Féidearthachtaí as Cuimse
Infinite Possibilities

Exam Prep Session

Forensics- Week 13 – 12th Dec 2025

OLLSCOIL TEICNEOLAÍOCHTA
BHAILE ÁTHA CLIATH
TU DUBLIN
TECHNOLOGICAL
UNIVERSITY DUBLIN

Overview

- High level overview of content covered
- Exam Paper format
- Past Exam Papers

Note

- This is just a guide used in the exam prep session

- All lecture notes, CA's and Labwork is examinable.

Exam Paper format

- Answer all questions.
- Question (1) is worth **40** marks. (4 questions)
- Questions (2) and (3) are worth **30** marks each (3 questions each)

Sample Q and A

- In-class samples of questions and answers

Week 1 – File Carving

- Intro to the module
- Intro to Digital Forensics
- Definitions of Digital Forensics
- File Carving

Week 2 – Intro to Digital Forensics

- What is a digital forensics?
- Forensic examination
- Anatomy of an investigation
- Digital Forensic Models
- Chain of Custody
- Incidents and Hacking
- Sources of Digital Evidence
- Evidence Exchange (Locard)
- Forensics Soundness
- Basic Model
- Casey Model

Week 3 – Exif Metadata

Week 3 – Stego

- Understand the concepts of Steganography

Week 4 – Case Management & Report Writing and Tools of the Digital Investigator

- Managing a case
- Investigation (steps to follow)
- Triage
- First response
- Scene management
- Lab preparation
- Evidence handling
- Evidence examination

- Report writing
- Presentation of results

- Tools of the investigator
- Measuring Suitability of Tools
  - Four necessary traits
- The Daubert Test
- Court Approved Tools

Week 5 – NTFS and MFT

- NTFS File System
- Master File Table Records
- Resident and non-resident files
- NTFS Journaling

- What is available via NTFS
- Operation of MFT
- NTFS – reserved files
- MFT Record
- Journaling

Week 6 – Incidence Response and Digital Evidence in the Courtroom

- Types of Crimes
- Incident Response
- Creating a CIRT
- Content for a CIRT Document
- Incident Handling
- Trying to determine:
  - Means
  - Opportunity
  - Motive

- Hardware and Software Environments
- Filesystems Evidence
- Categories
- Locating Evidence in Filesystems
- Duty of Experts
- Admissibility
- Levels of Certainty in Digital Forensics
- Direct versus Circumstantial Evidence
- Scientific Evidence
- Presenting Digital Evidence

Week 7 – Review Week

Week 8 – Memory Forensics

- Memory Forensics
- Volatility Framework

Week 9 – CyberCrime Law

- From a European Perspective
- From an Irish Perspective
- Jurisdiction
- Convention on Cybercrime
- Irish Laws Generally
- The Criminal Justice (offences relating to information systems) Act 2017
- Paragraph (e) of the General Scheme of Garda Síochána (Powers) Bill

Week 9 – OSINT Framework

- Intro to OSINT
- Tools
- Process to follow
- Who can benefit from using OSINT?
- Usage in an Investigation
- Steps to Perform OSINT
- Reverse Image Lookup

Week 10 – Windows Registry

- What is the Registry?
- Notable content in the Registry
- What is a Registry Hive
- Hive Locations
- General useful content from the registry
- Tracing a USB Device

Week 11 – Email Analysis

- Intro to main e-mail components
- E-mail Headers
- Walkthrough Example
- Key identifiers for an e-mail investigation

- Examining e-mail Headers
- Identify Key Forensic Information
- Interpret Findings
- Steps in Examining an Email
- Important Fields
- Suspicious Events

Week 11 – Mobile Forensics

- General Mobile Forensics
- Acquisition Procedures
- SWGDE Guidelines
- NIST Generic States
- Tools Demo

Week 12 – Web Forensics & Searching the Network

- Artifacts of Browsing
- Browser History
- Finding "Stuff" is Not Enough
- Knowledge of Possession
- Establishing User Actions
- Analysing log files
- Network capture (In-Class Demo – Video on Brightspace)
- Wireshark
- Examining content to create a timeline/narrative

Questions