
................

0x5fff0000 647472           JZ 0x5fff0075
0x5fff0003 52               PUSH EDX
0x5fff0004 0000             ADD [EAX], AL
0x5fff0006 0000             ADD [EAX], AL
0x5fff0008 2003             AND [EBX], AL
0x5fff000a ff5f00           CALL FAR DWORD [EDI+0x0]
0x5fff000d 0000             ADD [EAX], AL
0x5fff000f 0000             ADD [EAX], AL
0x5fff0011 0000             ADD [EAX], AL
0x5fff0013 0000             ADD [EAX], AL
0x5fff0015 0000             ADD [EAX], AL
0x5fff0017 0000             ADD [EAX], AL
0x5fff0019 0000             ADD [EAX], AL
0x5fff001b 0000             ADD [EAX], AL
0x5fff001d 0000             ADD [EAX], AL
0x5fff001f 0000             ADD [EAX], AL
0x5fff0021 0000             ADD [EAX], AL
0x5fff0023 0000             ADD [EAX], AL
0x5fff0025 0000             ADD [EAX], AL
0x5fff0027 0000             ADD [EAX], AL
0x5fff0029 0000             ADD [EAX], AL
0x5fff002b 0000             ADD [EAX], AL
0x5fff002d 0000             ADD [EAX], AL
0x5fff002f 0000             ADD [EAX], AL
0x5fff0031 0000             ADD [EAX], AL
0x5fff0033 0000             ADD [EAX], AL
0x5fff0035 0000             ADD [EAX], AL
0x5fff0037 0000             ADD [EAX], AL
0x5fff0039 0000             ADD [EAX], AL
0x5fff003b 0000             ADD [EAX], AL
0x5fff003d 0000             ADD [EAX], AL
0x5fff003f 00               DB 0x0

Process: firefox.exe Pid: 2996 Address: 0x7fb0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x07fb0000  a3 d0 42 7e 8b ff 55 8b ec e9 9a d0 47 76 00 00
..B~..U.....Gv..
0x07fb0010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
................
0x07fb0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
................
0x07fb0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
................

0x07fb0000 a3d0427e8b       MOV [0x8b7e42d0], EAX
0x07fb0005 ff558b           CALL DWORD [EBP-0x75]
0x07fb0008 ec               IN AL, DX
0x07fb0009 e99ad04776       JMP 0x7e42d0a8
0x07fb000e 0000             ADD [EAX], AL
0x07fb0010 0000             ADD [EAX], AL
0x07fb0012 0000             ADD [EAX], AL
0x07fb0014 0000             ADD [EAX], AL
0x07fb0016 0000             ADD [EAX], AL
0x07fb0018 0000             ADD [EAX], AL
0x07fb001a 0000             ADD [EAX], AL
0x07fb001c 0000             ADD [EAX], AL
0x07fb001e 0000             ADD [EAX], AL
0x07fb0020 0000             ADD [EAX], AL
0x07fb0022 0000             ADD [EAX], AL
0x07fb0024 0000             ADD [EAX], AL
0x07fb0026 0000             ADD [EAX], AL
0x07fb0028 0000             ADD [EAX], AL
0x07fb002a 0000             ADD [EAX], AL
0x07fb002c 0000             ADD [EAX], AL
0x07fb002e 0000             ADD [EAX], AL
0x07fb0030 0000             ADD [EAX], AL
0x07fb0032 0000             ADD [EAX], AL
0x07fb0034 0000             ADD [EAX], AL
0x07fb0036 0000             ADD [EAX], AL
0x07fb0038 0000             ADD [EAX], AL
0x07fb003a 0000             ADD [EAX], AL
0x07fb003c 0000             ADD [EAX], AL
0x07fb003e 0000             ADD [EAX], AL

Process: firefox.exe Pid: 2996 Address: 0x9ca0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x09ca0000  9c c4 42 7e 6a 10 68 70 c5 42 7e e9 93 c4 78 74
..B~j.hp.B~...xt
0x09ca0010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
................
0x09ca0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
................
0x09ca0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
................

0x09ca0000 9c               PUSHF
0x09ca0001 c4427e           LES EAX, [EDX+0x7e]
0x09ca0004 6a10             PUSH 0x10
0x09ca0006 6870c5427e       PUSH DWORD 0x7e42c570
```

```
0x09ca000b e993c47874       JMP 0x7e42c4a3
0x09ca0010 0000             ADD [EAX], AL
0x09ca0012 0000             ADD [EAX], AL
0x09ca0014 0000             ADD [EAX], AL
0x09ca0016 0000             ADD [EAX], AL
0x09ca0018 0000             ADD [EAX], AL
0x09ca001a 0000             ADD [EAX], AL
0x09ca001c 0000             ADD [EAX], AL
0x09ca001e 0000             ADD [EAX], AL
0x09ca0020 0000             ADD [EAX], AL
0x09ca0022 0000             ADD [EAX], AL
0x09ca0024 0000             ADD [EAX], AL
0x09ca0026 0000             ADD [EAX], AL
0x09ca0028 0000             ADD [EAX], AL
0x09ca002a 0000             ADD [EAX], AL
0x09ca002c 0000             ADD [EAX], AL
0x09ca002e 0000             ADD [EAX], AL
0x09ca0030 0000             ADD [EAX], AL
0x09ca0032 0000             ADD [EAX], AL
0x09ca0034 0000             ADD [EAX], AL
0x09ca0036 0000             ADD [EAX], AL
0x09ca0038 0000             ADD [EAX], AL
0x09ca003a 0000             ADD [EAX], AL
0x09ca003c 0000             ADD [EAX], AL
0x09ca003e 0000             ADD [EAX], AL

Process: firefox.exe Pid: 2996 Address: 0x188f0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 11, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x188f0000  03 00 00 00 00 00 00 00 d4 26 e8 66 a0 69 01 10
.........&.f.i..
0x188f0010  e8 74 02 10 03 00 00 00 01 00 00 00 55 e9 b3 26
.t..........U..&
0x188f0020  59 4e 00 00 00 00 00 00 00 00 00 00 00 00 00 00
YN..............
0x188f0030  02 00 00 00 55 89 e5 e9 9b 26 59 4e 00 00 00 00
....U....&YN....

0x188f0000 0300             ADD EAX, [EAX]
0x188f0002 0000             ADD [EAX], AL
0x188f0004 0000             ADD [EAX], AL
0x188f0006 0000             ADD [EAX], AL
0x188f0008 d426             AAM 0x26
0x188f000a e866a06901       CALL 0x19f8a075
0x188f000f 10e8             ADC AL, CH
0x188f0011 7402             JZ 0x188f0015
0x188f0013 1003             ADC [EBX], AL
0x188f0015 0000             ADD [EAX], AL
0x188f0017 0001             ADD [ECX], AL
0x188f0019 0000             ADD [EAX], AL
```

```
0x188f001b 0055e9           ADD [EBP-0x17], DL
0x188f001e b326             MOV BL, 0x26
0x188f0020 59               POP ECX
0x188f0021 4e               DEC ESI
0x188f0022 0000             ADD [EAX], AL
0x188f0024 0000             ADD [EAX], AL
0x188f0026 0000             ADD [EAX], AL
0x188f0028 0000             ADD [EAX], AL
0x188f002a 0000             ADD [EAX], AL
0x188f002c 0000             ADD [EAX], AL
0x188f002e 0000             ADD [EAX], AL
0x188f0030 0200             ADD AL, [EAX]
0x188f0032 0000             ADD [EAX], AL
0x188f0034 55               PUSH EBP
0x188f0035 89e5             MOV EBP, ESP
0x188f0037 e99b26594e       JMP 0x66e826d7
0x188f003c 0000             ADD [EAX], AL
0x188f003e 0000             ADD [EAX], AL

Process: firefox.exe Pid: 2996 Address: 0x71000000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 11, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x71000000  01 00 00 00 00 00 00 00 35 5c 91 7c 10 db 00 10
........5\.|....
0x71000010  d8 67 02 10 03 00 00 00 05 00 00 00 68 6c 02 00
.g..........hl..
0x71000020  00 e9 14 5c 91 0b 00 00 00 00 00 00 00 00 00 00
...\............
0x71000030  05 00 00 00 68 6c 02 00 00 68 88 5d 91 7c e9 fc
....hl...h.].|..

