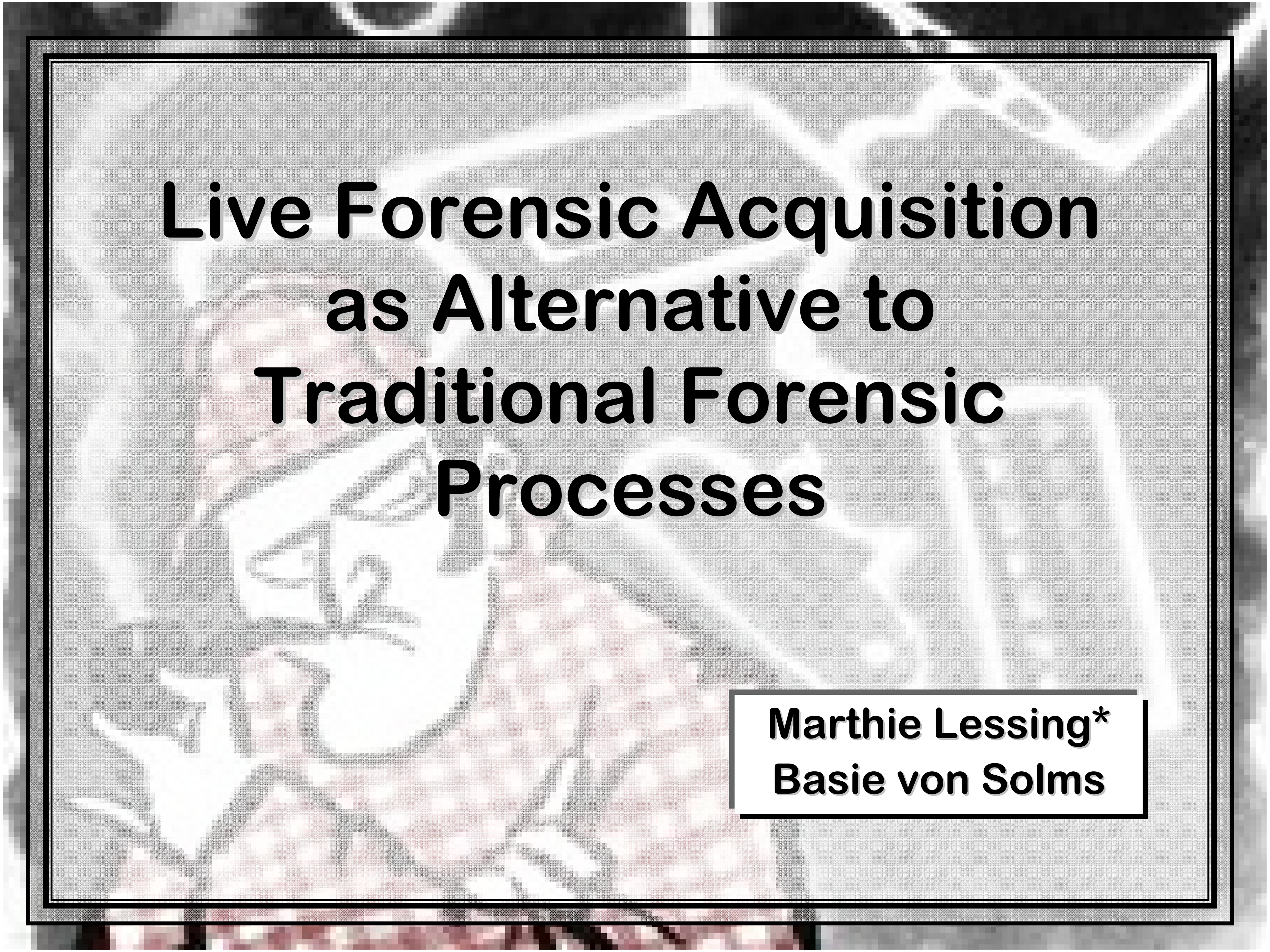


Live Forensic Acquisition as Alternative to Traditional Forensic Processes

Marthie Lessing*
Basie von Solms

Introduction

- The Internet and technology developments introduced a sharp increase in computer related crime
- Cyber forensics aim to act against these electronic offenders

