18- Explaining Digital Forensics

Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

Outlines

18.1- Explain Key Aspects of Digital Forensics Documentation

Labs

Lab 26: Acquiring Digital Forensics Evidence

KEY ASPECTS OF DIGITAL FORENSICS

- Digital forensics is the practice of collecting evidence from computer systems to a standard that will be accepted in a court of law.
- Forensics investigations are most likely to be launched against crimes arising from insider threats, notably fraud or misuse of equipment (to download or store obscene material, for instance).
- Like DNA or fingerprints, digital evidence is latent.
- Latent means that the evidence cannot be seen with the naked eye; rather, it must be interpreted using a machine or process.
- As well as the physical evidence (a hard drive, for instance), digital forensics requires documentation showing how the evidence was collected and analyzed without tampering.

DIGITAL FORENSICS REPORTS

- A digital forensics report summarizes the significant contents of the digital data and the conclusions from the investigator's analysis.
- It is important to note that strong ethical principles must guide forensics analysis.
  - ✓ Analysis must be performed without bias.
  - ✓ Conclusions and opinions should be formed only from the direct evidence under analysis.
  - ✓ Analysis methods must be repeatable by third parties with access to the same evidence.
  - ✓ Ideally, the evidence must not be changed or manipulated.

E-DISCOVERY

- A forensic examination of a device such as a fixed drive that contains Electronically Stored Information (ESI) entails a search of the whole drive (including both allocated and unallocated sectors, for instance).
- E-discovery is a means of filtering the relevant evidence produced from all the data gathered by a forensic examination and storing it in a database in a format such that it can be used as evidence in a trial.

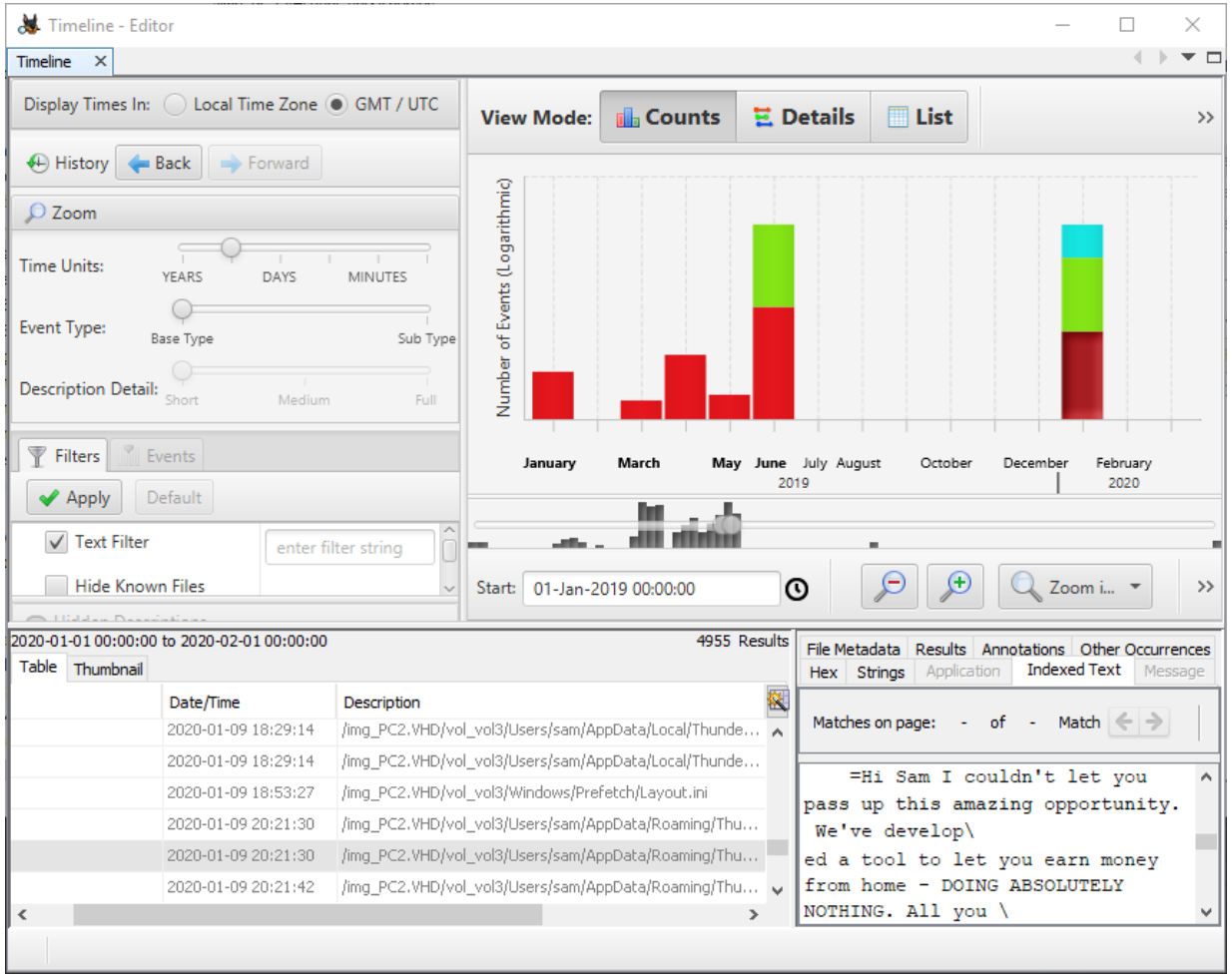
VIDEO AND WITNESS INTERVIEWS

- The first phase of a forensics investigation is to document the scene.
- The crime scene must be recorded using photographs and ideally audio and video.
- Investigators must capture every action they take in identifying, collecting, and handling evidence.
- Remember that if the matter comes to trial, the trial could take place months or years after the event.
- It is vital to record impressions and actions in notes.
- Also consider that in-place CCTV systems or webcams might have captured valuable evidence.

TIMELINES

- A significant part of a forensic investigation will involve tying events to specific times to establish a consistent and verifiable narrative.
- The visual representation of events happening in chronological order is called a timeline.
- Operating systems and file systems use a variety of methods to identify the time at which something occurred.
- The benchmark time is Coordinated **Universal Time (UTC)**, which is essentially the time at the Greenwich meridian.

TIMELINES (cont.)



EVENT LOGS AND NETWORK TRAFFIC

- Digital evidence is not just drawn from analysis of host system memory and data drives.
- An investigation may also obtain the event logs for one or more network appliances and/or server hosts.
- Similarly, network packet captures and traces/flows might provide valuable evidence.
- On a typical network, sensor and logging systems are not configured to record all network traffic, as this would generate a very considerable amount of data.
- On the other hand, an organization with sufficient IT resources could choose to preserve a huge amount of data.

Lab

Lab 26: Acquiring Digital Forensics Evidence