0x71000000 0100             ADD [EAX], EAX
0x71000002 0000             ADD [EAX], AL
0x71000004 0000             ADD [EAX], AL
0x71000006 0000             ADD [EAX], AL
0x71000008 355c917c10       XOR EAX, 0x107c915c
0x7100000d db00             FILD DWORD [EAX]
0x7100000f 10d8             ADC AL, BL
0x71000011 670210           ADD DL, [BX+SI]
0x71000014 0300             ADD EAX, [EAX]
0x71000016 0000             ADD [EAX], AL
0x71000018 0500000068       ADD EAX, 0x68000000
0x7100001d 6c               INS BYTE [ES:EDI], DX
0x7100001e 0200             ADD AL, [EAX]
0x71000020 00e9             ADD CL, CH
0x71000022 145c             ADC AL, 0x5c
0x71000024 91               XCHG ECX, EAX
0x71000025 0b00             OR EAX, [EAX]
0x71000027 0000             ADD [EAX], AL
0x71000029 0000             ADD [EAX], AL
```

```
0x7100002b 0000              ADD [EAX], AL
0x7100002d 0000              ADD [EAX], AL
0x7100002f 000500000068      ADD [0x68000000], AL
0x71000035 6c                INS BYTE [ES:EDI], DX
0x71000036 0200              ADD AL, [EAX]
0x71000038 006888            ADD [EAX-0x78], CH
0x7100003b 5d                POP EBP
0x7100003c 91                XCHG ECX, EAX
0x7100003d 7ce9              JL 0x71000028
0x7100003f fc                CLD
```

Detect Malware inside kernel mode processes and DDLs that are loaded inside the processes:

```
root@caine:/local# vol.py --profile=WinXPSP3x86 -f memory.raw moddump --
dump-dir malwareResults/

root@caine:/local# vol.py --profile=WinXPSP3x86 -f memory.raw dlldump --
dump-dir malwareResults/
```

I will use clamav to detect malware:

```
root@caine:/local# apt install clamav
root@caine:/local# freshclam
root@caine:/local# clamscan malwareResults/

----------- SCAN SUMMARY -----------
Known viruses: 4566249
Engine version: 0.99.3
Scanned directories: 1
Scanned files: 807
Infected files: 0
Data scanned: 351.77 MB
Data read: 468.80 MB (ratio 0.75:1)
Time: 86.181 sec (1 m 26 s)
```

5. What kind of connections are currently open?

Answer:

I will use the connections plugin for this:

```
root@caine:/local# vol.py --profile=WinXPSP3x86 -f memory.raw connections
Volatility Foundation Volatility Framework 2.6
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------- ---
0x8144ed00 127.0.0.1:1770           127.0.0.1:1769            2996
0x8149d270 127.0.0.1:1775           127.0.0.1:1776            2916
0x81879008 127.0.0.1:1776           127.0.0.1:1775            2916
```

```
0x81980008 127.0.0.1:1769            127.0.0.1:1770            2996
0x81ae0e68 10.0.2.15:1209            212.4.153.164:443         3872
0x814155d0 127.0.0.1:9151            127.0.0.1:1784            2916
0x81d89808 127.0.0.1:1784            127.0.0.1:9151            2996
0x81cc9a58 10.0.2.15:1959            77.234.45.63:80           2444
0x8145be68 10.0.2.15:1783            178.63.198.113:443        2916
0x81b4e008 10.0.2.15:1265            209.10.120.24:80          3872
0x818c8e68 10.0.2.15:1594            209.10.120.50:443         2064
0x81baccd8 10.0.2.15:1754            151.101.36.64:443         2812
0x81b47008 10.0.2.15:1739            40.85.224.10:80           552
0x81210e68 127.0.0.1:1777            127.0.0.1:9151            2996
0x81a46668 127.0.0.1:9151            127.0.0.1:1777            2916
0x8121e298 10.0.2.15:1634            209.10.120.24:80          2064
0x81968008 10.0.2.15:1755            151.101.36.64:443         2812
0x81802928 127.0.0.1:9151            127.0.0.1:1778            2916
0x81e0bbe8 127.0.0.1:1778            127.0.0.1:9151            2996
0x8120bb28 10.0.2.15:1758            77.234.45.55:443          2864
0x81441e68 10.0.2.15:1728            13.107.21.200:80          552
0x81ab1298 10.0.2.15:1732            204.79.197.200:80         552
0x81b48b28 10.0.2.15:1597            209.10.120.53:443         2064
0x81bbbd00 10.0.2.15:1601            209.10.120.50:443         2064
0x81801008 10.0.2.15:1733            204.79.197.200:80         552
0x81caae68 10.0.2.15:1392            23.38.32.178:443          3872
0x819a2e68 10.0.2.15:1744            40.86.224.10:80           552
0x81bb02f8 10.0.2.15:1325            5.45.58.149:80            2444
```

6. Find out what programs and services are running.

Answer:

I will use pslist for opened proceeses:

```
root@caine:/local# vol.py --profile=WinXPSP3x86 -f memory.raw pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64
Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------
------------------------------ ------------------------------
0x81fc8830 System                    4      0     65     2373 ------      0
0x81e4e700 smss.exe                428      4      3       19 ------      0
2017-02-12 12:55:55 UTC+0000
0x81e50020 csrss.exe               560    428     11      712      0      0
2017-02-12 12:55:55 UTC+0000
0x81e057c8 winlogon.exe            584    428     20      630      0      0
2017-02-12 12:55:56 UTC+0000
0x81e7dda0 services.exe            628    584     15      286      0      0
2017-02-12 12:55:56 UTC+0000
0x81e04750 lsass.exe               640    584     22      504      0      0
```

```
2017-02-12 12:55:56 UTC+0000
0x81dcba00 svchost.exe             828    628     19      237      0      0
2017-02-12 12:55:56 UTC+0000
0x81db2a48 svchost.exe             920    628     11      340      0      0
2017-02-12 12:55:56 UTC+0000
0x81d9bda0 svchost.exe            1016    628     73     1735      0      0
2017-02-12 12:55:56 UTC+0000
0x81d1a7a8 svchost.exe            1232    628      5       76      0      0
2017-02-12 12:56:15 UTC+0000
0x81cf09f0 svchost.exe            1352    628     11      180      0      0
2017-02-12 12:56:15 UTC+0000
0x81cdd4f0 spoolsv.exe            1560    628     11      119      0      0
2017-02-12 12:56:15 UTC+0000
0x81caf308 svchost.exe            1660    628      5      107      0      0
2017-02-12 12:56:23 UTC+0000
0x81c17020 alg.exe                 760    628      5      103      0      0
2017-02-12 12:56:27 UTC+0000
0x81c10020 explorer.exe           1704   1856     15      556      0      0
2017-02-12 12:57:01 UTC+0000
0x81b19b88 wuauclt.exe            1584   1016      3      124      0      0
2017-02-12 12:57:42 UTC+0000
0x81d8b020 IEXPLORE.EXE           1108   1704     13      615      0      0
2017-02-12 12:58:24 UTC+0000
0x81da8020 ctfmon.exe             1760   1108      1       88      0      0
2017-02-12 12:58:24 UTC+0000
0x81bc3b40 IEXPLORE.EXE            552   1108     21      812      0      0
2017-02-12 12:58:24 UTC+0000
0x81c38708 sol.exe                3856   1704      1       54      0      0
2017-02-12 13:00:49 UTC+0000
0x81ad0390 avgsvcx.exe            3872    628     31     1433      0      0
2017-02-12 13:00:51 UTC+0000
0x81acd620 avguix.exe             1528   2580     26     1047      0      0
2017-02-12 13:00:52 UTC+0000
0x81a9fc68 AVGSvc.exe             2444    628     87     2697      0      0
2017-02-12 13:02:12 UTC+0000
0x81a491f0 AVGUI.exe              2864   3564     40      805      0      0
2017-02-12 13:02:13 UTC+0000
0x81968da0 TuneUpUtilities        2064    628     28      839      0      0
2017-02-12 13:04:06 UTC+0000
0x81a6f3b8 TuneUpUtilities        2316   2064     11      239      0      0
2017-02-12 13:04:11 UTC+0000
0x81222020 avguix.exe             3304   1528     10      198      0      0
2017-02-12 13:04:16 UTC+0000
0x8149b020 CCleaner.exe           2812   1964      7      384      0      0
2017-02-12 13:05:46 UTC+0000
0x81454458 CCleaner.exe           2828   2812      4      116      0      0
2017-02-12 13:05:50 UTC+0000
0x8120b020 IEXPLORE.EXE           1996   1108     18      643      0      0
2017-02-12 13:06:13 UTC+0000
0x81416da0 firefox.exe            2996   3804     49      901      0      0
2017-02-12 13:06:24 UTC+0000
```

