

Digital Forensics in Privacy-aware World

Sebastian Edassery
Sep 2019



Agenda

Digital Forensic

- Introduction
- Methodology & Practice

Challenges to Privacy in Digital Forensic

- Technology Perspective
- Tool Perspective
- User Perspective
- Investigator Perspective
- Case Studies

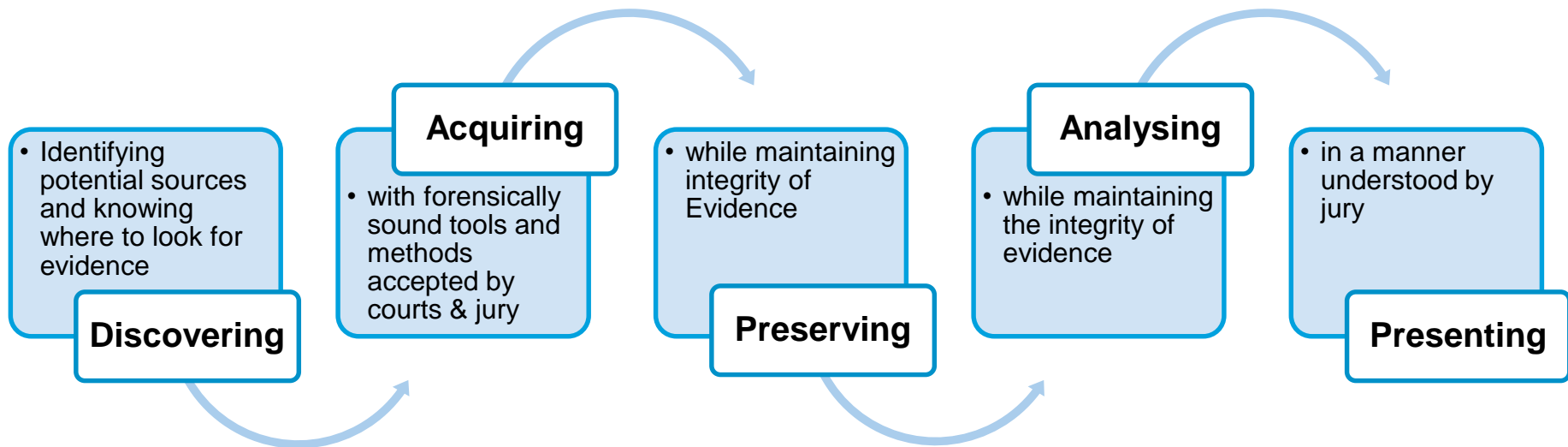
Proposed solution



Digital Forensics


Introduction to Digital Forensics


Branch of forensic science dealing with methodologies to preserve, recover, and document electronic evidence.





Digital Forensic Methodology & Practice

Reliable and tested tool sets
Systematic and Scientifically proven procedures
Typically 4 phases.


Acquisition
Identifying and gathering electronic evidence.
Initiating point for Chain of Custody documentation.


Preservation
Non-destructive examination.
Conserving the original.
Examination without fear.
Availability of original for court reviews.


Analysis
A structured and detailed Examination.
Audit trail.
Interpret


Presentation
For Judicial Review.
Acceptance depends on

- Tools used & Process followed
- Quals & Experience Examiner
- Manner and Language of reporting and presentation

Agenda

Digital Forensic

- Introduction
- Methodology & Practice

Challenges to Privacy in Digital Forensic

- Technology Perspective
- Tool Perspective
- User Perspective
- Investigator Perspective
- Case Studies

Proposed solution



Challenges to Privacy in Digital Forensic

Technology Perspective

- Multiple frameworks and models.
- Hard to design a fully protected system.
- NIST Challenges – Mainly from Cloud Forensic Standards
- TRIM in SSD Devices/ Pen Drives

Tool Perspective

- Authentication and Chain of Custody
- Recovery of Deleted data
- Dependencies with multiple Cloud systems
- Meta data, Log Formats, Time Zones
- Virtual Machine Environment

Challenges to Privacy in Digital Forensic

User Perspective

- ignorance about processing and management of data
- Ignorance about potential avenues for misuses, abuses

Investigator Perspective

- Evidence Analysis - Where to stop
- Criminal Intent VS criminal action
- Secondary Evidence
- Ethical Conduct

Case Studies



Agenda

Digital Forensic

- Introduction
- Methodology & Practice

Challenges to Privacy in Digital Forensic

- Technology Perspective
- Tool Perspective
- User Perspective
- Investigator Perspective
- Case Studies

