Higher Education Academy

BIRMINGHAM CITY University

Digital Forensics Case Studies

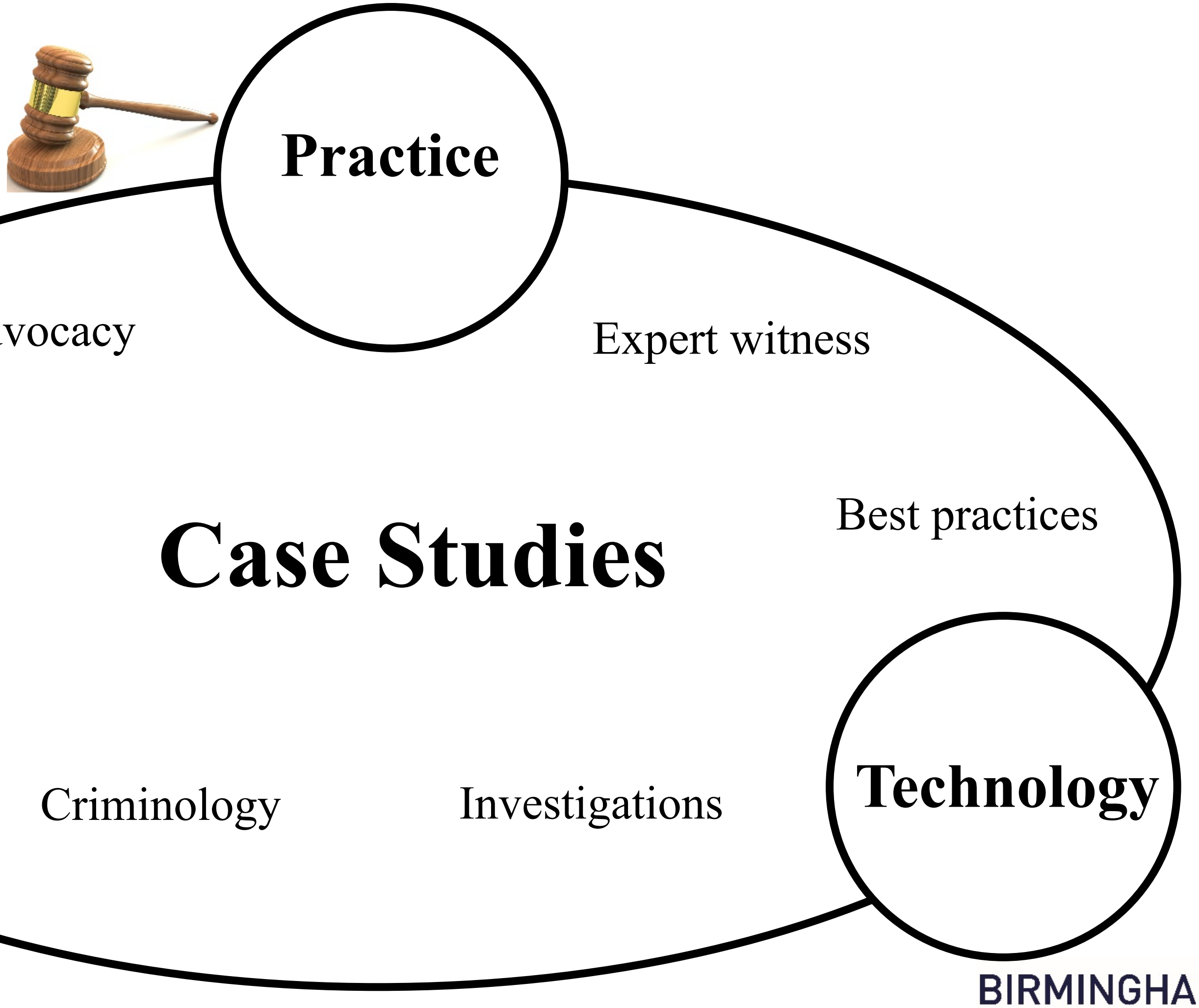
Dr Syed Naqvi

syed.naqvi@bcu.ac.uk

Outline

- Introduction
- Digital Forensics – Standard procedures
- Case studies
  - Forensic soundness when manual processing is required
  - Cloud forensics
  - Virtual machines (VM) forensics
  - Acquisition of evidence from a live source
  - Smart environments forensics
- Conclusions and perspectives