```
0x81992da0 tor.exe                2916   2996      1      118      0      0
2017-02-12 13:06:32 UTC+0000
0x81826360 taskmgr.exe            1740    584      3       83      0      0
2017-02-12 13:08:48 UTC+0000
0x81a1d020 avgdiagex.exe          3568   3872      0 --------      0      0
2017-02-12 13:15:52 UTC+0000   2017-02-12 13:15:52 UTC+0000
```

svcscan plugin for list of running services:

```
caine@caine:/local$ vol.py --profile=WinXPSP3x86 -f memory.raw svcscan
Volatility Foundation Volatility Framework 2.6
Offset: 0x671e90
Order: 1
Start: SERVICE_DISABLED
Process ID: -
Service Name: Abiosdsk
Display Name: Abiosdsk
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x671f20
Order: 2
Start: SERVICE_DISABLED
Process ID: -
Service Name: abp480n5
Display Name: abp480n5
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x671fb0
Order: 3
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: ac97intc
Display Name: Intel(r) 82801 Audio Driver Install Service (WDM)
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\ac97intc

Offset: 0x672040
Order: 4
Start: SERVICE_BOOT_START
Process ID: -
Service Name: ACPI
Display Name: Microsoft ACPI Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\ACPI
```

```
Offset: 0x6720c8
Order: 5
Start: SERVICE_DISABLED
Process ID: -
Service Name: ACPIEC
Display Name: ACPIEC
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x672158
Order: 6
Start: SERVICE_DISABLED
Process ID: -
Service Name: adpu160m
Display Name: adpu160m
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x6721e8
Order: 7
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: aec
Display Name: Microsoft Kernel Acoustic Echo Canceller
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x672270
Order: 8
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: AFD
Display Name: AFD
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\AFD

Offset: 0x6722f8
Order: 9
Start: SERVICE_DISABLED
Process ID: -
Service Name: Aha154x
Display Name: Aha154x
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x672388
```

```
Order: 10
Start: SERVICE_DISABLED
Process ID: -
Service Name: aic78u2
Display Name: aic78u2
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x672418
Order: 11
Start: SERVICE_DISABLED
Process ID: -
Service Name: aic78xx
Display Name: aic78xx
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x6724a8
Order: 12
Start: SERVICE_DISABLED
Process ID: -
Service Name: Alerter
Display Name: Alerter
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x672538
Order: 13
Start: SERVICE_DEMAND_START
Process ID: 760
Service Name: ALG
Display Name: Application Layer Gateway Service
Service Type: SERVICE_WIN32_OWN_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\alg.exe

Offset: 0x6725c0
Order: 14
Start: SERVICE_DISABLED
Process ID: -
Service Name: AliIde
Display Name: AliIde
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x672650
Order: 15
```

```
Start: SERVICE_DISABLED
Process ID: -
Service Name: amsint
Display Name: amsint
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x6726e0
Order: 16
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: AppMgmt
Display Name: -
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x672770
Order: 17
Start: SERVICE_DISABLED
Process ID: -
Service Name: asc
Display Name: asc
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x6727f8
Order: 18
Start: SERVICE_DISABLED
Process ID: -
Service Name: asc3350p
Display Name: asc3350p
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x672888
Order: 19
Start: SERVICE_DISABLED
Process ID: -
Service Name: asc3550
Display Name: asc3550
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x672918
Order: 20
Start: SERVICE_DEMAND_START
```

```
Process ID: -
Service Name: AsyncMac
Display Name: -
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x6729a8
Order: 21
Start: SERVICE_BOOT_START
Process ID: -
Service Name: atapi
Display Name: -
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\atapi

Offset: 0x672a30
Order: 22
Start: SERVICE_DISABLED
Process ID: -
Service Name: Atdisk
Display Name: Atdisk
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x672ac0
Order: 23
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: Atmarpc
Display Name: -
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x672b50
Order: 24
Start: SERVICE_AUTO_START
Process ID: 1016
Service Name: AudioSrv
Display Name: -
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

Offset: 0x672be0
Order: 25
Start: SERVICE_DEMAND_START
Process ID: -
```

```
Service Name: audstub
Display Name: -
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\audstub

Offset: 0x672c70
Order: 26
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: Beep
Display Name: Beep
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\Beep

Offset: 0x672cf8
Order: 27
Start: SERVICE_DEMAND_START
Process ID: 1016
Service Name: BITS
Display Name: Background Intelligent Transfer Service
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

Offset: 0x672d80
Order: 28
Start: SERVICE_AUTO_START
Process ID: -
Service Name: Browser
Display Name: Computer Browser
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x672e10
Order: 29
Start: SERVICE_DISABLED
Process ID: -
Service Name: cbidf2k
Display Name: cbidf2k
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x672ea0
Order: 30
Start: SERVICE_DISABLED
Process ID: -
Service Name: cd20xrnt
```

```
Display Name: cd20xrnt
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x672f30
Order: 31
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: Cdaudio
Display Name: Cdaudio
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x672fc0
Order: 32
Start: SERVICE_DISABLED
Process ID: -
Service Name: Cdfs
Display Name: Cdfs
Service Type: SERVICE_FILE_SYSTEM_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \FileSystem\Cdfs

Offset: 0x673048
Order: 33
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: Cdrom
Display Name: -
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\Cdrom

Offset: 0x6730d0
Order: 34
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: Changer
Display Name: Changer
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x673160
Order: 35
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: CiSvc
Display Name: -
```

```
Service Type: SERVICE_INTERACTIVE_PROCESS, SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x6731e8
Order: 36
Start: SERVICE_DISABLED
Process ID: -
Service Name: ClipSrv
Display Name: ClipBook
Service Type: SERVICE_WIN32_OWN_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x673278
Order: 37
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: CmBatt
Display Name: -
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\CmBatt

Offset: 0x673308
Order: 38
Start: SERVICE_DISABLED
Process ID: -
Service Name: CmdIde
Display Name: CmdIde
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x673398
Order: 39
Start: SERVICE_BOOT_START
Process ID: -
Service Name: Compbatt
Display Name: -
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\Compbatt

Offset: 0x673428
Order: 40
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: COMSysApp
Display Name: COM+ System Application
Service Type: SERVICE_WIN32_OWN_PROCESS
```

```
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x6734b8
Order: 41
Start: SERVICE_DISABLED
Process ID: -
Service Name: Cpqarray
Display Name: Cpqarray
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x673548
Order: 42
Start: SERVICE_AUTO_START
Process ID: 1016
Service Name: CryptSvc
Display Name: Cryptographic Services
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

Offset: 0x6735d8
Order: 43
Start: SERVICE_DISABLED
Process ID: -
Service Name: dac960nt
Display Name: dac960nt
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x673668
Order: 44
Start: SERVICE_AUTO_START
Process ID: 828
Service Name: DcomLaunch
Display Name: DCOM Server Process Launcher
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\system32\svchost -k DcomLaunch

Offset: 0x673700
Order: 45
Start: SERVICE_AUTO_START
Process ID: 1016
Service Name: Dhcp
Display Name: -
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
```

```
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

Offset: 0x673788
Order: 46
Start: SERVICE_BOOT_START
Process ID: -
Service Name: Disk
Display Name: -
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\Disk

Offset: 0x673810
Order: 47
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: dmadmin
Display Name: Logical Disk Manager Administrative Service
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x6738a0
Order: 48
Start: SERVICE_BOOT_START
Process ID: -
Service Name: dmboot
Display Name: dmboot
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\dmboot

Offset: 0x673930
Order: 49
Start: SERVICE_BOOT_START
Process ID: -
Service Name: dmio
Display Name: Logical Disk Manager Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\dmio

Offset: 0x6739b8
Order: 50
Start: SERVICE_BOOT_START
Process ID: -
Service Name: dmload
Display Name: dmload
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\dmload
```

```
Offset: 0x673a48
Order: 51
Start: SERVICE_AUTO_START
Process ID: 1016
Service Name: dmserver
Display Name: Logical Disk Manager
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

