IT-Security (ITS) B1

DIKU, E2021

Today’s agenda

1: Forensics

2: (Defensive) Cyber security in practice (guest)

3: Exam Q/A

Forensics defined

Digital forensics is a branch of forensic science encompassing the recovery and investigation of material found on digital devices

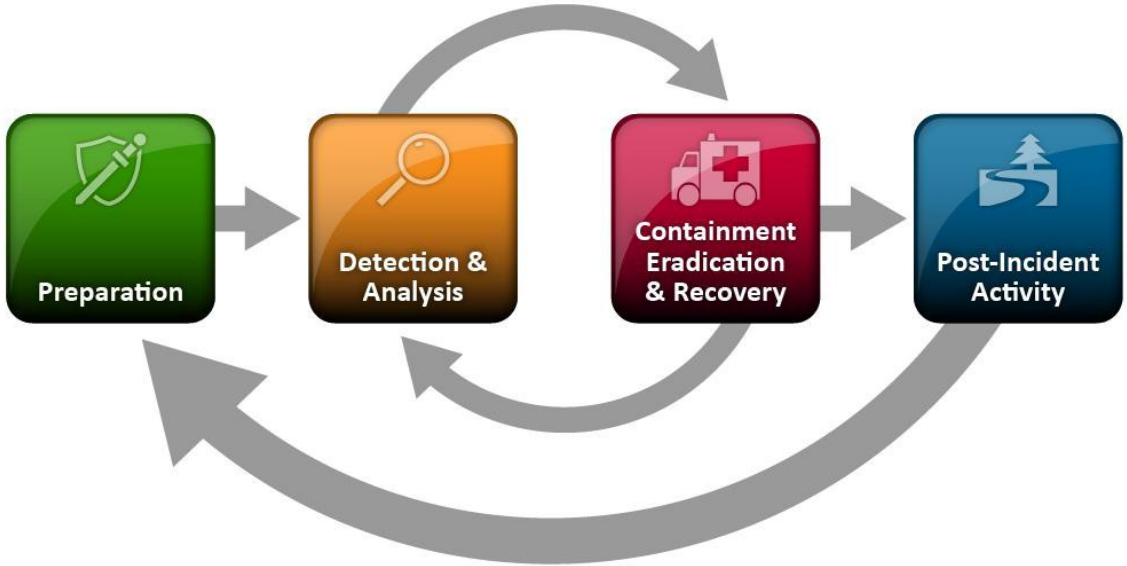
Applied in a **corporate**, **civil**, or **criminal** setting (originated in law enforcement)

Applied to a **security** investigation or **personnel** investigation

In security investigations, forensics either means a **root cause or impact analysis** of a cyber-attack, often post-mortem, **or simply techniques** used in the process of uncovering, understanding, and responding to a security incident

In security, **DFIRMA** = digital forensics + incident response + malware analysis

Recap: Intrusion detection



DFIRMA in practice

```
while true:
        intrusion analysis

        if intrusion suspected:
                preliminary analysis

                if intrusion verified:
                        repeat until incident fully grasped:
                                incident analysis
                                forensic analysis
                                malware anaysis

                        incident response

        update plans
```

Sidebar: Many forms of forensics

Digital forensics =

- Computer forensics
- Memory forensics
- Network forensics
- Mobile forensics
- Etc. forensics

Memory forensics

Situation: Evil code is running

Out job: Find it in memory

Memory forensics

From Wikipedia:

“Memory forensics is forensic analysis of a computer's **memory dump**.

Its primary application is investigation of advanced computer attacks which are stealthy enough to avoid leaving data on the computer's hard drive.”

First, get a copy

- Live acquisition
  - Different techiniques
- Live analysis
  - Direct analysis of the running kernel
- Dead acquisition
  - Hibernation files, page files
- Virtualization - thank you

What to find in memory?

- Running processes
- Listening sockets
- Open connections
- Encryption keys
- Credentials
- Memory only malware
- Closed connections
- Terminated processes
- Open file handles
- Deobfuscated code

