SWINBURNE UNIVERSITY OF TECHNOLOGY

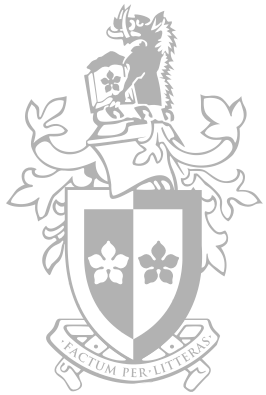
# ICT30010 eForensic Fundamentals

## Lecture 12

## Unit Review

**Troy Pretty**

Digital Forensic Analyst




SWINBURNE UNIVERSITY OF TECHNOLOGY

# Week 1

Lecture 1:

Introduction to eForensics

Lab 1:

Introduction to Forensic Toolkits

# Week 1 - Lecture

- Definition of forensics
- Locard's exchange principle
- Challenges
  - Jurisdictional boundaries
  - Volatility of digital evidence
  - Proliferation of digital devices
  - Volumes of Data

# Week 1 - Lecture

- Scope
  - Identification of Facts
  - Evidence Collection
  - Event Reconstruction
- Uses
  - Attribution
  - Alibis
  - Intent

# Week 1 - Lecture

- Process
  - Identification
  - Acquisition
  - Authentication
  - Analysis
  - Presentation
- Order of Volatility
  - Most volatile to least volatile

# Week 1 - Lecture

- Types of Data Acquisition
  - Physical
  - Logical
  - File Copy
- Investigation Types
  - Computer
  - Network
  - Database
  - Mobile Devices
- Associate of Chief Police Officer's (ACPO) Good Practise Guide

# Week 1 - Lab

- Document the Exhibit
  - Make/Model
  - Description
  - Colour
  - Damage
  - Storage Devices
- Document BIOS Date and Time
- Boot Computer from Forensic CD (Paladin)

# Week 1 - Lab

- Identifying Partitions
  - Name
  - Type
  - Start Sector
  - End Sector
  - Total Size
  - Offset
- Mounting Partitions

# Week 2

Lecture 2:

PC Architecture and Operating Systems

Lab 2:

Forensic Disk Copying

# Week 2 - Lecture

- Numbering Systems
  - Binary
    - Base 2
    - Digits 0,1
  - Octal
    - Base 8
    - Digits 0,1,2,3,4,5,6,7

# Week 2 - Lecture

- Decimal
  - Base 10
  - Digits 0,1,2,3,4,5,6,7,8,9
- Hex
  - Base 16
  - Digits 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F

# Week 2 - Lecture

- Units of measure
  - Bit (b)
  - Byte (B)
  - Kilobyte (KB)
  - Megabyte (MB)
  - Gigabyte (GB)
  - Terabyte (TB)
  - Others
    - Nibble, WORD, DWORD, QWORD

# Week 2 - Lecture

- Character Sets
  - ASCII (American Standard Code for Information Interchange)
  - Extended ASCII
  - Unicode
- Offsetting

# Week 2 - Lecture

- Personal Computer
  - Motherboard
  - CPU
  - Memory
  - Storage Devices
  - Adapter Card
  - Ports

# Week 2 - Lecture

- Operating Systems
  - BIOS
  - Windows
  - Linux
  - OSX

# Week 2 - Lab

- Partition Identification
- Forensic Disk Copying
- Hashing
- Examining a Disk Image

# Week 3

Lecture 3:

Computer Forensics

Lab 3:

Basic File System Forensics (Assignment 1)

# Week 3 - Lecture

- Types of Analysis
  - Live Analysis
  - Static Analysis
- Live Analysis Methodology
  - Local Response
  - Remote Response
  - Hybrid
- Order of Volatility
- Live Analysis Toolkits
  - Don’t trust local tools

# Week 3 - Lab

- Assignment 1
  - Hashing
  - Partition Identification
  - Deleted Files
  - Recover files
  - File Signature Analysis
  - Keyword Searching
  - Hash comparison

# Week 4

Lecture 4:

Forensic Report Writing

Lab 3:

Continue Assignment 1

# Week 4 - Lecture

- Chain of Custody
  - When
  - Where
  - How
- Authentication/Hashing
  - Disk
  - Partition
  - Item

# Week 4 - Lecture

- Audience
  - Lawyers
  - Courts
  - Employers / Clients
  - Forensic Professionals

# Week 4 - Lecture

- Report Types
  - Artifact
  - Automatically Generated
  - Forensic Case Report
  - Statement

# Week 4 - Lecture

- Report Content
  - Factual
  - Stick to only your work
  - Balance technical / not technical
  - Relevant metadata
  - Full date/time and timezone
  - Only relevant content

# Week 5

Lecture 5:

Disk and Filesystems

Lab 4:

Windows Forensics

# Week 5 - Lecture

- Hierarchy of Static Data
  - Disk
  - Volume/Partition
  - File
  - Application
  - Acquire at lowest level first where possible