Offset: 0x673ad8
Order: 52
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: DMusic
Display Name: Microsoft Kernel DLS Syntheiszer
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x673b68
Order: 53
Start: SERVICE_AUTO_START
Process ID: 1232
Service Name: Dnscache
Display Name: DNS Client
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\system32\svchost.exe -k NetworkService

Offset: 0x673bf8
Order: 54
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: Dot3svc
Display Name: Wired AutoConfig
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x673c88
Order: 55
Start: SERVICE_DISABLED
Process ID: -
Service Name: dpti2o
Display Name: dpti2o
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x673d18
```

```
Order: 56
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: drmkaud
Display Name: Microsoft Kernel DRM Audio Descrambler
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x673da8
Order: 57
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: EapHost
Display Name: Extensible Authentication Protocol Service
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x673e38
Order: 58
Start: SERVICE_AUTO_START
Process ID: 1016
Service Name: ERSvc
Display Name: Error Reporting Service
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

Offset: 0x673ec0
Order: 59
Start: SERVICE_AUTO_START
Process ID: 628
Service Name: Eventlog
Display Name: Event Log
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\system32\services.exe

Offset: 0x673f50
Order: 60
Start: SERVICE_DEMAND_START
Process ID: 1016
Service Name: EventSystem
Display Name: COM+ Event System
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

Offset: 0x673fe8
Order: 61
```

```
Start: SERVICE_DISABLED
Process ID: -
Service Name: exFat
Display Name: exFat
Service Type: SERVICE_FILE_SYSTEM_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x674070
Order: 62
Start: SERVICE_DISABLED
Process ID: -
Service Name: Fastfat
Display Name: Fastfat
Service Type: SERVICE_FILE_SYSTEM_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x674100
Order: 63
Start: SERVICE_DEMAND_START
Process ID: 1016
Service Name: FastUserSwitchingCompatibility
Display Name: Fast User Switching Compatibility
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

Offset: 0x6741c0
Order: 64
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: Fdc
Display Name: Fdc
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x674248
Order: 65
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: Fips
Display Name: Fips
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\Fips

Offset: 0x6742d0
Order: 66
Start: SERVICE_SYSTEM_START
```

```
Process ID: -
Service Name: Flpydisk
Display Name: Flpydisk
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x674360
Order: 67
Start: SERVICE_BOOT_START
Process ID: -
Service Name: FltMgr
Display Name: FltMgr
Service Type: SERVICE_FILE_SYSTEM_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \FileSystem\FltMgr

Offset: 0x6743f0
Order: 68
Start: SERVICE_BOOT_START
Process ID: -
Service Name: Ftdisk
Display Name: Volume Manager Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\Ftdisk

Offset: 0x674480
Order: 69
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: Gpc
Display Name: Generic Packet Classifier
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\Gpc

Offset: 0x674508
Order: 70
Start: SERVICE_AUTO_START
Process ID: 1016
Service Name: helpsvc
Display Name: Help and Support
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

Offset: 0x674598
Order: 71
Start: SERVICE_DISABLED
Process ID: -
```

```
Service Name: HidServ
Display Name: Human Interface Device Access
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x674628
Order: 72
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: hidusb
Display Name: Microsoft HID Class Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\hidusb

Offset: 0x6746b8
Order: 73
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: hkmsvc
Display Name: Health Key and Certificate Management Service
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x674748
Order: 74
Start: SERVICE_DISABLED
Process ID: -
Service Name: hpn
Display Name: hpn
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x6747d0
Order: 75
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: HTTP
Display Name: HTTP
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\HTTP

Offset: 0x674858
Order: 76
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: HTTPFilter
```

```
Display Name: HTTP SSL
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x6748f0
Order: 77
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: i2omgmt
Display Name: i2omgmt
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x674980
Order: 78
Start: SERVICE_DISABLED
Process ID: -
Service Name: i2omp
Display Name: i2omp
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x674a08
Order: 79
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: i8042prt
Display Name: i8042 Keyboard and PS/2 Mouse Port Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\i8042prt

Offset: 0x674a98
Order: 80
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: Imapi
Display Name: CD-Burning Filter Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x674b20
Order: 81
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: ImapiService
Display Name: IMAPI CD-Burning COM Service
```

```
Service Type: SERVICE_WIN32_OWN_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x674bb8
Order: 82
Start: SERVICE_DISABLED
Process ID: -
Service Name: ini910u
Display Name: ini910u
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x674c48
Order: 83
Start: SERVICE_BOOT_START
Process ID: -
Service Name: IntelIde
Display Name: IntelIde
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\IntelIde

Offset: 0x674cd8
Order: 84
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: Ip6Fw
Display Name: IPv6 Windows Firewall Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x674d60
Order: 85
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: IpFilterDriver
Display Name: IP Traffic Filter Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x674e00
Order: 86
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: IpInIp
Display Name: IP in IP Tunnel Driver
Service Type: SERVICE_KERNEL_DRIVER
```

```
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x674e90
Order: 87
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: IpNat
Display Name: IP Network Address Translator
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\IpNat

Offset: 0x674f18
Order: 88
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: IPSec
Display Name: IPSEC driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\IPSec

Offset: 0x674fa0
Order: 89
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: IRENUM
Display Name: IR Enumerator Service
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x675030
Order: 90
Start: SERVICE_BOOT_START
Process ID: -
Service Name: isapnp
Display Name: PnP ISA/EISA Bus Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\isapnp

Offset: 0x6750c0
Order: 91
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: Kbdclass
Display Name: Keyboard Class Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
```

```
Binary Path: \Driver\Kbdclass

Offset: 0x675150
Order: 92
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: kmixer
Display Name: Microsoft Kernel Wave Audio Mixer
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\kmixer

Offset: 0x6751e0
Order: 93
Start: SERVICE_BOOT_START
Process ID: -
Service Name: KSecDD
Display Name: KSecDD
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\KSecDD

Offset: 0x675270
Order: 94
Start: SERVICE_AUTO_START
Process ID: 1016
Service Name: LanmanServer
Display Name: Server
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

Offset: 0x675308
Order: 95
Start: SERVICE_AUTO_START
Process ID: 1016
Service Name: lanmanworkstation
Display Name: Workstation
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

Offset: 0x6753a8
Order: 96
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: lbrtfdc
Display Name: lbrtfdc
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -
```

```
Offset: 0x675438
Order: 97
Start: SERVICE_AUTO_START
Process ID: 1352
Service Name: LmHosts
Display Name: TCP/IP NetBIOS Helper
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\system32\svchost.exe -k LocalService

Offset: 0x6754c8
Order: 98
Start: SERVICE_DISABLED
Process ID: -
Service Name: Messenger
Display Name: Messenger
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x675558
Order: 99
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: mnmdd
Display Name: mnmdd
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\mnmdd

Offset: 0x6755e0
Order: 100
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: mnmsrvc
Display Name: NetMeeting Remote Desktop Sharing
Service Type: SERVICE_INTERACTIVE_PROCESS, SERVICE_WIN32_OWN_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x675670
Order: 101
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: Modem
Display Name: Modem
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x6756f8
```

```
Order: 102
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: Mouclass
Display Name: Mouse Class Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\Mouclass

Offset: 0x675788
Order: 103
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: mouhid
Display Name: Mouse HID Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\mouhid

Offset: 0x675818
Order: 104
Start: SERVICE_BOOT_START
Process ID: -
Service Name: MountMgr
Display Name: MountMgr
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\MountMgr

Offset: 0x6758a8
Order: 105
Start: SERVICE_DISABLED
Process ID: -
Service Name: mraid35x
Display Name: mraid35x
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x675938
Order: 106
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: MRxDAV
Display Name: WebDav Client Redirector
Service Type: SERVICE_FILE_SYSTEM_DRIVER
Service State: SERVICE_RUNNING
Binary Path: -

Offset: 0x6759c8
Order: 107
```

```
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: MRxSmb
Display Name: MRxSmb
Service Type: SERVICE_FILE_SYSTEM_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \FileSystem\MRxSmb

Offset: 0x675a58
Order: 108
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: MSDTC
Display Name: Distributed Transaction Coordinator
Service Type: SERVICE_WIN32_OWN_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x675ae0
Order: 109
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: Msfs
Display Name: Msfs
Service Type: SERVICE_FILE_SYSTEM_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \FileSystem\Msfs

Offset: 0x675b68
Order: 110
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: MSIServer
Display Name: Windows Installer
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x675bf8
Order: 111
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: MSKSSRV
Display Name: Microsoft Streaming Service Proxy
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x675c88
Order: 112
Start: SERVICE_DEMAND_START
```