Memory forensic analysis process

1: Find rogue processes

2: Analyse DLLs

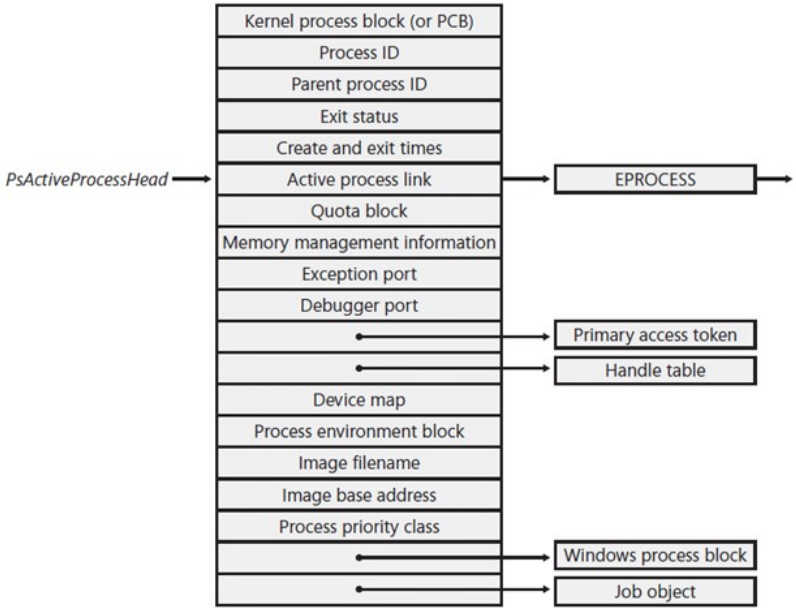
3: Review network artefacts

4: Look for evidence of code injections

5: Dump suspicious processes → further analysis

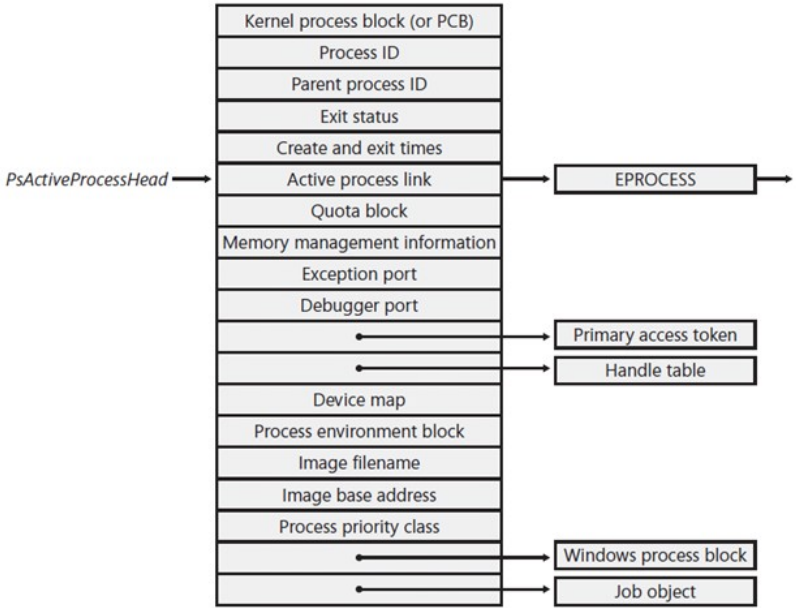
How to find processes (on Windows)

EPROCESS objects in memory:

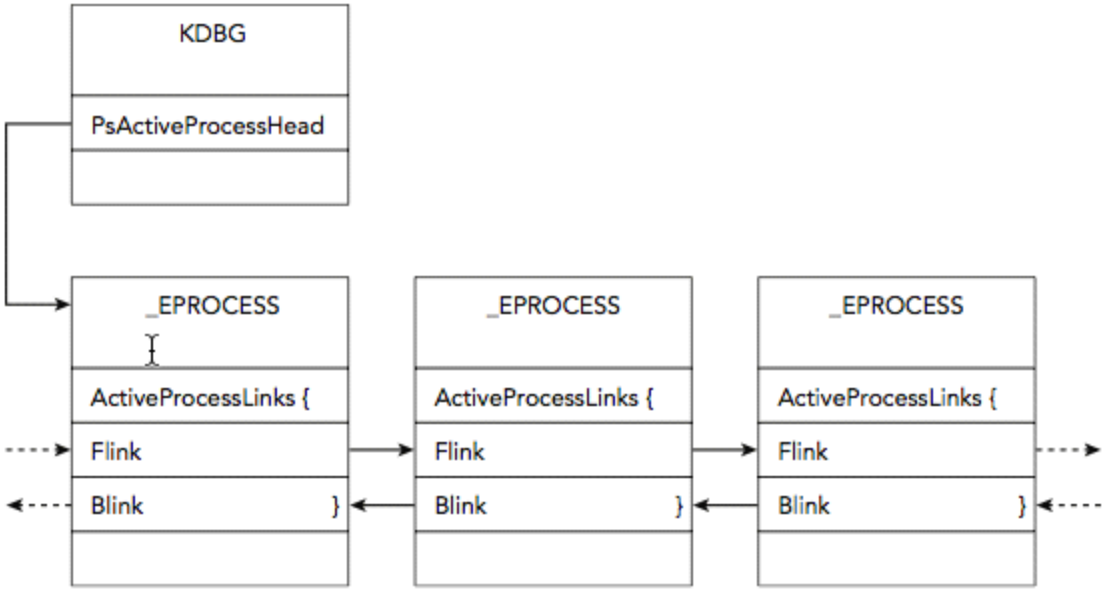


How to find processes (on Windows)

Scan for EPROCESS objects:



Process enumeration (on Windows)



Key concept in memory forensics:

