Computer Forensics (CFR712S)

INTRODUCTION TO COMPUTER FORENSICS

Course Overview

- Introduction to Computer Forensics
- The Digital Forensics Process

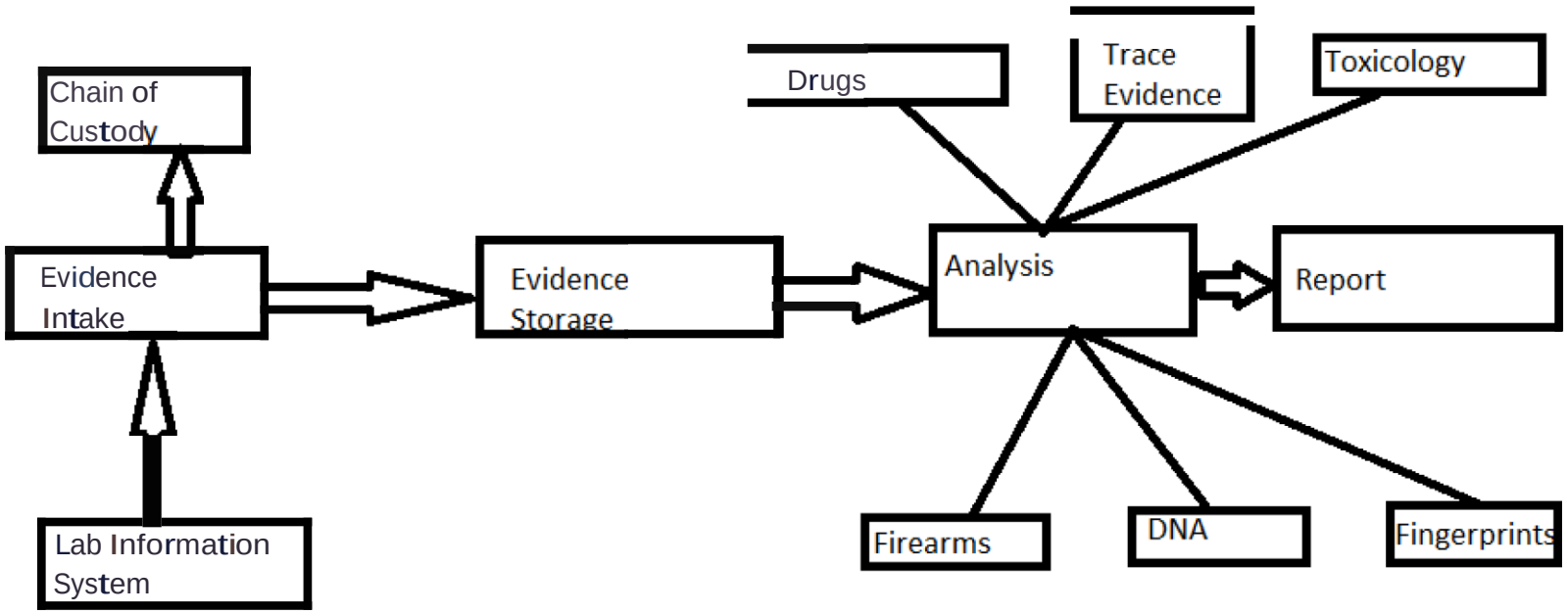
content

- What Is Digital Forensics
- Digital Forensics Techniques
- Illegal and legal activities warranting digital forensic investigations
- Types of digital forensic investigations
- Conclusion

The field of Forensic Science

- **Historically**– Romans meet in a public place called a "forum"
  – The term "forensic" means "of the forum"
- **Forensics definitions**
  – The methods of science applied to public matters
  – A "mixed science": associating people, places, and things involved in – usually criminal–activities
- **Forensic fields**
  – criminalistics, pathology, odontology, engineering, entomology and many more…

Typical Forensic Science Lab



What is Computer Forensics?

- Definitions
  - a means for gathering electronic evidence during a forensic investigation
  - Any information of probative value that is either stored or transmitted
    - The Scientific Working Group for Digital Evidence
  - The Application of Science and Engineering to the legal problem of digital evidence – it is a syntheses between science and law
    - Mark Pollit – retired FBI Agent
  - The Discipline that combines elements of law and digital science to collect and analyze data from digital systems in a way admissible to court
    - US-CERT

