Digital Forensics

Investigations

Tools & Techniques

Presented By : Hichem Belguendouz

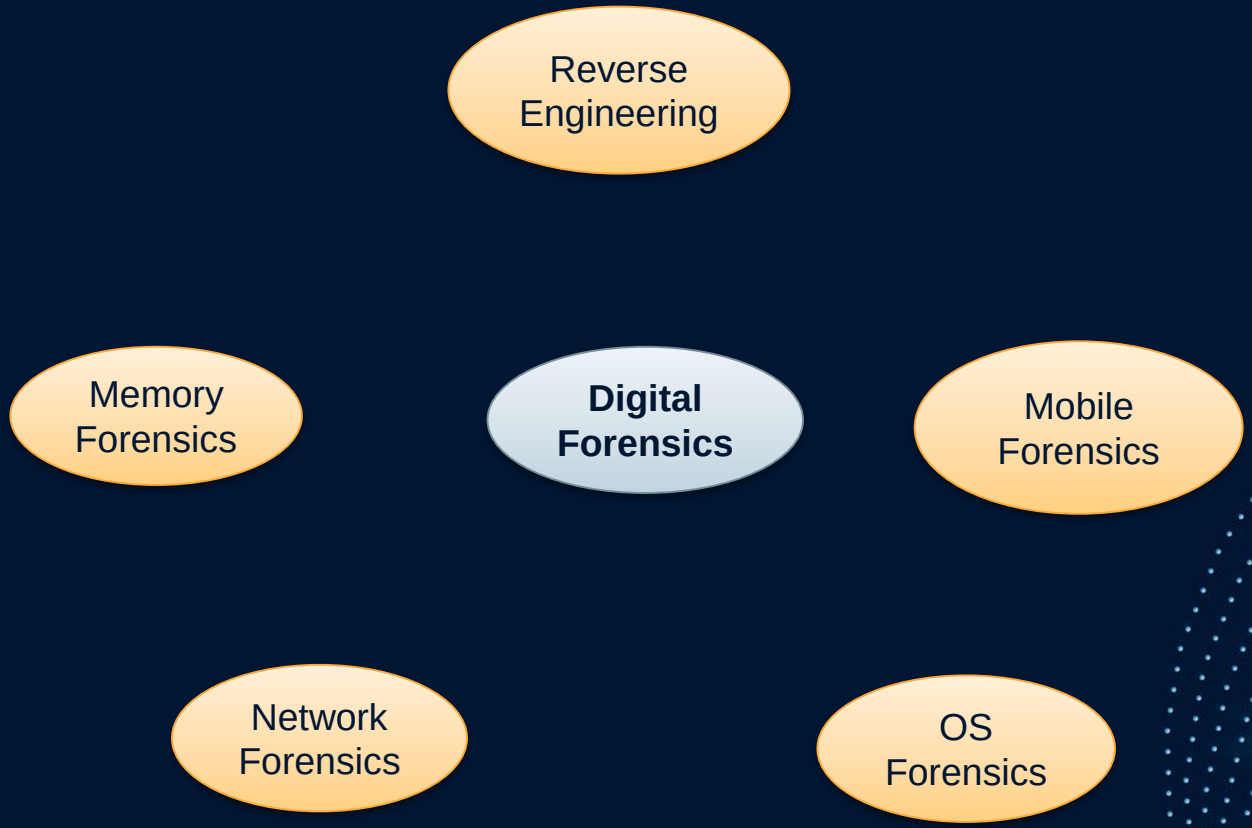
Agenda

1. Introduction To Digital Forensics
2. Who uses DF
3. Volatile vs Non Volatile data .
4. **First Reponder**.
5. Digital Forensics Steps,
6. Defeating Anti-Forensics Techniques.
7. DF Tools(Hardware & Software).
8. Disk Imaging.
9. Memory Analysis.
10. Q&A.

