CYBER ENRICH TRAINING PROGRAM | MODULE II

Mobile Forensics

Mobile Forensics

- Branch of Digital Forensics
- Forensically Sound Data Extraction
- Mobile Forensics Process
  - Seizure
  - Acquisition
  - Analysis/Examination
- Mobile Status (on/off)
- Faraday bag (isolate Cell Phone)

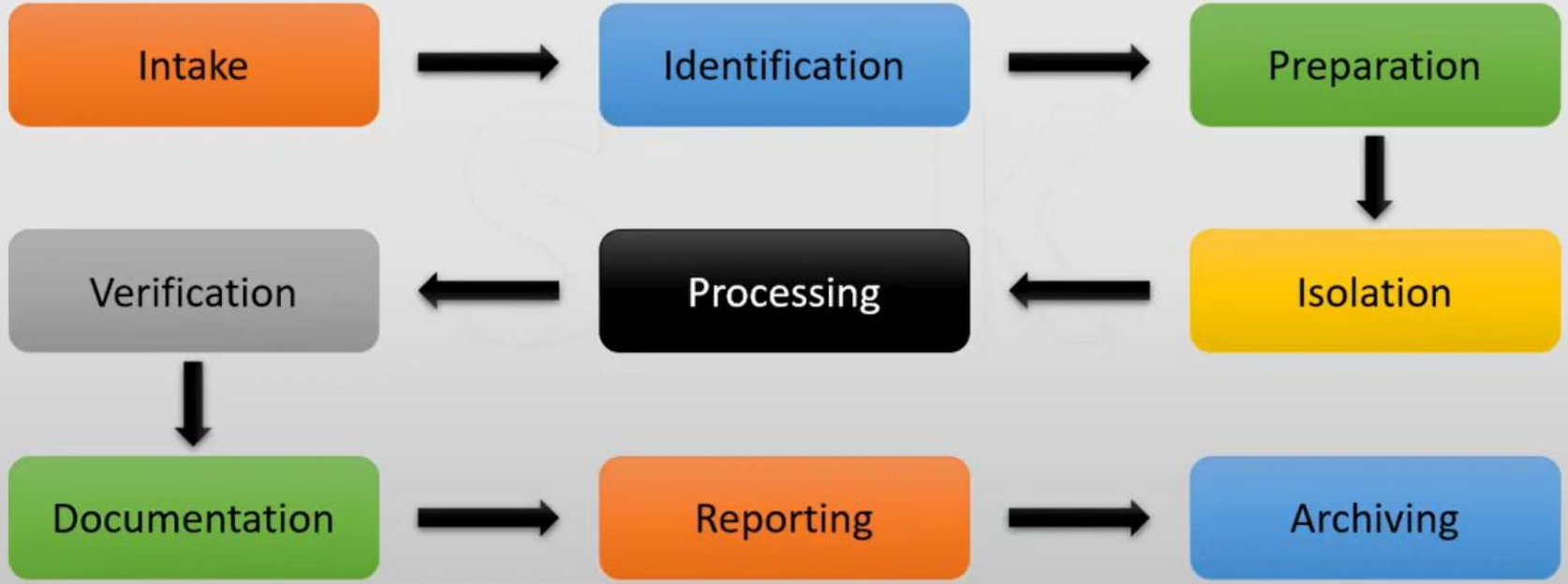
Challenges in Mobile Forensics

- Hardware Differences
- Mobile Operating Systems
- Mobile Platform Security Features
- Preventing Data Modification
- Anti-Forensics Techniques
- Passcode Recovery
- Lack of Resources

