Module Overview

IT3525 Cyber Forensic Process

Module Lecturer & Tutor

Victor Chua

Victor_Chua@nyp.edu.sg

Telephone 65501820

Aim

This module introduces students with processes involved in

- **conducting effective cyber forensic practices, preliminary planning, equipment seizing, evidence collection, recording, and safeguarding,**
- **opening and developing a forensic case, forensic anomaly investigation,**
- **reporting and presenting evidence in legal and civil cases.**

Objectives

After completion of this module, you be able to

- Understand the evolution of cyber forensics
- describe the phases in a cyber forensic process
- describe and apply the steps in preliminary planning, equipment seizing, evidence collection, recording, safeguarding process
- describe and apply the steps in examination of data
- describe and apply forensic anomaly investigation process on cyber attacks and espionage
- describe the reporting and presenting process in legal and civil cases
- report and present digital evidence in a case
- describe Singapore laws, legal practices and past court rulings
- describe the setup and processes in a cyber forensic laboratory

Mode of Assessment

Examination	50%
Participation, Practical Submission	10%
Review Questions	5%
Quiz	10%
Practical Test	15%
Practical Assignment	10%
Total	100%

Module Overview

- Evolution of cyber forensics
- Planning and collection of media
- Data extraction, duplication and conversion process
- Forensic investigation and analysis process
- Documentation and reporting of evidence
- Singapore Laws and legal practices
- Presentation of expert forensic evidence in courts
- Cyber forensic laboratory processes

Topic 1
Evolution of Cyber Forensics

- History of forensic science
- Physical and cyber forensics evolution
- Cyber forensic services
- Overview of a cyber forensics process

What is “Forensics”?

- The word forensic comes from the Latin adjective forēnsis, meaning "of or before the forum."

- Now "forensics" = "forensic science" can be considered correct as the term "forensic" is effectively a synonym for "legal" or "related to courts"

What is “Forensics”?

- The word forensic comes from the Latin adjective forēnsis, meaning "of or before the forum."

- In Roman times, a criminal charge meant presenting the case before a group of public individuals in the forum. Both the person accused of the crime and the accuser would give speeches based on their sides of the story.
- The individual with the best argument and delivery would determine the outcome of the case. This origin is the source of the two modern usages of the word forensic – as a form of legal evidence and as a category of public presentation

Pop-Quiz Time

- What does “Forensic” originally mean?

Ans:

- What is the modern meaning of forensics”?

Ans:

Pop-Quiz Time

- What does “Forensic” originally mean?

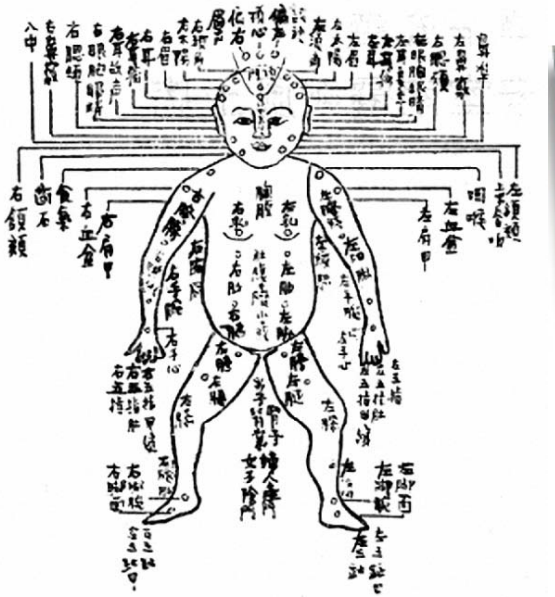
Ans: It means "of or before the forum”

