```
(gdb) b *0x7c00
Breakpoint 1 at 0x7c00
(gdb) c
Continuing.
[   0:7c00] => 0x7c00:  cli
```

Starting of Bootloader as bootasm.S

```
Thread 1 hit Breakpoint 1, 0x00007c00 in ?? ()
(gdb) b *0x7d3b
Breakpoint 2 at 0x7d3b
(gdb) c
Continuing.
The target architecture is assumed to be i386
```

Bootmain.c

```
=> 0x7d3b:  push   %ebp

Thread 1 hit Breakpoint 2, 0x00007d3b in ?? ()
(gdb) b *0x7d55
Breakpoint 3 at 0x7d55
(gdb) b *0x7c90
Breakpoint 4 at 0x7c90
(gdb) c
Continuing.
=> 0x7c90:  push   %ebp
```

readsect

```
Thread 1 hit Breakpoint 4, 0x00007c90 in ?? ()
(gdb) si
=> 0x7c91:  mov    %esp,%ebp
0x00007c91 in ?? ()
(gdb)
=> 0x7c93:  push   %edi
0x00007c93 in ?? ()
(gdb)
=> 0x7c94:  push   %ebx
0x00007c94 in ?? ()
(gdb)
=> 0x7c95:  mov    0xc(%ebp),%ebx
0x00007c95 in ?? ()
(gdb)
=> 0x7c98:  call   0x7c7e                                  // waitdisk();
```

```
0x00007c98 in ?? ()
(gdb)
```

waitdisk

```
=> 0x7c7e:  push   %ebp
0x00007c7e in ?? ()
(gdb)
=> 0x7c7f:  mov    %esp,%ebp
0x00007c7f in ?? ()
(gdb)
=> 0x7c81:  mov    $0x1f7,%edx
0x00007c81 in ?? ()
(gdb)
=> 0x7c86:  in     (%dx),%al
0x00007c86 in ?? ()
(gdb)
=> 0x7c87:  and    $0xffffffc0,%eax
0x00007c87 in ?? ()
(gdb)
=> 0x7c8a:  cmp    $0x40,%al
0x00007c8a in ?? ()
(gdb)
=> 0x7c8c:  jne    0x7c86
0x00007c8c in ?? ()
(gdb)
=> 0x7c8e:  pop    %ebp
0x00007c8e in ?? ()
(gdb)
=> 0x7c8f:  ret
0x00007c8f in ?? ()
(gdb)
```