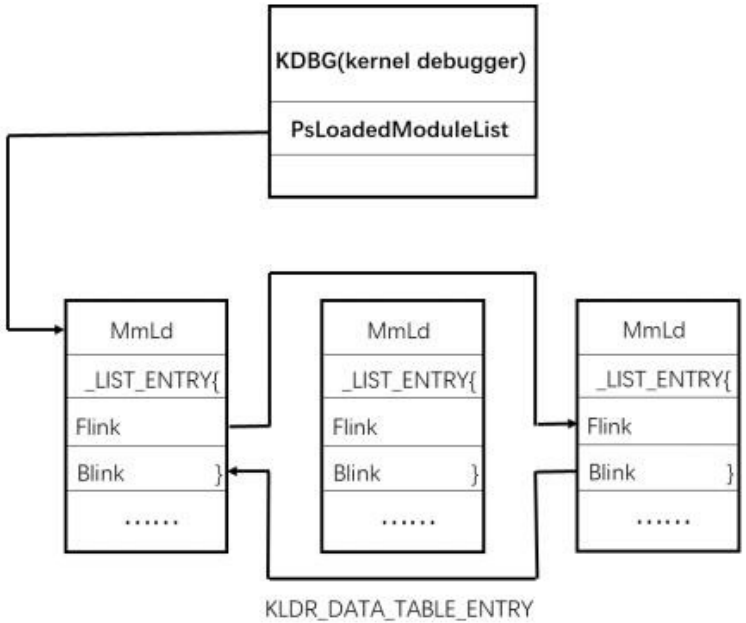
Walking a list, or **scanning for objects**

Step 1 revisited: Find rogue processes

Those that:

- Hide
- Have odd parents
- Do network comm but shouldn’t
- Have unusually many handles open
- Contain maliciously injected code
- ...

Direct kernel objection manipulation (DKOM)



Another example:

Zeus

Zeus

WANTED BY THE FBI

EVGENIY MIKHAILOVICH BOGACHEV

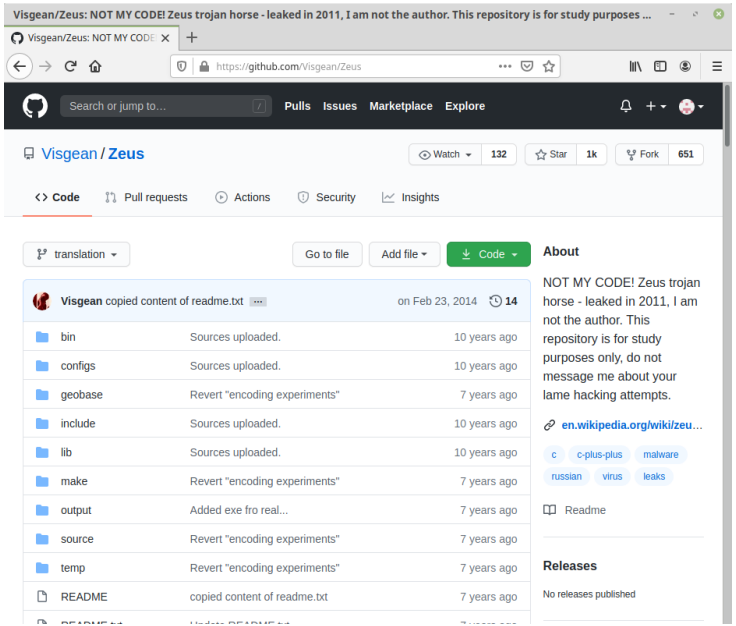
Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud

DESCRIPTION

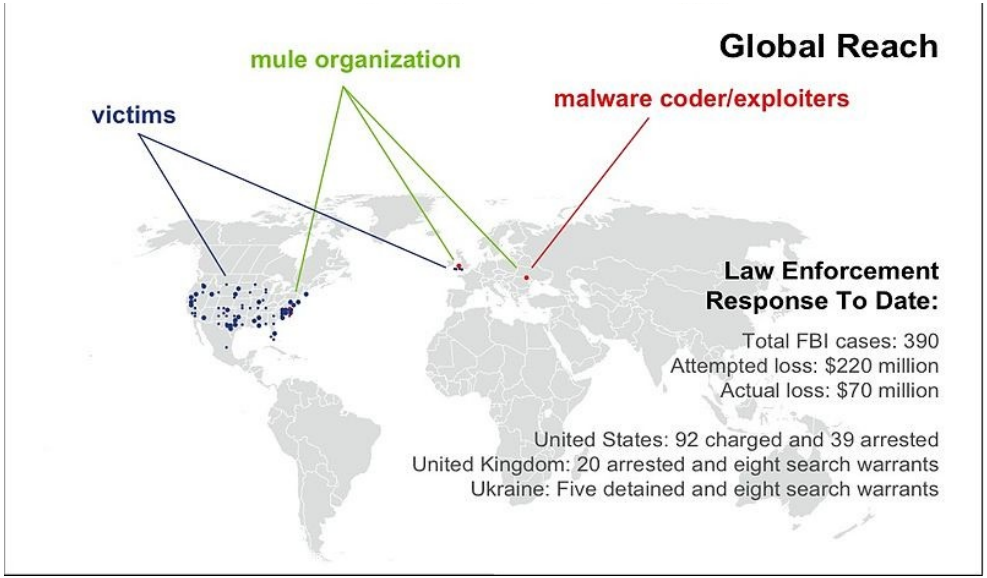
Aliases: Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"	
Date(s) of Birth Used: October 28, 1983	**Hair:** Brown (usually shaves his head)
Eyes: Brown	**Height:** Approximately 5'9"
Weight: Approximately 180 pounds	**Sex:** Male
Race: White	**Occupation:** Bogachev works in the Information Technology field.
NCIC: W890989955	