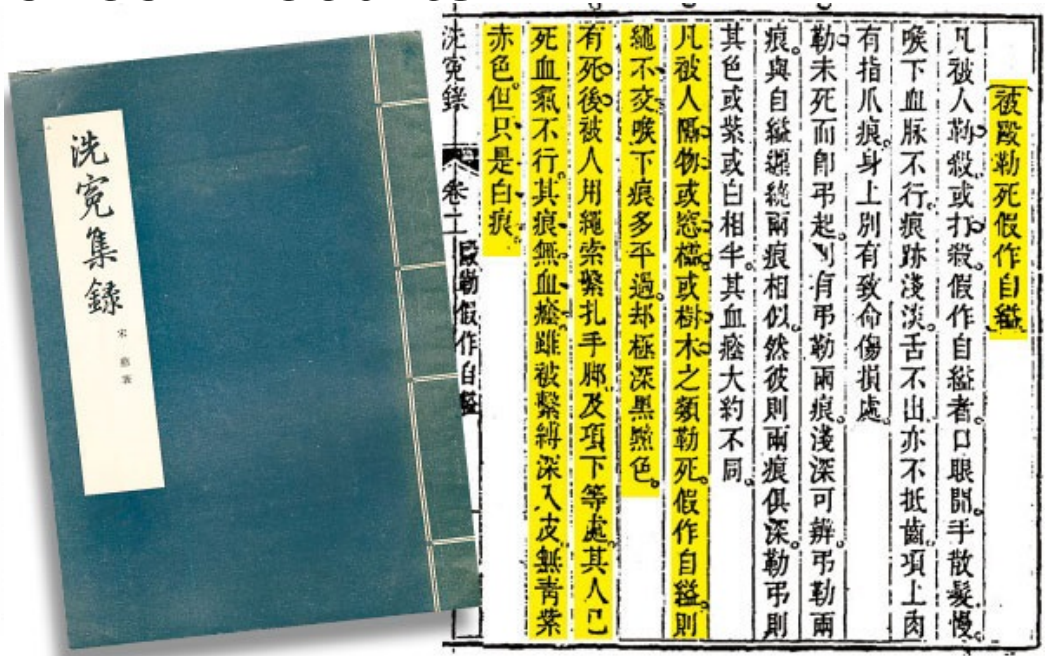
- What is the modern meaning of forensics”?

Ans: The modern meaning of “forensics” is a form of legal evidence and as a category of public presentation

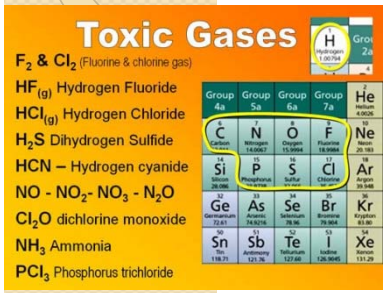
History of forensic science

- The origins of forensic science can be traced back to the 6th century, with legal medicine being practised by Chinese.
- During the next ten centuries advances in both medical and scientific knowledge were to contribute to a considerable increase in the use of medical evidence in courts.





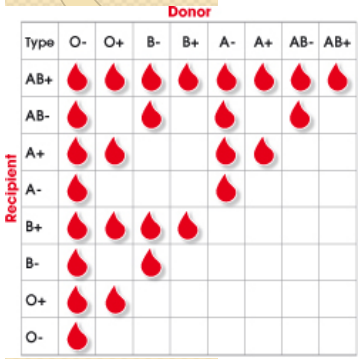
Physical and digital forensics evolution



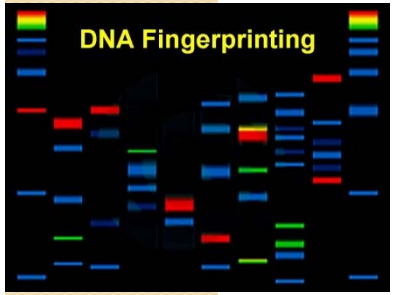
- Toxicology – in 1840 Orfila testified on the basis of chemical tests that the internal organs from a death body contained poisonous chemical which could be the cause of death

- Fingerprint – Sir Edward Henry devised a fingerprint classification scheme for cataloguing and retrieving fingerprint which could be used in forensic investigations

Physical and digital forensics evolution



- Body fluid – in 1900s, blood sample collected from crime scene could be classified into A, B , AB and O blood groups



- In 1980s, application of DNA profiling to criminal investigations started.

Pop-Quiz Time

- **What led the evolution of physical forensics?**

Ans:

- **What are the two questions can be answered by the physical forensics?**

Ans:

Pop-Quiz Time

- **What led the evolution of physical forensics?**

Ans: The advancements in both medical and scientific knowledge

- **What are the two questions can be answered by the physical forensics?**

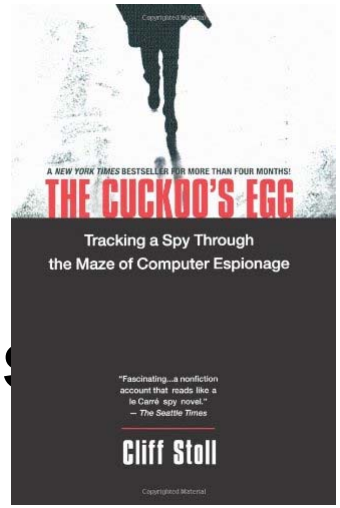
Ans: The two questions are: "What was the cause of death?" and "Who did it?"

Physical and digital forensics evolution

1978 – Computer crime were recognized in Florida Computer Crime Act

1984 – FBI launched a Computer Analysis and Response Team (CART) and setup computer crime department

1986 – computer and network forensic techniques were used to prosecute a hacker Markus Hess



Physical and digital forensics evolution

1993 – Singapore Computer Misuse Act established and Evidence Act amended to accept computer output as evidence.

