Introduction

- **Explores the capabilities of custom boot sector code on NT-family Windows**
  - What can it do? Anything – it's privileged code on the CPU
  - The trick is keeping control while allowing the OS to function
- **Overview**
  - BIOS boot process and Windows startup
  - eEye BootRoot: how it works, capabilities and shortcomings
  - Demo: eEye BootRootKit backdoor
- **Required Knowledge**
  - x86 real and protected modes, some Windows kernel

Booting Up

BIOS Handoff to Bootstrap Code

Booting Up – Summary

- **BIOS transfers execution to code from some other medium**
  - Disk drive (fixed or removable)
  - CD-ROM
  - Network boot
- **Windows startup from a hard drive installation**
  - Hard drive Master Boot Record
  - Windows bootstrap loader
  - NTLDR
  - OSLOADER.EXE
  - NTDETECT.COM
  - NTOSKRNL.EXE, HAL.DLL, boot drivers

Booting Up – Disk Drive

- **BIOS loads first sector of drive (200h bytes) at 0000h:7C00h**
  - Executes in real mode
  - SS:SP < 0000h:0400h, DS = 0040h (BIOS data area)
- **For hard drives, the first sector is the Master Boot Record**
  - Copies itself to 0000h:0600h
  - Locates a bootable partition in the partition table
  - Executes the first sector of the boot partition at 0000h:7C00h
- **Partition boot sector is always part of the operating system**
  - Loads and executes the next boot stage of the OS

Booting Up – MBR Partition Table

Master Boot Record Layout

- Partition 1 (offset 01BEh)
- Partition 2 (offset 01CEh)
- Partition 3 (offset 01DEh)
- Partition 4 (offset 01EEh)

Partition Table Entry Format

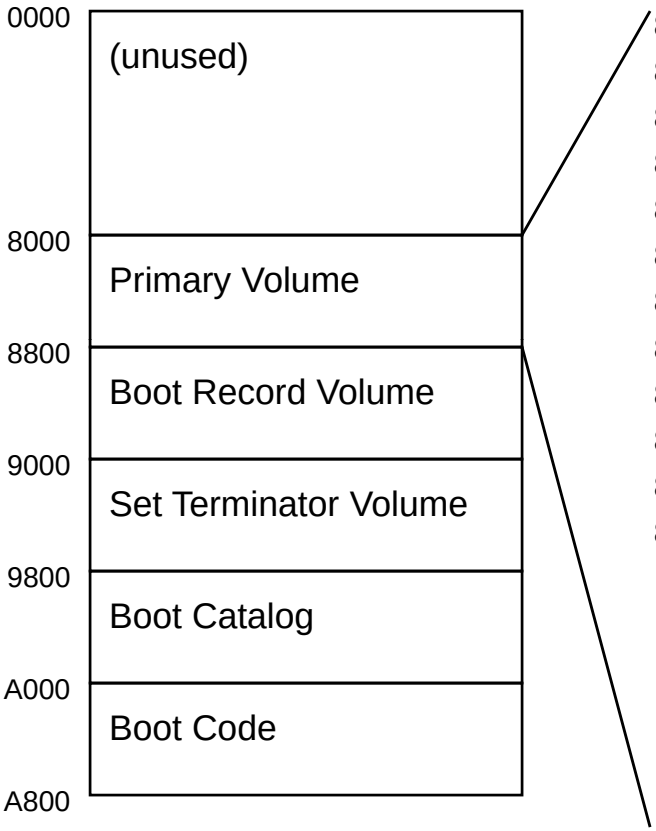
```
+00  BYTE    Boot Indicator
              -- bit 7: partition bootable
+01  BYTE    Starting Head
+02  BYTE    Starting Sector / Cylinder
              -- bits 5..0: sector
              -- bits 7..6: cylinder (bits 9..8)
+03  BYTE    Starting Cylinder (bits 7..0)
+04  BYTE    System ID (volume type)
+05  BYTE    Ending Head
+06  BYTE    Ending Sector / Cylinder
              -- bits 5..0: sector
              -- bits 7..6: cylinder (bits 9..8)
+07  BYTE    Ending Cylinder (bits 7..0)
+08  DWORD   Linear sector number of partition
+0C  DWORD   Size in sectors of partition
```

Source: *NTFS.com Hard Drive Partition - Partition Table.*
http://www.ntfs.com/partition-table.htm