What is Digital Forensics

- **Identifying** : Finding and collecting the suspected evidences
- **Preservation** : Ensuring the integrity of the collected evidence.
- **Analyzing** : Looking into the acquired asset or medias data to find evidences of the suspected crime.
- **Reporting** : Creating a report of finding from the investigation for presentation to stakeholders and, in some cases, an attorney or jury in court.

Fields of Digital Forensics



Who uses Digital Forensics

- Private Computer Forensics Organisations
- Military & Law Enforcement
- Security Enginner & IT Professional
- University Programs

Type of Computer Crimes

- **Internal**
  - Espionage
  - Theft of intellectual property
  - Manipulation of the Records
  - Trojan Horse attacks
- **External**
  - SQL Injection
  - Brute Force attack
  - Identity Theft
  - Phishing
  - Denial of Service

Challenges For Investigators

- Speed
- Anonymity
- Volatile Nature of data
- Evidence size & Complexity
- Anti-Forensics Techniques
- Global Origin & Differences in laws

Digital Forensics Process

- **Pre-Investigation**
  - Forensics Lab
  - Investigation team & getting approval from relevent authrority
  - Planning The Process, define mission goal and secure the case
- **Investigation Phase**
  - Acquisition, preservation and analysis the data
  - Find the Evidence , Examine , Document & preserve the findings
  - **Repeat and reproduce**
- **Post Investigation**
  - Ensure that the target Audience can understand it easliy
  - Ensure report Provide adequate and accepable evidences
  - Report should comply with local laws & standars

Order of Volatility

Volatile : Information that will be lost at shutdown

- Ram
- Network Connection
- CPU Register & Cache

Non Volatile

- Hard Disks
- USB Sticks

Order of Volatility

- Registers and cache
- Arp Cache, Routing table, process, and memory
- Temporary file systems
- Disk or other storage media
- Remote logging and monitoring data is relevent to the system in questions
- Phyisican Configuration, network topology
- Archival media

First Responder

- Prepare Tool Box
- Secure the Scene
- Indentify Potential Evidences
- Data Preservation
- Photography / Document the Scene

What Can Digital Forensics Do :

- Recover Deleted Files
- Determine what programs ran
- Recover emails and users who read them
- Recover Phone Records and SMS text messages from mobile devices
- Find Malwares

Evidence Preservation

You must Answer the following Questions

- Is the system compromised
- How , When , Why ?
- Malware Involved?
- Persistence Mechanisms
- Leteral Movement Inside LAN
- Detect The root cause of the incident
- Access sensitive Data
- Data exfiltration

Hardware Forensics Tools

Write Blocker

Faraday Cage

Forensics Imager

Software Forensics Tools

- **Autopsy**
- SANS SIFT
- Volatility
- ProDiscover
- **Wireshark**
- **FTKImager**

