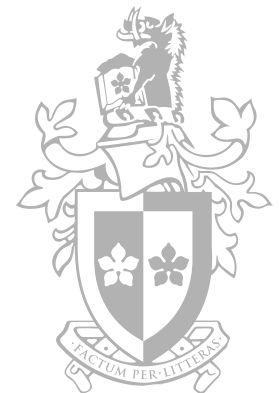


Lecture 1

Introduction to eForensics

Troy Pretty
Digital Forensic Analyst



Teaching Team

- Mr Troy Pretty
 - Lecturer and Tutorial
 - Email: tpretty@swin.edu.au
 - 11 years experience in computer forensics
 - 6 years teaching ICT30010
 - Interests:
 - Malware
 - Reverse Engineering

Teaching Team

- Mr Aldin Dautcehajic
 - Tutorial
 - Email: adautcehajic@swin.edu.au
 - 9 years experience in computer forensics
 - 5 years teaching ICT30010
 - Interests:
 - Mobile Forensics
 - Password Cracking

Teaching Team

- Mr Andrew Marriott
 - Tutorial
 - Email: amarriott@swin.edu.au
 - 11 years experience in computer forensics
 - 3 years teaching ICT30010
 - Interests:
 - Cloud Forensics
 - Network Forensics

Outline and Learning Goals

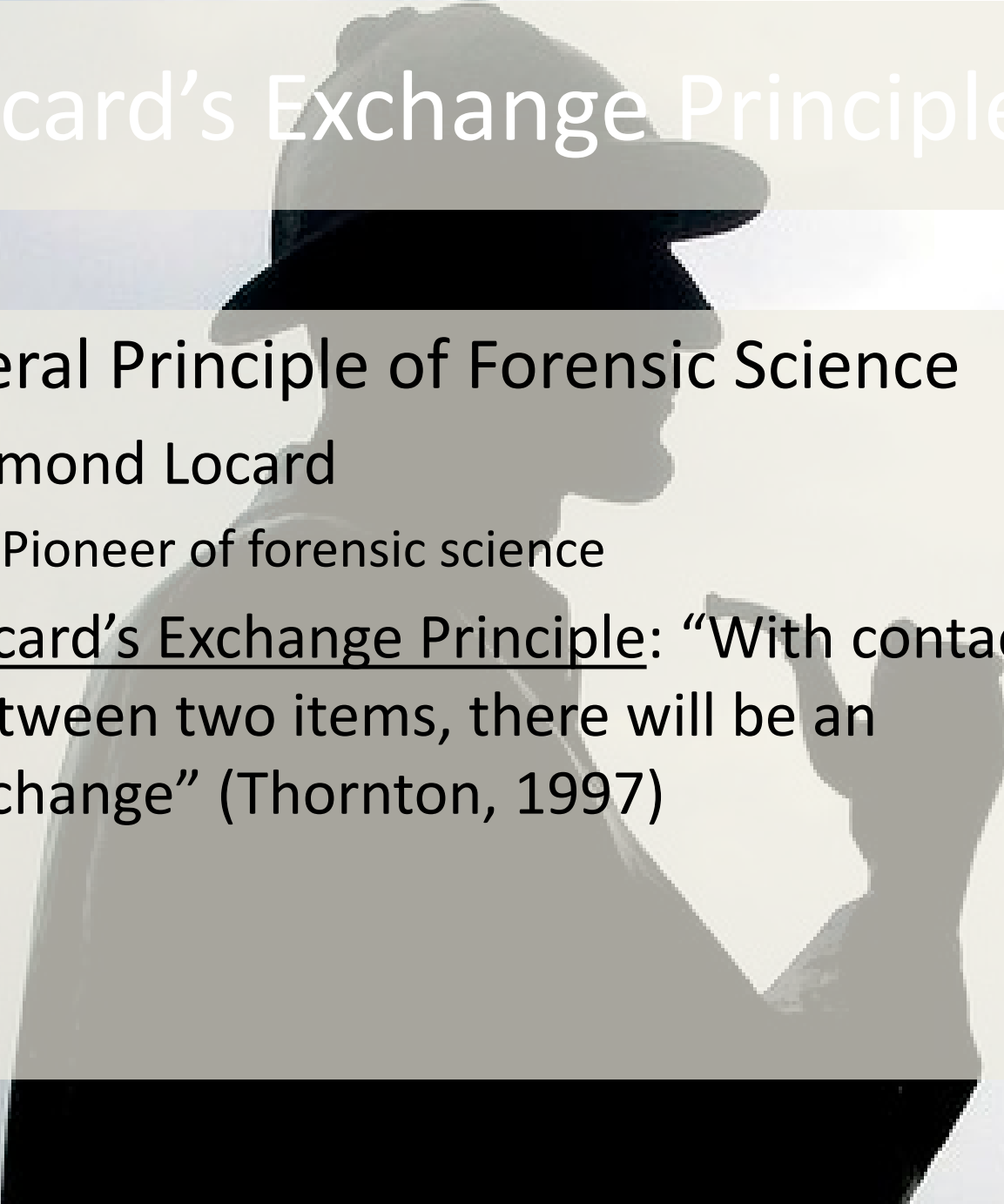
- The nature of eForensics
 - It's purpose, objectives and scope
 - Forensic analysis and procedures
- eForensic areas
 - Computer forensics
 - Network forensics
 - Database forensics
 - Mobile device forensics
- Forensic toolkits

WHAT IS FORENSICS?

