# INFO 310

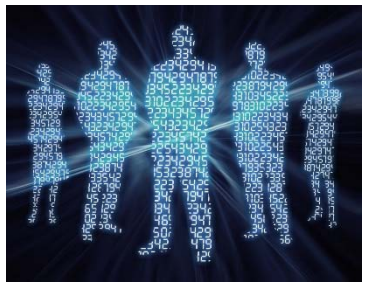
Fall 2016

# Week 11 – Lecture 1

# HOUSEKEEPING

- Attendance
- Position Paper II turn-in

# Computer Forensics



- The application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law.

- The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

# Why Forensics?

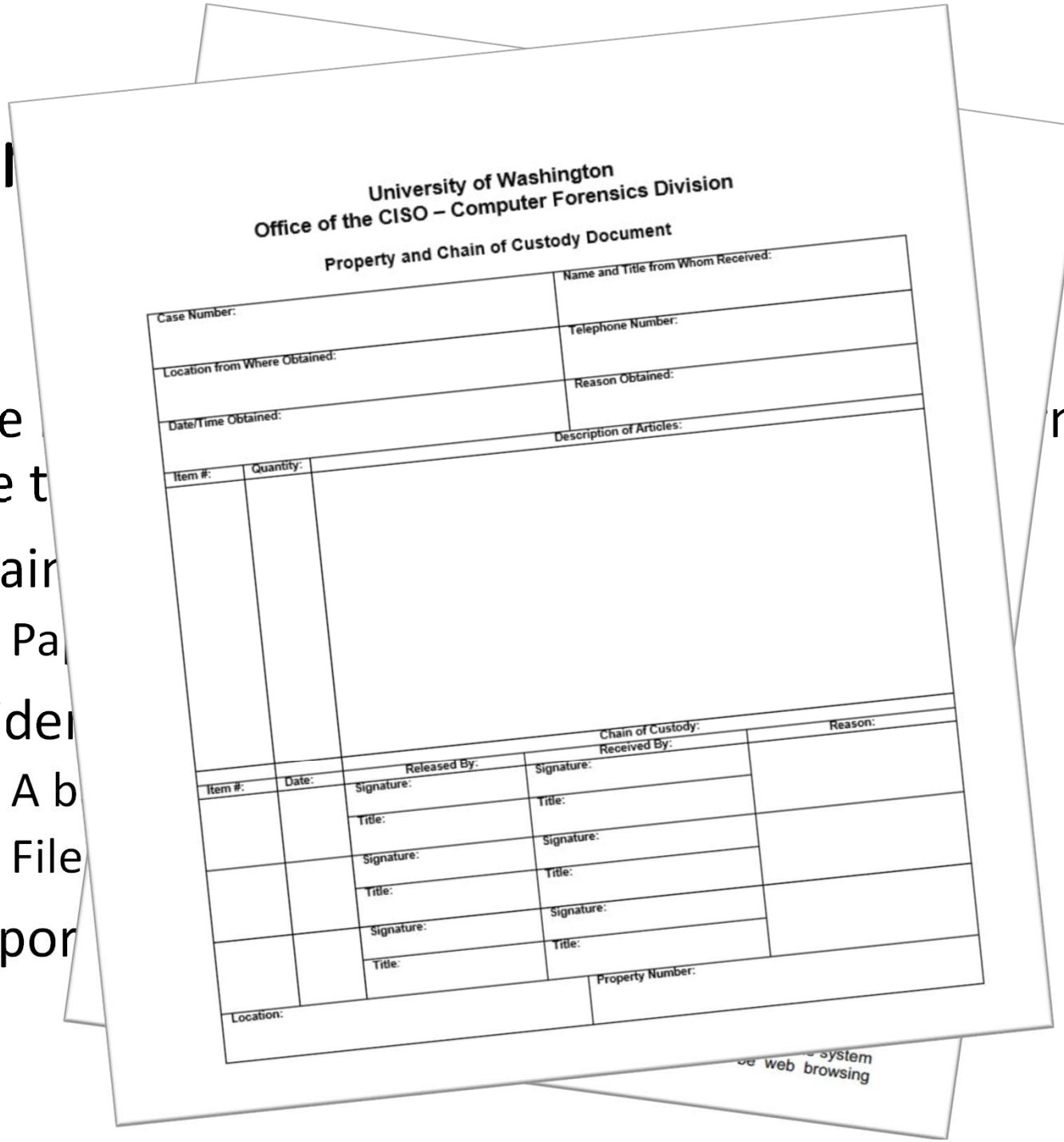
- What happened?
- When did it happen?
- Who did it?
- What did they do?
- Where else did they go?
- (Profit!)