Proposed solution



Proposed Solution

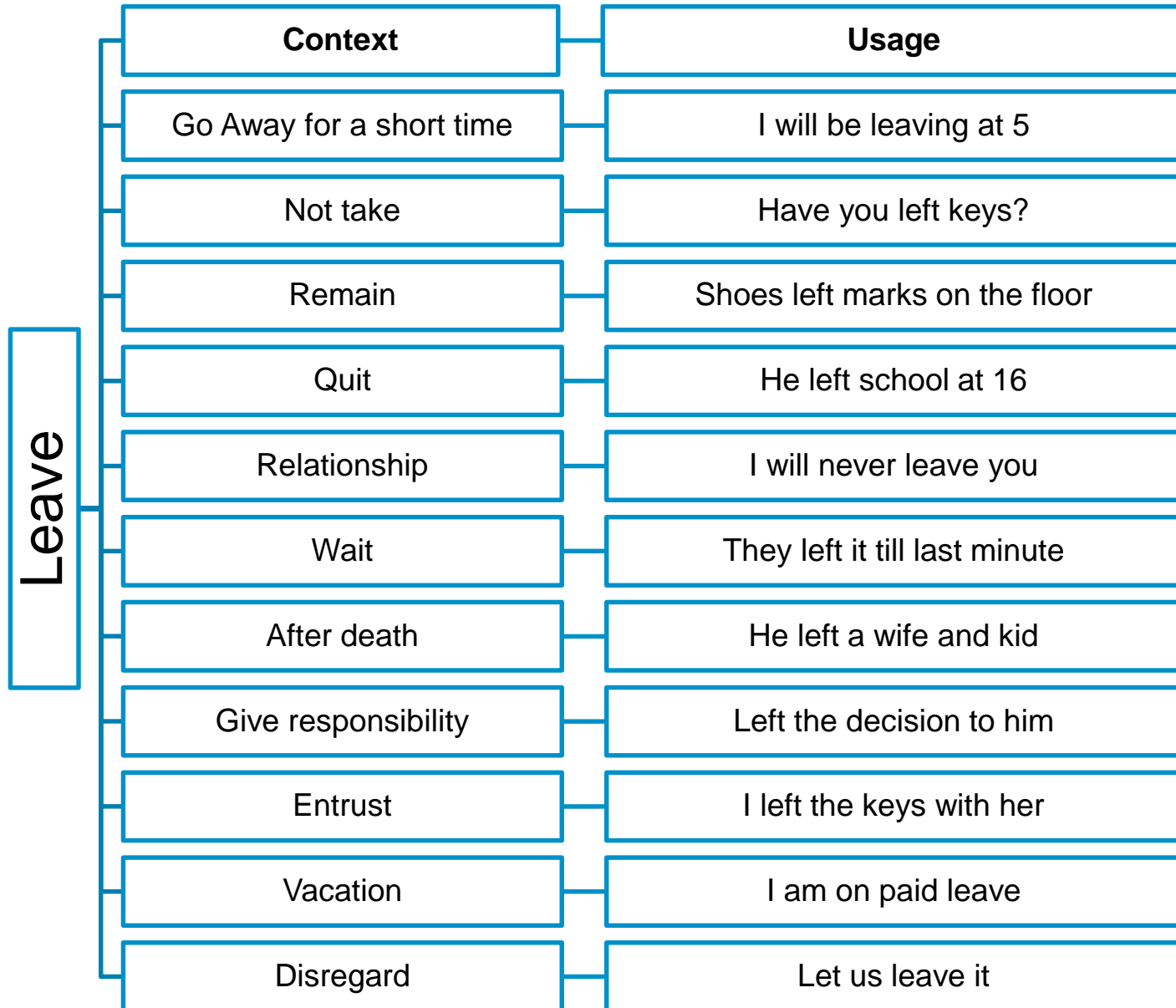
Forensic Imaging, Validation & Recovery

- Bit to bit replication using approved forensic tools
- validation using hashing techniques
- Recovery – Deleted, Over written etc

Keywords, Validation & Contextual Search

- Develop keywords specific to the case
- Validate with appropriate supervisory control
- Context based search

Contextual Search



Proposed Solution

Forensic Imaging & Validation & Recovery

- Bit to bit replication using approved forensic tools
- validation using hashing techniques
- Recovery – Deleted, Over written etc

Keywords, Validation & Contextual Search

- Develop keywords specific to the case
- Validate with appropriate supervisory control
- Run first level of context based search

Refine & Revise Key words

- Based on results thrown out
- Maintaining audit trails
- And do it Ethically

Recap

Digital Forensic

- Introduction
- Methodology & Practice

Challenges to Privacy in Digital Forensic

- Technology Perspective
- Tool Perspective
- User Perspective
- Investigator Perspective
- Case Studies

Proposed solution

