Computer Forensics

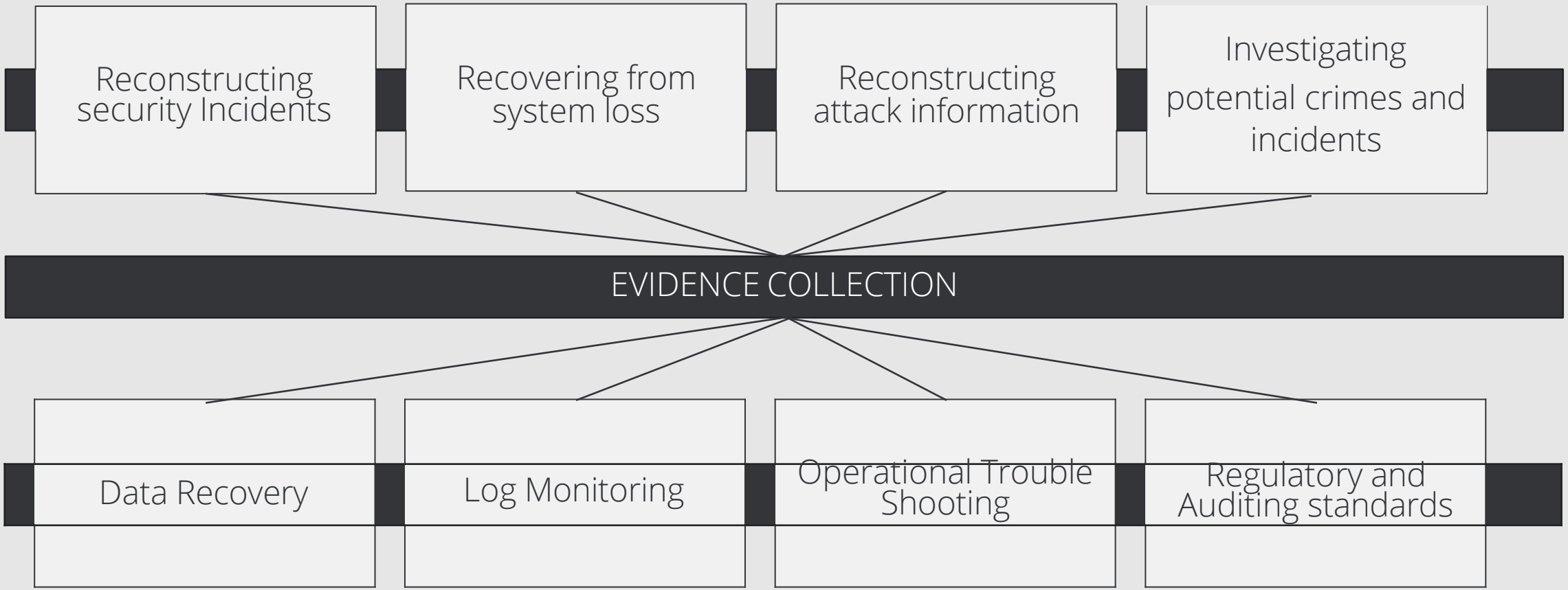
Computer Forensics

The application of science to the identification, collection, examination, and analysis, of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.

- *Identify how, what and depth of a cyber incident*
- *Identify the scope of a cyber incident (though the collection, analysis and preservation of forensic evidence*
- *Integrity remains vital*

