CompTIA Security + 5.0 Risk Management

Filename: comptia-secplussy0501-5-5-basic_concepts_of_forensics
Title: Basic Concepts of Forensics
Subtitle: CompTIA Security+ (SY0-501)

5.5 Incident Response Procedures

- 5.5 Summarize basic concepts of forensics.
  - Order of volatility
  - Chain of custody
  - Legal hold
    - This concept centers around protecting against deletion of data or spoliation of data that could be considered evidence
    - Legal hold is a notification from a legal team to employees instructing them to refrain from destroying data
  - Data acquisition
    - Capture system image
      - Ensuring data duplication
      - Bit-by-bit copy of the data in question
    - Network traffic and logs
      - Network traffic is "catch-it-as-you-go"
      - Logs can contain sensitive information of what users can and cannot do
      - Chronological record of activities
    - Capture video
      - CCTV, traffic intersections, malls, banks
      - Record in magnetic and digital format
    - Record time offset
      - This is the process of matching the local computer time against a known time standard
    - Take hashes
      - Ensures the integrity of the data when collect through the chain of custody until presented in a court of law
    - Screenshots
    - Witness interviews
  - Preservation
    - Ensuring that the data that is taken into custody is not spoiled, manipulated, damaged or misrepresented (whether intentional or unintentional)
  - Recovery
    - Data does not alway reside in default or obvious locations
    - Hidden files, page files, system files, deleted files, formatted drives, TRIM command(*in SSDs zeroing data immediately*), cookies, temp files, mem dumps, metadata, configuration files (*holding the date the file was last accessed*)
  - Strategic intelligence/counterintelligence gathering
    - The methods, techniques, activities used by senior decision makers formulate policies and procedures
    - CounterIntel Gathering is the information and activities used to stop outside intelligence activities and/ or sabatoge on behalf of other organizations
    - Active logging
  - Track man-hours