REWARD

The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to $3 million for information leading to the arrest and/or conviction of Evgeniy Mikhailovich Bogachev.

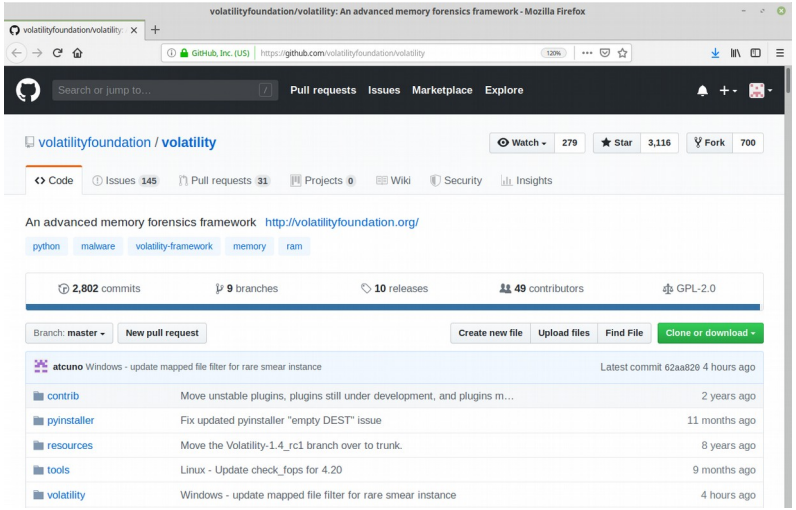


Zeus infection



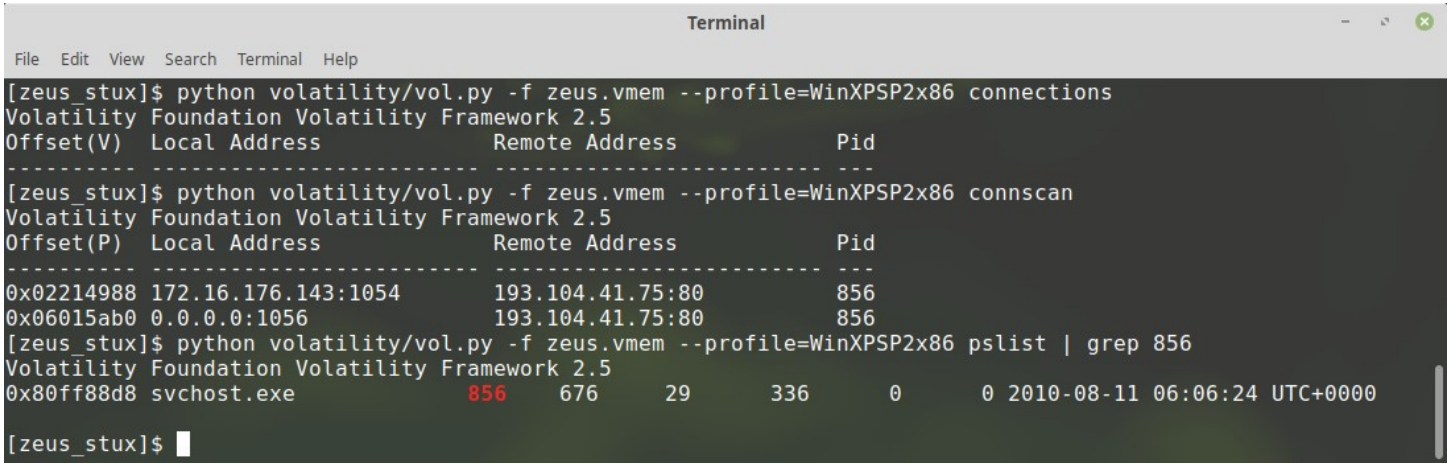
Volatility

Volatility is an open source memory analysis framework writtin in Python



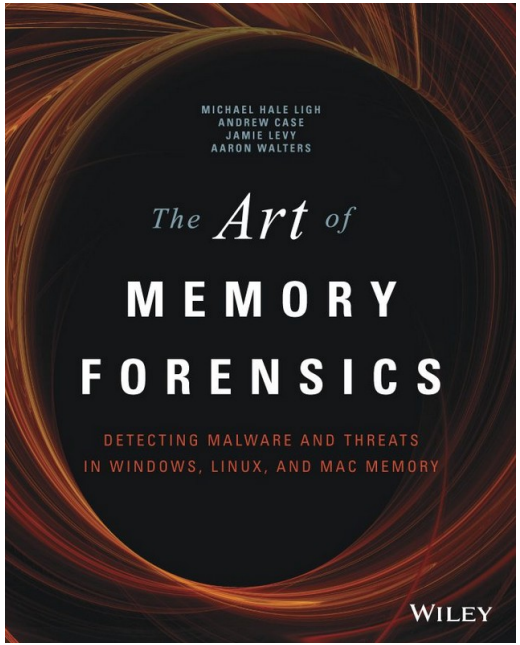
Example memory analyses

Volatility and Zeus



Don’t pull the plug

Further reading



Disk (or, file system) forensics