# Forensics on what?

- Hard Drive
- Thumb Drive
- Mobile Phone
- Any electronic media
- Logs
- Emails
- Digital Files
- Network!

# Cri

- The
  the t
- Chair
  - Pa
- Evide
  - A b
  - File
- Repor



University of Washington
Office of the CISO – Computer Forensics Division

Property and Chain of Custody Document

| | |
|---|---|
| Case Number: | Name and Title from Whom Received: |
| Location from Where Obtained: | Telephone Number: |
| Date/Time Obtained: | Reason Obtained: |

| Item #: | Quantity: | Description of Articles: |
|---|---|---|
| | | |

| Item #: | Date: | Chain of Custody: Released By: | Received By: | Reason: |
|---|---|---|---|---|
| | | Signature: | Signature: | |
| | | Title: | Title: | |
| | | Signature: | Signature: | |
| | | Title: | Title: | |
| | | Signature: | Signature: | |
| | | Title: | Title: | |

Location: Property Number:

mine

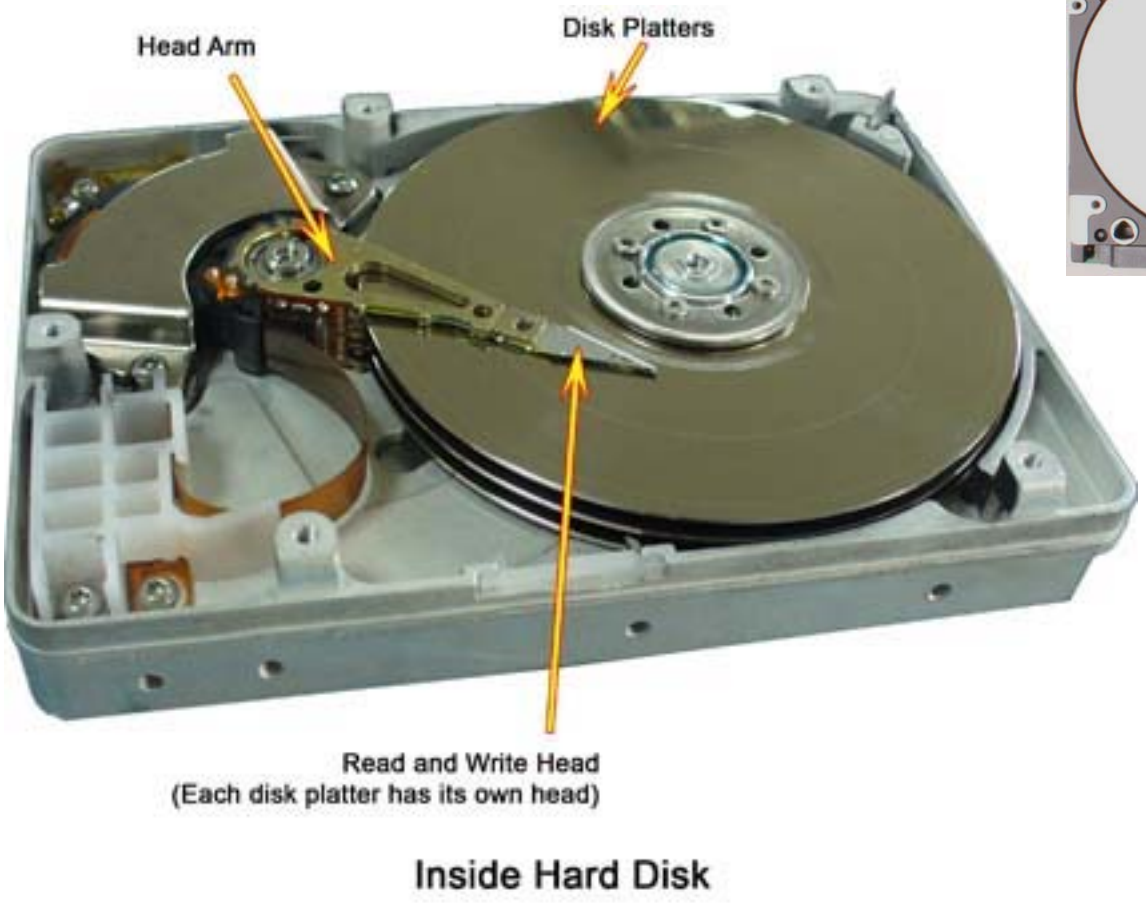
system
web browsing

# Evidence acquisition

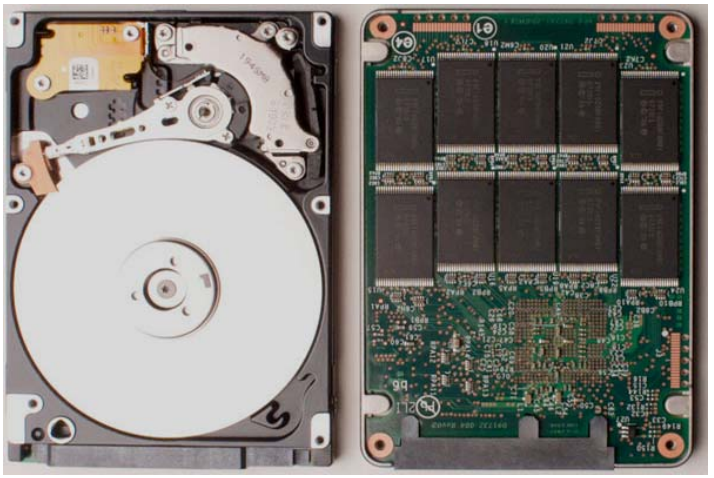

# Forensic Software Tools

- EnCase
- FTK
- Sleuth Kit / Autopsy
- Volatility
- ‘dd’
- Various Live CDs
- …
- https://urlquery.net
- https://www.virustotal.com

# A quick crash course in data storage




Inside Hard Disk



- In computer disk storage, a sector is a subdivision of a track on a magnetic disk or optical disc. Each sector stores a fixed amount of user-accessible data, traditionally 512 bytes for hard disk drives (HDDs) and 2048 bytes for CD-ROMs and DVD-ROMs. Newer HDDs use 4096-byte (4 KB) sectors, which are known as the Advanced Format (AF).
- Geometrically, the word sector means a portion of a disk between a center, two radii and a corresponding , which is shaped like a slice of a pie.
- In disk drives, each physical sector is made up of three basic parts, the sector header, the data area and the error-correcting code (ECC).
- Early in the computing industry, the term *block* was loosely used to refer to a small chunk of data. Later the term referring to the data area was replaced by sector