SWINBURNE UNIVERSITY OF TECHNOLOGY

Purpose of Information Collection



Computer Forensics VS Data Recovery

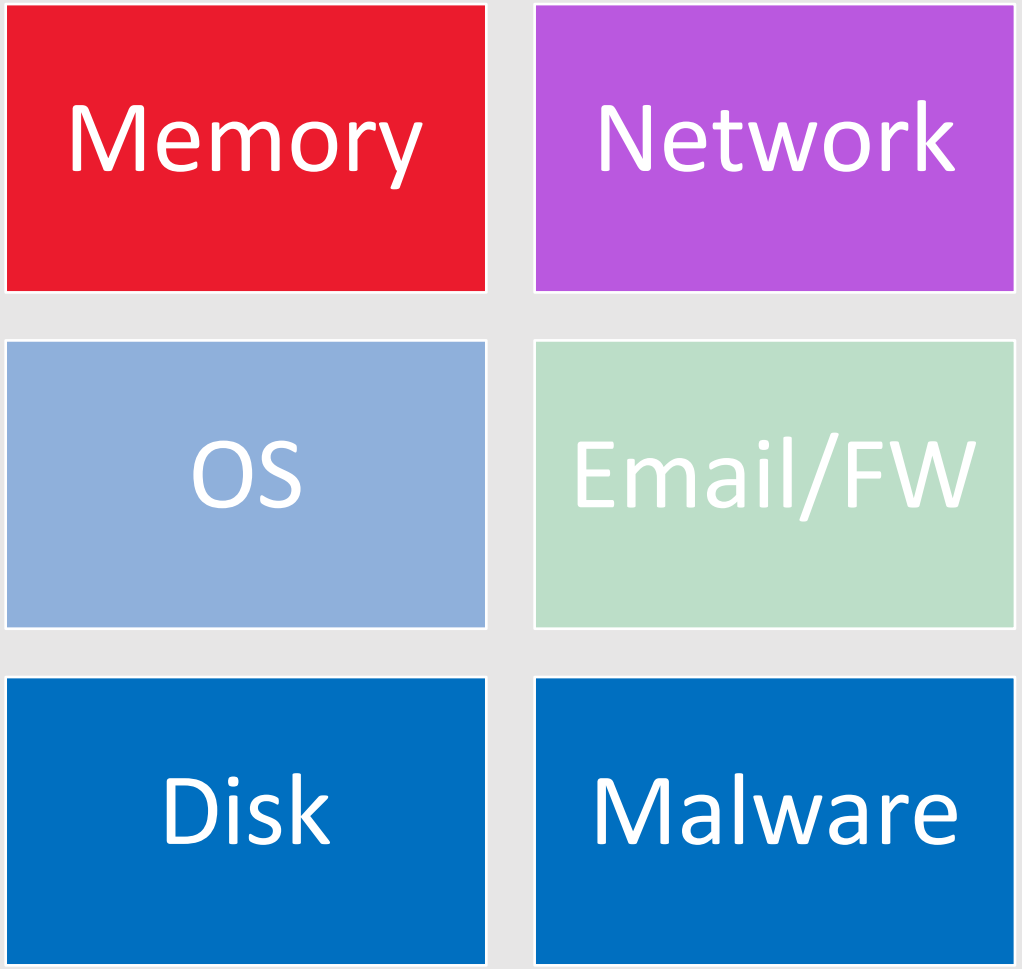
Digital Investigation	Data Recovery
Data collected securely	Information retrieval
Determine surrounding aspects of data	Cause maybe disk lost, power incident, crash or accident
Legal considerations	

Standards

- ISO/IEC 27xxx
- NIST 800-86
- Others (SANS, Interpol)

Areas of Study

Example areas, but not exhaustive



Public Investigations

- Government agency cases involved with criminal aspects and prosecution
- Search Warrant
- Adhere to legal processes
- Cases may not just be “cyber” specific but also typical offences

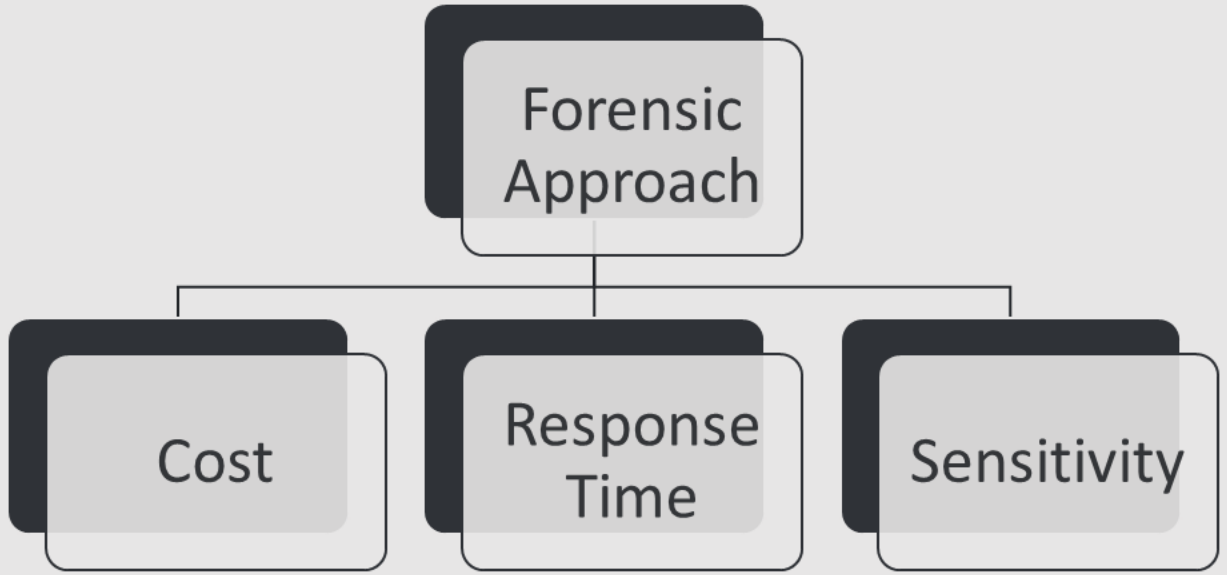
Private Investigations

- Corporate investigations, non-law enforcement bodies, individuals and lawyers
- Not criminal law, but may end up so
- Governed by internal policies