Understanding Data Acquisition

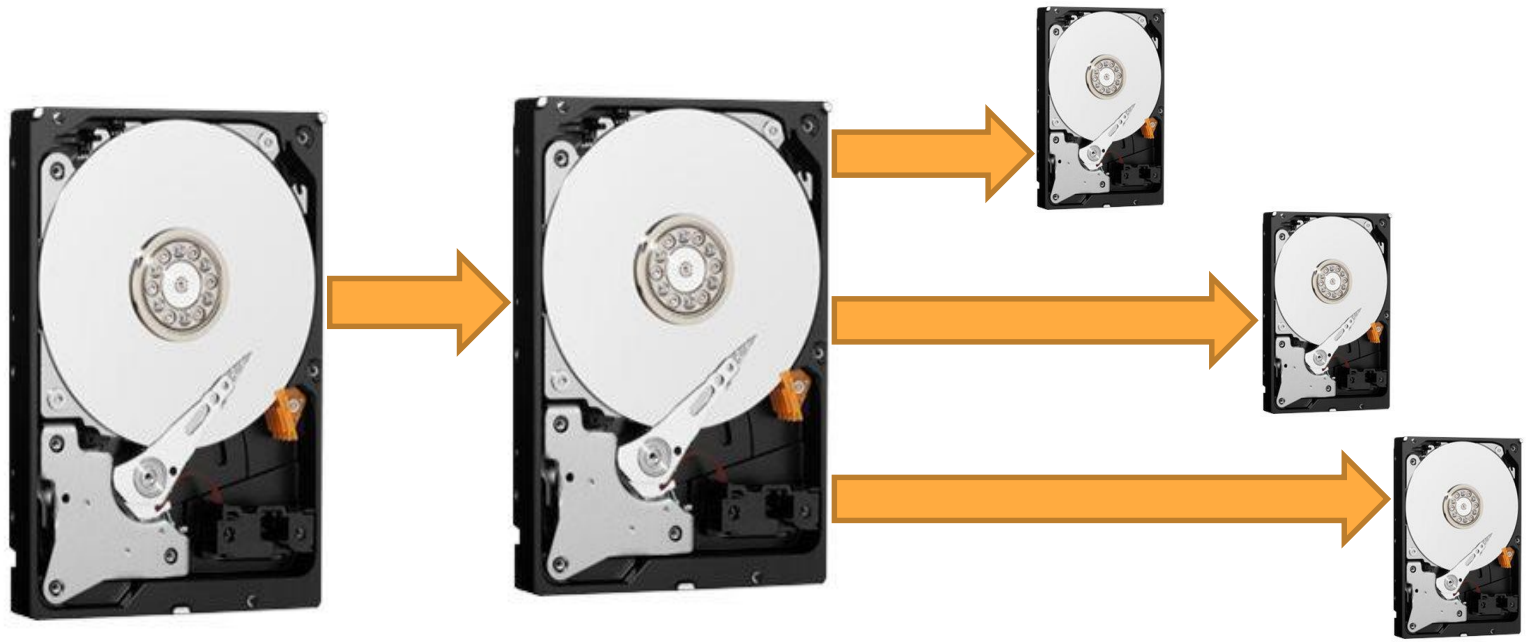
- **Live Acquisition**

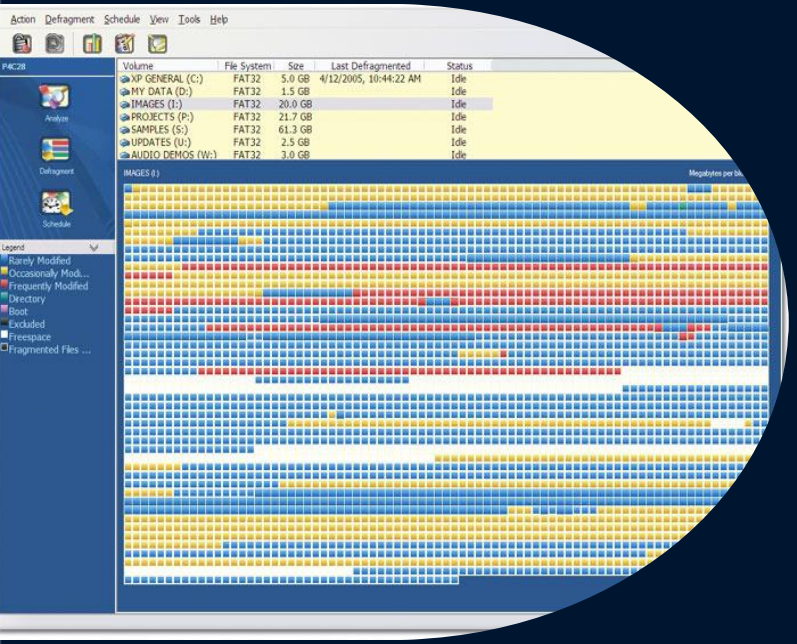
  Involves collecting volatile information that resides in registries, cache and Ram