Introduction

- Live forensics remedies some of the problems introduced by traditional forensic acquisition
- Still in the starting phase…
  - theoretically produce comprehensive forensically sound evidence

Cyber Forensics

- *"… The discipline that combines elements of law and computer science…*
- *"… To collect and analyse data from computer systems, networks, wireless communications and storage devices…*
- *"… In a way that is admissible as evidence in a court of law…"*

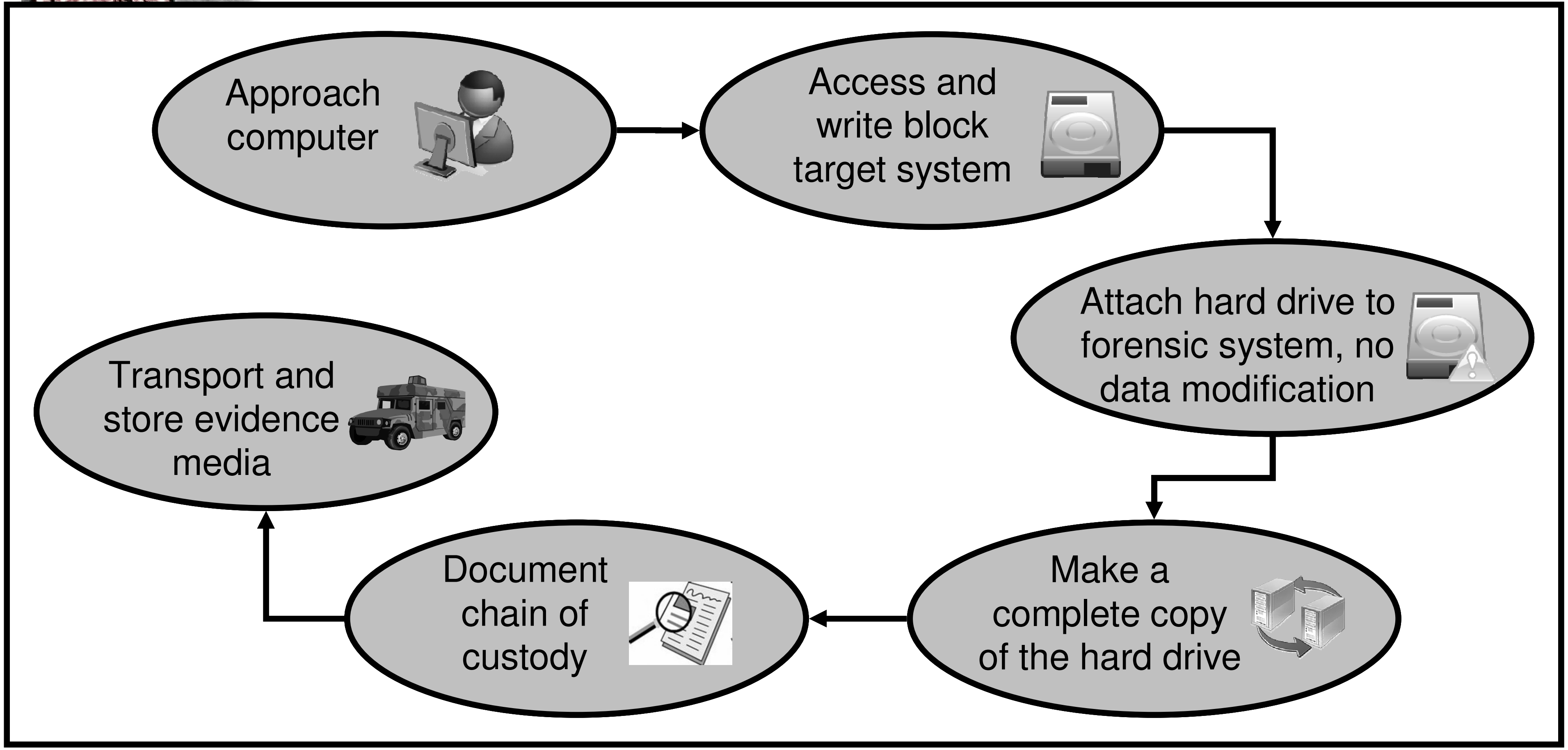
Cyber Forensics History

- FBI started with Cyber Forensics in 1984
- Considered as retrospective profiling
  - – case specific
  - – reactive procedure

