

# 7. Derived Evidence

- Material created from primary evidence to illustrate how certain conclusions might be drawn.
- Typical examples:
  - Diagram
  - Chart
  - Video

# Digital Forensics Evidence

# 1. Hard disk Evidence

- Most common type of digital evidence
- Typical examples include:
  - Documents
  - Logs
  - Images

## 2. Mobile Phone Evidence

- Increasingly important due to the massive volume of phone calls & SMS messages
  - More difficult than hard disk forensics
  - Not every phone is extractable
  - No hard disk
- Smart phones generate communication data
  - Geo-location data
  - ISPs recording location data

# Use of mobile phone forensics

- Advantage from the investigation's point of view
  - Drawing pictures of communications
  - Racky before a criminal event, such as bank robbery or assassination, has taken place

# Sources of mobile phone forensics

- Information available from network
  - Public network such as Internet
  - ISP records of connections to websites
- Logging activity for system maintenance
  - Highly detailed log of who was doing what
- Information available from Cloud
  - Storage media
  - Cloud services