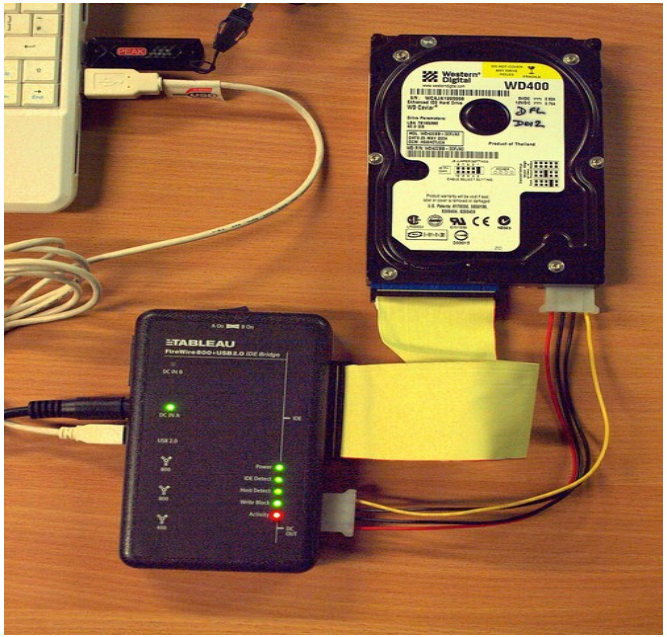
Situation: Evil file has reached disk

Out job: Find the malware

Typical disk forensic approach

Forensic workstation

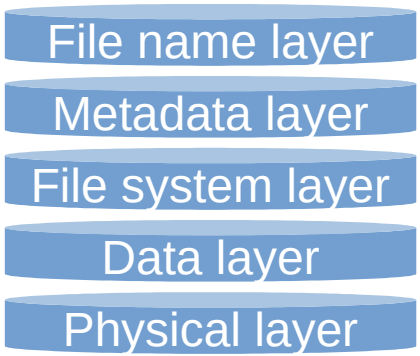
Write blocker



Seized harddrive

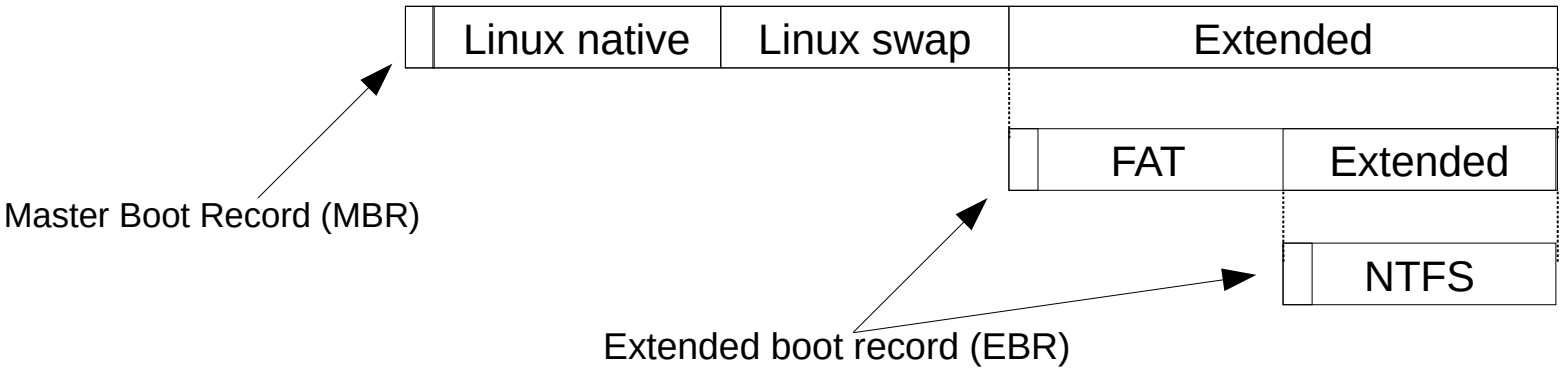
Forensics in a nutshell

Understanding the low-level details



- File names, directories
- Structure information about files/directories
- Partition information
- Sectors, blocks, clusters
- The drive itself, and partitions