Cyber Forensics Methodology

- Acquire evidence without altering or damaging original
- Authenticate that recovered evidence is the same as the originally seized data
- Analyse data without modifying it

Forensic Acquisition



Approach computer

Access and write block target system

Attach hard drive to forensic system, no data modification

Make a complete copy of the hard drive

Document chain of custody

Transport and store evidence media

Forensic Acquisition

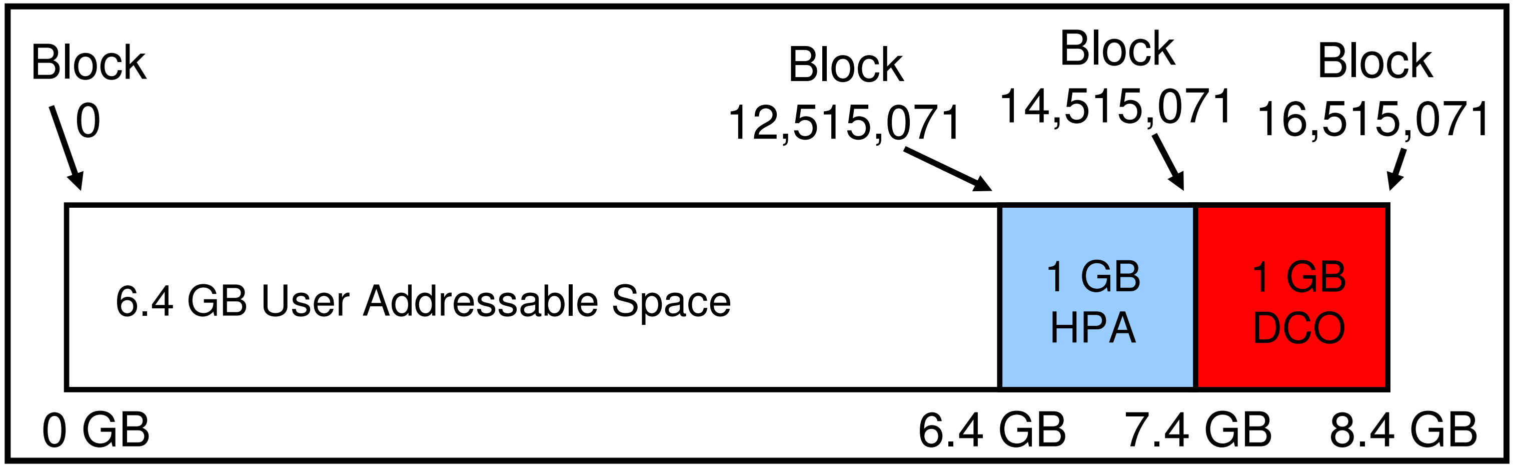
- Isolate system
- Approach computer/access device
  - Pull power plug (dead)
  - Normal administrative shutdown (dead)
  - Keep system running (live)
- Interviews
- Begin timeline establishment

Forensic Acquisition

- Write block target system
  - Allows system to read from external drive
  - Blocks any write commands to external drive
  - Prevents unauthorised modification or formatting of drive under examination
  - Hardware or software blockers

Forensic Acquisition

- Forensically sound copy
  - Bit by bit copy
  - Identify hidden data:
    - HPA (Hardware Protected Areas)
    - DCO (Device Configuration Overlays)



Forensic Acquisition

- Chain of custody
  - Data and devices should be accounted for at all times
  - *"… The gathering and preservation of the identity and the integrity of the evidential proof that is required to prosecute the suspect in court…"*

Forensic Acquisition

- Transport evidence
  – From crime scene to forensic laboratory
  – Guidelines:
    - minimise physical shocks
    - protect from magnetic fields
    - use anti-static bags

Forensic Acquisition

- Store evidence
  - Minimise *bit rot*
  - Guidelines:
    - temperature range of 18 - 20℃
    - humidity of 35 - 40%
    - protect from dust, dirt, grease and chemical pollutants

