COMPUTER FOUNDATIONS

COMP 597 – Computer Forensics

Data Representation

Data Representation

- Number System:
  - Decimal
  - Binary
  - Hexadecimal

Data Representation

01100010

Data Representation

How do we represent the following decimal number in memory *555*?

Data Representation

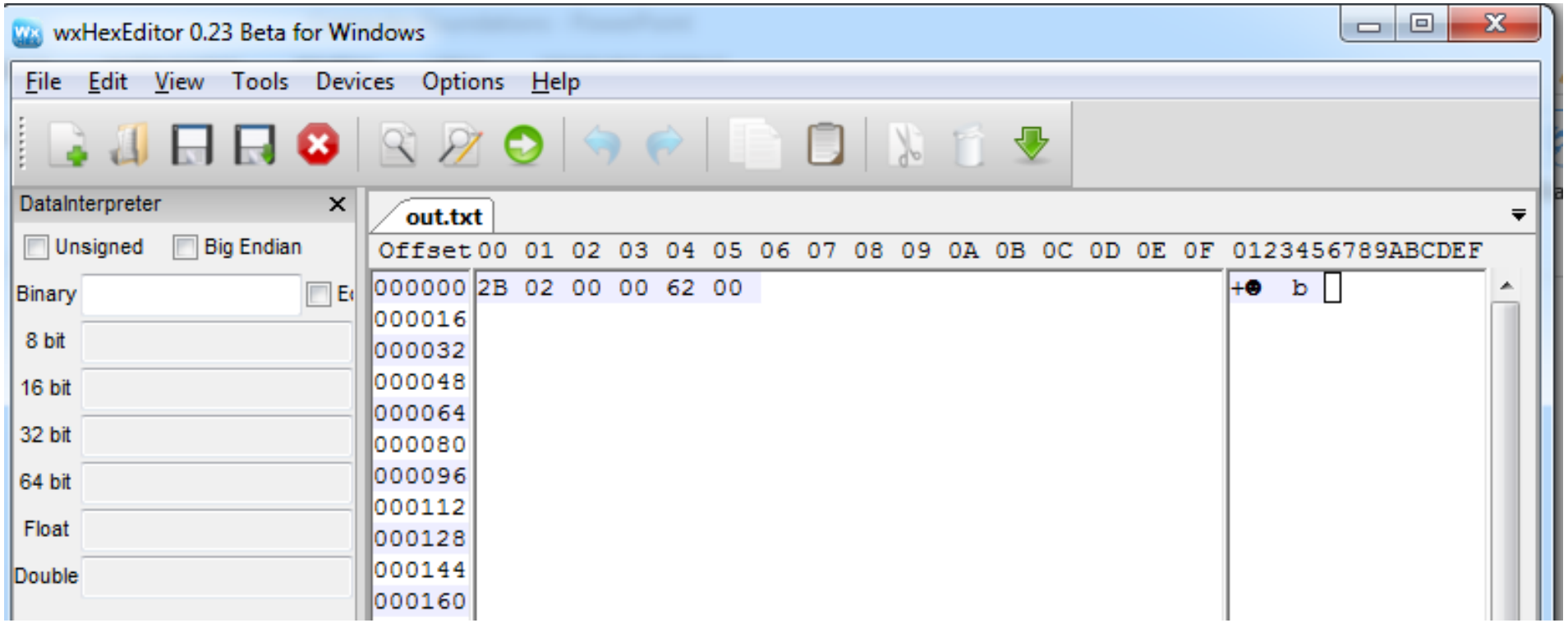
- *big-endian* architecture
- little-*endian* architecture

Data Representation

```
#include <iostream>
#include <fstream>
using namespace std;

int main() {
    ofstream myfile;
    myfile.open("out.txt", ofstream::binary);
    int num1 = 555;
    short num2 = 98;
    myfile.write((const char*)&num1, sizeof(int));
    myfile.write((const char*)&num2, sizeof(short));
    myfile.close();
    return 0;
}
```

wxHexEditor



Data Representation

- How do we represent the following hexadecimal number in memory ?

  0x12345678

Data Representation

- How do we represent a string in memory, for example "5 Market St."?

