CONTENTS

WEEK 1

- Lectures
    - Incident Response v Computer Forensics; Types of Witnesses; Evaluation of Evidence; Standards of Proof; Relevant, Reliable, Sufficient, Persuasive
    - Forensic Copying; E01; dd; Write Blocking; File Systems; Data Recovery
- Readings
    - FAT
    - E01
    - What is Forensics
- Labs
    - Mr Bond Car Hashing and Dissecting Activity

WEEK 2

- Lectures
    - Evidence in pre-trial, evidence in chief, cross examination, re-examination; Fact vs opinion; admissibility and weighting; Hearsay vs Opinion; Evidence by processes, machines and other devices; document definition; Digital footprints and online behaviour; Expert report format; Expert privileges
    - Time; Time synch, time zones, representations of time; Windows Forensics
- Readings
    - Digital Evidence
    - Sample Export Report
    - Expert witness code of conduct
    - Forensic File Carving
    - Window Registry Tool
- Labs
    - Mounting Images and Recovering them

WEEK 3

- Lectures
    - Latin definition of forensics and forensic concepts; Locard's principle; Traces; History of computer forensics; dealing with digital evidence (IOCE); definition of digital forensics and network forensics; DFRWS network forensic challenges; RFC 3227 - Guidelines for Evidence Collection and Archiving; Guidelines for Management of IT evidence;
    - Memory Forensics; pagefile.sys and hibefil.sys; Memory; RAMMap; VMMap; Workflow for Memory Forensics; Windows vs MAC; Volatility
- Readings
    - Bulk Extractor
    - Memory Forensics
    - The CSI effect (jury not understanding evidence)

- Labs
    - Windows Volatility and Cridex
    - Bulk Extractor

WEEK 4

- Lectures
    - Disk Geometry; HDDs and SDDs; Partition table; Volume slack; File System; Directories; File Allocation Table; Deleted Files; NTFS; Timeline Analysis; Update Rules (metadata); Time; Antiforensics;
- Labs
    - M57 Tuck Gorge scenario with Jean and Alison

WEEK 5

- Lectures
    - Traumatic Talk
    - PLIST files; Apple File Systems; APFS and HFS/HFS+; Encryption; T2 SoC; FILEVAULT 2; T2 Secure Boot; Forensic Explorer
- Readings
    - Trauma Reading
    - Apple T2 Security Chip
    - MAC APFS
- Labs
    - MAC analysis and plist files

WEEK 6

- Lectures
    - Network Forensics; Time; Volume of extraneous data; Translating IP address to person or geographical address; DNS and Internet Registries; Whois and IP lookups; IP address and geolocation tools; Mandatory Data retention; Law enforcement requests; PCAP and Netflow;
- Readings
    - Telecommunication Acts
    - UTC
- Labs
    - Wireshark Computers infected; Enisa; Dabber

WEEk 7

- Lectures
    - Expert Witness Code of Conduct; Expert’s report; Presentation in Court
    - QGIS and Google MyMaps

WEEK 8

- Lectures

    - Telecommunications data and metadata; Rights to access of phone without warrant; Right to access communications; Teleco vs Data; Onus of Proof; Sources of Data; Interception and stored communications; Mandatory data retention; Creating a CCR; Coverage Maps;
- Readings
    - Law enforcement request for data
- Labs
    - Graphiz Network Construction

WEEK 9

- Lectures
    - Types of phones; Backups; Key Artefacts; Phone Forensic Software; Challenge of many phones; Establishing Credibility; Spoiling or Tampering with phone evidence;
- Readings
    - Guideline on mobile device forensics
- Labs
    - Cellebrite Phone Extraction

WEEK 10

- Readings
    - Legal Aspects of Artificial Intelligence