Overview



Practice

Advocacy

Expert witness

Psychology

Case Studies

Best practices

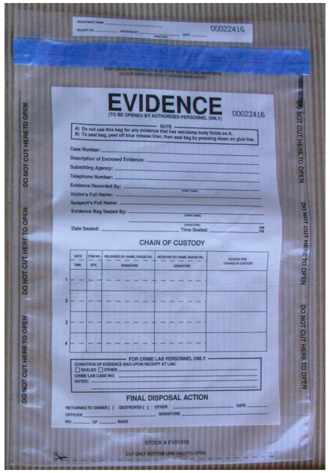
Law

Criminology

Investigations

Technology

Collection and Preservation



Digital Forensic Analysis

- Generally third party specialised intervention
  - Evidence collection, examination, analysis and presentation

EnCase®
FTK
Autopsy®
OPEN | EXTENSIBLE | FAST
nuix
cellebrite
mobile data secured
.XRY
OXYGEN FORENSICS
Helping good people to make this world safer
Relativity®

Digital Forensic Case Studies

1. Forensic Soundness

When HD can't be removed …
Device needs to be powered on …

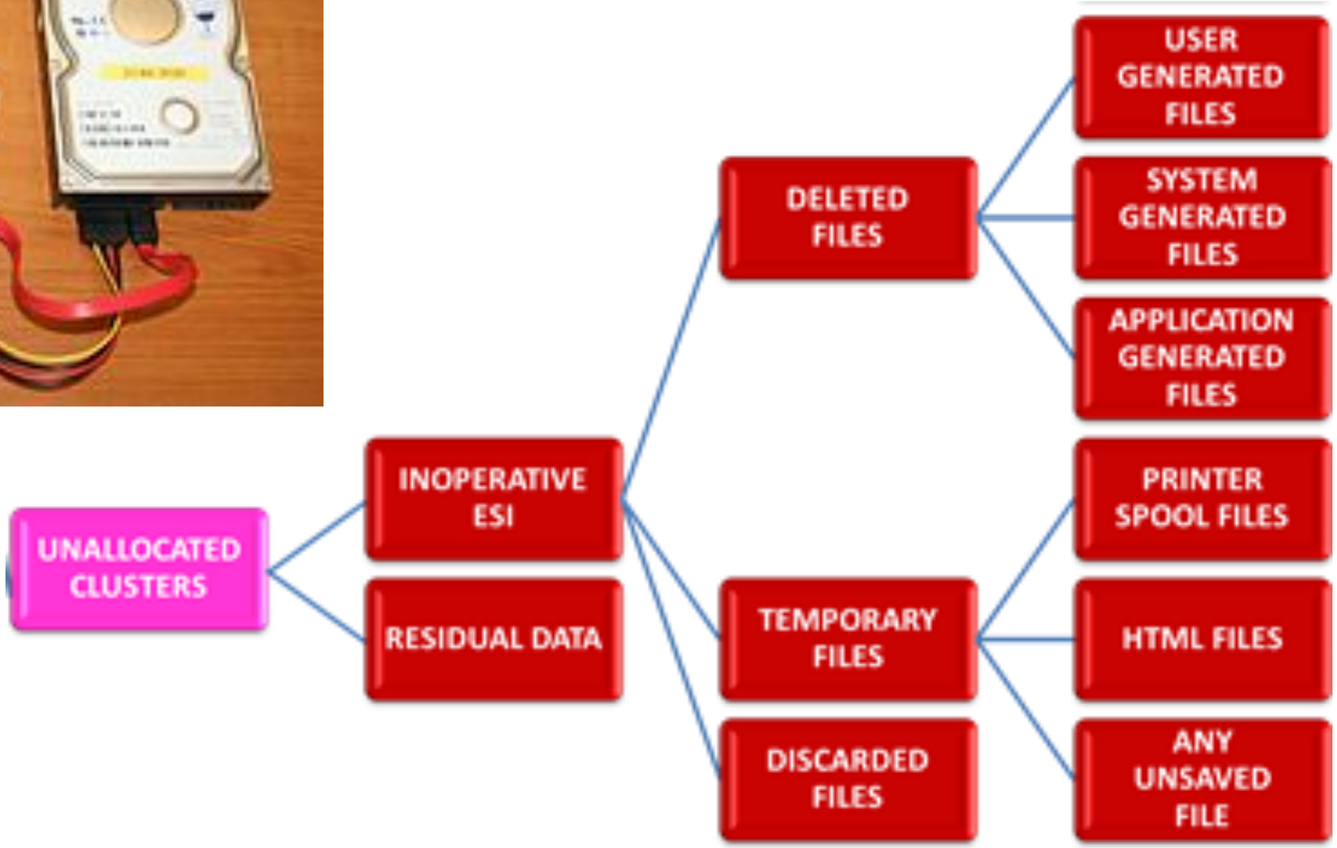