Data Representation

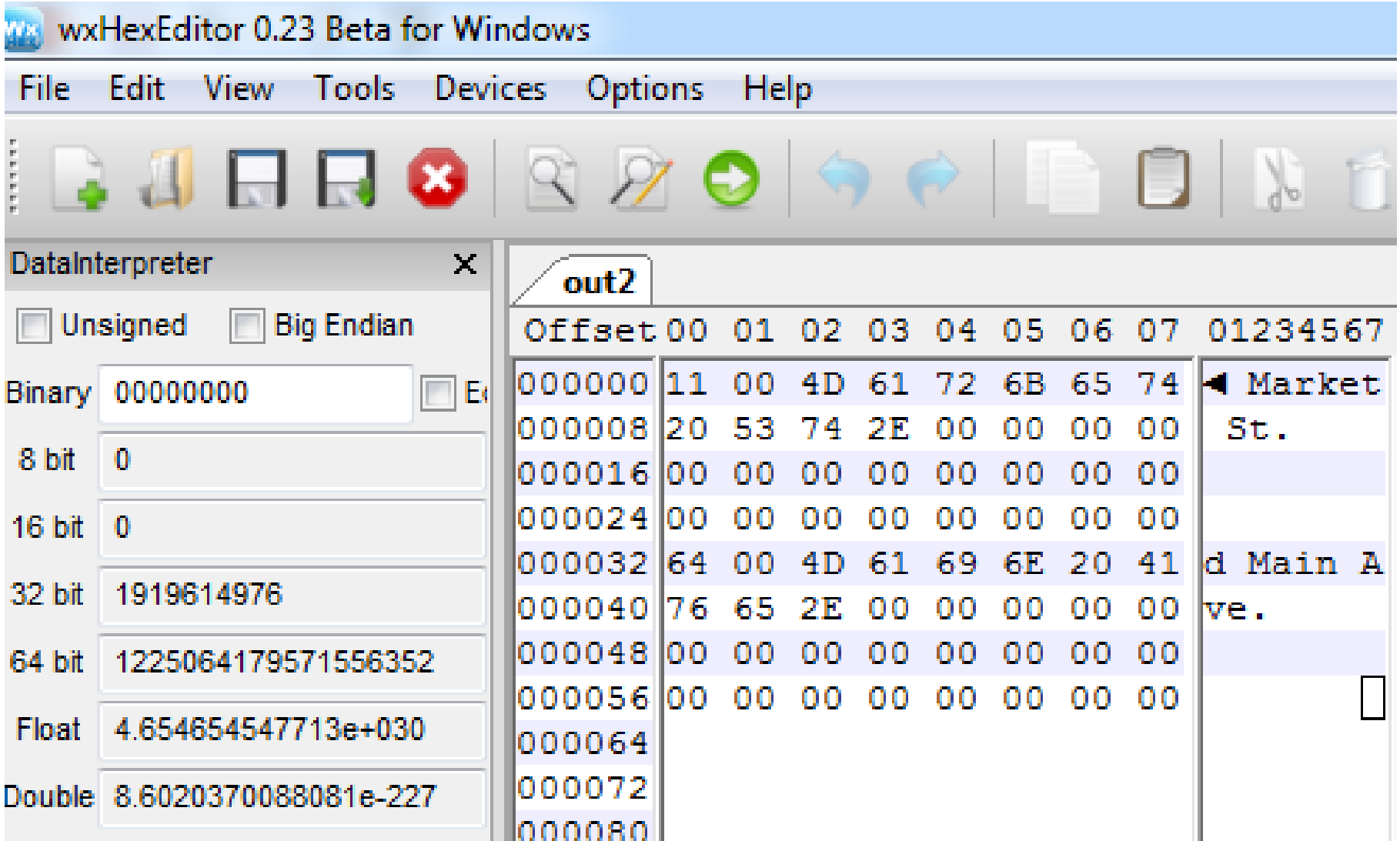
- Data Structures:
  - Are broken up into fields
  - A field has a size and name

Data Structures

- How do we represent the following data structure:

Bytes	Description
2	street number
30	street name

Data Structures



Bit Flags

Bytes	Description
30	Name
1	busy
1	tired
1	hungry
1	studying
1	sleepy
1	Location included
17	Location (optional)

Bit Flags

- How do we represent the following data structure:

