Between Life and Death

Problems with Live Forensics

Marthie Lessing

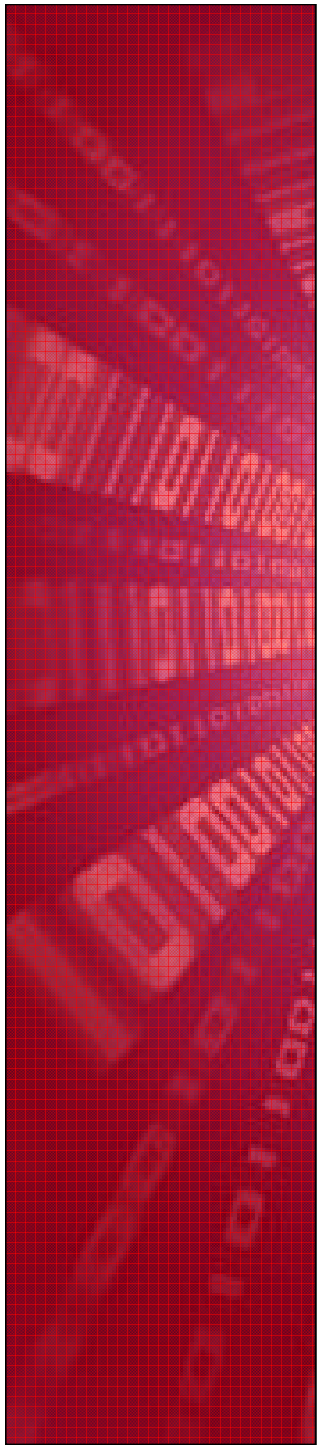
Cyber Security Expert, CSIR

Introduction

- Traditional (dead) digital forensics is a technique to assist forensic investigators in solving crimes that involve computers
- Live digital forensics are much more versatile and allows digital investigators to retrieve more data from computers

Introduction

- Live forensics remedies some of the problems introduced by traditional forensic acquisition
- Still in the starting phase in SA…
  - 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…

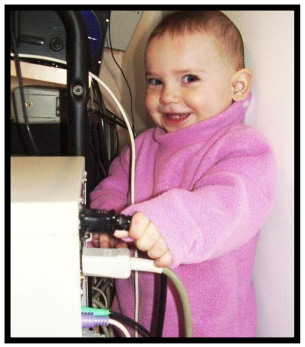
… In a way that is admissible as evidence in a court of law…"

Cyber Forensics Methodology

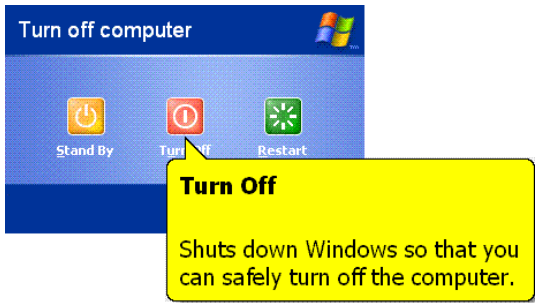
- Acquire evidence without altering or damaging original
- Authenticate that recovered evidence is the same as the originally seized data
- Analyse data without modifying it