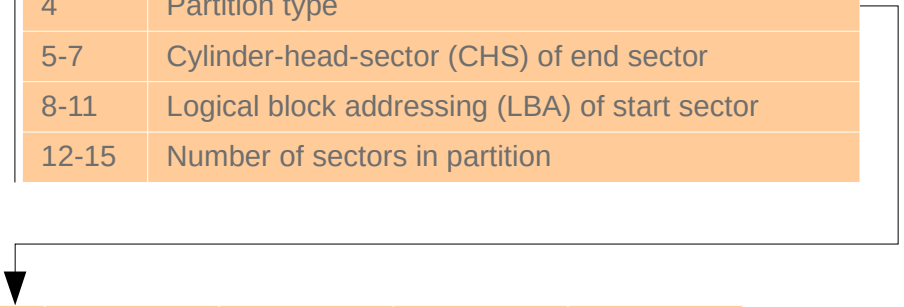
Disk forensic example: DOS partitions



MBR/EBR same layout

Bytes	Content
0-445	Upstart code, disk signature
446-461	Partition entry 1
462-477	Partition entry 2
478-493	Partition entry 3
494-509	Partition entry 4
510-511	MBR/EBR signature (0xAA55)

Bytes	Content
0	0x00 not boot, 0x80 boot
1-3	Cylinder-head-sector (CHS) of start sector
4	Partition type
5-7	Cylinder-head-sector (CHS) of end sector
8-11	Logical block addressing (LBA) of start sector
12-15	Number of sectors in partition



Type	FAT12	FAT16	FAT32	Linux native	Linux swap	Extended	NFTS
Hex value	0x01	0x0E	0x0C	0x83	0x82	0x05	0x07

File system example: NTFS

NTFS boot sector	Master File Table	File storage area	Master File Table Copy

Master File Table (MFT)

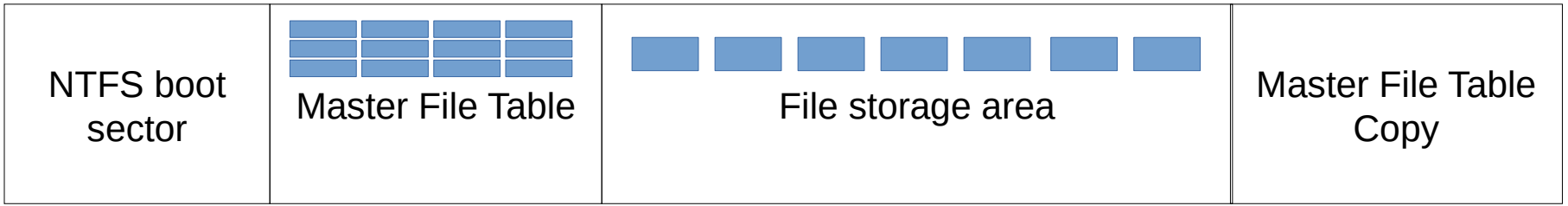
An entry in the MFT describes a file

- Filename and metadata like permissions, timestamps

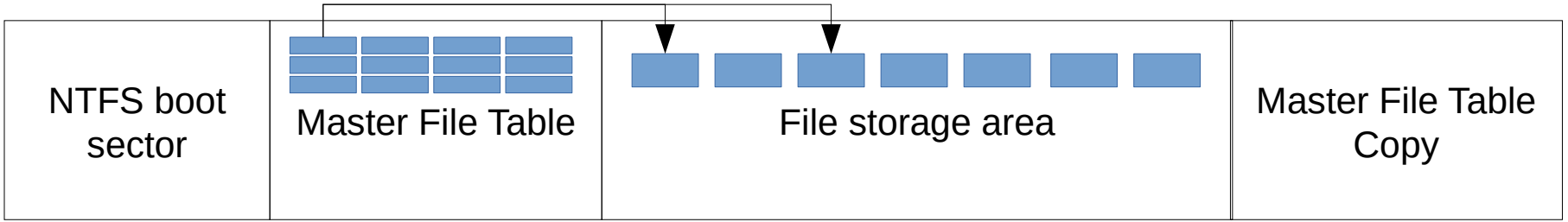
Entries are 1024 bytes

For larger files (non-resident files), the MFT entry contains links to areas of the disk where the file data resides