Current Debate

Traditional (dead) digital forensics

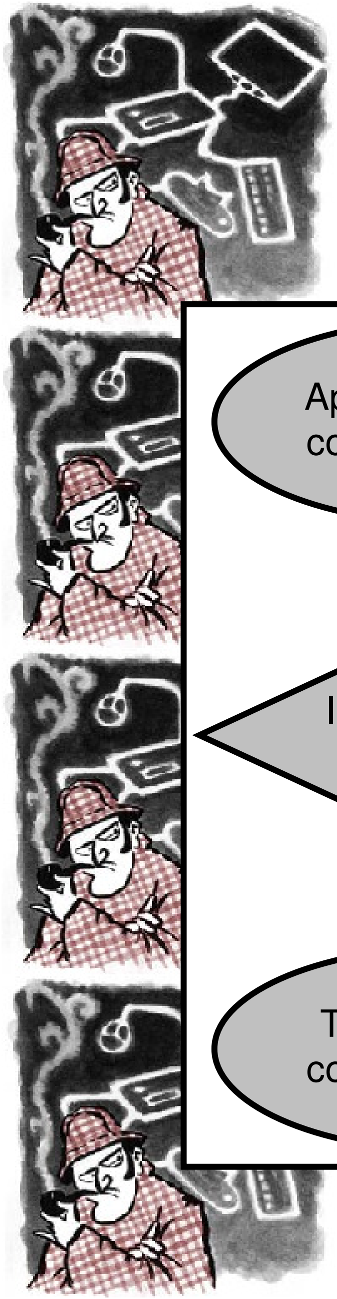
OR

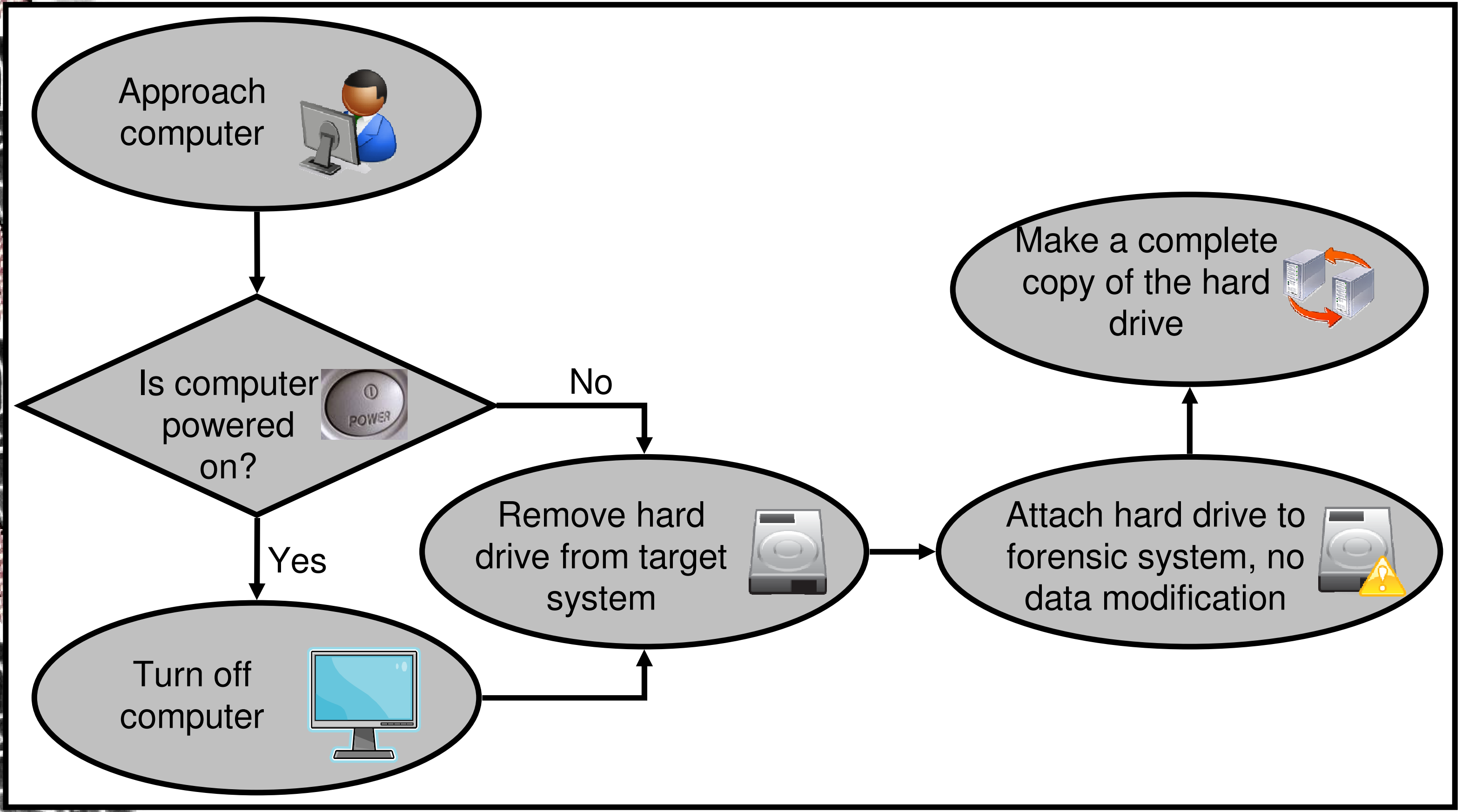
Live digital forensics

Dead Forensics

- *"… Analysis done on a powered off computer…"*
- Pulling the plug to avoid any malicious process from running and potentially deleting evidence
- Creates snapshot of system information and swap files

Dead Forensics





Approach computer
Is computer powered on?
POWER
No
Yes
Turn off computer
Remove hard drive from target system
Attach hard drive to forensic system, no data modification
Make a complete copy of the hard drive

Advantages: Dead Forensics

- Slim chance of data modification
- Small window of opportunity for volatile data retrieval

