GALGOTIAS UNIVERSITY

CSCN4021
Cyber Crime Investigations

Documenting and Reporting

Course Co-Ordinator

Dr. Jayakumar

Assistant Professor

Department of Computer Science and Engineering
Galgotias University

Documenting Evidence

Documentation

- In this process, a record of all the visible data must be created. It helps in recreating the crime scene and reviewing it. It Involves proper documentation of the crime scene along with photographing, sketching, and crime-scene mapping.

Reporting

- In this last step, the process of summarization and explanation of conclusions is done.
- However, it should be written in a layperson's terms using abstracted terminologies. All abstracted terminologies should reference the specific details.

Documenting Evidence

- Create or use an evidence custody form
- An evidence custody form serves the following functions:
  - Identifies the evidence
  - Identifies who has handled the evidence
  - Lists dates and times the evidence was handled
- You can add more information to your form
  - Such as a section listing MD5 and SHA-1 hash values

Documenting Evidence (continued)

- Include any detailed information you might need to reference
- Evidence bags also include labels or evidence forms you can use to document your evidence

Documenting Evidence (continued)

- Forensic Documentation & Reports " refers to the document or paper trail showing the seizure, custody, control, transfer, analysis, and disposition of physical and electronic evidence.
- It is the process of validating how any kind of evidence has been gathered, tracked and protected. A piece of evidence is worthless without a proper documentation.

Documenting Evidence (continued)

- What is the evidence?
- How did the analyst get it?
- When was it collected?
- Who all have handled it?
- Why did the mentioned persons handle it?
- Where all has the evidence travelled?
- Where the evidence was ultimately stored?

Documenting Evidence (continued)

- In addition to fully documenting information related to hardware and software specs, computer forensic investigators must keep an accurate record of all activity related to the investigation, including all methods used for testing system functionality and retrieving, copying, and storing data, as well as all actions taken to acquire, examine and assess evidence.

Documenting Evidence (continued)

- Not only does this demonstrate how the integrity of user data has been preserved, but it also ensures proper policies and procedures have been adhered to by all parties.
- As the purpose of the entire process is to acquire data that can be presented as evidence in a court of law, an investigator's failure to accurately document his or her process could compromise the validity of that evidence and ultimately, the case itself.

Documenting Evidence (continued)

- For computer forensic investigators, all actions related to a particular case should be accounted for in a digital format and saved in properly designated archives.
- This helps ensure the authenticity of any findings by allowing these cybersecurity experts to show exactly when, where, and how evidence was recovered. It also allows experts to confirm the validity of evidence by matching the investigator's digitally recorded documentation to dates and times when this data was accessed by potential suspects via external sources.

Documenting Evidence (continued)

- It also allows experts to confirm the validity of evidence by matching the investigator's digitally recorded documentation to dates and times when this data was accessed by potential suspects via external sources.