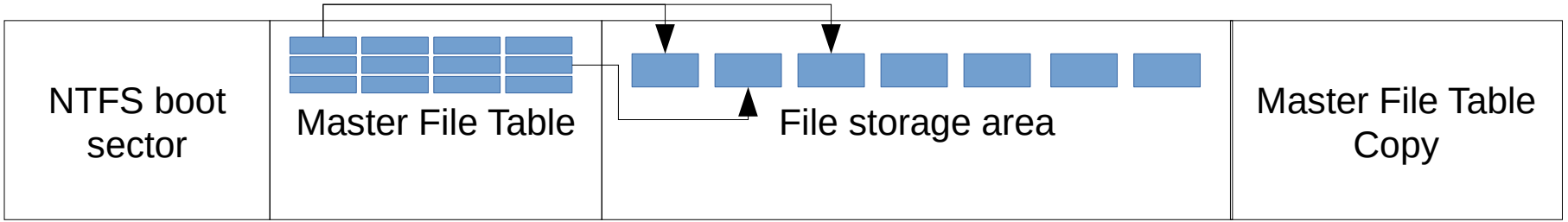
File system example: NTFS



File system example: NTFS



File system example: NTFS



Data / File storage area

Clusters (Windows) or **blocks** (Unix) = 1 or more 512-byte **sectors**

Custers/blocks either **allocated**

- Actively being used by a file

Or **unallocated**

- Not being used by a file
- May contain deleted or unused data

Deleted != destroyed

When a file is deleted, **data still exists** on disk until overwritten

If overwritten, **remnants may still exist** in

- extra copies of the file
- page/swap/hibernation file, or
- elsewhere on the disk due to (de)fragmentation