- **fo·ren·sic** /fə'renzik/
 - *adj.* Of or used in courts of law
- Latin root “forensis” (before the forum)

*Application of scientific method to
answer questions of interest to a legal
system*

Locard's Exchange Principle



- General Principle of Forensic Science
 - Edmond Locard
 - Pioneer of forensic science
 - Locard's Exchange Principle: “With contact between two items, there will be an exchange” (Thornton, 1997)

Challenges in Digital Forensics

- Jurisdictional boundaries
 - Victim in “A”, suspect in “B”, evidence located in “C”
 - Who investigates? What laws apply? How do “A” or “B” obtain evidence to investigate/prosecute?
 - What if event is only a crime in one jurisdiction?
- Volatility of digital evidence
 - Acquiring data without changing it
- Proliferation of digital devices
- Volumes of data
 - All of Wikipedia would fit on an iPhone
- “CSI Effect”

Ubiquity of electronic devices

- Modern life is lived on electronic devices
 - Mobile devices for phone calls, texts, twitter, websurfing
 - Computer for communication, paying bills, ordering goods and services, entertainment, blogs, facebook...
 - Video game consoles, MP3 player, electronic books, digital video recorder...
- Consequent rise in related crime, civil litigation, security incidents, privacy invasion
- eForensics is about investigating these sorts of cases

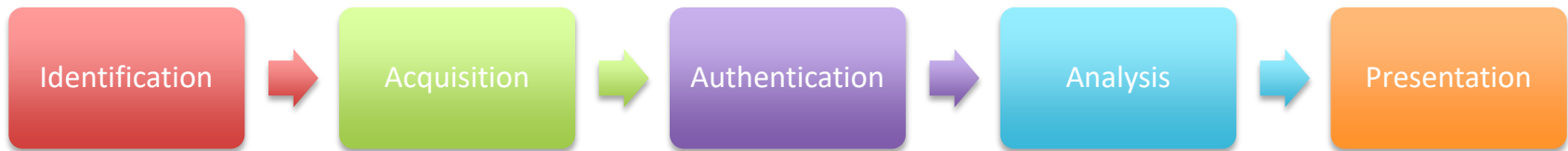
Sources of Electronic Evidence



eForensics Scope and Goals

- At the high level, eForensics is concerned with the following
 - Identification of the facts
 - Evidence collection
 - Event reconstruction
- eForensics can be used in the following ways
 - Attribution
 - Assessing alibis and statements
 - Determining intent
 - Authenticating digital documents

Digital Forensics Process



- Identification
 - Find potential evidence storage
 - Determine authority to acquire (warrant / anton piller)
- Acquisition
 - Preserve digital crime scene
 - May include live or static analysis, and include taking logical or physical copies
- Authentication
 - Use of hash functions to validate data has not changed
- Analysis
 - Find evidence to support or refute hypothesis
 - How did an item appear on the computer? (e.g. image, log record)
- Presentation
 - Reports, evidence in court, etc.

Acquisition Phase

- Acquire forensic copies of identified data
 - Secure, traceable, verifiable
- Acquire data in “order of volatility”
 - Most likely -> least likely to change
 - Move quickly!
- Use of specialist tools
 - Commercial: EnCase, FTK, Tableau, WiebeTech, Logicube
 - Open Source: Helix, SIFT, Paladin

Order of Volatility

CPU Registers / Cache

Main Memory (RAM)

Network State / Running Processes

Hard Disk Drives, USB Flash, etc.

Backups/Printouts/CD ROM/etc.

Types of Data Acquisition

Physical

- “bit for bit” copy, includes deleted (unallocated) areas of disk
- Usually requires computer to be off (“dead”/“static”)

Logical

- File system (or specific files) only, in tamper-evident container
- Often best option for “live” analysis

File Copy

- Individual file contents only, easily modified
- Metadata (e.g. MFT dates and times) lost

Digital Investigation Types

- Computer forensics
- Network forensics
- Database forensics
- Mobile device forensics

Emphasis on this unit is Computer and Network forensics but we will talk about database and mobile devices

ACPO Good Practice Guide

Associate of Chief Police Officer's (ACPO)

1. No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.
2. In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions
3. An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
4. The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

ACPO Good Practice Guide

1. Don't change original data
2. If you must change data, only use competent people who understand the implications of their actions
3. Log everything! (Must be repeatable)
4. Investigator has ultimate responsibility

http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf

Examples of Computer Forensic Activities

- Has a user of a particular computer downloaded child pornography?
- Has a user of a particular computer participated in illegal upload or download of unlicensed software?
- Has a user of a particular computer broken non-disclosure agreements by emailing trade-secrets (customer lists, pricing details) to a competitor?