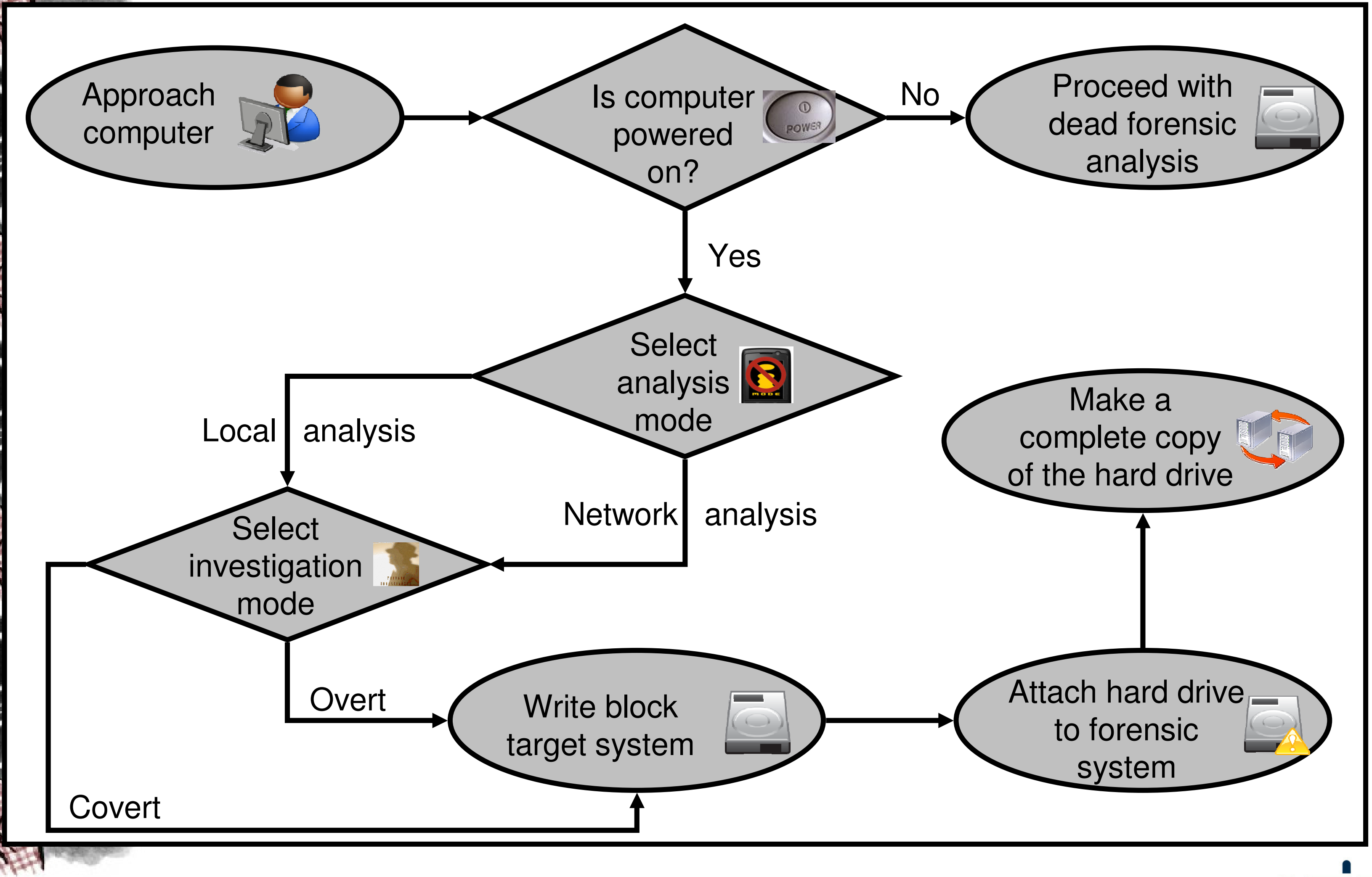
Disadvantages: Dead Forensics

- Cryptography
- Volatile network data
- Gigabytes of data to analyse
- Lack of standardised procedures
- Practical and legal constraints
- Evidence easily rendered inadmissible

Live Forensics

- Analysis is done on a live system
- Developed in response to shortcomings of dead forensic acquisition
- General process remains the same

Live Forensics


Approach computer
Is computer powered on?
No
Proceed with dead forensic analysis
Yes
Select analysis mode
Local analysis
Network analysis
Make a complete copy of the hard drive
Select investigation mode
Overt
Covert
Write block target system
Attach hard drive to forensic system

Real vs Virtual Environment

- Virtual machine requires further analysis
  - copyright notes or vendor strings
  - VMWare specific hardware drivers
  - VMWare specific BIOS
  - VMWare specific MAC addresses
  - installed VMWare tools
  - hardware virtualisation