However, if disk wiped, only just once, recovery infeasible

Think libraries

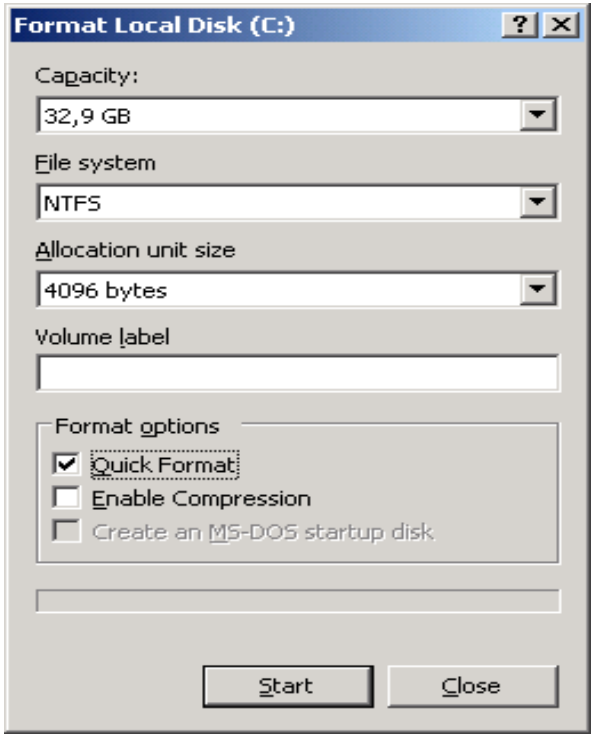
Format is not wiping

Formats create and replace file system structures

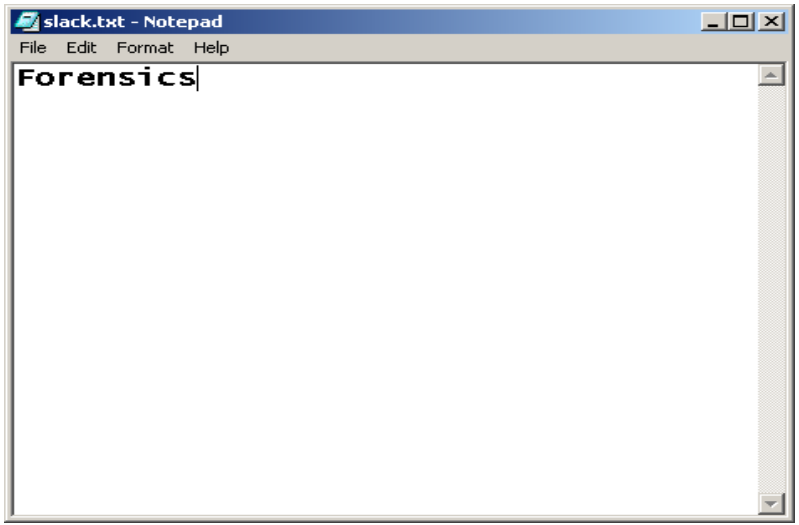
Files are not overwritten

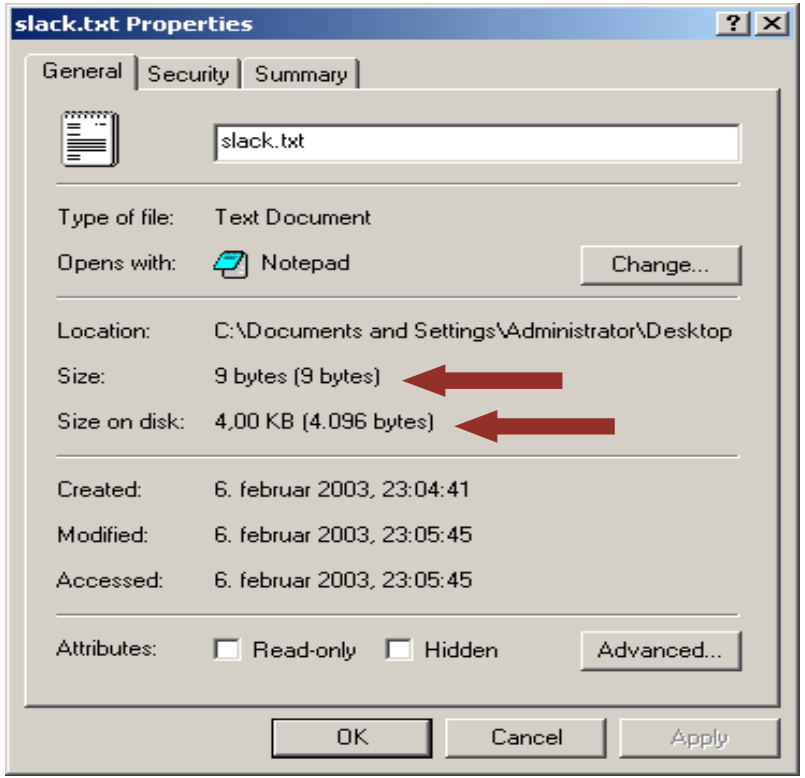
Regular formats take longer as the disk is scanned for bad sectors

Use wiping software for wiping

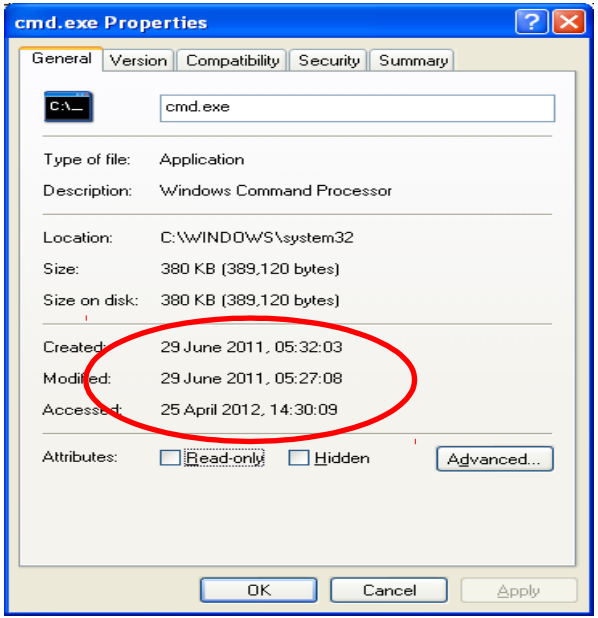


Slack space


slack.txt - Notepad
File Edit Format Help
Forensics

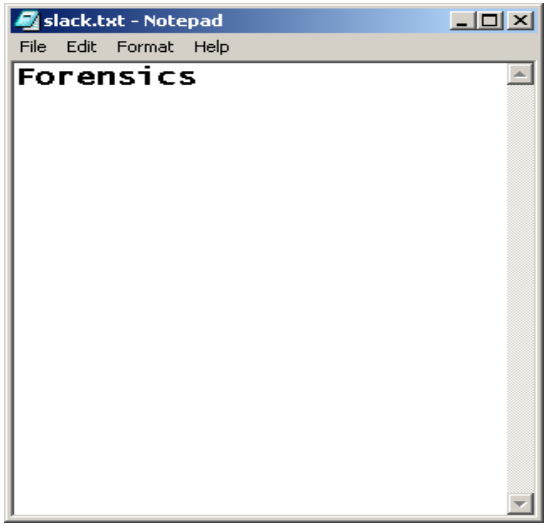

slack.txt Properties
General
Security
Summary
slack.txt
Type of file: Text Document
Opens with: Notepad
Change...
Location: C:\Documents and Settings\Administrator\Desktop
Size: 9 bytes (9 bytes)
Size on disk: 4,00 KB (4.096 bytes)
Created: 6. februar 2003, 23:04:41
Modified: 6. februar 2003, 23:05:45
Accessed: 6. februar 2003, 23:05:45
Attributes: Read-only Hidden
Advanced...
OK
Cancel
Apply

Timeline (Modified, Accessed, Changed)



Searching for file types

Slack.txt



Slack.exe

Slack.pdf

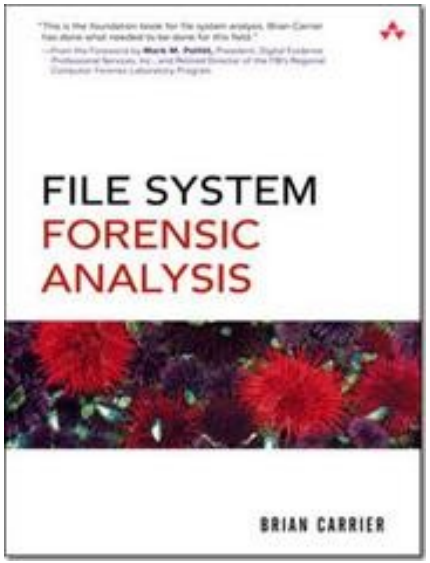
Slack.zip

Slack.dat

Slack.mp3

Slack.dll

Further reading



Wrap-up