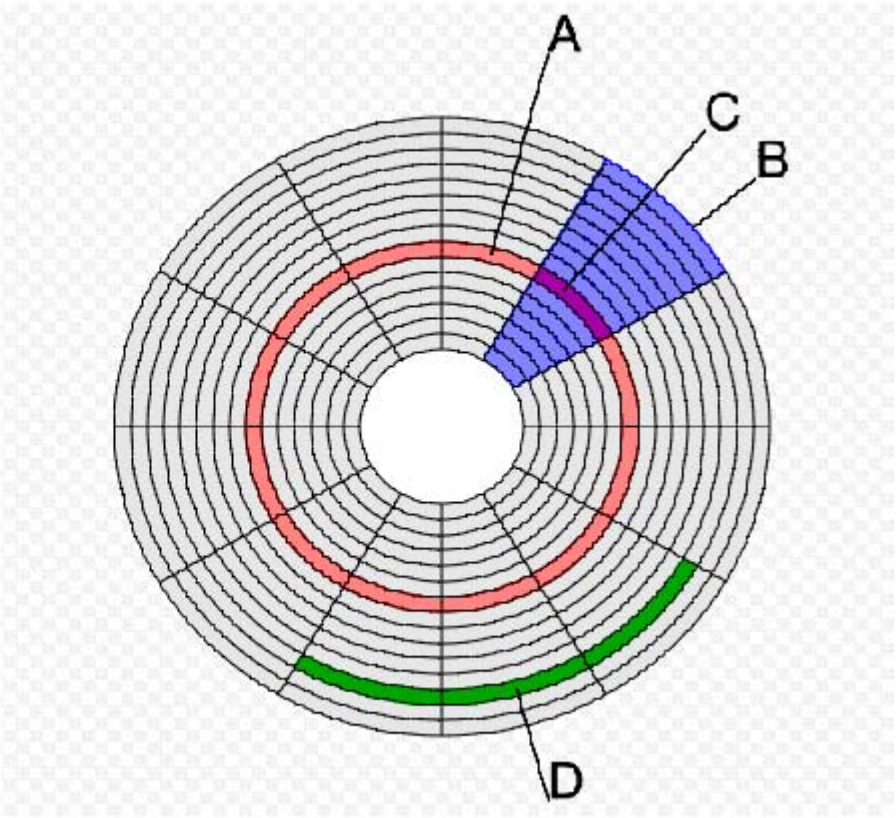
# Drive geometry

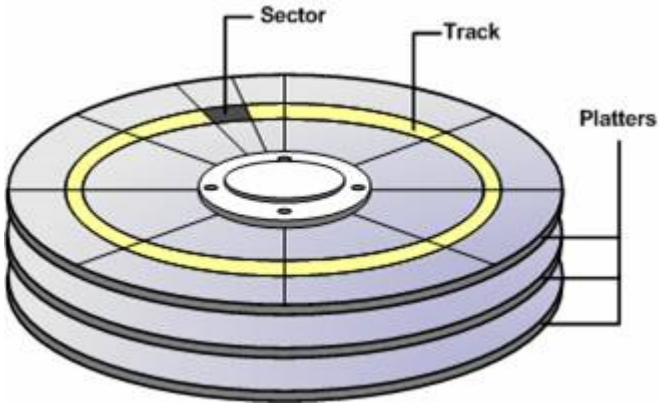
A : Track

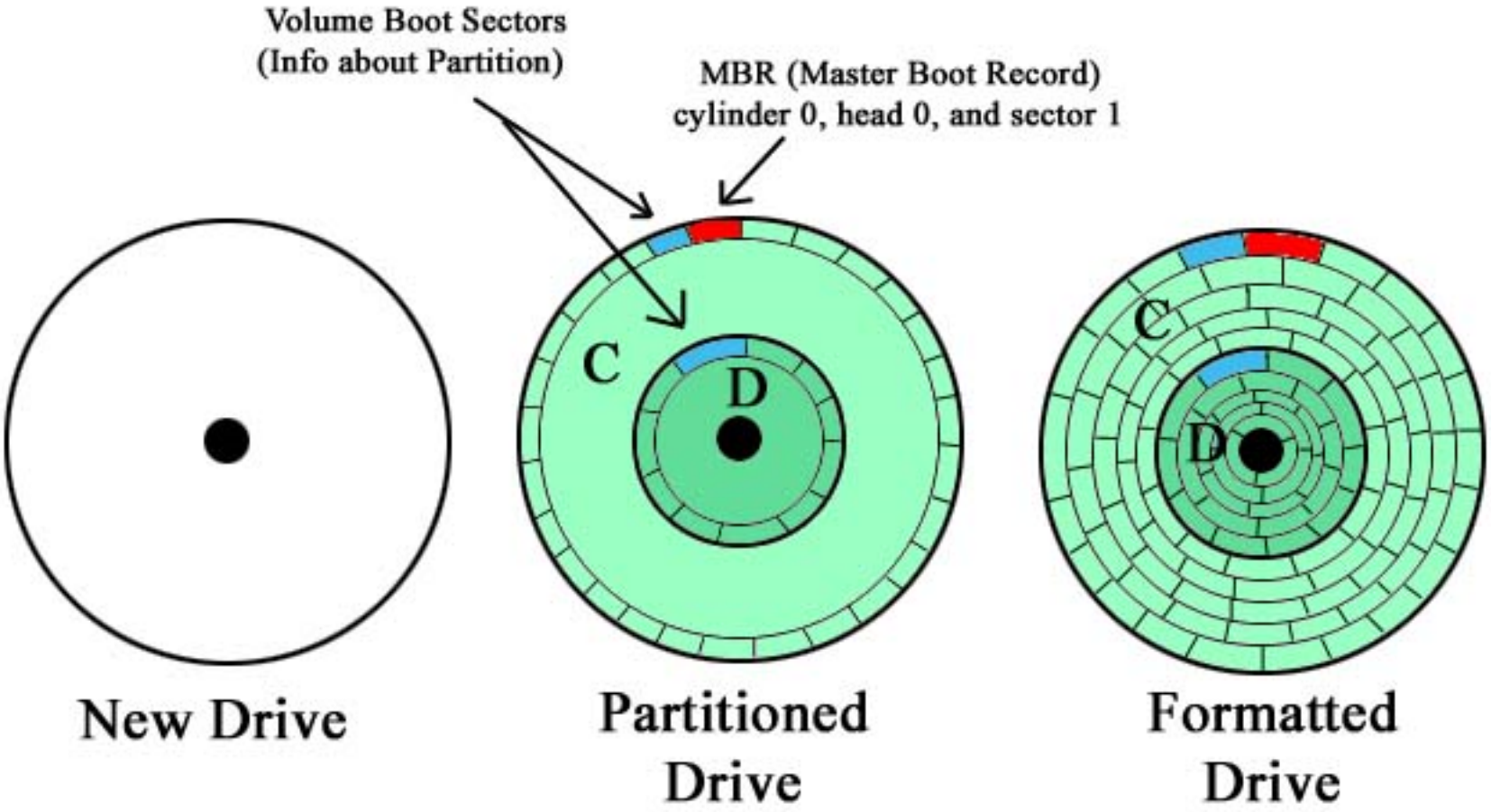
B : Geometrical Sector

C: Track Sector

D: Cluster

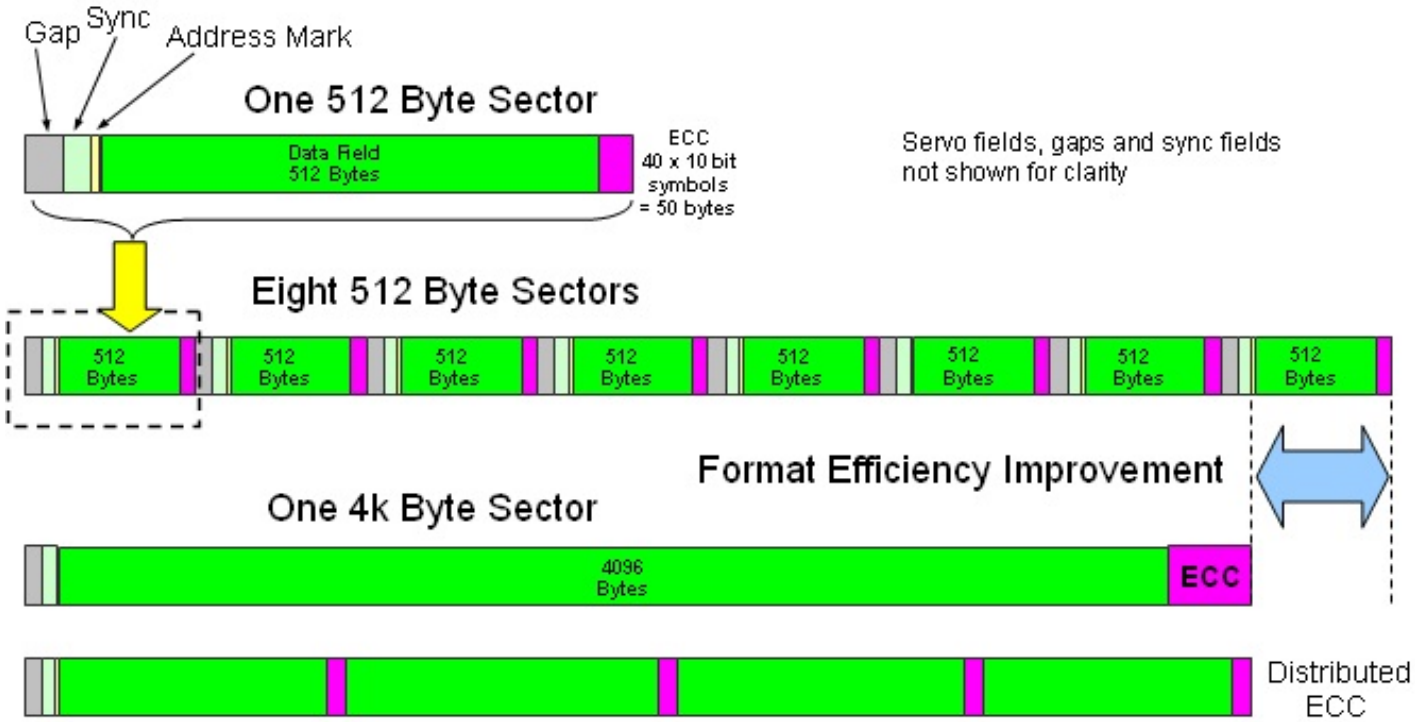




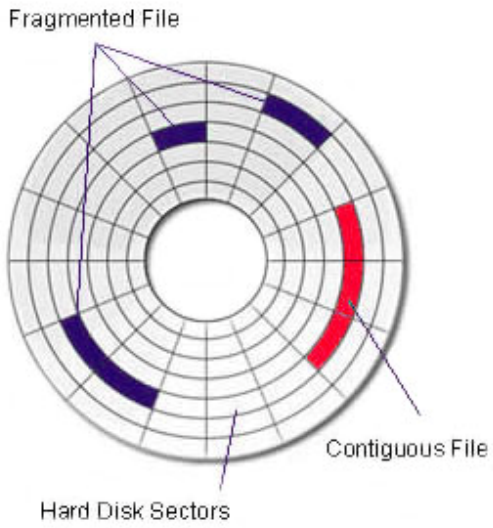

The presence of boot loader for x86-CPUs in the boot sector is by convention indicated by a two-byte hexadecimal sequence `0x55 0xAA` (called