Micko Wiyono Rohman Soleh

121103028

Summary Kuliah Umum: Pengumpulan Barang Bukti Data Live Streaming

Digital forensic

- Is a practice of collecting, analysing, and preserving electronic evidence for investigate purposes
- What for:
  - o to be used for law
  - o Enhance security posture

- Who:
  - o Cybersecurity agencies
  - o Law enforcement
  - o Professionals
- steps
  - o Identification
  - o Preservation
  - o Acquisition
  - o Analysis
  - o Interpretation
  - o Documentation n Reporting
- Tools
  - o The sleuth kit
  - o Autopsy
  - o FTK Imager
  - o Etc.

- Live Forensics

o Process of digital forensics that being done on live machine

o Usually done to preserve the volatile memory

o When

▪ Perform investigation on critical system that cannot be shut down

▪ Perform malware analysis

▪ Perform investigation when attack/incident going

o What object

▪ Memory

▪ Running services

▪ Network connection

▪ System and network log

o Steps:

▪ Planning

▪ Preparation

▪ Documentation

▪ Volatile data collection

▪ Memory acquisition

▪ Network traffic analysis

▪ Live data analysis

▪ Documentation and reporting

▪ Legal considerations

▪ Post-Investigation step

- Summary

  Digital forensics is a branch of forensic science, especially for the investigation and discovery of digital device content, and is often associated with computer crime. The term digital forensics was originally synonymous with computer forensics but has now expanded to cover all devices that can store digital data. Digital forensics is necessary because usually the data on the target device is locked, erased or hidden.