BIRMINGHAM CITY University

Developing a Repository of Digital Forensics Case Studies to Provide Flexible Learning Environment

Syed Naqvi, Ali Abdallah

Centre for Cyber Security & Forensics

Outline

- Introduction
- Flexible Learning Environments
- 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

Practice

Advocacy

Expert witness

Psychology

Case Studies

Best practices

Law

Criminology

Investigations

Technology

Flexible Learning Environments

- Students with different learning abilities
  - Curriculum inclusive of students diversity
  - Sustainable learning resources
  - Self directed studies versus studying with own pace

- Case-studies
  - Modern legal briefs
  - Technical challenges
  - Expert industrial input
  - Discussion activities

Multidisciplinary DF Education

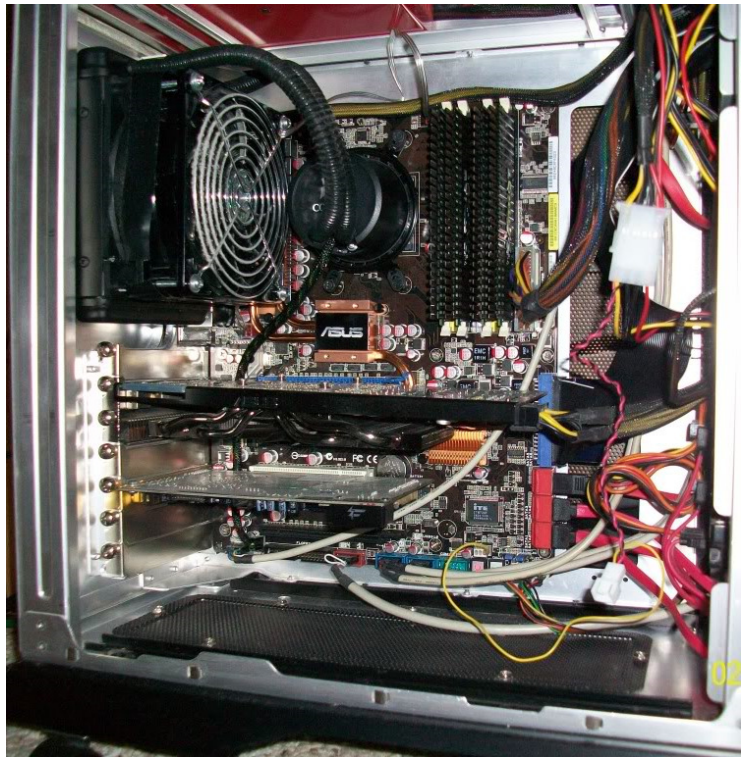
- Scenario-based learning (SBL)
  - Learning best takes place in the context where it is going to be used.
  - It involves students working their way through a storyline, usually based around a real-life case study.
  - Students are encouraged to play active role by using their subject knowledge, critical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