2000 – The Technology Crime Forensics Branch was officially launched. It conducts investigation and forensic examination into technology-related offences committed under the Computer Misuse Act, such as hacking and unauthorised access to account.

CID

2013 - Computer Misuse Act is renamed as Computer Misuse & Cybersecurity Act to allow Govt to prevent, detect and counter cyber attacks on critical information services & infrastructure

Physical and cyber forensics evolution

- Cyber Forensics
  - Computer Forensics
    - File system forensics
      - Windows Files systems forensics
      - UNIX File systems forensics
    - Database Forensics
    - Applications Forensics
    - Memory Forensics
  - Network Forensics
  - Mobile Devices Forensics
  - Social Media Forensics

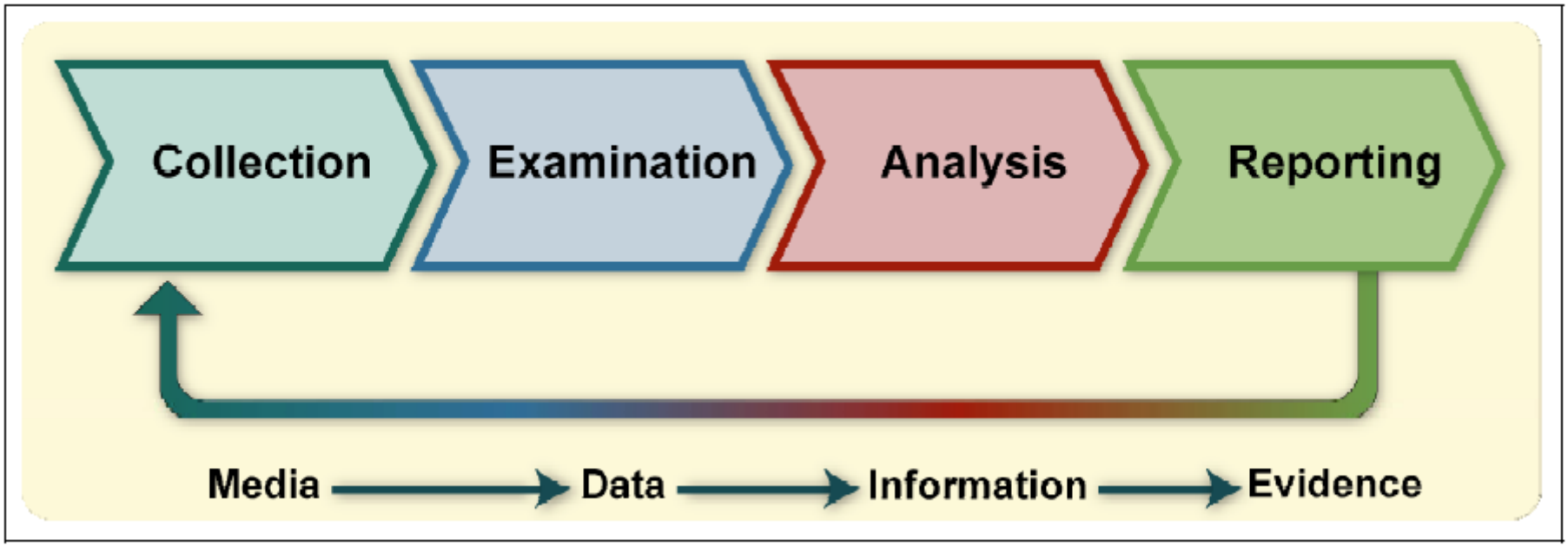
Digital forensic services

FBI provide the following computer forensic services to law enforcement agency

- **Content**
- **Comparison**
- **Transaction**
- **Extraction**
- **Deleted Data Files**
- **Format Conversion**
- **Keyword Searching**
- **Passwords**
- **Limited Source Code**

Get the details in Handbook of Forensic Services at http://www.fbi.gov/about-us/lab/handbook-of-forensic-services-pdf