Computer Forensic Tasks We Will Carry Out

- Capture an image of a hard disk
 - Use the image to identify the file system
- Ensure the chain of custody of captured images
 - Use hash functions to do so
- Reconstruct deleted files from disk images
 - From NTFS file system
- Search disk images for specific keywords
 - Use free Linux-based tools for searching captured images

Network Forensics

- Examine a network to determine whether or not it has been used to commit some illicit activity
- Need to monitor the network for such activity
- Different aspects to network forensics
 - Have hosts (computers, servers, databases) attached to your network been the victim of illicit activity?
 - Have hosts on your network been a party to illicit activity?
 - Such activity may or may not have been carried out knowingly

Example of Network Forensic Activities

- Was security of network compromised?
- How was system/network compromised?
- What data may have been exfiltrated during the attack?

Common Network Forensic Tasks

- Capture a sequence of messages (packets)
- Ensure the chain of custody of such a sequence
- Reconstruct the events represented by the sequence of packets
- Search packets for particular message types transmitted to or from particular hosts

Network Forensic Tasks We Will Carry Out

- Use of network tools wireshark and tcpdump to listen and capture traffic
 - Capture traffic for later analysis
- Use of wireshark and tcpdump to extract content of packets
 - Using wireshark to extract conversations
 - Using tcpdump to explore the detailed contents of packets
- Interpreting the contents of particular packets
 - Particularly interested in identifying anomalous events

Wireshark Analysis

The image displays the Wireshark network traffic analysis interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture, and analysis. The main window is divided into three panes:

- Packets List:** A table showing a list of captured packets. The columns are No., Time, Source, Destination, Protocol, and Info. The selected packet is 741, which is an Ethernet II frame from 136.186.228.16 to 136.186.50.78, containing an Internet Protocol (IP) packet and a Transmission Control Protocol (TCP) segment.
- Packet Details:** A hierarchical tree view showing the structure of the selected packet. It includes Ethernet II, Internet Protocol, and Transmission Control Protocol. The selected packet is 741, which is an Ethernet II frame from 136.186.228.16 to 136.186.50.78, containing an Internet Protocol (IP) packet and a Transmission Control Protocol (TCP) segment.
- Packet Bytes:** A hex dump and ASCII representation of the selected packet's raw data. The hex dump shows the raw bytes of the packet, and the ASCII representation shows the corresponding text.

The status bar at the bottom indicates that 1975 packets were displayed, 1975 were marked, and 0 were dropped. The profile is set to Default.

Database / Log Forensics

- Analysing records in a database to determine whether or not illicit activities have occurred
- A simple example might be a web (http) logfile
 - Might be interested in specific addresses that have accessed the webserver
 - Might be interested in what information has been retrieved
- Often analyse contents of database systems (such as SQL) for time and date information to correlate with other events

Common Database Forensic Tasks

- Search a database for activity from a particular user
 - Perhaps defined by IP address or user name
- Search a database for events that occurred between specific times
 - Large amounts of money deposited following successful scams detected elsewhere
- Search a log file for access to a particular object
 - Illegal content on a webserver. We might want to find who (which IP address) has downloaded it
- Search a log for anomalous events
 - Large volumes of money entering and leaving an account within a very short timeframe

HTTP logfile analysis

- Can make use of specific pattern match tools to find strings within a logfile
 - `cat httplogfile | grep "rrosalion-laptop" | more`

Mobile Device Forensics

- Mobile phones, Memory sticks...
 - Devices with significant capabilities that can
 - Store data of interest
 - Be used as a malware vector
 - Be used to assist in attacks such as Distributed Denial of Service
 - Be used to plan and control a crime
- Most of the techniques for computer and network forensics can be applied to mobile device forensics, however there are additional areas

Forensic Software / Toolkits

- There are a number of toolkits available for forensic analysis
 - Mostly for analysing PCs
 - Many generalist networking analysis tools available
- In this unit we will make use of open source tools and toolkits
 - Computer forensics – SANS investigative forensic toolkit
 - Network forensics – wireshark
 - Database forensics – Linux command line
- It is important that you understand the details of what happens rather than have it hidden by a more complex system

Conclusion

- eForensics a wide ranging area
 - Technical, legal, procedural, investigative, administrative...
- Our interest is (primarily) technical
- Four areas of technical investigation
 - Computer
 - Network
 - Database
 - Mobile devices