# Week 5 - Lecture

- Hard Disk Geometry
  - Platters
  - Tracks
    - Start at 0, outside to in
  - Cylinder (Same track across all platters)
  - Tracks divided into sectors (typically 512b)
    - Smallest addressable unit
  - Clusters (contiguous sectors)

# Week 5 - Lecture

- Flash Based Storage
  - SSD
  - Forensic Considerations
- Slack Space
  - Forensic Value

# Week 5 - Lecture

- Partitions
  - MBR
  - GUID
  - Primary
  - Extended

# Week 5 - Lecture

- RAID
  - Used for speed or reliability
  - Various levels – 0,1,5 most common
  - Hardware or Software controlled
  - Physical or logical acquisition methods
- Disk Spanning

# Week 5 - Lecture

- Interfaces
  - ATA/IDE
  - SATA
  - ATAPI
  - SCSI
  - Fibre
  - USB
- Hashing

# Week 5 - Lab

- Autopsy in SIFT
- Image verification
- Partition Identification
- Timezone checking and setting
- Email recovery
- Timelining
- Tagging files
- Decoding times

# Week 6

Lecture 6:

File Systems and Pattern Matching

Lab 5:

Introduction to Networks

# Week 6 - Lecture

- Filesystems
  - Organise and store data
  - Imposes structure on top of partition
- Common Filesystems
  - FAT
    - Simple and widely used on removable media
    - File Allocation Table (FAT)
  - exFAT
    - Extended File Allocation Table
    - Designed to be lightweight like FAT but without the extra overhead of NTFS
    - Overcomes volume and file size limitations of FAT

# Week 6 - Lecture

- NTFS
  - Journaled file system
  - Master File Table (MFT)
  - MFT fixed size, can include file content, otherwise has a pointer
- EXT
- UFS
- HFS/HFS+

# Week 6 - Lecture

- Common Features
  - Filesystem information
  - Filename
  - Metadata
  - Content
  - Application specific information
- Deleting vs Erasing
  - Recoverability of deleted files

# Week 6 - Lab

- Tinyweb Server
- Wireshark
- Analysing packet captures
  - HTTP
  - ARP

# Week 7

Lecture 7:

Malware

Lab 6:

Network Forensic Techniques (Assignment 2)

# Week 7 - Lecture

- Hacking/Malware
  - Curiosity
  - Peer recognition
  - Driven by greed
- History of notable virus attacks
- Internet not designed with security in mind
- Zero Day
- Buffer overflow

# Week 7 - Lecture

- Different Types of Malware
  - Viruses
  - Worms
  - Trojans
  - Rootkits
  - Backdoors
  - Spyware
  - Cryptolocker
  - Botnets

# Week 7 - Lecture

- Finding and Detecting
  - Memory Forensics
  - OS Forensics
  - Manual Analysis
  - Signatures

# Week 7 - Lab

- Assignment 2
  - Tinyweb
  - Wireshark
  - Packet Capture
  - Malware

# Week 8

Lecture 8:

Mobile Technologies

Lab 6:

Continue Assignment 2

# Week 8 - Lecture

- Move between towers
  - Handoff/Handover
- Networks designed using cells
- Mobile Station = SIM + Mobile Equipment
- Network Equipment
  - Base Station
    - Antenna
  - Base Station Controller (BSC)
    - Frequency Allocation
  - Mobile Switching Centre (MSC)

# Week 8 - Lecture

- Unique IDs
  - ICCID
  - IMSI
  - IMEI
- Data storage
  - SIM
  - Phone
  - Memory Card
  - Network/Cloud

# Week 8 - Lecture

- Data Types on Mobile Devices
- Online account encryption
  - At rest, in transit or both
  - Challenges
- Complexities
  - Multiple Providers – ISP, Cloud Storage

# Week 8 - Lecture

- Value of Mobile Data
  - Source of crime
  - Planning a crime
  - Evidence of a crime
- Legal Authority
  - Can we access online accounts?

# Week 9

Lecture 9:

Time Zones and Time Lines

Lab:

Final Capstone Lab

# Week 9 - Lecture

- Different Time zone names
  - Greenwich Mean Time (GMT)
  - Coordinated Universal Time (UTC)
  - Zulu Time (Z Time)
- Time zones represent the time offset from GMT/UTC
  - - hours behind GMT/UTC
  - + hours ahead of GMT/UTC

# Week 9 - Lecture

- Importance of timelines in forensics
  - Manual Creation
  - Automated Tools
- Timeline Pivoting
  - Start with known events, look either side
- Time Event Sources
  - Computer based events
  - 3rd Parties
  - Non computer based

# Week 10

Lecture 10:

Anti-Forensics

Lab:

Continue Final Capstone Lab

# Week 10 - Lecture

- Computer anti-forensics
  - Steganography
  - Alternate datastreams
  - Disk encryption
  - Secure data deletion
  - Overwriting metadata
- Network anti-forensics
  - Cryptography
  - Proxying, VPN and Anonymisation
  - Covert channels
- Anti-Forensics can hinder an investigation

# Week 11

Lecture 10:

Capstone Project

Lab:

Continue Final Capstone Lab