```
Process ID: -
Service Name: MSPCLOCK
Display Name: Microsoft Streaming Clock Proxy
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x675d18
Order: 113
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: MSPQM
Display Name: Microsoft Streaming Quality Manager Proxy
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x675da0
Order: 114
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: mssmbios
Display Name: Microsoft System Management BIOS Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\mssmbios

Offset: 0x675e30
Order: 115
Start: SERVICE_BOOT_START
Process ID: -
Service Name: Mup
Display Name: Mup
Service Type: SERVICE_FILE_SYSTEM_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \FileSystem\Mup

Offset: 0x675eb8
Order: 116
Start: SERVICE_BOOT_START
Process ID: -
Service Name: mv61xxmm
Display Name: mv61xxmm
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\mv61xxmm

Offset: 0x675f48
Order: 117
Start: SERVICE_BOOT_START
Process ID: -
```

```
Service Name: mv64xxmm
Display Name: mv64xxmm
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\mv64xxmm

Offset: 0x675fd8
Order: 118
Start: SERVICE_BOOT_START
Process ID: -
Service Name: mvxxmm
Display Name: mvxxmm
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\mvxxmm

Offset: 0x676068
Order: 119
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: napagent
Display Name: Network Access Protection Agent
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x6760f8
Order: 120
Start: SERVICE_BOOT_START
Process ID: -
Service Name: NDIS
Display Name: NDIS System Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\NDIS

Offset: 0x676180
Order: 121
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: NdisTapi
Display Name: -
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\NdisTapi

Offset: 0x676210
Order: 122
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: Ndisuio
```

```
Display Name: -
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\Ndisuio

Offset: 0x6762a0
Order: 123
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: NdisWan
Display Name: -
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\NdisWan

Offset: 0x676330
Order: 124
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: NDProxy
Display Name: NDIS Proxy
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\NDProxy

Offset: 0x6763c0
Order: 125
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: NetBIOS
Display Name: -
Service Type: SERVICE_FILE_SYSTEM_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \FileSystem\NetBIOS

Offset: 0x676450
Order: 126
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: NetBT
Display Name: -
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\NetBT

Offset: 0x6764d8
Order: 127
Start: SERVICE_DISABLED
Process ID: -
Service Name: NetDDE
Display Name: -
```

```
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x676568
Order: 128
Start: SERVICE_DISABLED
Process ID: -
Service Name: NetDDEdsdm
Display Name: -
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x676600
Order: 129
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: Netlogon
Display Name: Net Logon
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x676690
Order: 130
Start: SERVICE_DEMAND_START
Process ID: 1016
Service Name: Netman
Display Name: Network Connections
Service Type: SERVICE_INTERACTIVE_PROCESS, SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

Offset: 0x676720
Order: 131
Start: SERVICE_DEMAND_START
Process ID: 1016
Service Name: Nla
Display Name: -
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

Offset: 0x6767a8
Order: 132
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: Npfs
Display Name: Npfs
Service Type: SERVICE_FILE_SYSTEM_DRIVER
```

```
Service State: SERVICE_RUNNING
Binary Path: \FileSystem\Npfs

Offset: 0x676830
Order: 133
Start: SERVICE_DISABLED
Process ID: -
Service Name: Ntfs
Display Name: Ntfs
Service Type: SERVICE_FILE_SYSTEM_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \FileSystem\Ntfs

Offset: 0x6768b8
Order: 134
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: NtLmSsp
Display Name: -
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x676948
Order: 135
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: NtmsSvc
Display Name: -
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x6769d8
Order: 136
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: Null
Display Name: Null
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\Null

Offset: 0x676a60
Order: 137
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: NwlnkFlt
Display Name: -
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
```

```
Binary Path: -

Offset: 0x676af0
Order: 138
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: NwlnkFwd
Display Name: -
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x676b80
Order: 139
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: Parport
Display Name: Parport
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x676c10
Order: 140
Start: SERVICE_BOOT_START
Process ID: -
Service Name: PartMgr
Display Name: PartMgr
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\PartMgr

Offset: 0x676ca0
Order: 141
Start: SERVICE_AUTO_START
Process ID: -
Service Name: ParVdm
Display Name: ParVdm
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x676d30
Order: 142
Start: SERVICE_BOOT_START
Process ID: -
Service Name: PCI
Display Name: -
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\PCI
```

```
Offset: 0x676db8
Order: 143
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: PCIDump
Display Name: PCIDump
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x676e48
Order: 144
Start: SERVICE_DISABLED
Process ID: -
Service Name: PCIIde
Display Name: PCIIde
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x676ed8
Order: 145
Start: SERVICE_DISABLED
Process ID: -
Service Name: Pcmcia
Display Name: Pcmcia
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x676f68
Order: 146
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: PCnet
Display Name: -
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\PCnet

Offset: 0x676ff0
Order: 147
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: PDCOMP
Display Name: PDCOMP
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x677080
```

```
Order: 148
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: PDFRAME
Display Name: PDFRAME
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x677110
Order: 149
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: PDRELI
Display Name: PDRELI
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x6771a0
Order: 150
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: PDRFRAME
Display Name: PDRFRAME
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x677230
Order: 151
Start: SERVICE_DISABLED
Process ID: -
Service Name: perc2
Display Name: perc2
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x6772b8
Order: 152
Start: SERVICE_DISABLED
Process ID: -
Service Name: perc2hib
Display Name: perc2hib
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x677348
Order: 153
```

```
Start: SERVICE_AUTO_START
Process ID: 628
Service Name: PlugPlay
Display Name: -
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\system32\services.exe

Offset: 0x6773d8
Order: 154
Start: SERVICE_AUTO_START
Process ID: 640
Service Name: PolicyAgent
Display Name: -
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\system32\lsass.exe

Offset: 0x677470
Order: 155
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: PptpMiniport
Display Name: -
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\PptpMiniport

Offset: 0x677508
Order: 156
Start: SERVICE_AUTO_START
Process ID: 640
Service Name: ProtectedStorage
Display Name: -
Service Type: SERVICE_INTERACTIVE_PROCESS, SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\system32\lsass.exe

Offset: 0x6775a8
Order: 157
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: PSched
Display Name: QoS Packet Scheduler
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\PSched

Offset: 0x677638
Order: 158
Start: SERVICE_DEMAND_START
```

```
Process ID: -
Service Name: Ptilink
Display Name: Direct Parallel Link Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\Ptilink

Offset: 0x6776c8
Order: 159
Start: SERVICE_DISABLED
Process ID: -
Service Name: ql1080
Display Name: ql1080
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x677758
Order: 160
Start: SERVICE_DISABLED
Process ID: -
Service Name: Ql10wnt
Display Name: Ql10wnt
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x6777e8
Order: 161
Start: SERVICE_DISABLED
Process ID: -
Service Name: ql12160
Display Name: ql12160
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x677878
Order: 162
Start: SERVICE_DISABLED
Process ID: -
Service Name: ql1240
Display Name: ql1240
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x677908
Order: 163
Start: SERVICE_DISABLED
Process ID: -
```

```
Service Name: ql1280
Display Name: ql1280
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x677998
Order: 164
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: RasAcd
Display Name: Remote Access Auto Connection Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\RasAcd

Offset: 0x677a28
Order: 165
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: RasAuto
Display Name: Remote Access Auto Connection Manager
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x677ab8
Order: 166
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: Rasl2tp
Display Name: WAN Miniport (L2TP)
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\Rasl2tp

Offset: 0x677b48
Order: 167
Start: SERVICE_DEMAND_START
Process ID: 1016
Service Name: RasMan
Display Name: Remote Access Connection Manager
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

Offset: 0x677bd8
Order: 168
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: RasPppoe
```

```
Display Name: Remote Access PPPOE Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\RasPppoe

Offset: 0x677c68
Order: 169
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: Raspti
Display Name: Direct Parallel
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\Raspti

Offset: 0x677cf8
Order: 170
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: Rdbss
Display Name: Rdbss
Service Type: SERVICE_FILE_SYSTEM_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \FileSystem\Rdbss

Offset: 0x677d80
Order: 171
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: RDPCDD
Display Name: RDPCDD
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\RDPCDD

Offset: 0x677e10
Order: 172
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: rdpdr
Display Name: Terminal Server Device Redirector Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\rdpdr

Offset: 0x677e98
Order: 173
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: RDPWD
Display Name: RDPWD
```