  - hardware fingerprinting

Advantages: Live Forensics

- Retrieve volatile information
- Limits data gathered to relevant data

Disadvantages: Live Forensics

- Every computer installation is unique
- Data modification a reality
- Slurred images
- Authenticity and reliability more difficult to prove
- Anti-forensic toolkits
- Limited amounts of information gathered

Forensic Soundness

- Evidence can make or break an investigation
- All evidence should be forensically sound to ensure admission in a court of law

Forensic Soundness

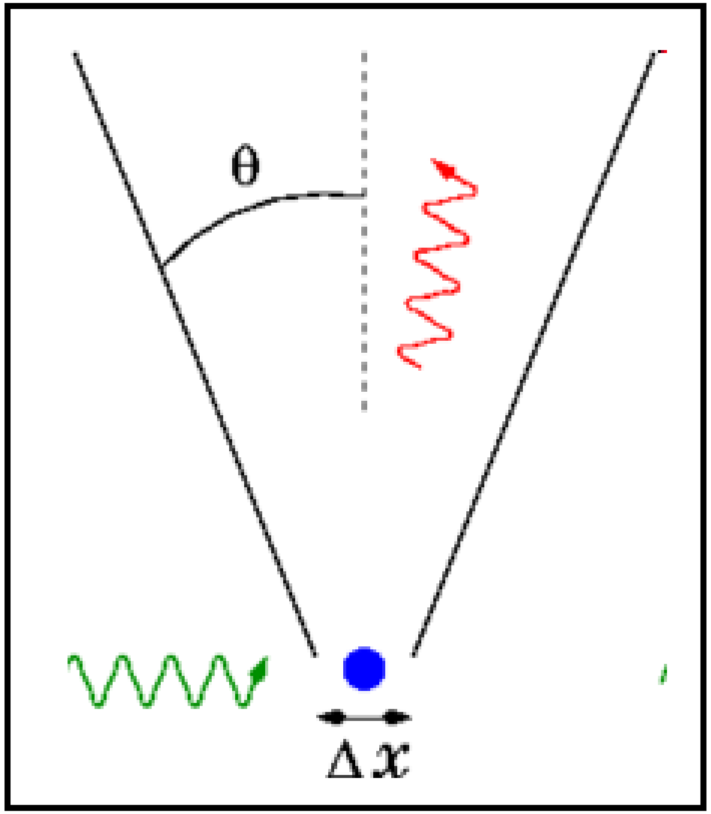
- *"… Created by a method that does not, in any way, alter any data on the drive being duplicated…"*
- *"… Must contain a copy of every bit, byte and sector of the source drive, including unallocated empty space and slack space, precisely as such data appears on the source drive…"*
- *"… The manner used to obtain the evidence must be documented, and should be justified to the extent applicable…"*

