BIRMINGHAM CITY University

Building Open Education Resources for Digital Forensics Programmes

Syed Naqvi, Ali Abdallah
Centre for Cyber Security & Forensics

28 October 2015

Outline

- Introduction
- Open Educational Resources
- Digital Forensics Case Studies
- Summary & Perspectives

Project ConSoLiDatE

- Multi-disciplinary Cooperation for Cyber Security, Legal and Digital Forensics Education

- Objectives:
  - Development of educational resources conveying:
    - essential cyber security knowledge
    - essential digital forensic investigations
    - essential legal principles
  - Provision of educational audio-visual resources that facilitate active student learning, debate, critical thinking and classroom engagement.
  - Development of strong links between theory and practice through consolidation of student's understanding of principles by examining applicability to carefully constructed practical scenarios.

Project ConSoLiDatE

Open Educational Resources

- Cybersecurity Essentials
  - Includes Digital Forensics
- Case-studies
  - Modern legal briefs
  - Technical challenges
  - Expert industrial input
  - Discussion activities
- Sustainable Pedagogy
  - Videos

Multidisciplinary DF Education

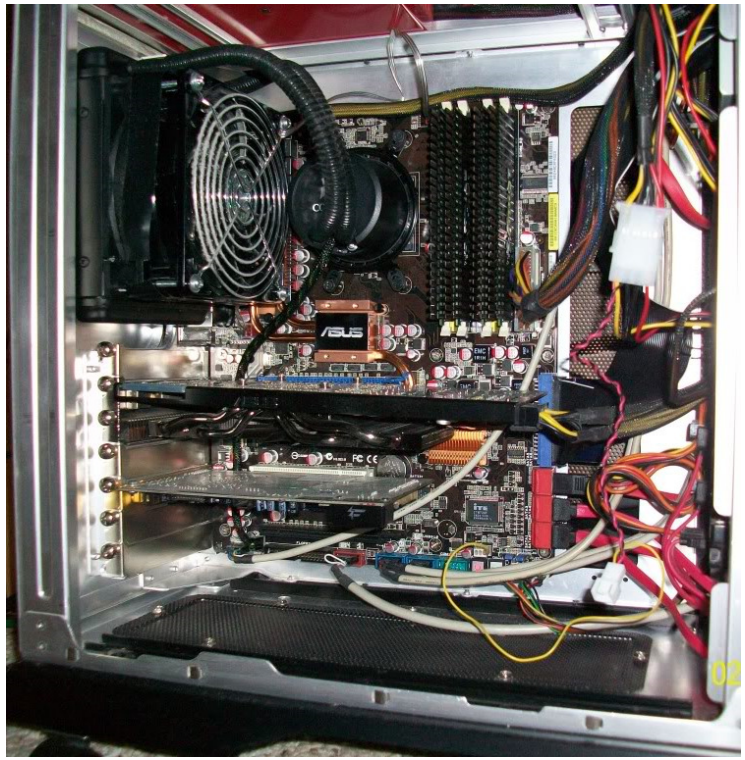
- Scenario-based learning (SBL)
  - Learning best takes place in the context where it is going to be used.
  - It involves students working their way through a storyline, usually based around a real-life case study.
  - Students are encouraged to play active role by using their subject knowledge, critical thinking and problem solving skills in real-world environment.

- SBL in the area of digital forensics
  - Set of scenarios to cover various stages of digital forensic analysis from evidence collection to the events correlation.
  - Legal dimension: Chain of custody, paperwork, evidence handling, etc.
  - Technical dimension: Imaging, password extraction, pin code, device connectors, etc.