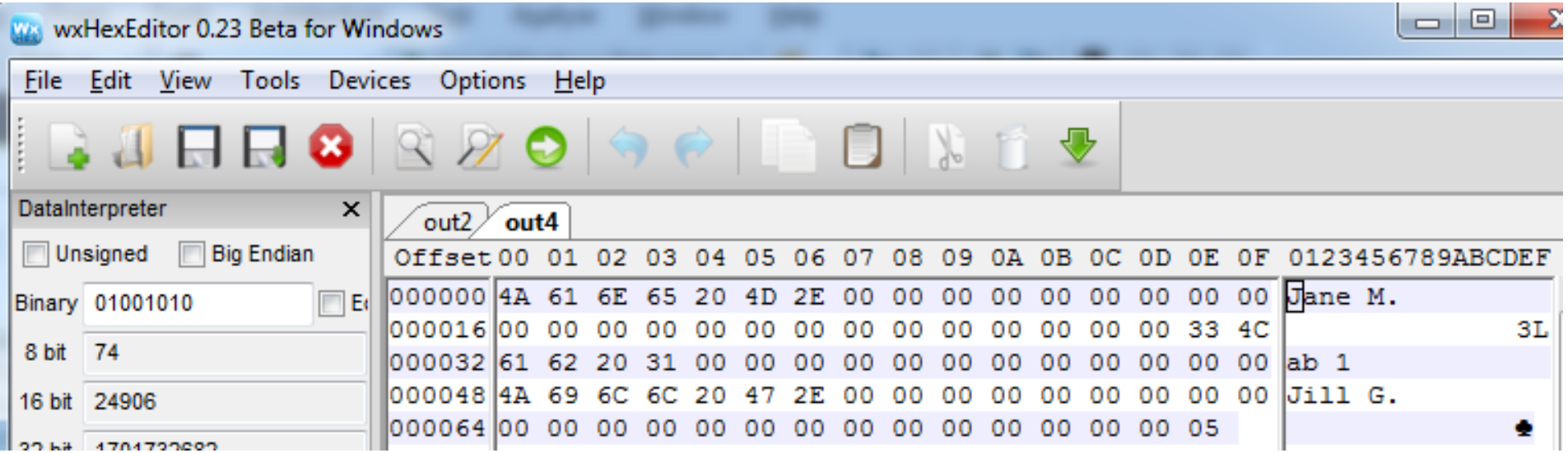
Bytes	Description
30	Name
1	flags
17	Location (optional)

Bit Flags

```
#include <iostream>
using namespace std;
int main()
{
    enum Options {BUSY = 0x01,   // 0000 0001
                  Tired = 0x02,  // 0000 0010
                  HUNGRY = 0x04, // 0000 0100
                  STUDY = 0x08,  // 0000 1000
                  SLEEPY = 0x10, // 0001 0000
                  LOC = 0x20, }; // 0010 0000
    // In C++11, we can use "uint8_t" instead of "unsigned char"
    unsigned char me = 0; // sleeping state
    me |= HUNGRY | SLEEPY | STUDY;
    me ^= HUNGRY;   // no longer hungry

    cout << "Am I Busy? " << (bool)(me & BUSY) << endl;
    cout << "Am I Sleepy? " << (bool)(me & SLEEPY) << endl;
    cout << "Am I Hungry? " << (bool)(me & HUNGRY) << endl;
    cout << "Am I Studying ? " << (bool)(me & STUDY) << endl;
    return 0;
}
```

Bit Flags


wxHexEditor 0.23 Beta for Windows
File Edit View Tools Devices Options Help
DataInterpreter
Unsigned
Big Endian
Binary 01001010
8 bit 74
16 bit 24906
out2
out4
Offset 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 0123456789ABCDEF
000000 4A 61 6E 65 20 4D 2E 00 00 00 00 00 00 00 00 00 Jane M.
000016 00 00 00 00 00 00 00 00 00 00 00 00 00 00 33 4C 3L
000032 61 62 20 31 00 00 00 00 00 00 00 00 00 00 00 00 ab 1
000048 4A 69 6C 6C 20 47 2E 00 00 00 00 00 00 00 00 00 Jill G.
000064 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 05