Booting Up – CD-ROM

- **Differences from disks and diskettes**
  - Sector size is 800h bytes (2KB)
  - Data format is more complicated (ECMA-119 / ISO 9660)
  - Bootable CD format dictated by “El Torito” Specification
- **Boot sector (only first 200h bytes) loads at 07C0h:0000h**
  - Executes in real mode
  - SS:SP = 0000h:0400h, DS = 0040h (BIOS data area)
- **Additional disc contents are accessed via INT 13h**
  - Boot catalog entry indicates “emulation mode” (floppy or HD)

Booting Up – Bootable CD Layout (1)

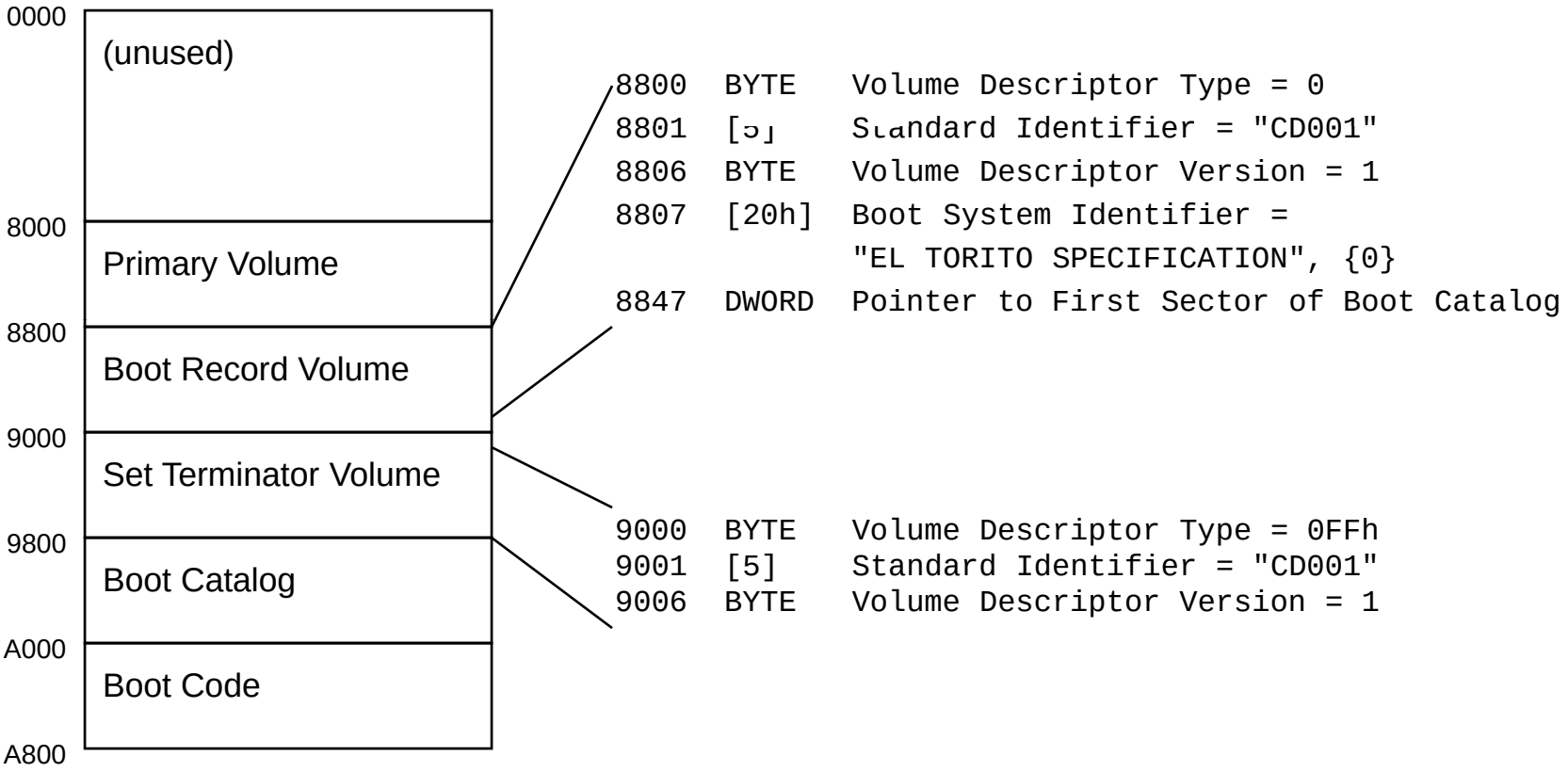



```
8000  BYTE   Volume Descriptor Type = 1
8001  [5]    Standard Identifier = "CD001"
8006  BYTE   Volume Descriptor Version = 1
8050  DWORD  Volume Space Size (sectors) = 15h
8054  DWORD  Volume Space Size (big-endian)
8078  WORD   Volume Set Size = 1
807A  WORD   Volume Set Size (big-endian)
807C  WORD   Volume Sequence Number = 1
807E  WORD   Volume Sequence Number (big-endian)
8080  WORD   Logical Block Size = 0800h
8082  WORD   Logical Block Size (big-endian)
809C  ¸22h¸  Director¸ Record for Root Director¸
  809C  BYTE   Length of Directory Record = 1
  80B5  BYTE   File Flags = 02h (Directory)
  80B8  WORD   Volume Sequence Number = 1
  80BA  WORD   Volume Sequence Number (big-endian)
  80BB  BYTE   Length of File Identifier = 1
  80BC  [1]    File Identifier = {0}
```