the boot sector signature) at the end of the boot sector (offsets `0x1FE` and `0x1FF`)

# The Advanced Format (AF)



# Data Recovery

- If you delete it, it's not really gone
- Formatting does not erase data
- Deleting a partition does not erase data
- File Carving

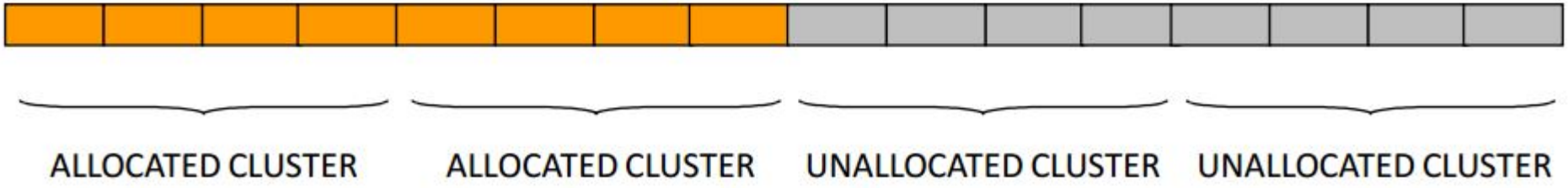


# Slack Space vs. Unallocated space

- **Slack space** is the unused space between the end of the actual file and the end of the defined data unit (cluster). *Cluster* is the smallest unit of storage that the operating system can deal with. When a file is written, and does not occupy the entire cluster, the remaining space is slack space.
- **Unallocated space** is free space on hard drive that can be used for store data. Unallocated space is different from Slack space. The difference, in the unallocated space the system can put files in it.