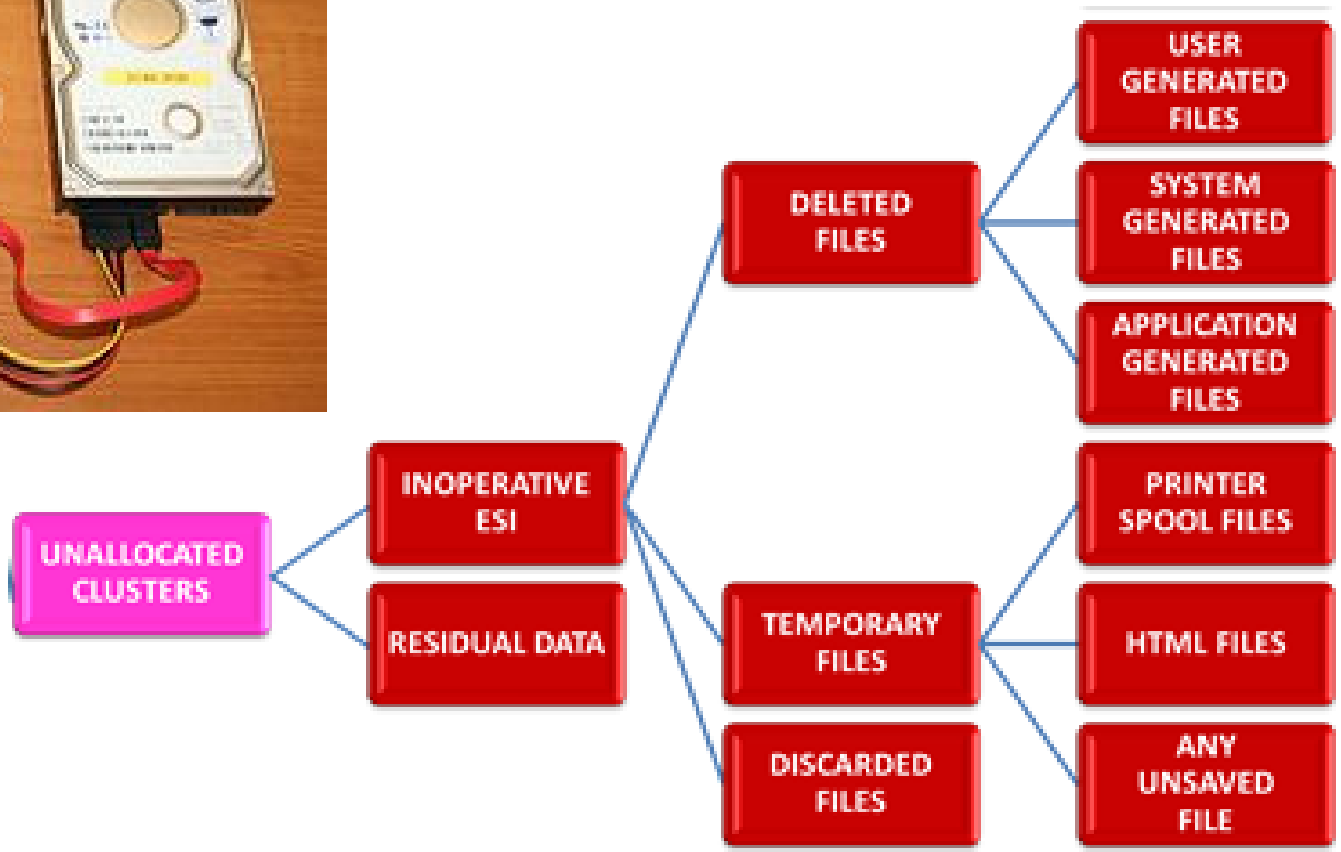
1. Forensic Soundness

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

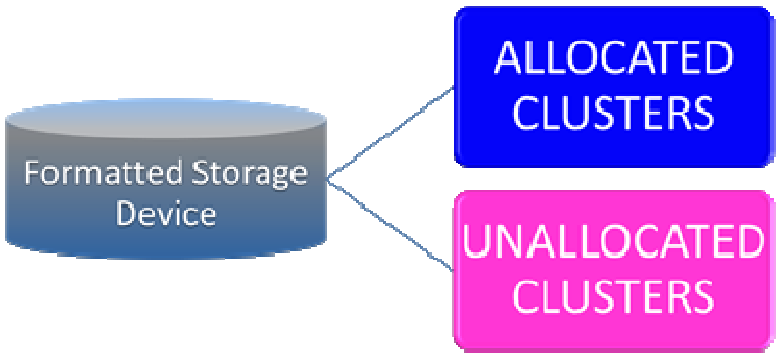
When Physical image of a HD (.E01) cannot be taken …