Current Debate

Dead digital forensics



OR



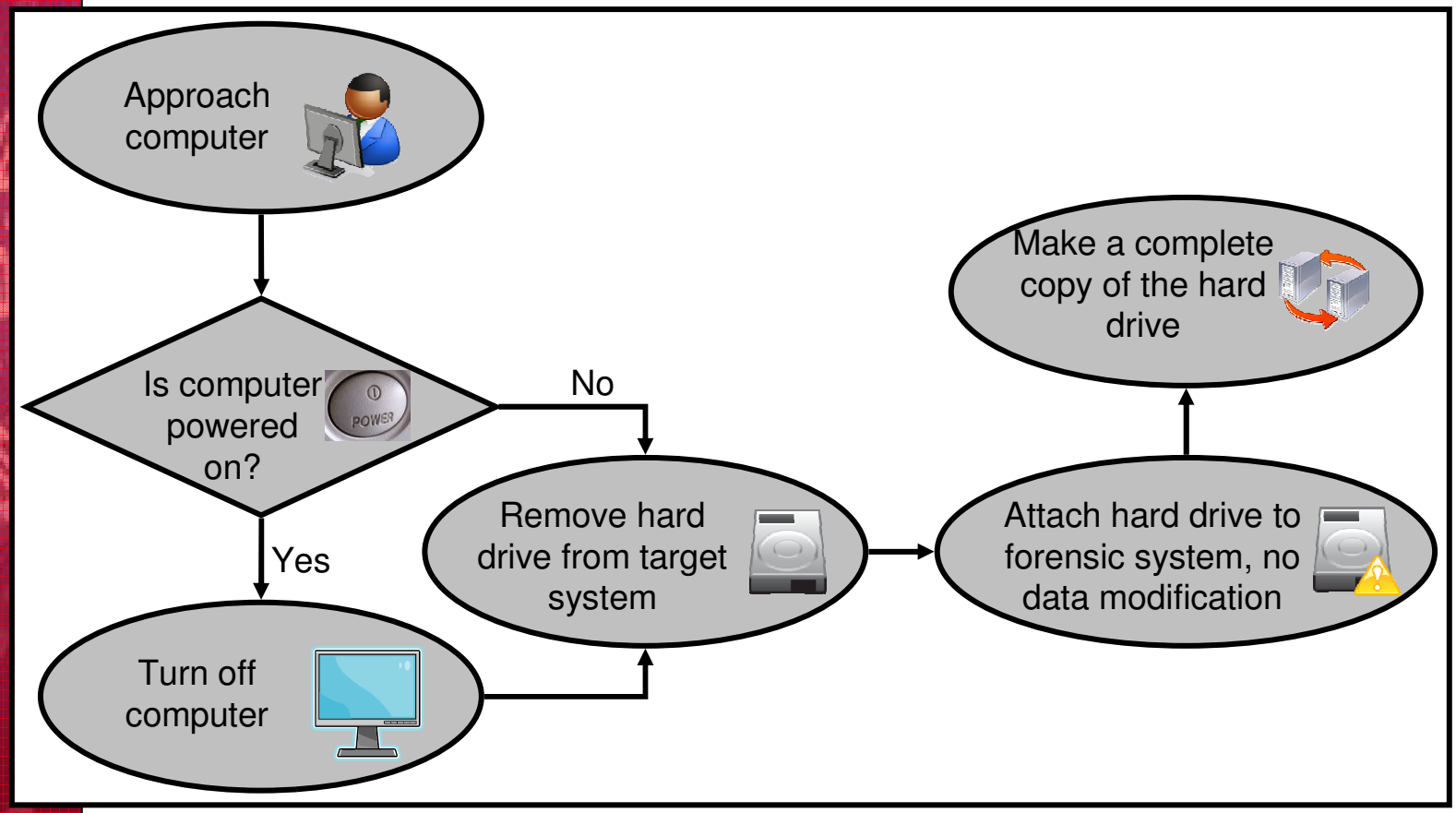
Live digital forensics

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



Advantages: Dead Forensics

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

Disadvantages: Dead Forensics

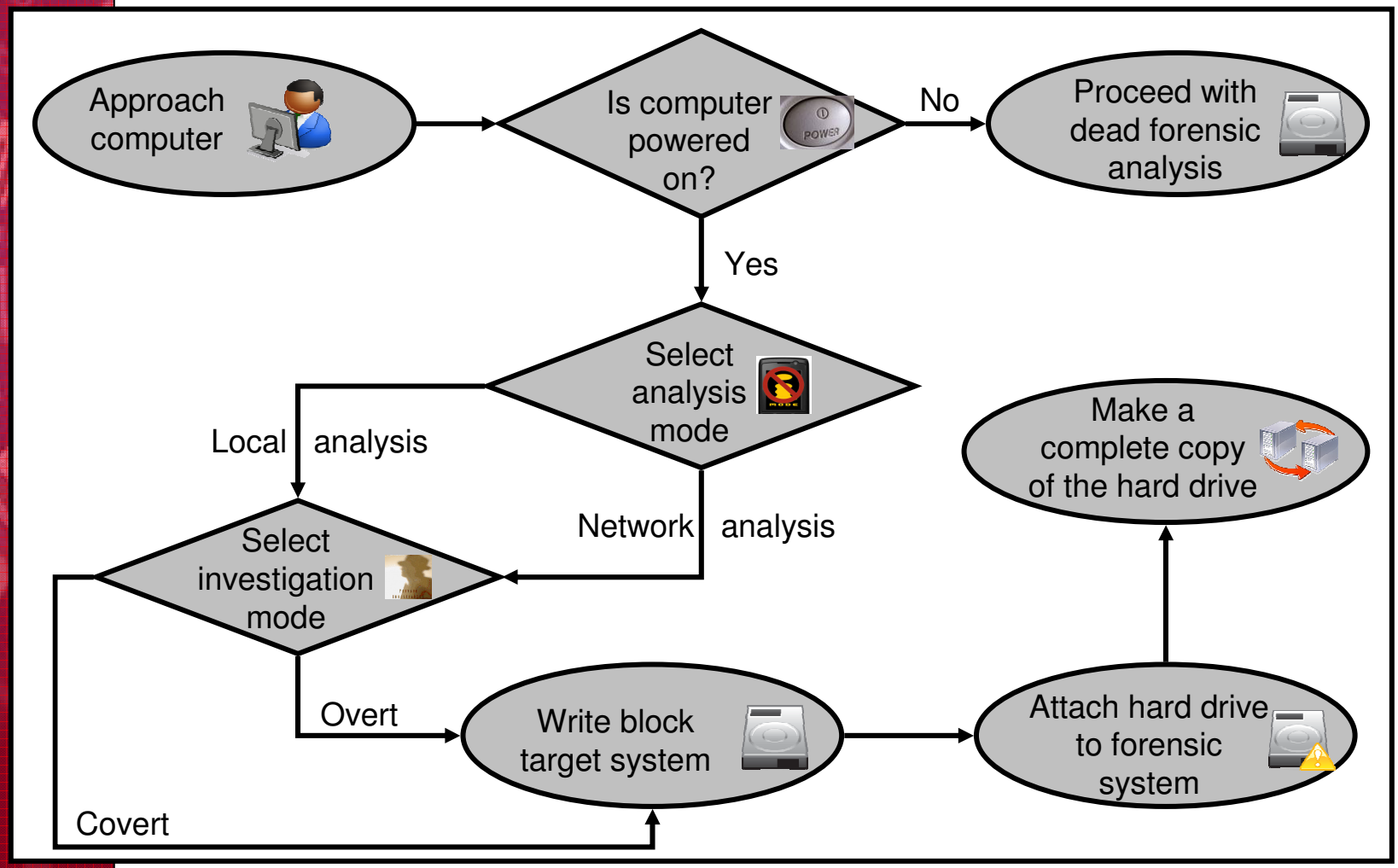
- Cryptography
- Volatile network data
- Gigabytes of data to analyse
- Lack of standardised procedures
- Practical and legal constraints
- Evidence easily rendered inadmissible

Live Forensics

"… Analysis done on a live computer system…"

- Developed in response to shortcomings of dead forensic acquisition
- General process remains the same