```
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x677f20
Order: 174
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: RDSessMgr
Display Name: Remote Desktop Help Session Manager
Service Type: SERVICE_WIN32_OWN_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x677fb0
Order: 175
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: redbook
Display Name: Digital CD Audio Playback Filter Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x678040
Order: 176
Start: SERVICE_DISABLED
Process ID: -
Service Name: RemoteAccess
Display Name: Routing and Remote Access
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x6780d8
Order: 177
Start: SERVICE_AUTO_START
Process ID: 1352
Service Name: RemoteRegistry
Display Name: Remote Registry
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\system32\svchost.exe -k LocalService

Offset: 0x678178
Order: 178
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: RpcLocator
Display Name: Remote Procedure Call (RPC) Locator
Service Type: SERVICE_WIN32_OWN_PROCESS
```

```
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x678210
Order: 179
Start: SERVICE_AUTO_START
Process ID: 920
Service Name: RpcSs
Display Name: Remote Procedure Call (RPC)
Service Type: SERVICE_WIN32_OWN_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\system32\svchost -k rpcss

Offset: 0x678298
Order: 180
Start: SERVICE_AUTO_START
Process ID: -
Service Name: rspndr
Display Name: Link-Layer Topology Discovery Responder
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\rspndr

Offset: 0x678328
Order: 181
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: RSVP
Display Name: QoS RSVP
Service Type: SERVICE_WIN32_OWN_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x6783b0
Order: 182
Start: SERVICE_AUTO_START
Process ID: 640
Service Name: SamSs
Display Name: Security Accounts Manager
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\system32\lsass.exe

Offset: 0x678438
Order: 183
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: SCardSvr
Display Name: -
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
```

```
Binary Path: -

Offset: 0x6784c8
Order: 184
Start: SERVICE_AUTO_START
Process ID: 1016
Service Name: Schedule
Display Name: Task Scheduler
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

Offset: 0x678558
Order: 185
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: Secdrv
Display Name: Secdrv
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x6785e8
Order: 186
Start: SERVICE_AUTO_START
Process ID: 1016
Service Name: seclogon
Display Name: Secondary Logon
Service Type: SERVICE_INTERACTIVE_PROCESS, SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

Offset: 0x678678
Order: 187
Start: SERVICE_AUTO_START
Process ID: 1016
Service Name: SENS
Display Name: System Event Notification
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

Offset: 0x678700
Order: 188
Start: SERVICE_AUTO_START
Process ID: -
Service Name: Serial
Display Name: Serial
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -
```

```
Offset: 0x678790
Order: 189
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: Sfloppy
Display Name: Sfloppy
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x678820
Order: 190
Start: SERVICE_AUTO_START
Process ID: 1016
Service Name: SharedAccess
Display Name: Windows Firewall/Internet Connection Sharing (ICS)
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

Offset: 0x6788b8
Order: 191
Start: SERVICE_AUTO_START
Process ID: 1016
Service Name: ShellHWDetection
Display Name: -
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

Offset: 0x678958
Order: 192
Start: SERVICE_DISABLED
Process ID: -
Service Name: Simbad
Display Name: Simbad
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x6789e8
Order: 193
Start: SERVICE_DISABLED
Process ID: -
Service Name: Sparrow
Display Name: Sparrow
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x678a78
```

```
Order: 194
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: splitter
Display Name: -
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x678b08
Order: 195
Start: SERVICE_AUTO_START
Process ID: 1560
Service Name: Spooler
Display Name: -
Service Type: SERVICE_INTERACTIVE_PROCESS, SERVICE_WIN32_OWN_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\system32\spoolsv.exe

Offset: 0x678b98
Order: 196
Start: SERVICE_BOOT_START
Process ID: -
Service Name: sr
Display Name: -
Service Type: SERVICE_FILE_SYSTEM_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \FileSystem\sr

Offset: 0x678c20
Order: 197
Start: SERVICE_AUTO_START
Process ID: 1016
Service Name: srservice
Display Name: -
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

Offset: 0x678cb0
Order: 198
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: Srv
Display Name: Srv
Service Type: SERVICE_FILE_SYSTEM_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \FileSystem\Srv

Offset: 0x678d38
Order: 199
```

```
Start: SERVICE_DEMAND_START
Process ID: 1352
Service Name: SSDPSRV
Display Name: -
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\system32\svchost.exe -k LocalService

Offset: 0x678dc8
Order: 200
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: stisvc
Display Name: -
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x678e58
Order: 201
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: swenum
Display Name: -
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\swenum

Offset: 0x678ee8
Order: 202
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: swmidi
Display Name: -
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x678f78
Order: 203
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: SwPrv
Display Name: -
Service Type: SERVICE_WIN32_OWN_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x679000
Order: 204
Start: SERVICE_DISABLED
```

```
Process ID: -
Service Name: symc810
Display Name: symc810
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x679090
Order: 205
Start: SERVICE_DISABLED
Process ID: -
Service Name: symc8xx
Display Name: symc8xx
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x679120
Order: 206
Start: SERVICE_DISABLED
Process ID: -
Service Name: sym_hi
Display Name: sym_hi
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x6791b0
Order: 207
Start: SERVICE_DISABLED
Process ID: -
Service Name: sym_u3
Display Name: sym_u3
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x679240
Order: 208
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: sysaudio
Display Name: -
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\sysaudio

Offset: 0x6792d0
Order: 209
Start: SERVICE_DEMAND_START
Process ID: -
```

```
Service Name: SysmonLog
Display Name: -
Service Type: SERVICE_WIN32_OWN_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x679360
Order: 210
Start: SERVICE_DEMAND_START
Process ID: 1016
Service Name: TapiSrv
Display Name: Telephony
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

Offset: 0x6793f0
Order: 211
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: Tcpip
Display Name: TCP/IP Protocol Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\Tcpip

Offset: 0x679478
Order: 212
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: TDPIPE
Display Name: TDPIPE
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x679508
Order: 213
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: TDTCP
Display Name: TDTCP
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x679590
Order: 214
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: TermDD
```

```
Display Name: Terminal Device Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\TermDD

Offset: 0x679620
Order: 215
Start: SERVICE_DEMAND_START
Process ID: 828
Service Name: TermService
Display Name: Terminal Services
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\system32\svchost -k DcomLaunch

Offset: 0x6796b8
Order: 216
Start: SERVICE_AUTO_START
Process ID: 1016
Service Name: Themes
Display Name: Themes
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

Offset: 0x679748
Order: 217
Start: SERVICE_DISABLED
Process ID: -
Service Name: TlntSvr
Display Name: -
Service Type: SERVICE_WIN32_OWN_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x6797d8
Order: 218
Start: SERVICE_DISABLED
Process ID: -
Service Name: TosIde
Display Name: TosIde
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x679868
Order: 219
Start: SERVICE_AUTO_START
Process ID: 1016
Service Name: TrkWks
Display Name: -
```

```
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

Offset: 0x6798f8
Order: 220
Start: SERVICE_DISABLED
Process ID: -
Service Name: Udfs
Display Name: Udfs
Service Type: SERVICE_FILE_SYSTEM_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x679980
Order: 221
Start: SERVICE_DISABLED
Process ID: -
Service Name: ultra
Display Name: ultra
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x679a08
Order: 222
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: Update
Display Name: Microcode Update Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\Update

Offset: 0x679a98
Order: 223
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: upnphost
Display Name: Universal Plug and Play Device Host
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x679b28
Order: 224
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: UPS
Display Name: Uninterruptible Power Supply
Service Type: SERVICE_WIN32_OWN_PROCESS
```

```
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x679bb0
Order: 225
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: usbhub
Display Name: USB2 Enabled Hub
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\usbhub

Offset: 0x679c40
Order: 226
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: usbohci
Display Name: Microsoft USB Open Host Controller Miniport Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\usbohci

Offset: 0x679cd0
Order: 227
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: VgaSave
Display Name: VgaSave
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\VgaSave

Offset: 0x679d60
Order: 228
Start: SERVICE_DISABLED
Process ID: -
Service Name: ViaIde
Display Name: ViaIde
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x679df0
Order: 229
Start: SERVICE_BOOT_START
Process ID: -
Service Name: VolSnap
Display Name: VolSnap
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
```

```
Binary Path: \Driver\VolSnap

Offset: 0x679e80
Order: 230
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: VSS
Display Name: Volume Shadow Copy
Service Type: SERVICE_WIN32_OWN_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x679f08
Order: 231
Start: SERVICE_AUTO_START
Process ID: 1016
Service Name: W32Time
Display Name: Windows Time
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