Boot Process

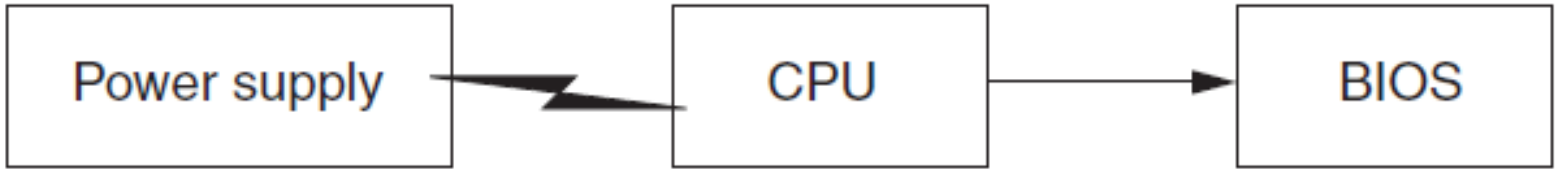
Boot Process

1. CPU Reset
2. POST process
3. Disk boot

BIOS

- Firmware
- A collection of programs

CPU Reset



From: Digital Evidence and Computer Crime 3rd edition, Eoghan Casey

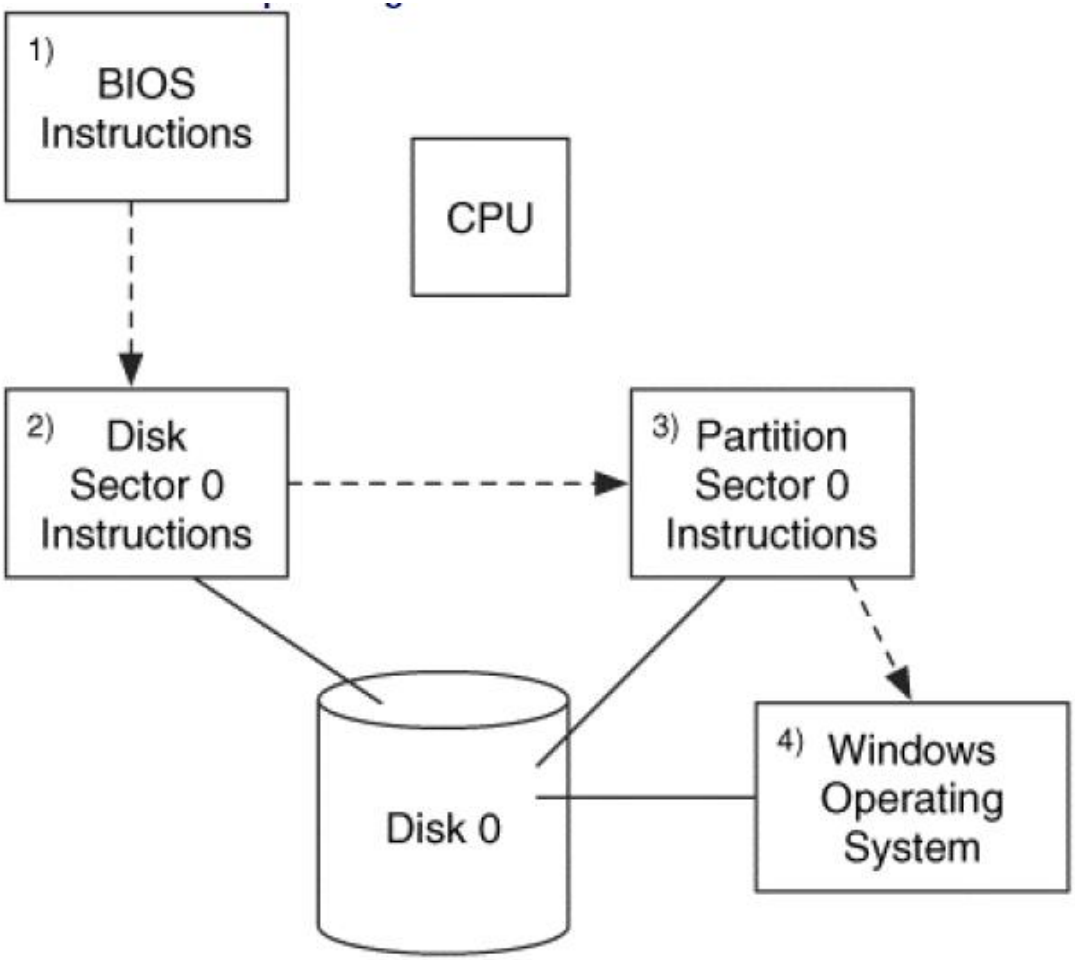
POST

- Verification
- Hardware test
- Error reporting

Disk Boot

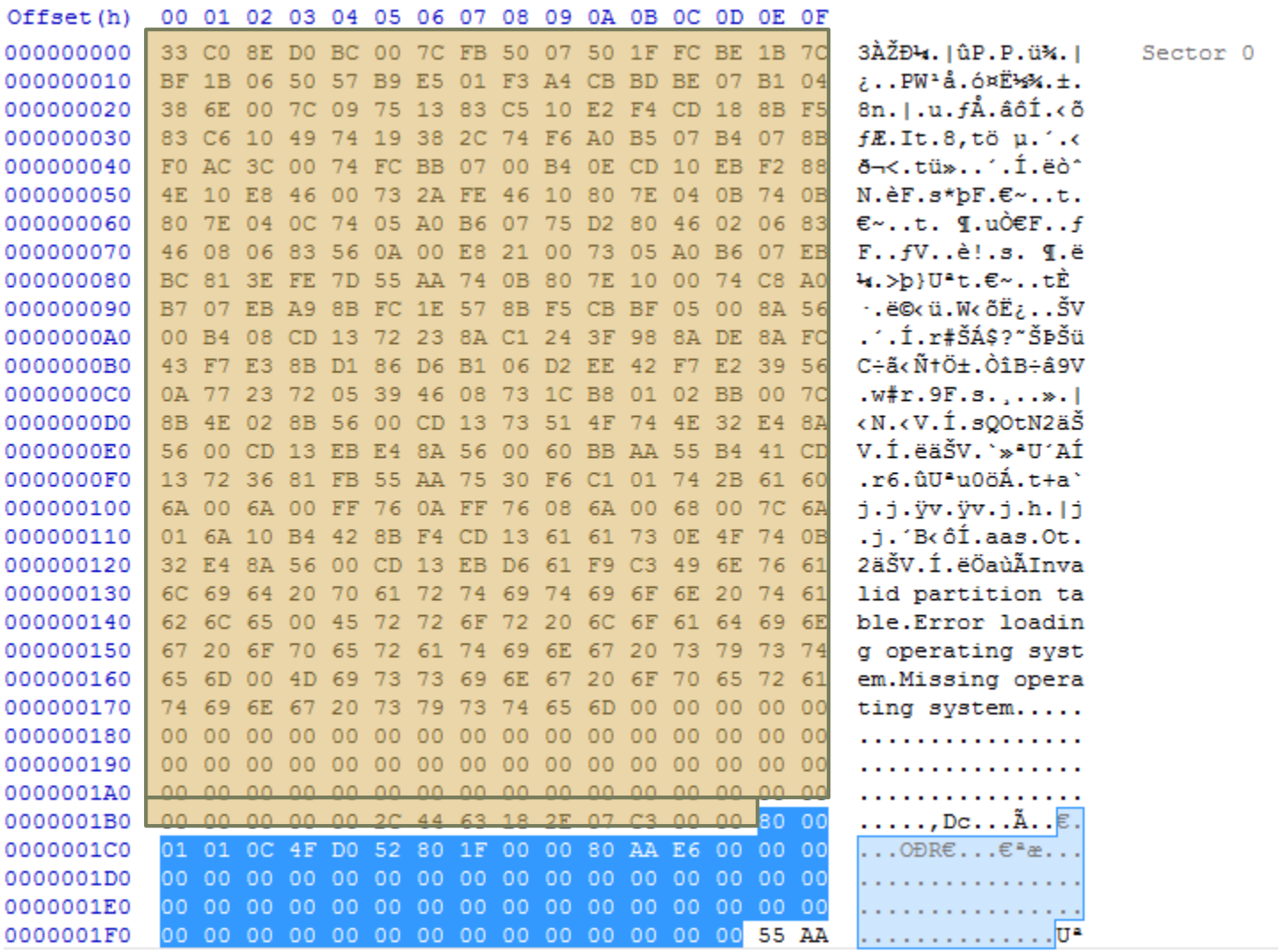
1. Boot sequence governed by BIOS
2. Control passes to the MBR
3. MBR points to boot record
4. Operating system gets loaded

