

Computer Forensics Recap Discussion

A space for students to review and discuss key concepts from previous lectures.

Foundations of Computer Forensics

↻ Find electronic evidence

👍 0 🗨️ 0 📌 0

↻ Collect evidence

👍 0 🗨️ 0 📌 0

Data Acquisition and Analysis

↻ Plases - Pre-investigation / Investigation/ Post Investigation

👍 0 🗨️ 0 📌 0

↻ Live, Logical, Sparse

👍 0 🗨️ 0 📌 0

↻ The importance of the witness

The witness must assist to all the step of the procedure and take note of the process.

The witness must not have any access to the case, in order to not being biased

👍 0 🗨️ 0 📌 0

↻ Evidence Image format

Raw, proprietary, AFF, AFF4

👍 0 🗨️ 0 📌 0

File Systems and File Recovery

↻ Recycle bin

👍 0 🗨️ 0 📌 0

↻ User Created Files, User Protected Files, Computer Created Files

👍 0 🗨️ 0 📌 0

↻ Hard disk partitions

	👍👎🔒🔓	
🔓	File carving	
	👍👎🔒🔓	
🔓	Hidden Partitions	
	👍👎🔒🔓	
🔓	Volatile and non volatile memory	
	👍👎🔒🔓	
🔓	Using diskpart command to recover data	
	👍👎🔒🔓	
🔓	Files created by the user and files completed by the computer	
	👍👎🔒🔓	

Legal and Ethical Considerations in Computer Forensics

🔓	Proper consent and warrant required to conduct an investigation	
	👍👎🔒🔓	
🔓	Have to have permission to conduct an investigation	
	👍👎🔒🔓	
🔓	Integrity of files	
	The integrity of files must be intact.	
	It is possible to check if a file as been modified with the help of the hash-value	
	Modified file are mostly not accepted in court	
	👍👎🔒🔓	

Investigation Process

🔓	Phases of investigation	
	Pre investigation, investigation and post investigation	
	👍👎🔒🔓	
🔓	SOP	
	standard operating procedure	

- ↩ Identification of resources
- Preservation
- Documentation & report of the findings
- Result Presentation

•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•	•	•	•	•	•	•	•