1. Forensic Soundness

When HD can’t be removed …
Device needs to be powered on …

Video of imaging and processing
Integrity of the video – MD5/SHA1

2. Logical Images

When Physical image of a HD (.E01) cannot be taken …



UNALLOCATED CLUSTERS

INOPERATIVE ESI

RESIDUAL DATA

DELETED FILES

TEMPORARY FILES

DISCARDED FILES

USER GENERATED FILES

SYSTEM GENERATED FILES

APPLICATION GENERATED FILES

PRINTER SPOOL FILES

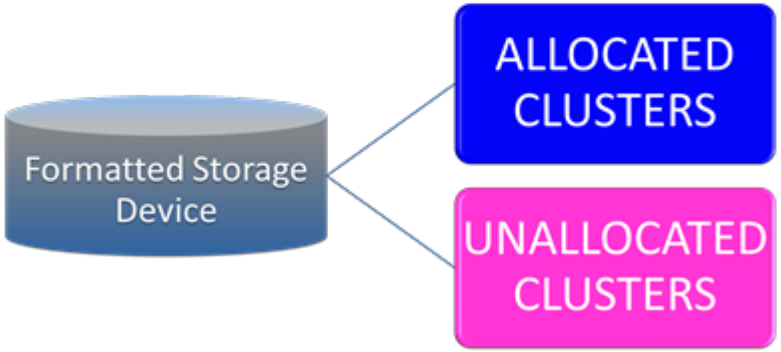
HTML FILES

ANY UNSAVED FILE

2. Logical Images

When Physical image of a HD (.E01) cannot be taken …

Make Logical image (.L01) Recovery from Unallocated clusters, deleted files, … – Product Support!

