

Introduction to Computer Security Lecture Slides

© 2023 by [Mihai Chiroiu](#)

is licensed under [Attribution-NonCommercial-ShareAlike 4.0
International](#)

Computer Forensics

Asst. Prof. Mihai Chiroiu

Objectives

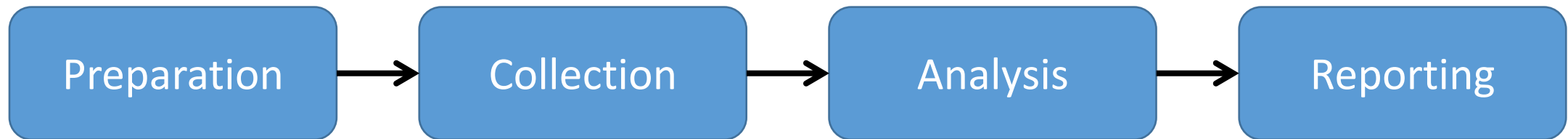
- Digital forensics vocabulary
- Methodology
- Use of investigation tools

Example

- “Prove that email **NOT** was received”
- Easy to prove that an email was received:
 - Look at email servers for logs
- Does not finding traces mean that it was not received?
 - Maybe the investigation was not complete
 - Maybe it was (cleverly) deleted
- Reason for third-party logs 😊

What is Computer Forensics?

- Interpretation of computer media for digital evidence
- Who uses it: Industry, Government, Individual
- Simplified Process Model:

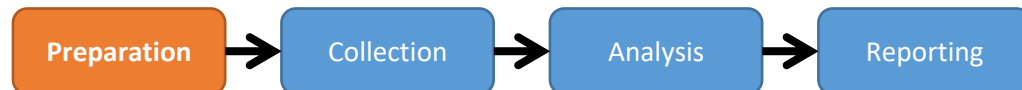


Principles of Computer Forensics

- Anything done to a system changes it!
 - Running systems
- Collection process should retain data integrity
 - How can you prove that you did not change it during the investigation
- All activities should be logged
- Hire an expert or become one 😊

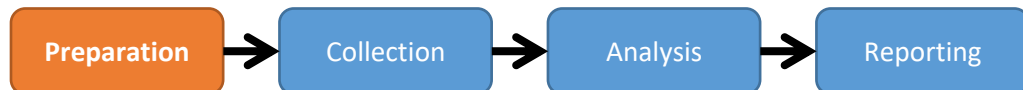
Questions to cover

*“I keep six honest serving-men
(They taught me all I knew);
Their names are What and Why
and When
And How and Where and Who.”*
Rudyard Kipling



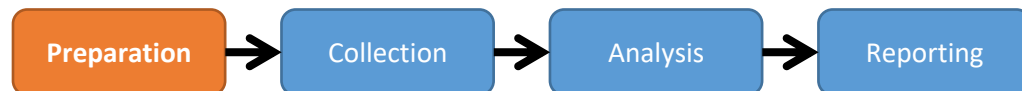
Questions to cover

- Has something happened at all?
 - Hacked vs Bugs vs Random effect
- When did it happen and for how long?
- What happened with what effects?
 - Read vs Delete vs Modification
- Who did it and why?
 - IP vs Username
- How did he do it?



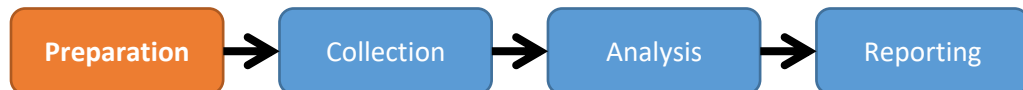
Data sources

- Make a list of possible data-sourcing
 - Brainstorming
 - e.g., Hard disk, flash drives, mobile phones, scanners, RAM, etc.
- Problem:
 - “Data integrity” -> one must build systems to ensure that it has not been changed
 - e.g., external logging, HSM,



Remote and secure data

- How to investigate the “cloud”?
 - Ask for remote access is not easy, even for governments
- Encrypted disks are hard to investigate
 - Remember TPM?
- Prepare for future investigation
 - IDS-like systems



Actions

- Conduct a search for evidence:
 - E.g., Data, Logs, Passwords, Waste paper basket 😊
- Package evidence:
 - When possible, duplicate the systems
 - E.g., make a copy of the hard drive
- Limit access to the collected data
 - Maybe the who is an insider



The order of volatility

- Registers, CPU caches
- Routing tables, time-based caches (e.g., arp), kernel statistics
- Running processes
- Memory, Temporary file systems (e.g., ramdisks)
- Media in use
- Remote data (USB drives)
- Backup data, read-only drives (e.g., DVDs)



Practical actions for systems

- Show active processes
- List network configuration
- Dump memory (including swap area)
- Stop system
- Duplicate HDD



Time difference

- Systems might not have synchronized clocks
- DON'T change the time for investigated systems



Methods of hiding data

- OS-level:
 - Use dot-files, mark as hidden/system
- Change extension/naming: “password.txt” -> “fun.png”
- Unallocated disk sectors
- Steganography (usable for small data, e.g., secrets)
- Encryption
- Fun stuff: encryption + steganography



HDD Analysis

- If possible (e.g., magnetic HDD) look at the physical level: platter, interfaces, etc.
- Second, look at low-level partitions, volumes, etc.
- Look at the boot process (ROM-> BIOS->BOOTLOADER->KERNEL)
- Inspect virtualization configuration (if implemented)
- Inspect OS configuration

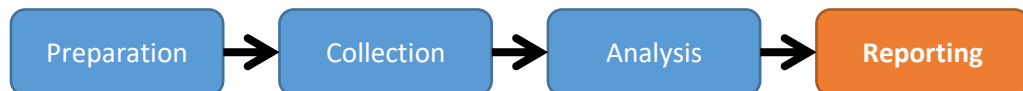
Time difference

- Systems might not have synchronized clocks
- DON'T change the time for investigated systems



Report

- Info of investigator/ Confidence levels
- Identification of case: Date, ID, etc.
- Subject of examination: system, network, etc.
- Summary of findings
- Procedural history: steps taken, detailed findings
- Results and conclusion: server was hacked by X, from Y to Z timeframe, A&B data was accessed; etc.
- Annex



Bibliography

- [http://www.fim.uni-linz.ac.at/lva/IT Recht Computerforensik/Introduction to Computer Forensics.pdf](http://www.fim.uni-linz.ac.at/lva/IT_Recht_Computerforensik/Introduction_to_Computer_Forensics.pdf)
- <https://www.cs.nmt.edu/~df/>