Offset: 0x679f98
Order: 232
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: Wanarp
Display Name: Remote Access IP ARP Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\Wanarp

Offset: 0x67a028
Order: 233
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: WDICA
Display Name: WDICA
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x67a0b0
Order: 234
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: wdmaud
Display Name: Microsoft WINMM WDM Audio Compatibility Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\wdmaud
```

```
Offset: 0x67a140
Order: 235
Start: SERVICE_AUTO_START
Process ID: 1660
Service Name: WebClient
Display Name: WebClient
Service Type: SERVICE_WIN32_OWN_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\system32\svchost.exe -k LocalService

Offset: 0x67a1d0
Order: 236
Start: SERVICE_AUTO_START
Process ID: 1016
Service Name: winmgmt
Display Name: Windows Management Instrumentation
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

Offset: 0x67a260
Order: 237
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: WmdmPmSN
Display Name: Portable Media Serial Number Service
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x67a2f0
Order: 238
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: Wmi
Display Name: Windows Management Instrumentation Driver Extensions
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x67a378
Order: 239
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: WmiApSrv
Display Name: WMI Performance Adapter
Service Type: SERVICE_WIN32_OWN_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x67a408
```

```
Order: 240
Start: SERVICE_AUTO_START
Process ID: 1016
Service Name: wscsvc
Display Name: Security Center
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

Offset: 0x67a498
Order: 241
Start: SERVICE_AUTO_START
Process ID: 1016
Service Name: wuauserv
Display Name: Automatic Updates
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

Offset: 0x67a528
Order: 242
Start: SERVICE_AUTO_START
Process ID: 1016
Service Name: WZCSVC
Display Name: Wireless Zero Configuration
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

Offset: 0x67a5b8
Order: 243
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: xmlprov
Display Name: Network Provisioning Service
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x67a648
Order: 244
Start: SERVICE_AUTO_START
Process ID: 3872
Service Name: avgsvc
Display Name: AVG Service
Service Type: SERVICE_WIN32_OWN_PROCESS
Service State: SERVICE_RUNNING
Binary Path: "C:\Program Files\AVG\Framework\Common\avgsvcx.exe"

Offset: 0x67a6d8
Order: 245
```

```
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: avgbdisk
Display Name: avgbdisk
Service Type: SERVICE_FILE_SYSTEM_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \FileSystem\avgbdisk

Offset: 0x67a768
Order: 246
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: avgbidsdriver
Display Name: avgbidsdriver
Service Type: SERVICE_FILE_SYSTEM_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \FileSystem\avgbidsdriver

Offset: 0x67a800
Order: 247
Start: SERVICE_BOOT_START
Process ID: -
Service Name: avgbidsh
Display Name: avgbidsh
Service Type: SERVICE_FILE_SYSTEM_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \FileSystem\avgbidsh

Offset: 0x67a890
Order: 248
Start: SERVICE_BOOT_START
Process ID: -
Service Name: avgblog
Display Name: avgblog
Service Type: SERVICE_FILE_SYSTEM_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \FileSystem\avgblog

Offset: 0x67a920
Order: 249
Start: SERVICE_BOOT_START
Process ID: -
Service Name: avgbuniv
Display Name: avgbuniv
Service Type: SERVICE_FILE_SYSTEM_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \FileSystem\avgbuniv

Offset: 0x67a9b0
Order: 250
Start: SERVICE_SYSTEM_START
```

```
Process ID: -
Service Name: avgSnx
Display Name: avgSnx
Service Type: SERVICE_FILE_SYSTEM_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \FileSystem\avgSnx

Offset: 0x67aa40
Order: 251
Start: SERVICE_SYSTEM_START
Process ID: -
Service Name: avgRdr
Display Name: avgRdr
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\avgRdr

Offset: 0x67aad0
Order: 252
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: avgHwid
Display Name: avgHwid
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x67ab60
Order: 253
Start: SERVICE_AUTO_START
Process ID: -
Service Name: avgMonFlt
Display Name: avgMonFlt
Service Type: SERVICE_FILE_SYSTEM_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \FileSystem\avgMonFlt

Offset: 0x67abf0
Order: 254
Start: SERVICE_BOOT_START
Process ID: -
Service Name: avgRvrt
Display Name: avgRvrt
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x67ac80
Order: 255
Start: SERVICE_SYSTEM_START
Process ID: -
```

```
Service Name: avgSP
Display Name: avgSP
Service Type: SERVICE_FILE_SYSTEM_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \FileSystem\avgSP

Offset: 0x67ad08
Order: 256
Start: SERVICE_BOOT_START
Process ID: -
Service Name: avgVmm
Display Name: avgVmm
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\avgVmm

Offset: 0x67ad98
Order: 257
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: avgStmXP
Display Name: avgStmXP
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\avgStmXP

Offset: 0x67ae28
Order: 258
Start: SERVICE_AUTO_START
Process ID: -
Service Name: avgbIDSAgent
Display Name: avgbIDSAgent
Service Type: SERVICE_WIN32_OWN_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x67aec0
Order: 259
Start: SERVICE_AUTO_START
Process ID: 2444
Service Name: AVG Antivirus
Display Name: AVG Antivirus
Service Type: SERVICE_INTERACTIVE_PROCESS, SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: "C:\Program Files\AVG\Antivirus\AVGSvc.exe"

Offset: 0x67af58
Order: 260
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: Wdf01000
```

```
Display Name: Kernel Mode Driver Frameworks service
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\Wdf01000

Offset: 0x67afe8
Order: 261
Start: SERVICE_AUTO_START
Process ID: 2064
Service Name: TuneUp.UtilitiesSvc
Display Name: AVG PC TuneUp Service
Service Type: SERVICE_WIN32_OWN_PROCESS
Service State: SERVICE_RUNNING
Binary Path: "C:\Program Files\AVG\AVG PC
TuneUp\TuneUpUtilitiesService32.exe"

Offset: 0x67b090
Order: 262
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: TuneUpUtilitiesDrv
Display Name: TuneUpUtilitiesDrv
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\TuneUpUtilitiesDrv

Offset: 0x67b138
Order: 263
Start: SERVICE_AUTO_START
Process ID: -
Service Name: gupdate
Display Name: Google Update Service (gupdate)
Service Type: SERVICE_WIN32_OWN_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x67b1c8
Order: 264
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: gupdatem
Display Name: Google Update Service (gupdatem)
Service Type: SERVICE_WIN32_OWN_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x67b258
Order: 265
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: gusvc
```

```
Display Name: Google Software Updater
Service Type: SERVICE_WIN32_OWN_PROCESS
Service State: SERVICE_STOPPED
Binary Path: -
```

7. How can you retrieve files out of the memory? What files can contain artifacts?

Answer:

There are many options for that.

- dumpregistry - Dumps registry files out to disk
- moddump - Dump a kernel driver to an executable file sample
- procdump - Dump a process to an executable file sample
- dlldump - Dumps DLL files from the memory
- dumpcerts - Dump RSA private and public SSL keys
- dumpfiles - Extract memory mapped and cached files

The password hashes of users on the system we can verify that the corresponding hive is loaded into memory using the hivelist plugin.