Cyber Forensics Process

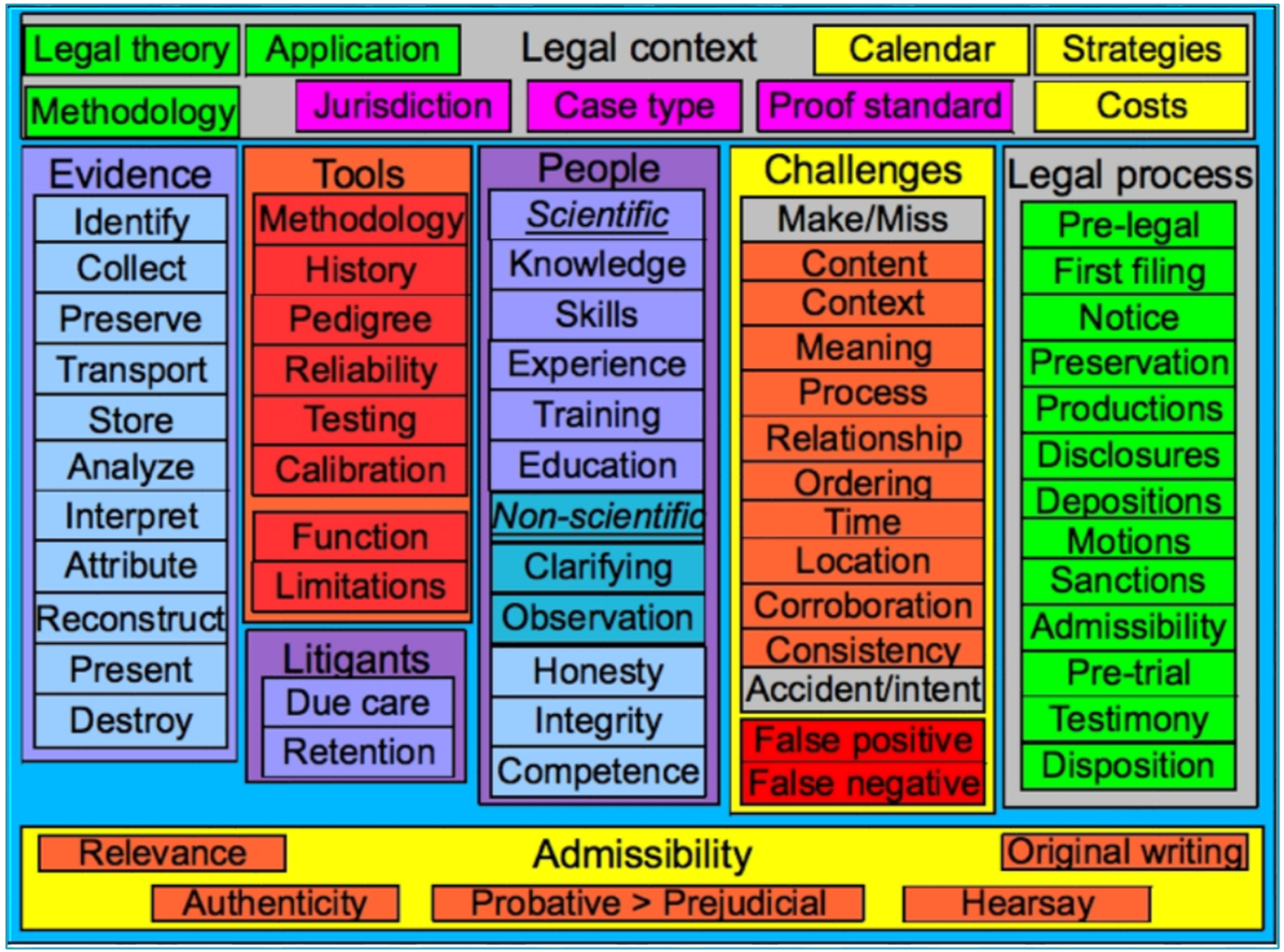


Guide to Integrating Forensic Techniques into Incident Response
SP800-86 NIST (csrc.nist.gov)

Cyber Forensics Process

- **Collection**
  - Collection of media/devices at the scene
  - Identification and Preservation
  - Transportation
- **Examination**
  - Extraction of data
  - Searching/locating data
- **Analysis**
  - Event analysis
  - Timeline analysis
- **Reporting**
  - Reporting and documentation

Digital Forensics Processes



Pop-Quiz Time

- At the crime scene, a cyber forensic examiner collects _____ that may contain evidence.
- In a forensic lab, an examiner extracts _____ from a hard disk.
- Timeline analysis can provide _____ on the past activities in a computer.
- Examiner reports the potential _____ after bookmarking the information related to the case.

Pop-Quiz Time

- At the crime scene, a digital forensic examiner collects media that may contain evidence
- In a forensic lab, an examiner extracts data from a hard disk.
- Timeline analysis can provide information on the past activities in a computer
- Examiner reports the potential evidence after bookmarking the information related to the case.

Summary

- What forensics means
- Evolution of physical and digital forensics
- Digital forensic services
- Digital forensics process and sub-processes

References

1. Crime Scene to Court The Essentials of Forensic Science, 3rd Edition, Peter White, 2010, RSC Publishing, B
2. Computer Evidence Collection & Preservation, Christopher L.T. Brown, 2006, Networking & Security Series, B
3. Handbook of Forensic Services, 2007, Federal Bureau of Investigation, U.S. Department of Justice
4. Guidelines on Integrating Forensic Techniques into Incident Response, 2006, NIST
5. Computer Forensics and Privacy, Michael A. Caloyannides, 2001, Artech House