- **Static Acquisition**

  Acquisition of data that remain unaltered even if the system is powered off

Imaging Methods



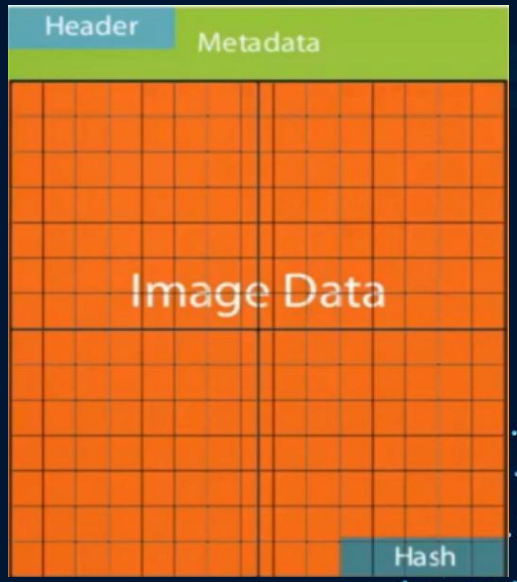


What to Image?

- Files and folders
- Erased files and folders space
- Operating system files
- Boot partition
- Partition Table
- File System Formating
- Bit copy or sector copy
- ,,,,,,,,

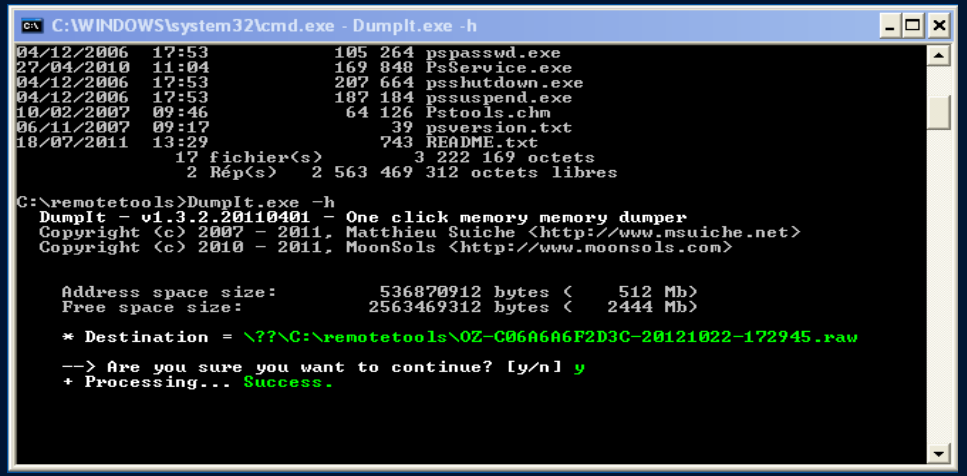
Inside Image

- Image data
- Metadata
  - Name of origin device
  - Name of forensics investigator
  - Time and date of acquisition
  - Case Number
- Cryptographic hash value
  - To check if changes have occured
- One Image in multiple physical files
- Data compression to reduce size