Digital Forensic Case Studies

1. Forensic Soundness

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



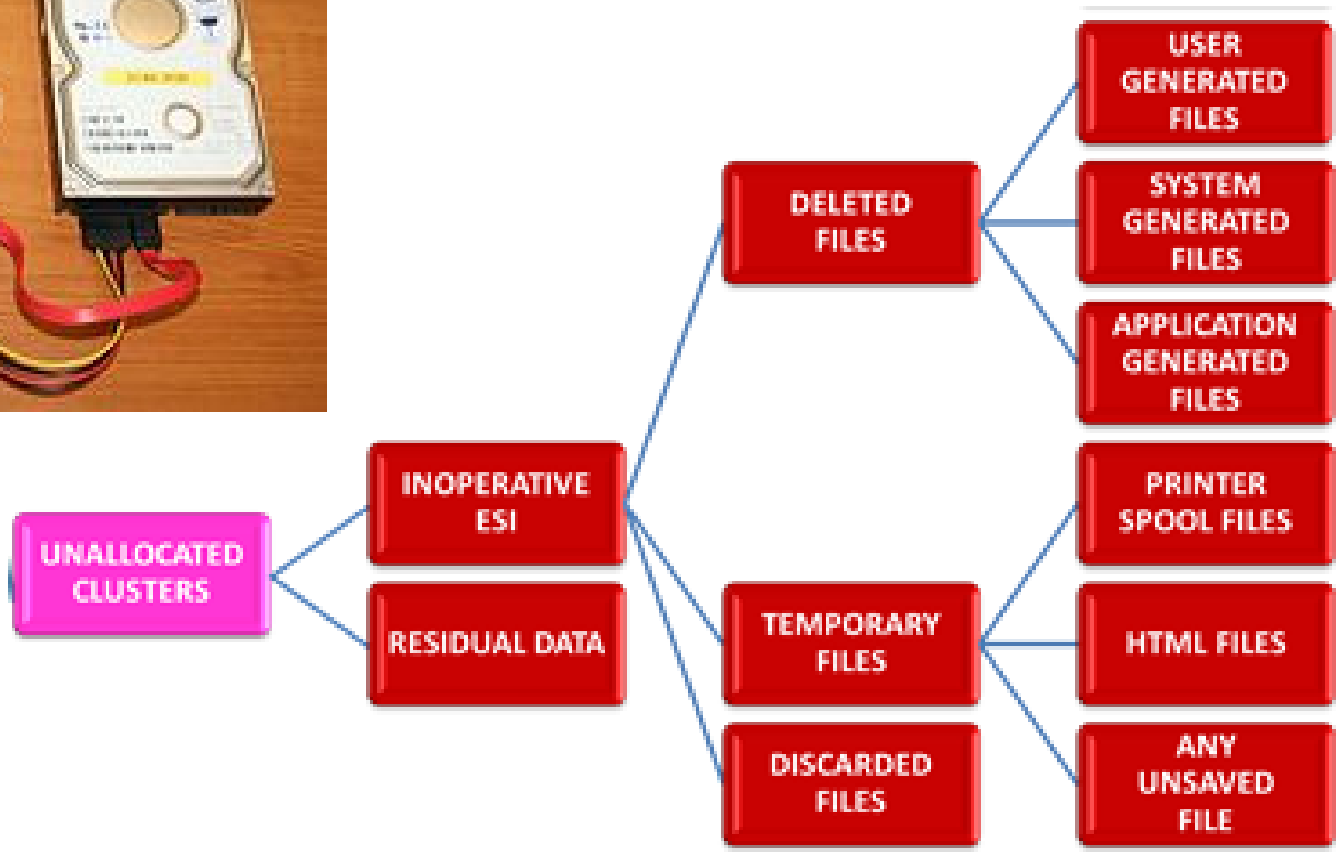
1. Forensic Soundness

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

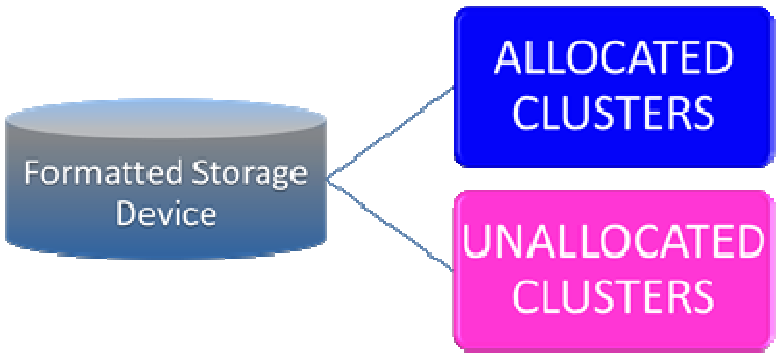
When Physical image of a HD (.E01) cannot be taken …