Disk Boot



File System Forensic Analysis, 2nd edition, Brian Carrier

Disk Boot - MBR

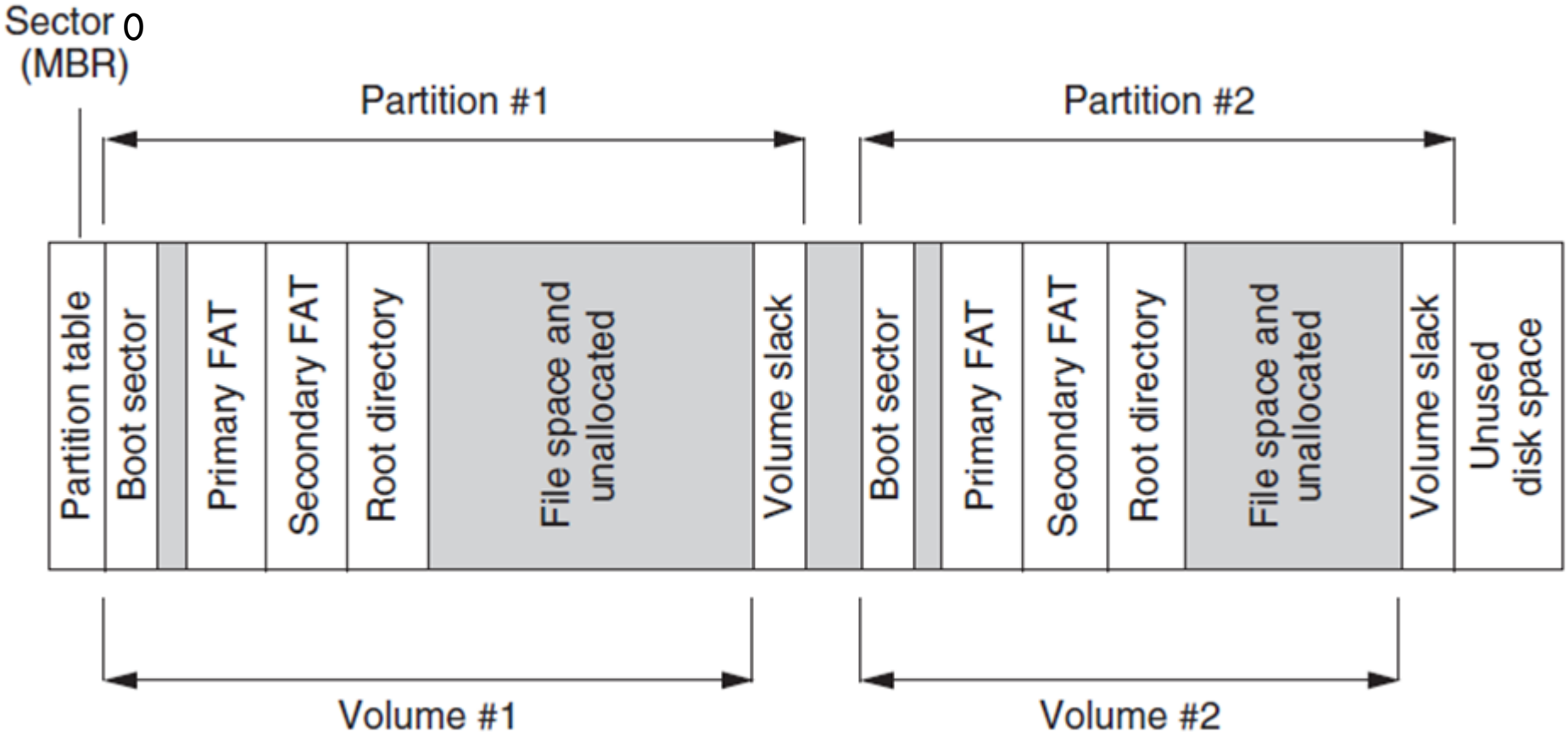


Disk Boot – Partition Table

Structure of a *16-byte* Partition Table Entry		
Relative Offsets (*within entry*)	**Length (*bytes*)**	**Contents**
0	**1**	**Boot Indicator (80h = *active*)**
1 – 3	**3**	**Starting CHS values**
4	**1**	***Partition-type* Descriptor**
5 – 7	**3**	**Ending CHS values**
8 – 11	**4**	**Starting Sector**
12 – 15	**4**	**Partition Size (in sectors)**