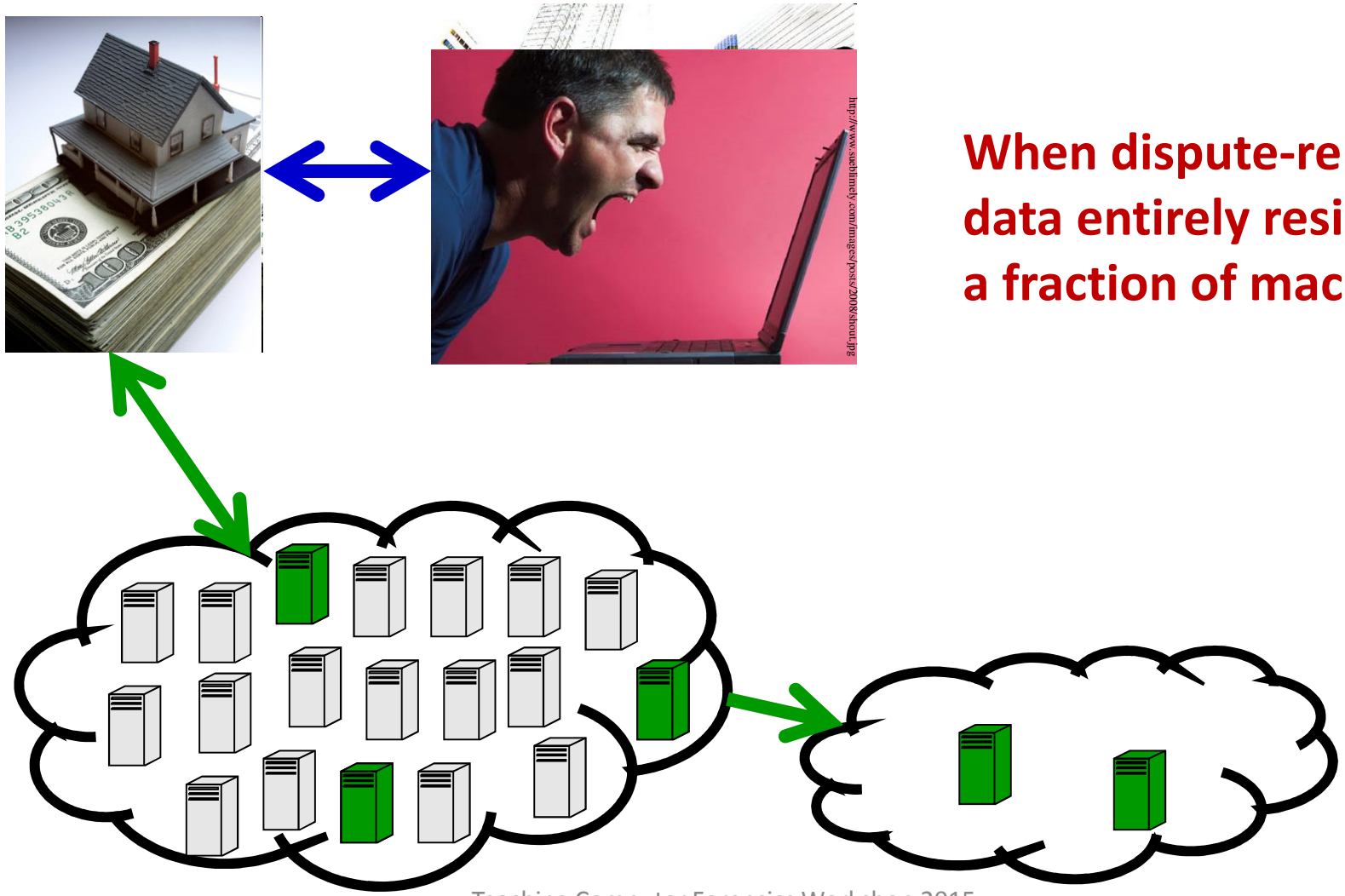
2. Logical Images

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

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

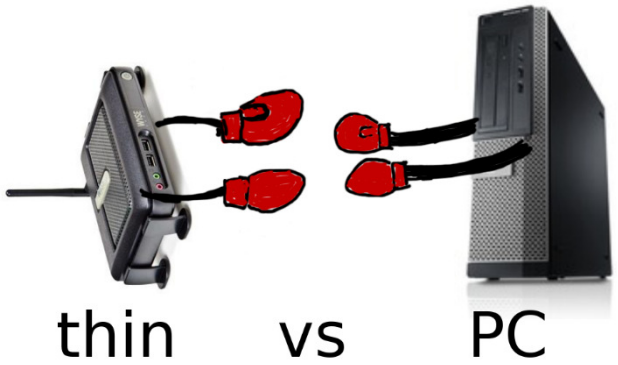


3. Cloud Forensics



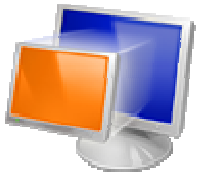
When dispute-related data entirely resides in a fraction of machines

3. Cloud Forensics



4. Virtual Machine Forensics

.lnk files
.dll files



Virtual Machines

BIRMINGHAM CITY University

Summary

- Teaching real life digital forensic case studies
- Provision of flexible learning environment
- Challenges of providing remote support
- Problems of using commercial tools remotely

- Future directions
  - Adaption to flipped curriculum
  - Evaluation of learning experience and skills level

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