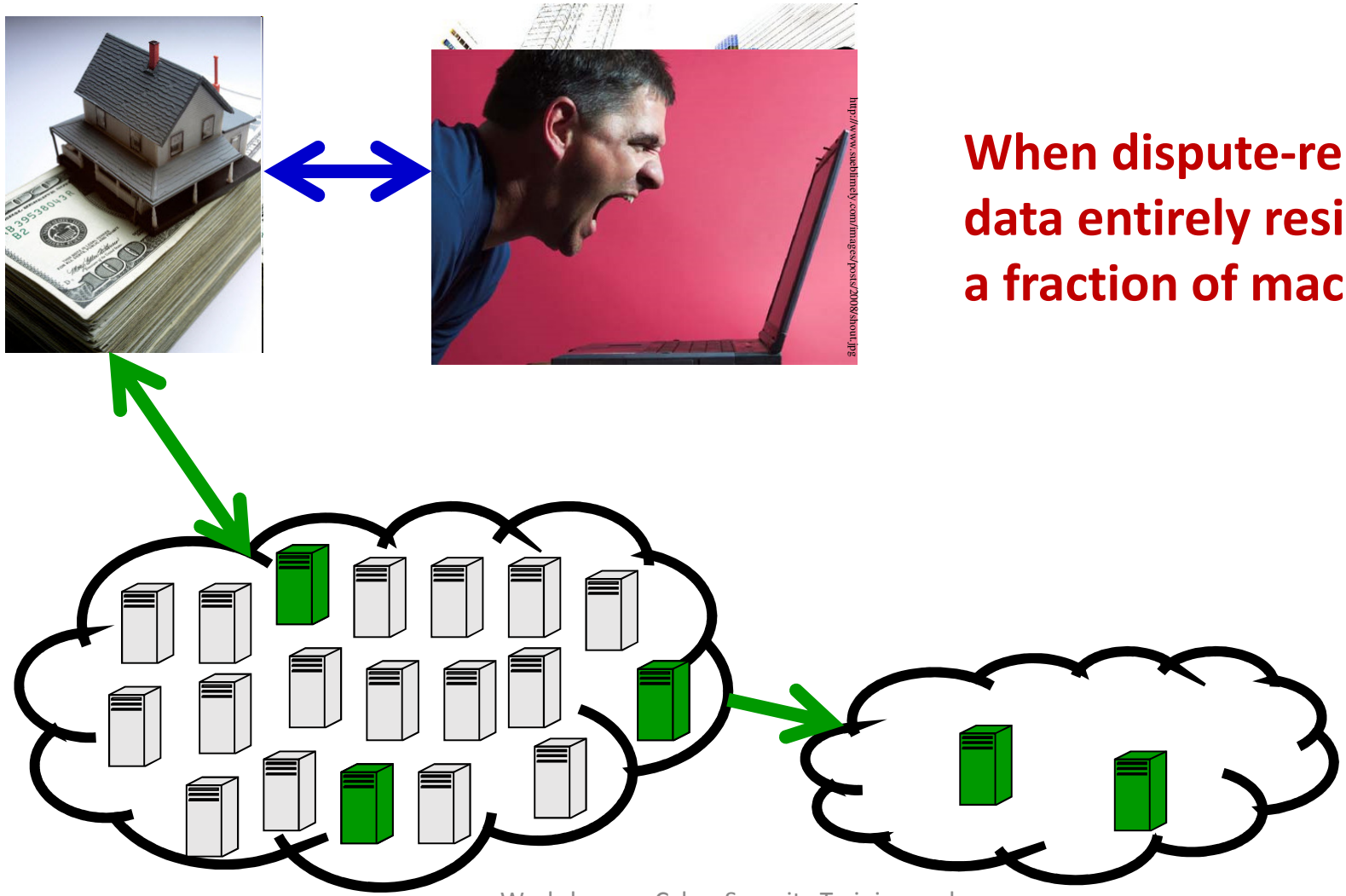
2. Logical Images

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

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

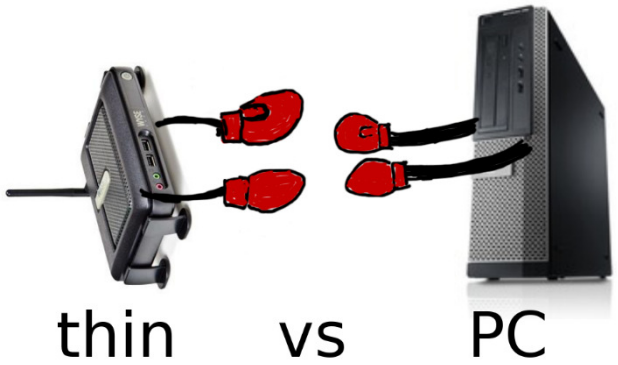


3. Cloud Forensics



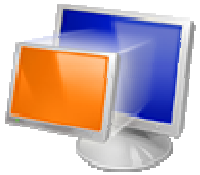
When dispute-related data entirely resides in a fraction of machines

3. Cloud Forensics



4. Virtual Machine Forensics

.lnk files
.dll files



Virtual Machines

Conclusions

BIRMINGHAM CITY University

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 (e.g. ICS Forensics)

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