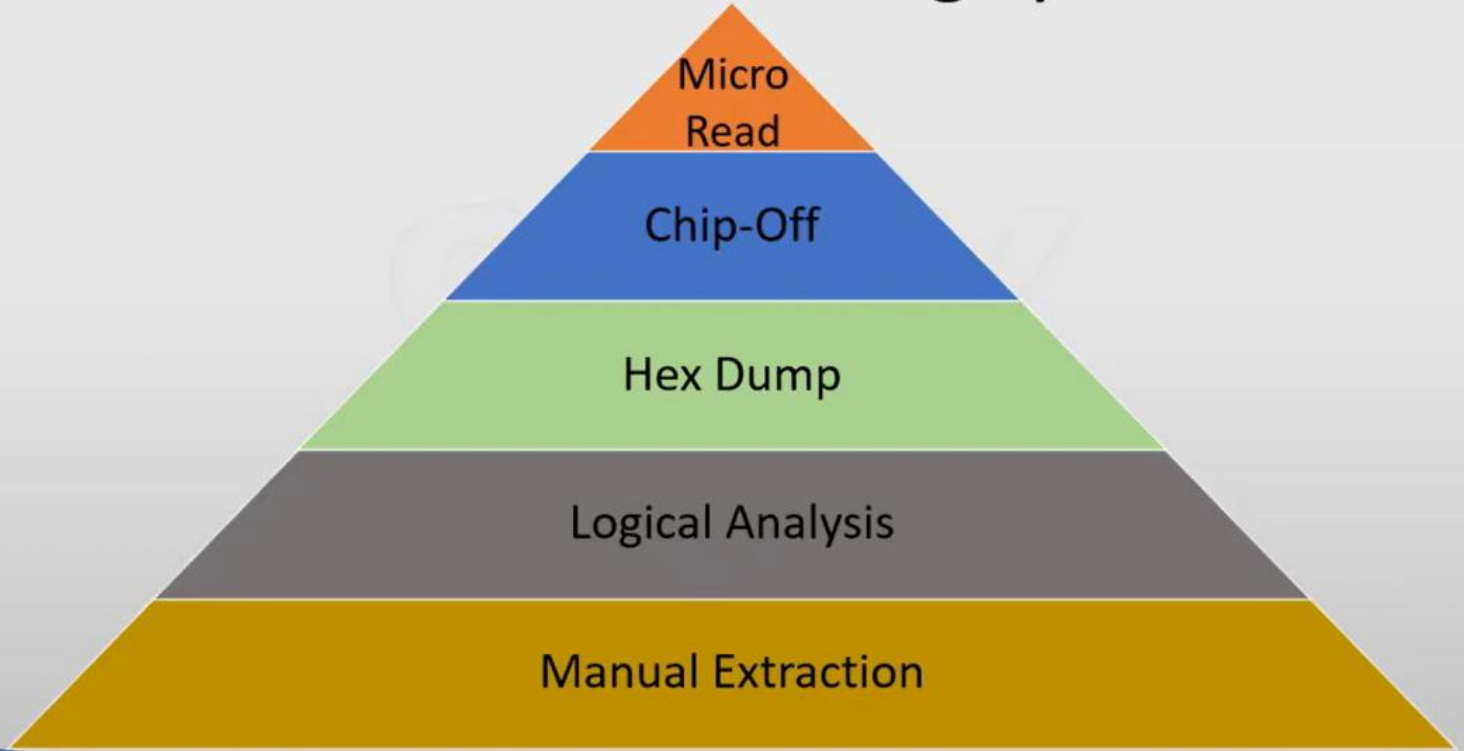
Challenges in Mobile Forensics

- Dynamic Nature of Evidence
- Accidental Reset
- Device Alteration
- Communication Shielding
- Lack of Availability of Tools
- Malicious Programs
- Legal Issues

Mobile Phone Evidence Extraction Process



Mobile Forensics Tool Leveling System



Data Acquisition Methods

- Physical Acquisition
- Logical Acquisition
- Manual Acquisition

Potential Evidences on Mobile Phone

- Address Book
- SMS, MMS, E-mail
- Web Browser History
- Photos, Videos, Music, Documents
- Calendar
- Network Communication, Social Media Data
- Maps
- Deleted Data