Forensic Team and Considerations

Forensic personnel

(Requires a mixture of partners and positioning)



Cost: Setup & Running, training, outsourcing
Response: Geography, SLA, data concerns
Sensitivity: Data, privacy, conflict of interest

Skills and Conduct

Conduct

- Ethics, morals and high standards
- Maintain objectivity, experience not emotion
- Credibility through confidentiality
- Training and upskilling
- Keeping up to date on training and technology

SWINBURNE UNIVERSITY OF TECHNOLOGY

Policy and Guidelines

Forensic personnel are guided by organisational policy and guidelines

Policy

- Roles and responsibilities
- Chain of command, teams, who makes decisions
- Legal constraints
- Safeguarding information
- Policy review

Guidelines

- Tasks and procedures documented
- Uphold integrity
- Define evidence handling process
- Process review

Lab and Resources

Physical Lab

- Secured as to control environment access and limit lost, corrupted or destroyed evidence
- Safe and/or secure lockers
- Visitors log
- Locking mechanism, audit trail
- Audit process

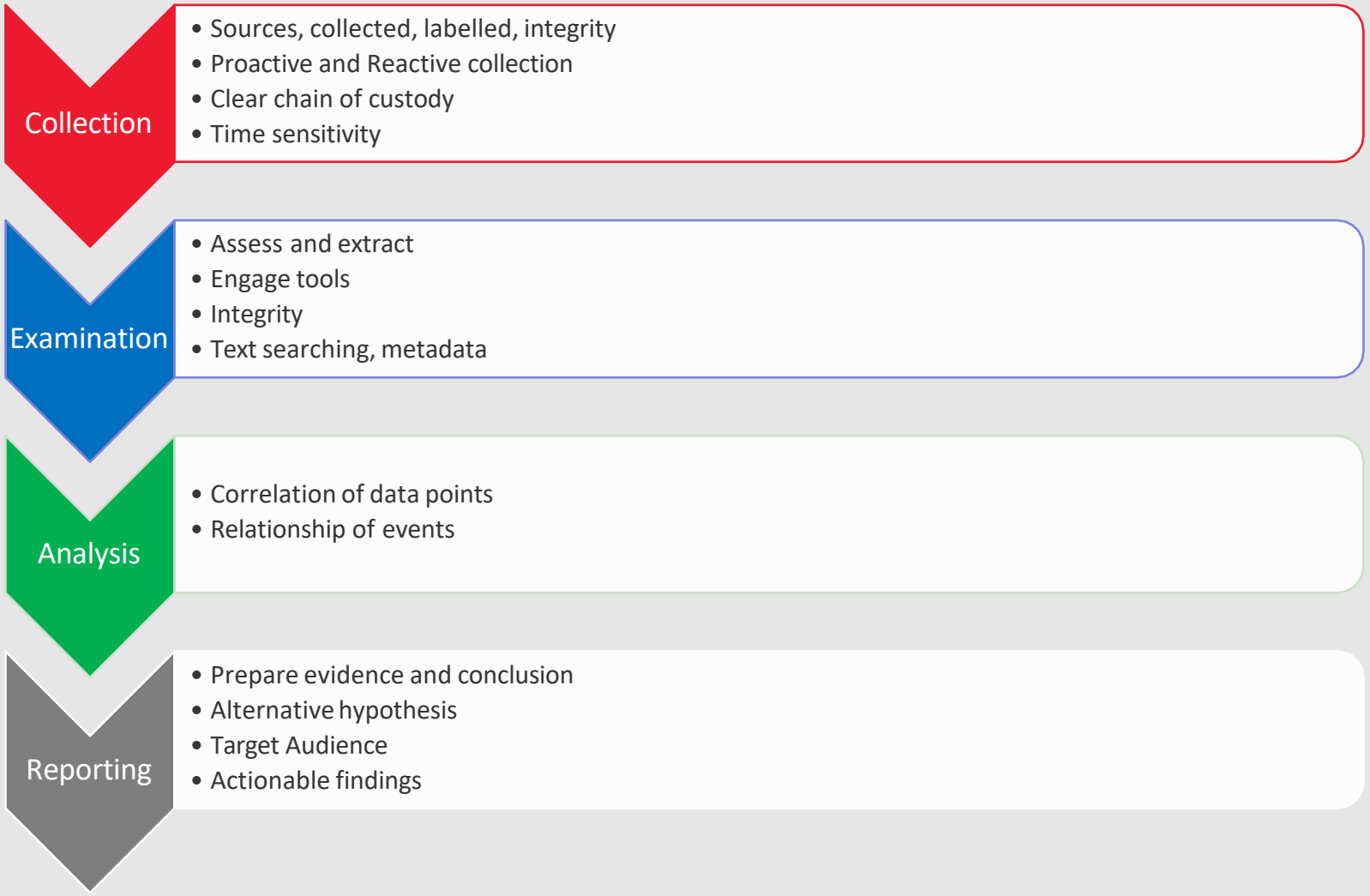
*At a minimum

Resources

- Multiple OS versions, devices
- Range of cables and storage media
- Potable device and tooling
- Range of software and specific programs
- SIFT, COFEE, Volatility,...

*At a minimum

Forensic Lifecycle



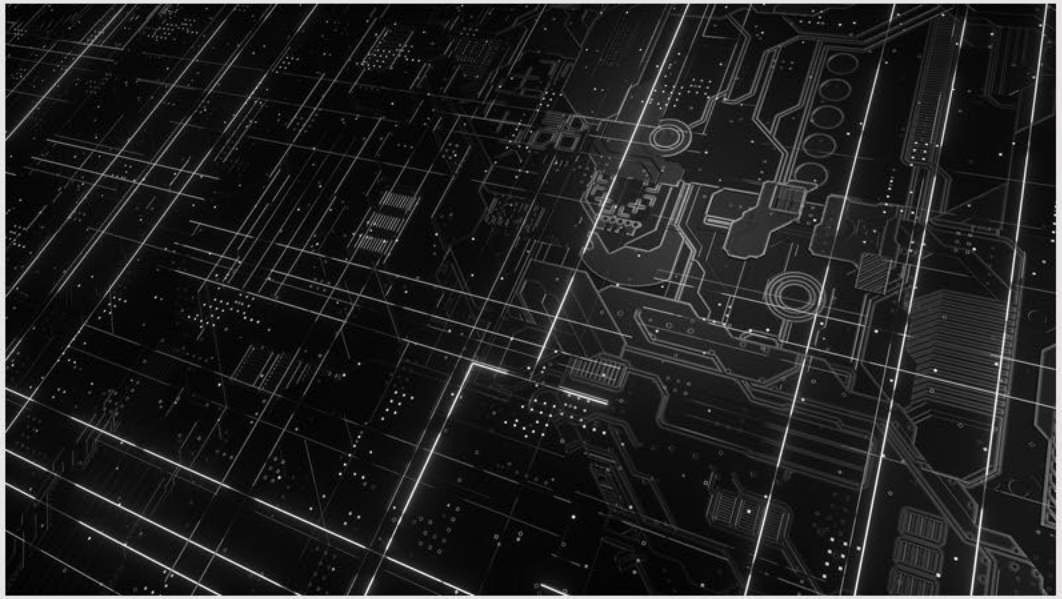
Anti-Forensics

Just as those who seek to retrieve evidence, attackers may sabotage or interfere with the process

- Removal of event indicators
- Expenditure increase for forensic process (time & skill)
- Inducing doubt or leaving weak indications of activity (blending in, needle in a haystack)

Traditional Methods