Forensic Soundness

- Practical problems
  - Live forensics requires the introduction of software into the suspect system’s memory, altering the original data evidence source
  - Volatile nature of Cyber Forensics
    - Heisenberg uncertainty principle
    - Observer effect
    - DNA analysis

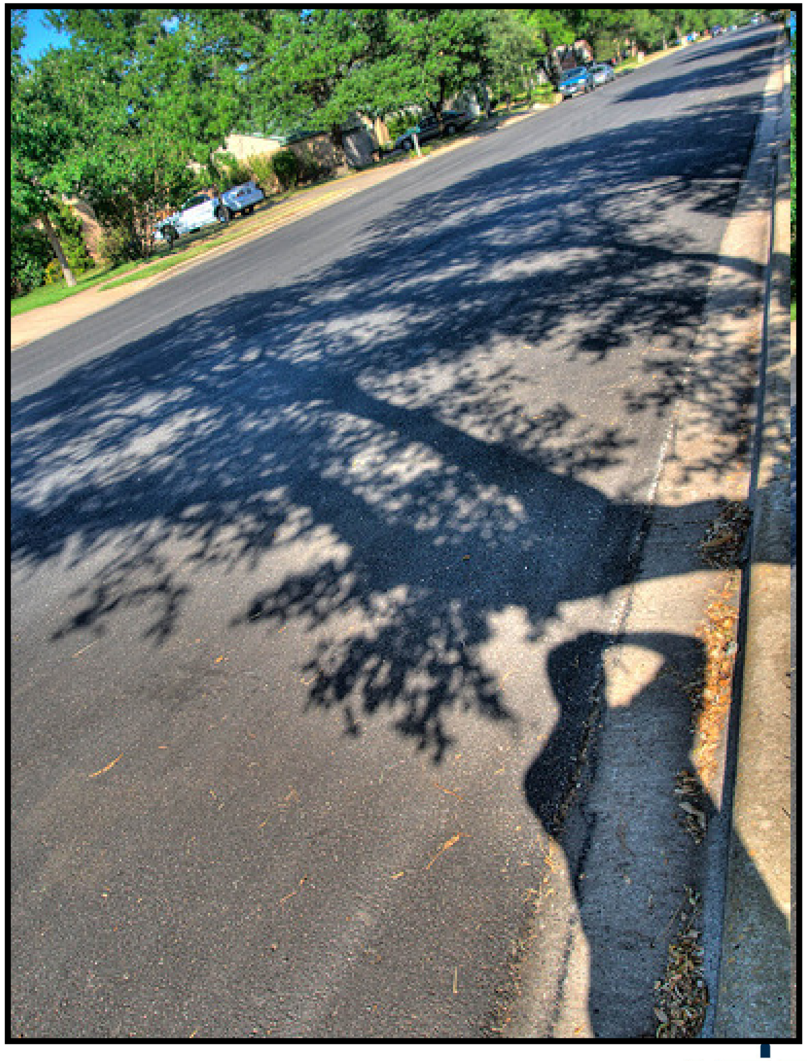
Forensic Soundness

- Heisenberg uncertainty principle



Forensic Soundness

- Observer effect



Forensic Soundness

- DNA analysis

Forensic Soundness

- Key to forensic soundness is documentation
  - Report on evidence origin
  - Report of handling by investigators
  - Ensures validation by courts

Forensic Soundness

- To ensure admission in court
  - *"… derived by scientific method…"*
  - *"… supported by appropriate validation…"*

Conclusion

- Intense research still needed
  - Preliminary study shows that live forensics measures up to traditional digital forensics
- Correct technique allows forensic soundness
  - Minor controlled modifications should be allowed, without rendering data inadmissible

marthie.lessing@gmail.com