Out of waitdisk. Again in readsect

```
=> 0x7c9d:  mov    $0x1,%eax
0x00007c9d in ?? ()
(gdb)
=> 0x7ca2:  mov    $0x1f2,%edx
0x00007ca2 in ?? ()
(gdb)
=> 0x7ca7:  out    %al,(%dx)                      // outb(0x1F2, 1);
0x00007ca7 in ?? ()
(gdb)
=> 0x7ca8:  mov    $0x1f3,%edx
0x00007ca8 in ?? ()
(gdb)
=> 0x7cad:  mov    %ebx,%eax
```

```
0x00007cad in ?? ()
(gdb)
=> 0x7caf:  out    %al,(%dx)                      // outb(0x1F3, offset);
0x00007caf in ?? ()
(gdb)
=> 0x7cb0:  mov    %ebx,%eax
0x00007cb0 in ?? ()
(gdb)
=> 0x7cb2:  shr    $0x8,%eax
0x00007cb2 in ?? ()
(gdb)
=> 0x7cb5:  mov    $0x1f4,%edx
0x00007cb5 in ?? ()
(gdb)
=> 0x7cba:  out    %al,(%dx)                      // outb(0x1F4, offset >> 8);
0x00007cba in ?? ()
(gdb)
=> 0x7cbb:  mov    %ebx,%eax
0x00007cbb in ?? ()
(gdb)
=> 0x7cbd:  shr    $0x10,%eax
0x00007cbd in ?? ()
(gdb)
=> 0x7cc0:  mov    $0x1f5,%edx
0x00007cc0 in ?? ()
(gdb)
=> 0x7cc5:  out    %al,(%dx)                      // outb(0x1F5, offset >> 16);
0x00007cc5 in ?? ()
(gdb)
=> 0x7cc6:  mov    %ebx,%eax
0x00007cc6 in ?? ()
(gdb)
=> 0x7cc8:  shr    $0x18,%eax
0x00007cc8 in ?? ()
(gdb)
=> 0x7ccb:  or     $0xffffffe0,%eax
0x00007ccb in ?? ()
(gdb)
=> 0x7cce:  mov    $0x1f6,%edx
0x00007cce in ?? ()
(gdb)
=> 0x7cd3:  out    %al,(%dx)
0x00007cd3 in ?? ()
(gdb)
=> 0x7cd4:  mov    $0x20,%eax
0x00007cd4 in ?? ()
(gdb)
=> 0x7cd9:  mov    $0x1f7,%edx
0x00007cd9 in ?? ()
```

```
(gdb)
=> 0x7cde:  out    %al,(%dx)                       // outb(0x1F6, (offset >> 24)
| 0xE0);
0x00007cde in ?? ()
(gdb)
=> 0x7cdf:  call   0x7c7e                          // waitdisk()
0x00007cdf in ?? ()
(gdb)
=> 0x7c7e:  push   %ebp
0x00007c7e in ?? ()
(gdb)
=> 0x7c7f:  mov    %esp,%ebp
0x00007c7f in ?? ()
(gdb)
=> 0x7c81:  mov    $0x1f7,%edx
0x00007c81 in ?? ()
(gdb)
=> 0x7c86:  in     (%dx),%al
0x00007c86 in ?? ()
(gdb)
=> 0x7c87:  and    $0xffffffc0,%eax
0x00007c87 in ?? ()
(gdb)
=> 0x7c8a:  cmp    $0x40,%al
0x00007c8a in ?? ()
(gdb)
=> 0x7c8c:  jne    0x7c86
0x00007c8c in ?? ()
(gdb)
=> 0x7c8e:  pop    %ebp
0x00007c8e in ?? ()
(gdb)
=> 0x7c8f:  ret
0x00007c8f in ?? ()
(gdb)
=> 0x7ce4:  mov    0x8(%ebp),%edi
0x00007ce4 in ?? ()
(gdb)
=> 0x7ce7:  mov    $0x80,%ecx
0x00007ce7 in ?? ()
(gdb)
=> 0x7cec:  mov    $0x1f0,%edx
0x00007cec in ?? ()
(gdb)
=> 0x7cf1:  cld
0x00007cf1 in ?? ()
(gdb)
=> 0x7cf2:  rep insl (%dx),%es:(%edi)                  // insl(0x1F0, dst,
SECTSIZE/4);
```

```
0x00007cf2 in ?? ()
(gdb)
=> 0x7cf2:  rep insl (%dx),%es:(%edi)
0x00007cf2 in ?? ()
(gdb)
=> 0x7cf2:  rep insl (%dx),%es:(%edi)
0x00007cf2 in ?? ()
(gdb)
.
.                                                      // multiple rep insl
instructions
.
=> 0x7cf2:  rep insl (%dx),%es:(%edi)
0x00007cf2 in ?? ()
(gdb)
=> 0x7cf2:  rep insl (%dx),%es:(%edi)
0x00007cf2 in ?? ()
(gdb)
=> 0x7cf4:  pop    %ebx
0x00007cf4 in ?? ()
(gdb)
=> 0x7cf5:  pop    %edi
0x00007cf5 in ?? ()
(gdb)
=> 0x7cf6:  pop    %ebp
0x00007cf6 in ?? ()
(gdb)
=> 0x7cf7:  ret
0x00007cf7 in ?? ()
(gdb)
```

Out of readsect. Now in readseg

```
=> 0x7d23:  add    $0x200,%ebx
0x00007d23 in ?? ()
(gdb)
=> 0x7d29:  add    $0x1,%esi
0x00007d29 in ?? ()
(gdb)
=> 0x7d2c:  add    $0x8,%esp
0x00007d2c in ?? ()
(gdb)
=> 0x7d2f:  cmp    %ebx,%edi
0x00007d2f in ?? ()
(gdb)
=> 0x7d31:  ja     0x7d1c
0x00007d31 in ?? ()
(gdb)
```

```
=> 0x7d1c:  push   %esi
0x00007d1c in ?? ()
(gdb)
=> 0x7d1d:  push   %ebx
0x00007d1d in ?? ()
(gdb)
=> 0x7d1e:  call   0x7c90
0x00007d1e in ?? ()
(gdb)
=> 0x7c90:  push   %ebp

Thread 1 hit Breakpoint 4, 0x00007c90 in ?? ()
(gdb)
=> 0x7c91:  mov    %esp,%ebp
0x00007c91 in ?? ()
(gdb)
=> 0x7c93:  push   %edi
0x00007c93 in ?? ()
(gdb)
=> 0x7c94:  push   %ebx
0x00007c94 in ?? ()
(gdb)
=> 0x7c95:  mov    0xc(%ebp),%ebx
0x00007c95 in ?? ()
(gdb)
=> 0x7c98:  call   0x7c7e
0x00007c98 in ?? ()
(gdb) c
Continuing.
=> 0x7c90:  push   %ebp
```