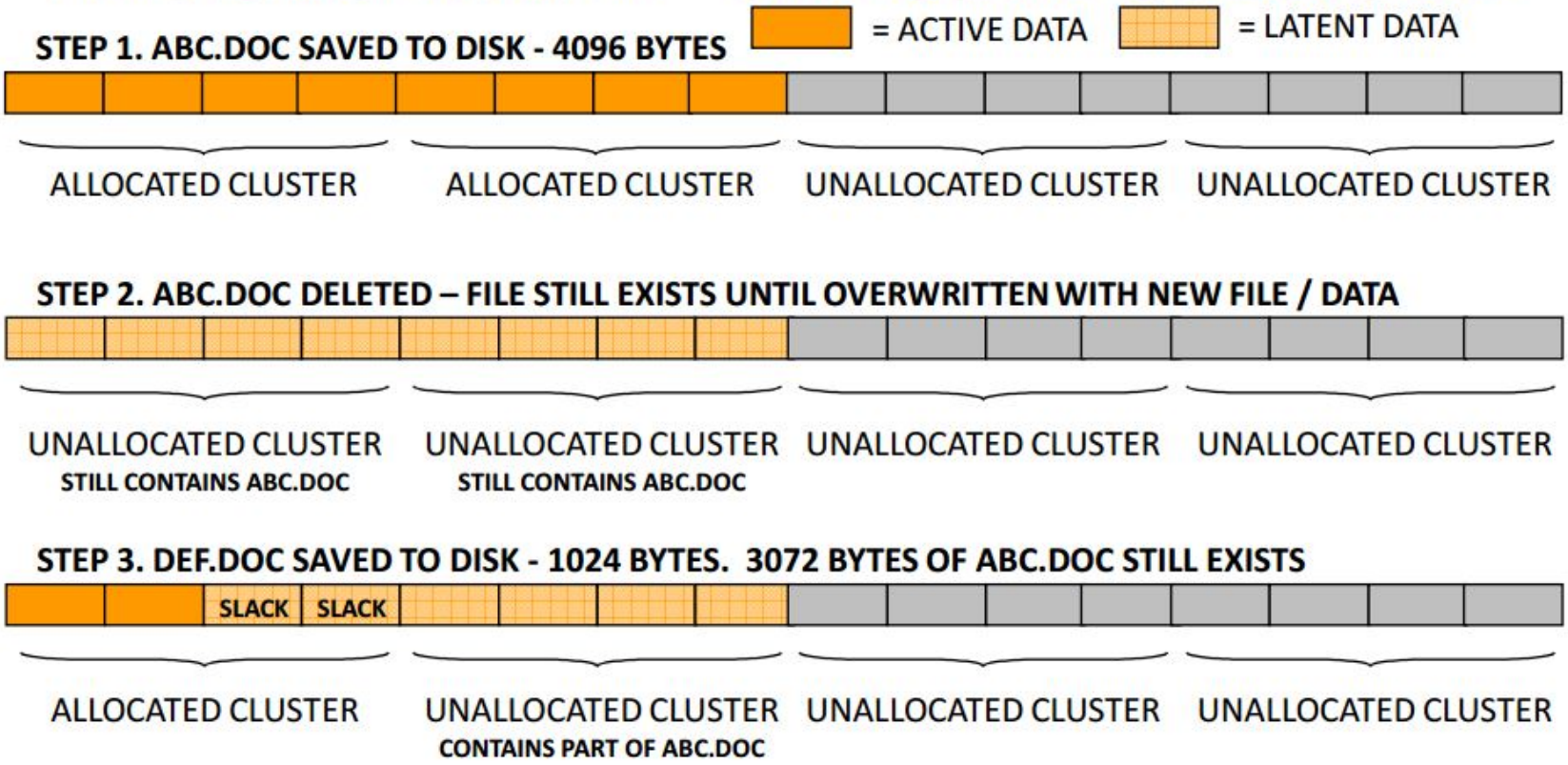
# FILE STORAGE EXAMPLE - CLUSTERS

CLUSTER SIZE FOR PARTITION: **2048 BYTES** (FOUR SECTORS)
EXAMPLE FILE SIZE: **4096 BYTES**
LOGICAL FILE SIZE: **4096 BYTES**
PHYSICAL FILE SIZE: **4096 BYTES**
**LOGICAL FILE WILL COMPLETELY OCCUPY TWO CLUSTERS**