Source: *ECMA-119: Volume and File Structure of CDROM for Information Interchange*.
`http://www.ecma-international.org/publications/files/ECMA-ST/Ecma-119.pdf`

Source: *"El Torito" Bootable CD-ROM Format Specification, Version 1.0*.
`http://www.phoenix.com/NR/rdonlyres/98D3219C-9CC9-4DF5-B496-A286D893E36A/0/specscdrom.pdf`

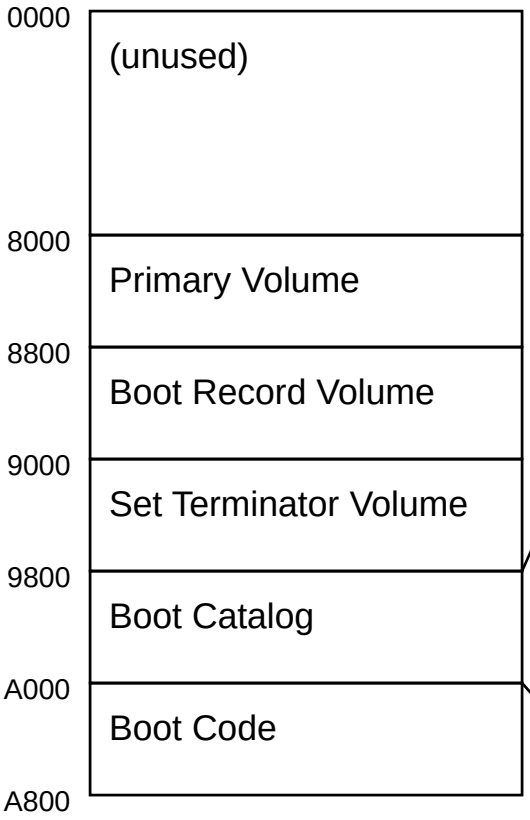
Booting Up – Bootable CD Layout (2)



Source: *ECMA-119: Volume and File Structure of CDROM for Information Interchange*.
`http://www.ecma-international.org/publications/files/ECMA-ST/Ecma-119.pdf`

Source: *"El Torito" Bootable CD-ROM Format Specification, Version 1.0*.
`http://www.phoenix.com/NR/rdonlyres/98D3219C-9CC9-4DF5-B496-A286D893E36A/0/specscdrom.pdf`

Booting Up – Bootable CD Layout (3)




```
9800  [20h]  Validation Entry
  9800  BYTE   Header ID = 1
  9801  BYTE   Platform ID = 0
  981C  WORD   Checksum = 55AAh
  981E  WORD   Key = AA55h
9820  [20h]  Initial/Default Entry
  9820  BYTE   Boot Indicator = 88h
  9821  BYTE   Boot Media Type = 2 (1.44MB floppy)
  9822  WORD   Load Segment = 0
  9824  BYTE   System Type = 0
  9826  WORD   Sector Count (virtual sectors) = 1
  9828  DWORD  Load RBA (sector) = 14h
```

Source: *ECMA-119: Volume and File Structure of CDROM for Information Interchange*.
http://www.ecma-international.org/publications/files/ECMA-ST/Ecma-119.pdf

Source: *"El Torito" Bootable CD-ROM Format Specification, Version 1.0*.
http://www.phoenix.com/NR/rdonlyres/98D3219C-9CC9-4DF5-B496-A286D893E36A/0/specscdrom.pdf