Live Forensics



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

Goal: Forensic Soundness

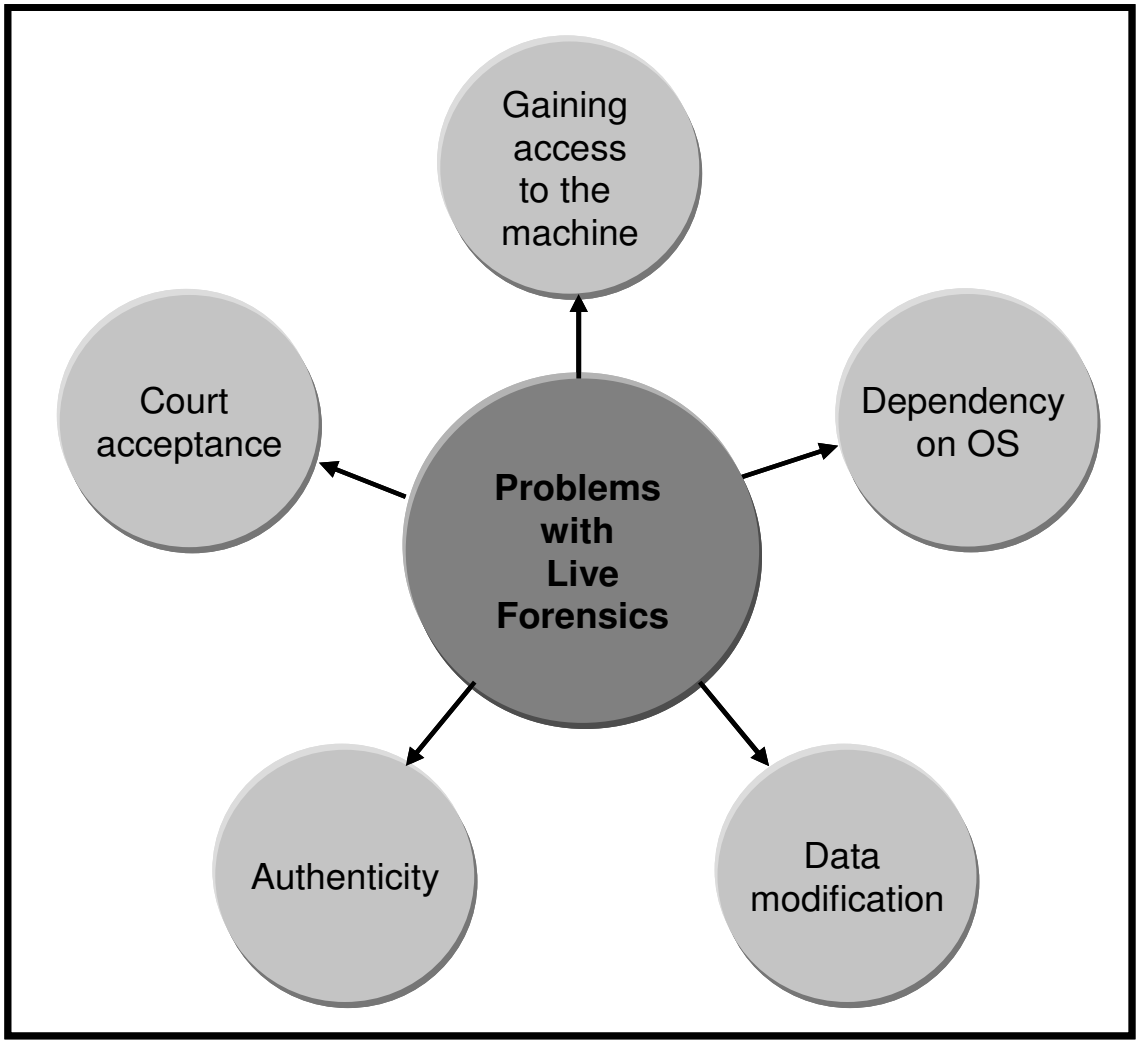
- Evidence can make or break an investigation
- All evidence should be forensically sound to ensure admission in a court of law

"… 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…"

Forensic Soundness

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

Problems with Live Forensics



CSIR
our future through science

Gaining Access

- Overt vs Covert

Acquisition Dependant on OS

- Potential for modifying evidentiary data
- Success depends on knowledge
- Some OS allows modifications

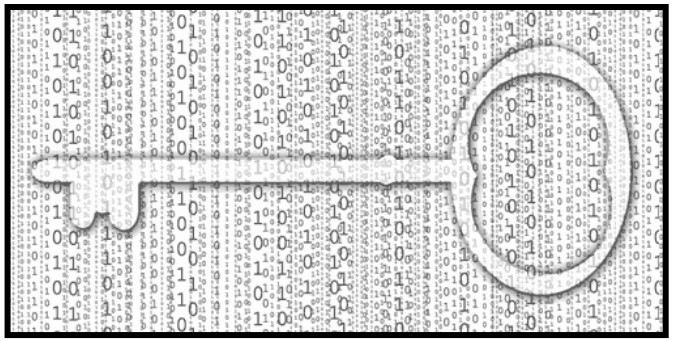
Data Modification

- Investigators can accidentally ruin evidence
- Anti-forensic programmes
- Slurred images

Authenticity

- Admissibility in court
- Evidential weight

- Possible controls:
  - Hashing techniques
  - Digital signatures
  - Timestamps
  - Checksums



Court Acceptance of Technology

- Education of judicial system
- Continuous forensic training

Live Acquisition Techniques

- Software techniques
  - Memory Dump
  - NotMyFault
  - Live Response Tool Kit

Live Acquisition Techniques

- Hardware techniques
  - Tribble Device
  - PCI Expansion Card
  - SPARC OpenBoot
  - COFEE

Conclusion

- Intense research still needed
  - Preliminary study shows that live forensics measures up to traditional digital forensics
- Correct technique allows forensic soundness

mlessing@csir.co.za
marthie.lessing@gmail.com