Stepping over remaining readsect calls

```
Thread 1 hit Breakpoint 4, 0x00007c90 in ?? ()
(gdb) c
Continuing.
=> 0x7c90:  push   %ebp

Thread 1 hit Breakpoint 4, 0x00007c90 in ?? ()
(gdb) c
Continuing.
=> 0x7c90:  push   %ebp

Thread 1 hit Breakpoint 4, 0x00007c90 in ?? ()
(gdb) c
Continuing.
=> 0x7c90:  push   %ebp
```

```
Thread 1 hit Breakpoint 4, 0x00007c90 in ?? ()
(gdb) c
Continuing.
=> 0x7c90:  push   %ebp

Thread 1 hit Breakpoint 4, 0x00007c90 in ?? ()
(gdb) c
Continuing.
=> 0x7c90:  push   %ebp

Thread 1 hit Breakpoint 4, 0x00007c90 in ?? ()
(gdb) c
Continuing.
=> 0x7d55:  add    $0xc,%esp
```

Back to bootmain

```
Thread 1 hit Breakpoint 3, 0x00007d55 in ?? ()
(gdb) si
=> 0x7d58:  cmpl   $0x464c457f,0x10000          // Checking magic number
0x00007d58 in ?? ()
(gdb)
=> 0x7d62:  je     0x7d6c
0x00007d62 in ?? ()
(gdb)
=> 0x7d6c:  mov    0x1001c,%eax
0x00007d6c in ?? ()
(gdb)
=> 0x7d71:  lea    0x10000(%eax),%ebx
0x00007d71 in ?? ()
(gdb)
=> 0x7d77:  movzwl 0x1002c,%esi
0x00007d77 in ?? ()
(gdb)
=> 0x7d7e:  shl    $0x5,%esi
0x00007d7e in ?? ()
(gdb)
=> 0x7d81:  add    %ebx,%esi
0x00007d81 in ?? ()
(gdb)
```

Starting of loop which reads kernel segments

```
=> 0x7d83:  cmp    %esi,%ebx
0x00007d83 in ?? ()
(gdb) b *0x7d8f
Breakpoint 5 at 0x7d8f
(gdb) b *0x7d94
```

```
Breakpoint 6 at 0x7d94
(gdb) c
Continuing.
=> 0x7c90:  push   %ebp

Thread 1 hit Breakpoint 4, 0x00007c90 in ?? ()
(gdb) disable 4
(gdb) c
Continuing.
=> 0x7d8f:  add    $0x20,%ebx

Thread 1 hit Breakpoint 5, 0x00007d8f in ?? ()
(gdb) c
Continuing.
=> 0x7d94:  jbe    0x7d87

Thread 1 hit Breakpoint 6, 0x00007d94 in ?? ()
(gdb) c
Continuing.
=> 0x7d8f:  add    $0x20,%ebx

Thread 1 hit Breakpoint 5, 0x00007d8f in ?? ()
(gdb)
Continuing.
=> 0x7d94:  jbe    0x7d87

Thread 1 hit Breakpoint 6, 0x00007d94 in ?? ()
(gdb)
Continuing.
=> 0x7d8f:  add    $0x20,%ebx

Thread 1 hit Breakpoint 5, 0x00007d8f in ?? ()
(gdb)
Continuing.
=> 0x7d94:  jbe    0x7d87

Thread 1 hit Breakpoint 6, 0x00007d94 in ?? ()
(gdb) si
```

End of Loop

```
=> 0x7d87:  call   *0x10018                     // Calling entry function of kernel
0x00007d87 in ?? ()
(gdb)
```

Now in kernel

```
=> 0x10000c:  mov    %cr4,%eax
0x0010000c in ?? ()
(gdb)
=> 0x10000f:  or     $0x10,%eax
0x0010000f in ?? ()
(gdb)
=> 0x100012:  mov    %eax,%cr4
0x00100012 in ?? ()
(gdb)
=> 0x100015:  mov    $0x109000,%eax
0x00100015 in ?? ()
(gdb)
=> 0x10001a:  mov    %eax,%cr3
0x0010001a in ?? ()
(gdb)
=> 0x10001d:  mov    %cr0,%eax
0x0010001d in ?? ()
(gdb)
=> 0x100020:  or     $0x80010000,%eax
0x00100020 in ?? ()
(gdb)
=> 0x100025:  mov    %eax,%cr0
0x00100025 in ?? ()
(gdb)
=> 0x100028:  mov    $0x8010b5c0,%esp
0x00100028 in ?? ()
(gdb)
=> 0x10002d:  mov    $0x80102ea0,%eax
0x0010002d in ?? ()
```