- Changing time stamps (e.g. Timestomp)
- Zeroing or writing other data to known sectors
- Challenge: Not the process of overwriting, but where and what
- Common data stores an attacker might seek to alter (logs, events)
- What degree would be less suspicious, remove all, or alter some?



Cryptography and Steganography

Encryption

- Disk, Application, File level
- Encryption can be loud given its presence, self-destruct
- Network level, common http protocols, protocol manipulation
- Application level, packers, password or environmental variables

Steganography

- Medium for hiding, transporting data (plaintext and encrypted alike)
- Common file formats (e.g., jpeg, mp3, pdf)
- Hidden in locations not reachable/investigated by forensic tools
- Hidden in plain sight (among say image bits), plain or encrypted

Minimisation

To what degree to altering and tampering of log and other data types raise more suspicions?

- Alter the mode of operation: process injection, live bootable media
- Process/Memory injection, buffer overflow, run within another process' address space

Vulnerabilities matter, point of entry vs ability to operate within another program

- Would standard operations be through an injected process, or blending in as a normal user (what restrictions would either have on lateral movement for example)?

Adopting a working profile of the typical user

C&C posting comments on common sites, abusing trusted domains

Avoid forensic searches all together, alter file header (e.g. Transmogrify)

Countermeasures

Beating Anit-Forensics

- Promiscuous mode devices found on a network
- DNS, location of source and destination frequently used or not?
- File hashes
- Block USB?
- Data stores, event management (SIEM)