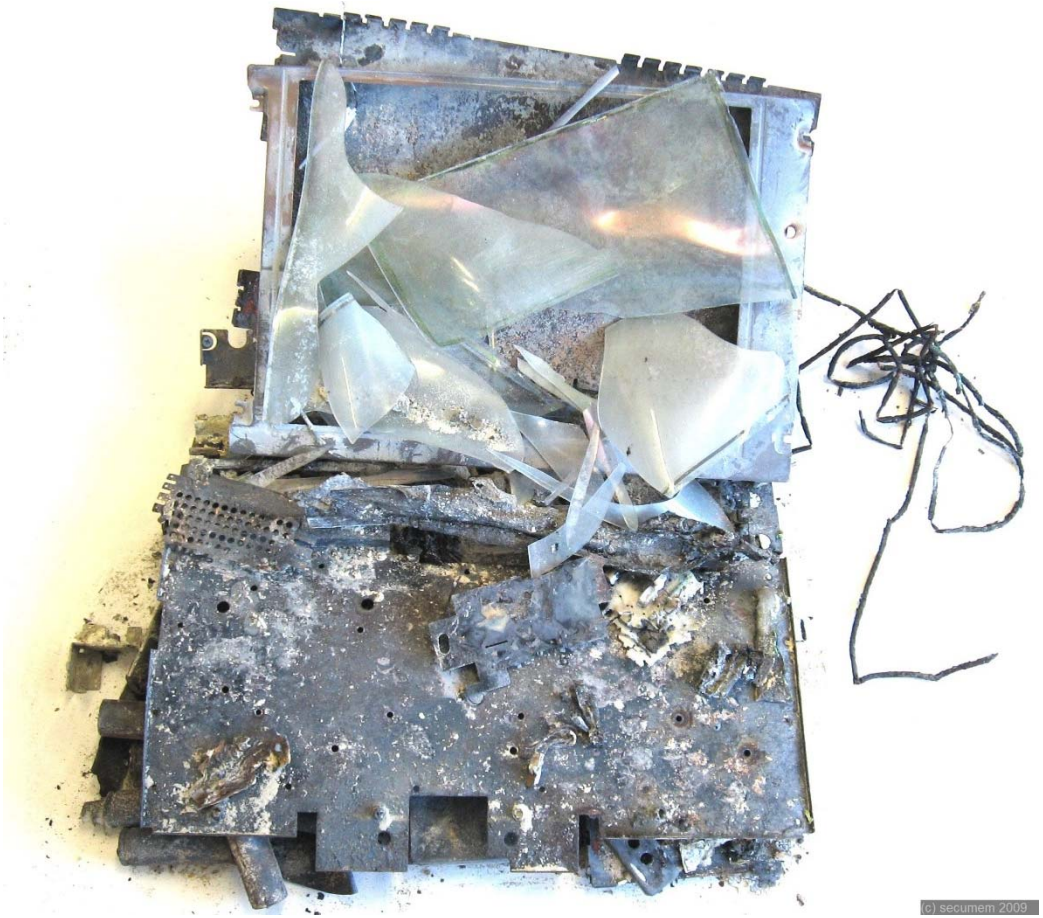



CLUSTER SIZE FOR PARTITION: **2048 BYTES** (FOUR SECTORS)
EXAMPLE FILE SIZE: **3072 BYTES**
LOGICAL FILE SIZE: **3072 BYTES**
PHYSICAL FILE SIZE: **4096 BYTES**
**LOGICAL FILE WILL COMPLETELY OCCUPY TWO CLUSTERS AND PART OF A THIRD CLUSTER**

# FILE STORAGE EXAMPLE – UNALLOCATED & SLACK SPACE



# Fact or fiction?



# Fact or fiction?

# What can you do to protect your privacy?

- Simply deleting does not delete, even formatting is not enough!
- Pull hard drives before recycling old computers
- Physically destroy them if possible (esp. SSDs)
- Use secure erase programs
  - DBAN
  - Blanco
  - KillDisk
  - …
- One pass zeros vs DoD 5220.22-M (NISPOM)
- Factory reset / wipe / erase on mobile devices (smash is better)

# Shooting them can be fun, but…


# Shattering the platters is better

(this page intentionally left blank)

# LAB VI

- Introduction
- Learning Objective
- Instructions
- Deliverable