From: http://thestarman.pcministry.com/asm/mbr/PartTables.htm

Disk Boot - Disk Partition



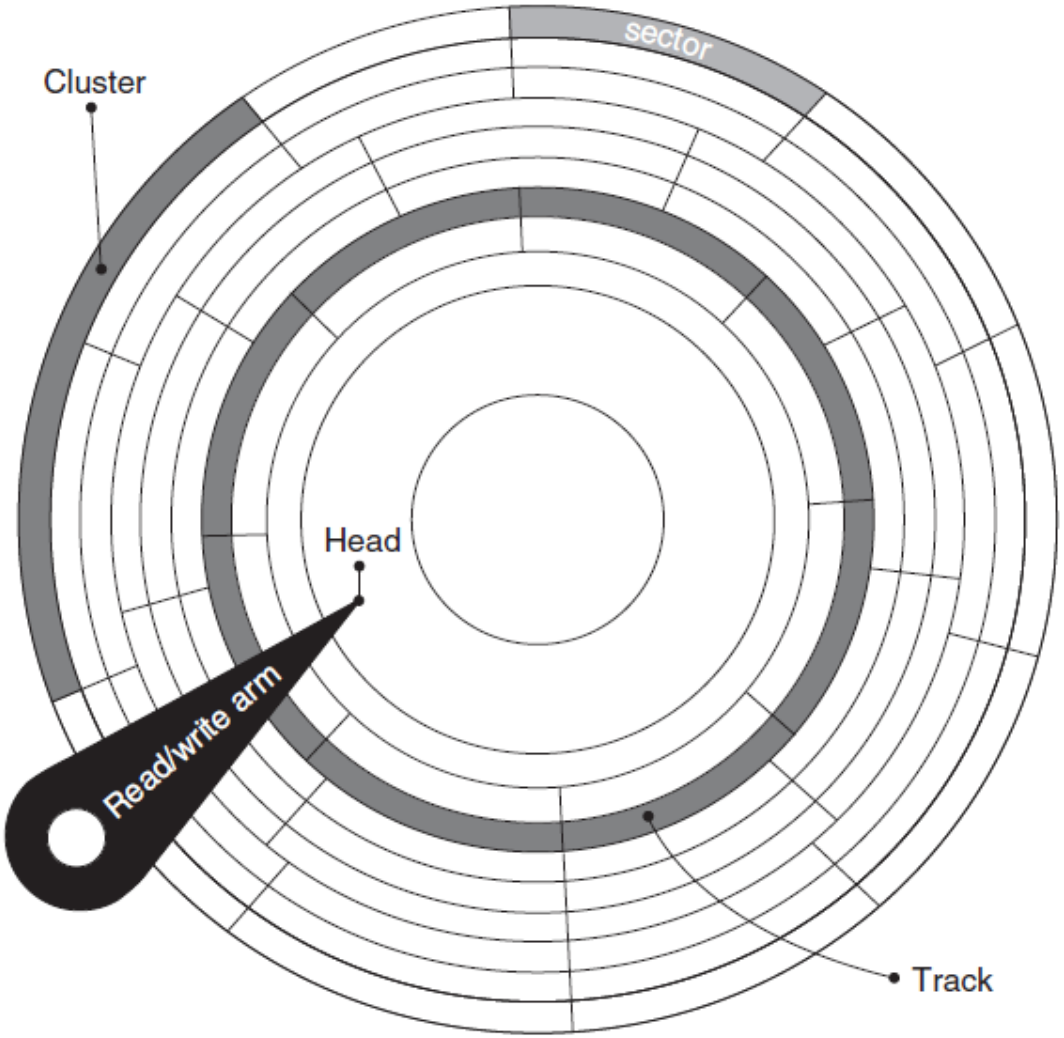
From: Digital Evidence and Computer Crime 3rd edition, Eoghan Casey

Hard Disk

Hard Disk

- Platters
- Track
- Cylinder
- Sector
- Cluster

Hard Disk - CHS addressing



From: Digital Evidence and Computer Crime 3rd edition, Eoghan Casey

Logical Block Addresses

LBA = (((C * hpc) + H) * spt) + S – 1

Where:

- hpc: heads per cylinder
- spt: sectors per track

Logical Block Addresses

- Suppose we have a hard disk with:
  - 16 heads
  - 63 sectors per track
- What is the LBA for a CHS address = 2, 3, 4?