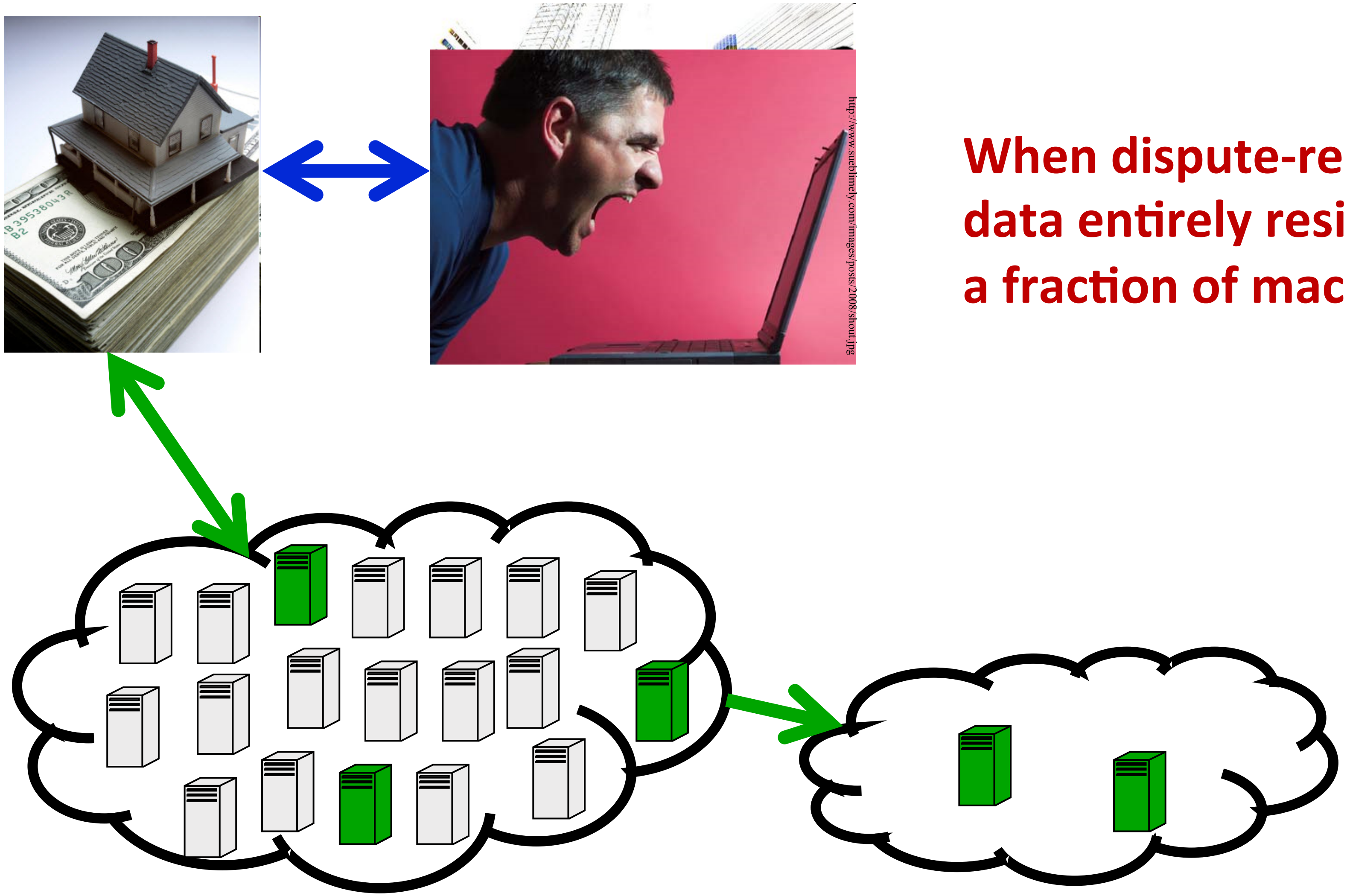


Formatted Storage Device

ALLOCATED CLUSTERS

UNALLOCATED CLUSTERS

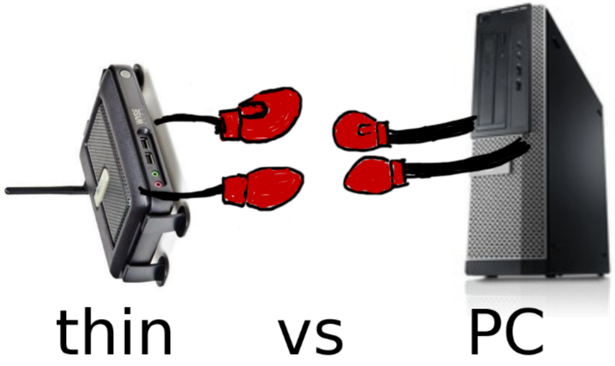
3. Cloud Forensics



http://www.sueblimely.com/images/posts/2008/shout.jpg

When dispute-related data entirely resides in a fraction of machines

3. Cloud Forensics



4. Virtual Machine Forensics

.lnk files
.dll files

5. Live Forensics

5. Live Forensics – Challenges

- Technical
  - Constantly updating records where full disk imaging process enters into indefinite loops

- Legal
  - In some countries live forensics may fall under the legislation(s) protecting "live communications" and therefore avoiding the crime of eavesdropping

5. Live Forensics – Way Forward

- Taking ‘still picture’ of the server at a given time instant
  - The best trade-off for acquiring digital evidence from a live source

- Downside of this technique: Snapshot image is taken by System Administrator
  - Whereas the image of a hard drive is taken by a digital forensic analyst
  - System Administrator is involved in the investigations!

6. Smart Environments

- Description