Memory Dumping Tools

Memory Dumping using dumpit.exe

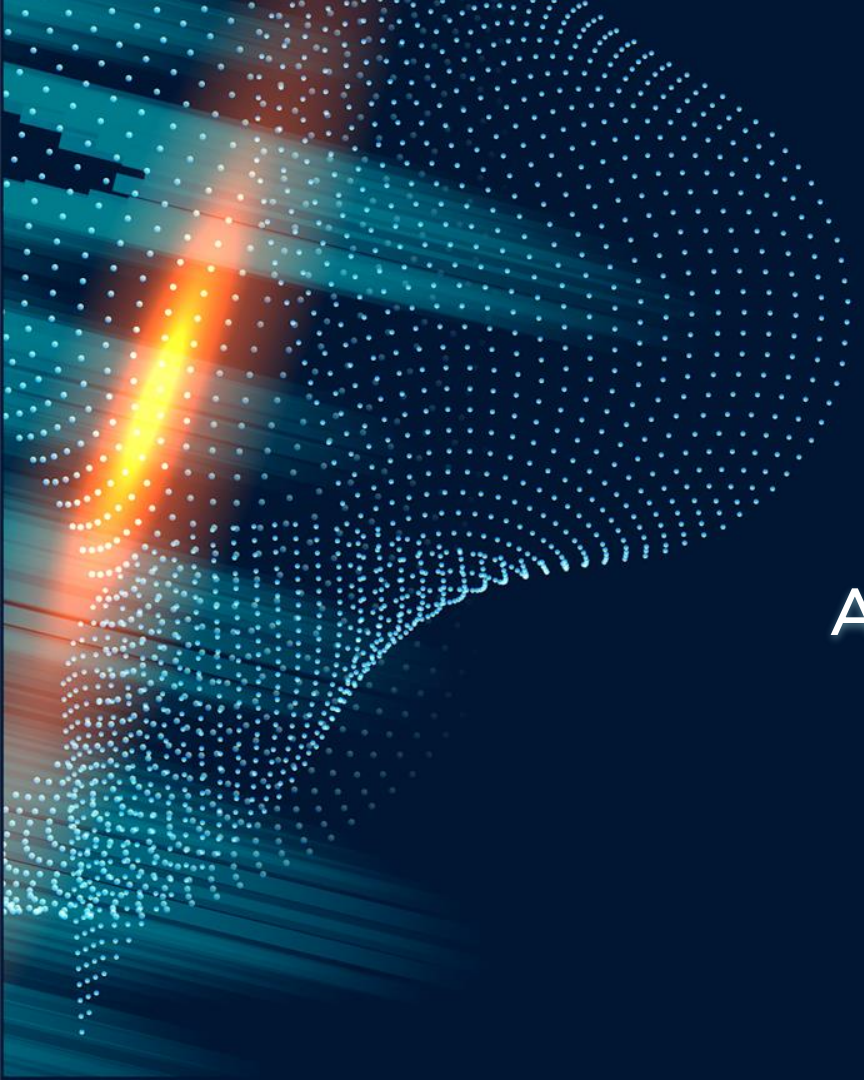


There is Other Tools for Windows Dump Such as :
Volatility , FastDump, Memoryze

Memory Forensics

What inside Memory ?

- Network Connections
- Suspicious Processes or DLLs
- Services(Listening)
- Malware
- Registry Content
- Possible decryption Keys reside in memory
- Check injected Code, Hooked APIs ,,, etc



Anti-forensics Techniques !

How to detect & Stop Them ?

What is Anti-forensics?

Tools and Techniques That Frustrate Forensics Tools

- **Why Anti Forensics is a challenge?**
  - Hard or Impossible to retrieve information during and investigation
  - Limit Identification and Collection of evidence by investigators
  - Analyst Confusion – Normal and abnormal Process
  - The Ability to remain invisible and stealthy

What to do to stop them?

- Update Your Skillsets
- Arm Yourself With Awesome and New Tools
- Know Your Adversary True Intents
- Check out Mittre Attack Regularly

Anti Forensics Methods

- Encryption(On storage and Network)
- Steganography
- File Wiping
- Disk Destruction

Anti Forensics Detecting & Countermeasure

How To Detect

1. **Live Forensics**
    - **Perform OS Scan**
    - **Volatile Data – Memory Dump**
    - **Toolset to capture AF Techniques**
2. **Dead Forensics**
    - **Full Disk Image**

How to countermeasure

- Acknowledge some tools and technique to overcome.
- Verifying result using Multiple Tools
- Save data where the attacker can not get at it for further analysis
- Improve the weaknesses in you forensics process

Windows Forensics

- Master File Table(MFT)
- Data Streams
- Registry Hives
- Prefetch
- Event Logs
- ThumbCache
- LNK (,lnk) Files

Windows Forensics

- Create a timeline of events occured before the incident
- Determine the root cause of the incident
- Collect all the related artifacts to the attack
- Restore deleted files & directories related to the incident

“What Doesn’t Kill You Makes You Stronger”

–Friedrich Nietzche-

THANKS!

Do you have any Questions?

Contact us:

- **Linkedin:** linkedin.com/in/hvb-xx7/
- **Facebook:** facebook.com/hvb.xx7/