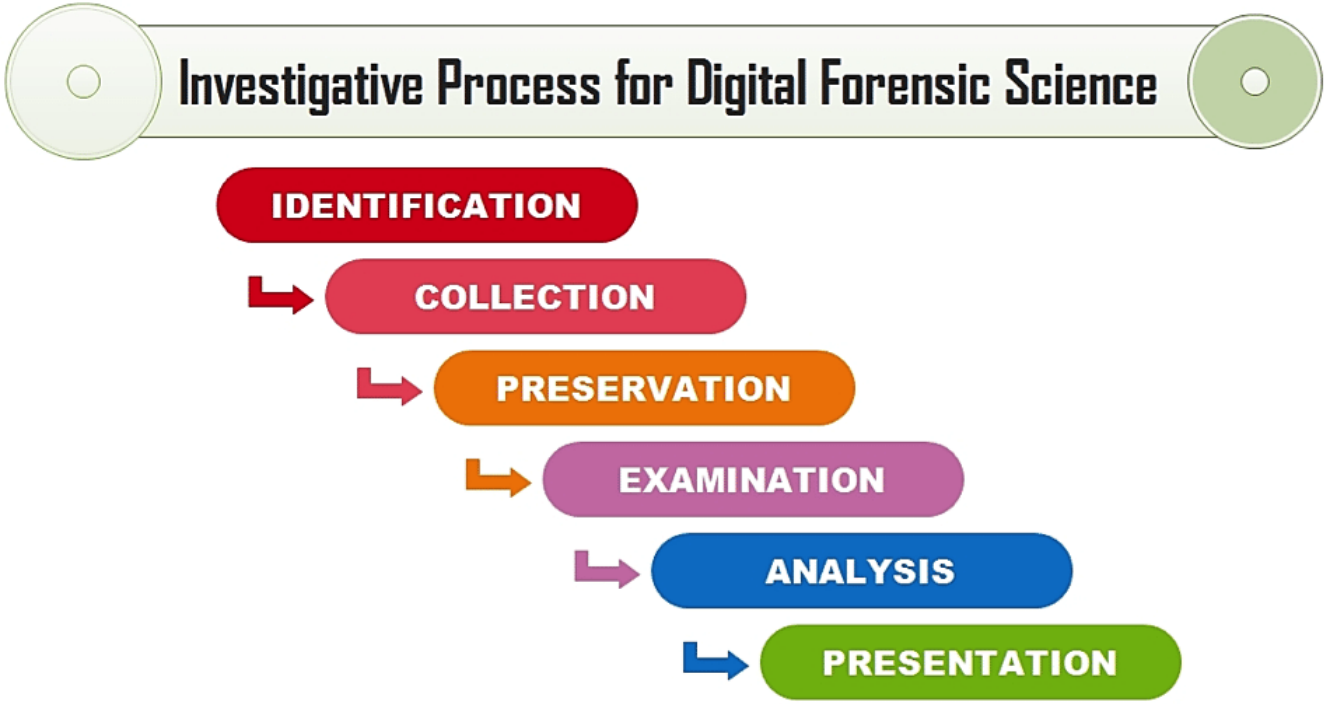
What is Computer Forensics?

- The main problem with CF
  - Many people involved in investigation
  - Evidence need to be presented in the same way as used to in "normal" forensics
  - Requirements
    - CF theory or technique must have been reliably tested
    - Must have been subjected to peer review and publication
    - Potential error rate of CF method used should be known
    - Must be generally accepted by scientific community
    - An acceptable process needs to be followed in acquiring and presenting the digital evidence

Computer Forensics Techniques

- Software assisted
- Hidden files
- Deleted Files
- Slack Space
- File type/extension modification
- Alternate Data Streams (ADS) in NTFS
- Live Digital Forensics
- Self-Organized Maps (SOMs) using AI

DF Process


Investigative Process for Digital Forensic Science
IDENTIFICATION
COLLECTION
PRESERVATION
EXAMINATION
ANALYSIS
PRESENTATION

Illegal Activities warranting computer forensics investigations

- Two main Categories
  - Criminal Investigations
  - Civil Litigation investigations
  - Corporate investigations

Illegal Activities warranting computer forensics investigations

- Fraud Audits
- Identity Thefts
- Hacking
- Embezzlement
- Instances of homicide
- Drug trafficking
- Child Pornography
- Civil Litigation
- Peer to Peer file sharing

Illegal Activities warranting computer forensics investigations

- Two main Categories
  - Data Discovery
  - Data Recovery

Types of Computer Forensic Investigations

- Dealing with a single computer
- Dealing with a networked computer
- Dealing with handheld devices
- Dealing with live forensics
  - Current Include
    - Cloud forensics
    - Mobile forensics
    - Multimedia forensics

Digital Forensics Readiness

- Managing/administering computer systems to make it easier to conduct a computer forensic investigation when needed
- Rowlingson outlines 10 steps to accomplish computer forensic readiness

Digital Forensics Readiness

1. Defining business scenarios that require digital evidence
2. Identify different sources and different types of potential evidence
3. Determine the evidence collection requirements
4. Establish capability for legally and securely gathering and storing evidence
5. Establish policy for secure storage and handling of potential evidence and ensure it is properly and regularly tested

Digital Forensics Readiness

6. Detect & deter major incidents
7. Specify circumstances in which incident should be escalated to full investigation
8. Train all relevant staff in incident awareness
9. Document case describing impact
10. Have procedures legally reviewed