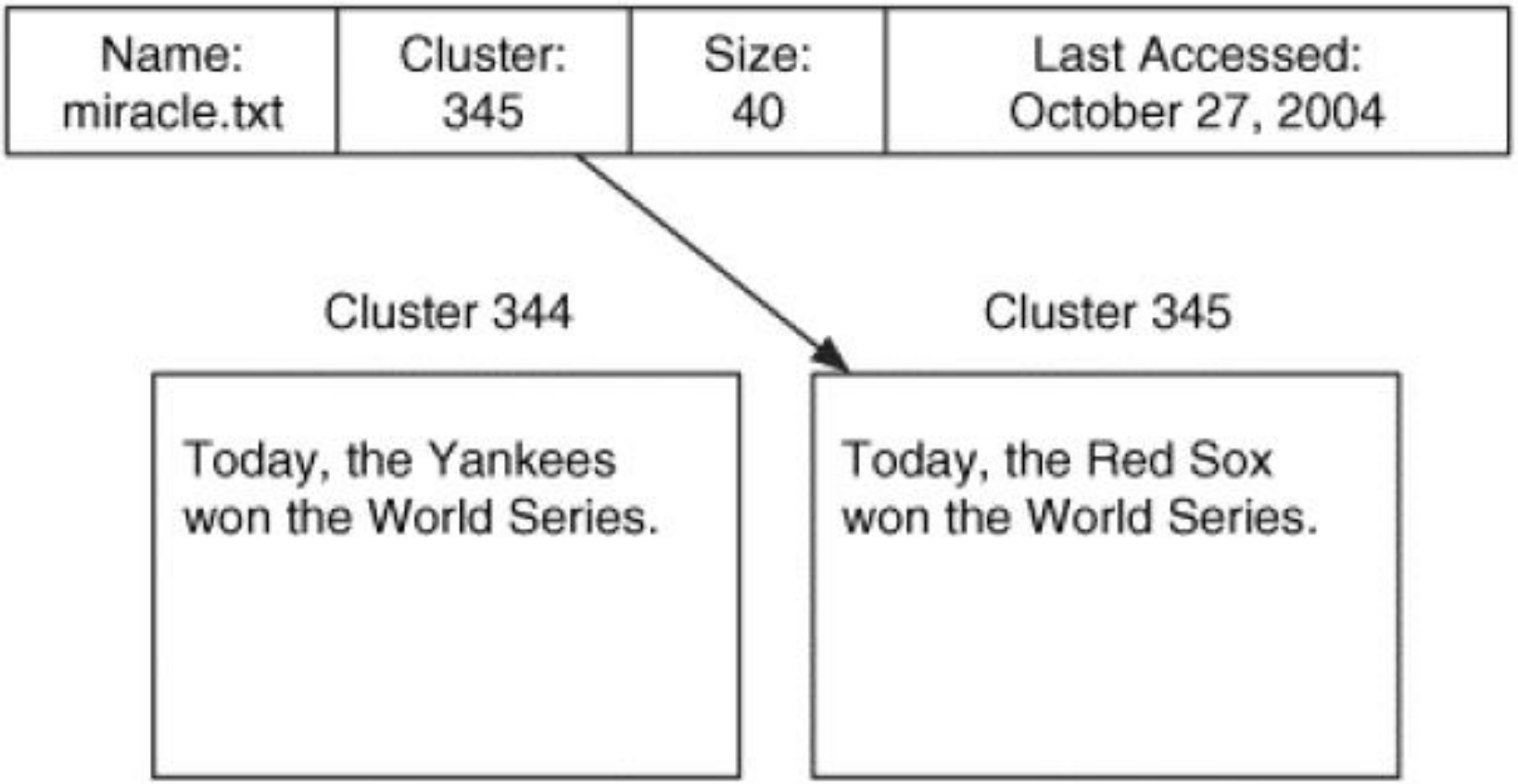
Cluster

File System	Cluster Min/Max
FAT12	512B/2KB
FAT16	2KB/32KB
FAT32	2KB/32KB
NTFS 1.1	512B/8KB
NTFS 3.0	512B/64KB

File Systems

- What is a file system?

File Systems



File System Forensic Analysis, 2nd edition, Brian Carrier

Self-Monitoring, Analysis, and Reporting Technology (smartmontools)

```
ID# ATTRIBUTE_NAME          FLAG     VALUE WORST THRESH TYPE      UPDATED  WHEN_FAILED RAW_VALUE
  9 Power_On_Hours          0x0032   099   099   ---    Old_age   Always       -       1482
 12 Power_Cycle_Count       0x0032   100   100   ---    Old_age   Always       -       1657
```

References

1. File System Forensic Analysis, 2nd edition, Brian Carrier, 2005.
2. Digital Evidence and Computer Crime, 3rd edition, Eoghan Casey, 2011.
3. Digital Archaeology: The Art and Science of Digital Forensics, Michael W Graves, 2013