```
caine@caine:/local$ vol.py --profile=WinXPSP3x86 -f memory.raw hivelist
Volatility Foundation Volatility Framework 2.6
Virtual    Physical   Name
---------- ---------- ----
0xe198d5d0 0x11eac5d0
\??\C:\WINDOWS\system32\config\systemprofile\NtUser.dat
0xe19d3008 0x130e4008 \??\C:\Documents and Settings\dave\Local
Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe17e8008 0x1242e008 \Device\HarddiskVolume1\Documents and
Settings\dave\NTUSER.DAT
0xe147cb60 0x0b286b60 \??\C:\Documents and Settings\LocalService\Local
Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1497008 0x0b337008 \Device\HarddiskVolume1\Documents and
Settings\LocalService\NTUSER.DAT
0xe10d8b60 0x07ff3b60 \??\C:\Documents and Settings\NetworkService\Local
Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe105c3e8 0x073e23e8 \Device\HarddiskVolume1\Documents and
Settings\NetworkService\NTUSER.DAT
0xe12c2b60 0x036fcb60
\Device\HarddiskVolume1\WINDOWS\system32\config\software
0xe12a6688 0x035a2688
\Device\HarddiskVolume1\WINDOWS\system32\config\default
0xe1301008 0x03eea008
\Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
0xe11e1b60 0x02a7ab60 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0xe11cc758 0x02aa8758 [no name]
```

```
0xe1035b60 0x0290fb60 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0xe102e008 0x02909008 [no name]
```

filescan plugin could be used to list files that are currently loaded into memory, and dump . txt files :

```
root@caine:/local$ vol.py --profile=WinXPSP3x86 -f memory.raw filescan

root@caine:/local$ vol.py --profile=WinXPSP3x86 -f memory.raw dumpfiles -n -
i -r \\.txt --dump-dir malwareResults/
```

Please answer second part too.

The following files possibly contain artifacts:

- pdf
- jpg
- png
- flv
- doc
- txt
- conf

8. Write a small paragraph of maximum 200 words about your findings. Please remain objective.

Answer: Memory acquisition of a running Windows XP Service Pack 3 OS. It was acquired on 2017-02-12. Although, the malfind plugin reported 4 possible malware infected processes. None of the reported malware were actually infected with malware according to the up to date signatures ClamAV had (freshcalm command to update them). At the time of the acquisition the TOR browser was running. The process of the AVG scanner was also active also with CCleaner. We were unable to gather any cached credentials from the acquisition because the SYSTEM hive wasn't loaded into memory. However, the SAM registry hive was loaded into memory.

2 Disk

9. Read up on Scalpel and its features. Explain what it does and how it works

Answer:

Scalpel is an open source program for recovering deleted data originally based on foremost, although significantly more efficient. it allows an examiner to specify a number of headers and footers to recover filetypes from a piece of media.

To recover deleted files we should -o option to specify directory where recovered files are stored:

Example:

```
caine@caine:~$ scalpel -h
Scalpel version 2.1
Written by Golden G. Richard III and Lodovico Marziale.
Scalpel carves files or data fragments from a disk image based on a set of
file carving patterns, which include headers, footers, and other
information.

Usage: scalpel [-b] [-c <config file>] [-d] [-e] [-h] [-i <file>]
[-n] [-o <outputdir>] [-O] [-p] [-q <clustersize>] [-r]
[-v] [-V] <imgfile> [<imgfile>] ...

Options:
-b  Carve files even if defined footers aren't discovered within
    maximum carve size for file type [foremost 0.69 compat mode].
-c  Choose configuration file.
-d  Generate header/footer database; will bypass certain optimizations
    and discover all footers, so performance suffers.  Doesn't affect
    the set of files carved.  **EXPERIMENTAL**
-e  Do nested header/footer matching, to deal with structured files that may
    contain embedded files of the same type.  Applicable only to
    FORWARD / NEXT patterns.
-h  Print this help message and exit.
-i  Read names of disk images from specified file.  Note that minimal
parsing of
    the pathnames is performed and they should be formatted to be compliant
C
    strings; e.g., under Windows, backslashes must be properly quoted, etc.
-n  Don't add extensions to extracted files.
-o  Set output directory for carved files.
-O  Don't organize carved files by type. Default is to organize carved files
    into subdirectories.
-p  Perform image file preview; audit log indicates which files
    would have been carved, but no files are actually carved.  Useful for
    indexing file or data fragment locations or supporting in-place file
    carving.
-q  Carve only when header is cluster-aligned.
-r  Find only first of overlapping headers/footers [foremost 0.69 compat
mode].
-V  Print copyright information and exit.
-v  Verbose mode.
```

Files are identified by a magic header also footers have unique signature. So Scalpel then carves out

the file from header until footer (included).

10. Inspect the image manually and look for any artifacts. Describe this process completely.

Answer:

```
root@caine:/local# fdisk -lu disk.img
Disk disk.img: 4 GiB, 4294950912 bytes, 8388576 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xc237c237

Device     Boot Start     End Sectors Size Id Type
disk.img1  *       63 8369864 8369802   4G  7 HPFS/NTFS/exFAT
```

The partition starts at block 63 $\Longrightarrow$ $63 * 512 = 32256$ bytes

Now, lets create a folder and mount the image to it:

```
root@caine:/local# mkdir mountFolder
root@caine:/local# sudo mount -o loop,offset=32256 disk.img mountFolder/
The disk contains an unclean file system (0, 0).
The file system wasn't safely closed on Windows. Fixing.
```

Check inside dave user:

```
root@caine:/local/mountFolder/Documents and Settings/dave/My Documents# ls
desktop.ini  Downloads  My Music  My Pictures  torbrowser-install-6.5_en-
US.exe
```

Inside the following path we might find interesting images from his Internet history which contains politics, family, activities and tor images (this implicates something), path:

```
root@caine:/local/mountFolder/Documents and Settings/dave/Local
Settings/Temporary Internet Files/Content.IE5#
```

11. Let Scalpel inspect the disk image. What files are useful for your investigation?

Answer:

I will first reconfigure scalpel in order to looks at the following file types that are useful in this

investigation:

- GRAPHICS FILES
- ANIMATION FILES
- MICROSOFT OFFICE
- HTML
- ADOBE PDF
- PGP (PRETTY GOOD PRIVACY)
- AOL (AMERICA ONLINE)
- SOUND FILES
- WINDOWS REGISTRY FILES
- ZIP
- JAVA
- PINs Password Manager program

I uncommented all of them in the scalpel configuration file.

```
root@caine:/local# nano /etc/scalpel/scalpel.conf
```

Now, execute scalpel:

```
root@caine:/local# scalpel disk.img -o scalpelOutput/ -c
/etc/scalpel/scalpel.conf
disk.img: 100.0% |*********************************************|    4.0 GB
00:00 ETAProcessing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 21883, elapsed  = 192 secs
```

I found a lot of interesting stuff, SSN lab , SNE trip picture <3, a bearded man picture on newspaper shown below, in addition to mailboxes and screen shots done on windows Xp, and so on.

12. Investigate the techniques that have been used to hide files.

Answer:

the techinques used here is by deleting the files (in mind that the files are hidden) however, according to the following article: (https://www.howtogeek.com/125521/htg-explains-why-deleted-files-can-be-recovered-and-how-you-can-prevent-it/)

Windows (and other operating systems) keep track of where files are on a hard drive through “pointers.” Each file and folder on your hard disk has a pointer that tells Windows where the file’s data begins and ends.

When you delete a file, Windows removes the pointer and marks the sectors containing the file's data as available. From the file system's point of view, the file is no longer present on your hard drive and the sectors containing its data are considered free space.

Deleting a file's pointer and marking its space as available is an extremely fast operation. In contrast, actually erasing a file by overwriting its data takes significantly longer. For example, if you're deleting a 10 GB file, that would be near-instantaneous **And possibly (Dave used stenography techniques to do that, but I couldn't investigate more to proof that)**

13. How would you securely hide or delete your information?

Answer:

I would use encryption then Write data to the hidden segments and then hide the data segments in order to securely hide data or i might use stenography techniques also to do that. In order to delete my information I will definitely use anti forensics tools to delete files in addition to temper in the physical storage like random shifting in bits and so on. In that case it will be nearly impossible to recover them.

14. Write a small paragraph of maximum 200 words about your findings. Please remain objective.

Answer:

I noticed that dave is the user of the computer. i found alot of intersting stuff including politics and military in addition to terrorist picture (Osama bin laden) which makes it suspicious. Also a lot of data is also removed from the hard disk. However, I successfully retrieve contained pictures and SSN lab assignments. There were also mailbox files recovered from Microsoft Outlook Express.

15. Did you find any traps that were interfering with your work?

Answer:

I didn't interfered any traps. By using the proper tools the operation was quite smooth.

3 Combining

16. Create a timeline of the evidence and explain what

happened. Include both the memory and the disk forensics. Use a maximum of 400 words

Answer:

```
root@caine:/local# log2timeline.py timeline.plaso disk.img
```

According to user dave cached Internet: Google was used to search for gratis antivirus, microsoft antivirus, and CCleaner. He used the search engine Bing to search for TOR

In the memory: at the time of the acquisition I found that the follwing application were used (CCleaner, AVG and TOR) which are related to the internet cached searches.

Based on CLAMAV there wasn't any malware active at the time of the memory acquisition. I used VirusTotal also to detect possible malware. However, the timeline didn't contains any possible malware.

Finally, recovering two MBOX. Which are used as email store in Microsoft Outlook Express