  - Emerging environments such as ICS (Industrial Control Systems), Smart Homes, etc.

6. Smart Environments

- Smart environments forensics
  - Analysis of the processes and resulting sequence of actions taken by the devices intelligently.
  - Different than IoT Forensics where the focus is the analysis of sensors data.

- Forensic challenges
  - Data format of these environments
    - Data is stored in different (often proprietary) formats
  - Scope of the NDA (Non-disclosure Agreement) holds vis-à-vis national legislations

Conclusions

Summary

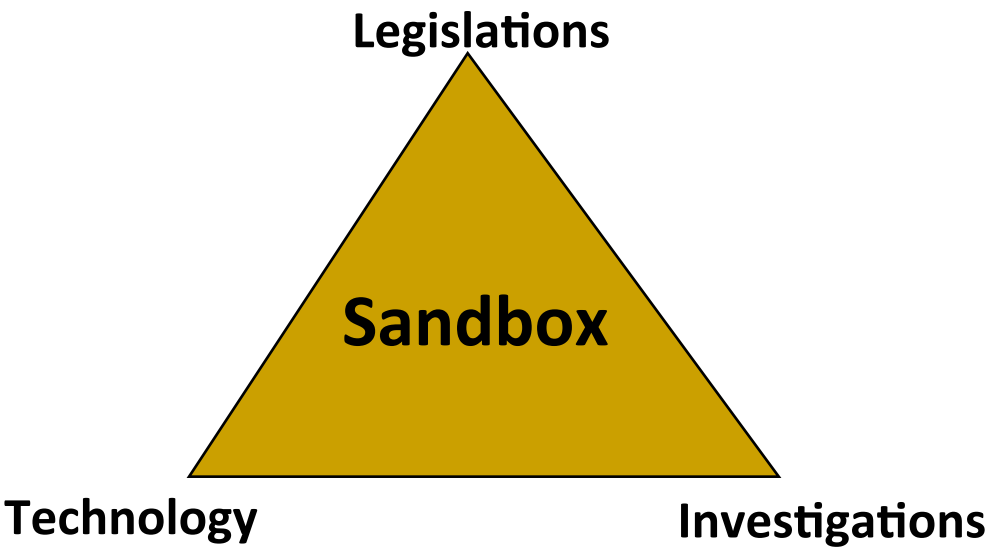
- Repository of real life case studies
- Flexible learning environment
- Better student experience
- Higher employability prospects

- Future directions
  - Available to the students of other HEI
  - More sophisticated scenarios

BIRMINGHAM CITY University

Perspectives

- We need to work on the **harmonisation** of digital forensic analysis methodologies and the governing policies
    - Scenarios-based testing
    - Identification of grey areas
    - Mutual validations



Legislations
Sandbox
Technology
Investigations