Seminar session 1: Principles of Digital Forensics and Cyber Law – Introductions

What is Cybercrime:

- Cybercrime is the crime that is done by using a computer network.
- It is illegal behaviour directed by means of any electronic operations, also known as virtual crime.
- Examples: Email and internet fraud, identity fraud (where personal information is stolen and used), theft of financial or card payment data, theft and sale of corporate data, cyberextortion (demanding money to prevent a threatend attack), ransomware attacks (a type of cyberextortion).

What is digital Forensics:

- Digital forensics is used to preserve any evidence in its most original form when performing investigation by collecting, identifying and validating the digital information in order to create a timeline of events.

Area of Forensics:

- Digital forensics can be used in many areas, such as computer forensics, memory forensics, network forensics, mobile forensics, IoT forensics and open source intelligence.
- Computer forensic is related to the forensic investigation in hard disks collected from PCs and laptops.
- In a crime scene, if the computer under investigation is left turned on by the user, the information stored on RAM (Random Access Memory) can be very important in knowing the user's activities.
- The digital evidence on RAM is volatile; therefore, expertise on how to complete the forensic investigation process (memory forensics) is required.

Digital Forensics Tools:

- There are many digital forensics tools that are used by forensics practitioners.
- For example: In Mobile Forensic, Cellebrite Physical Analyser (XPA software and Internet Evidence Finder (IEF) are used.
- IEF is well known software for social media and online investigation.

- CPA and IEF are also used in IoT forensics because many IoT devices are configured by mobile application.
- Autopsy is one of the best Open-source tools for forensics investigation. It is used on Windows and Linux platforms.
- For Hard disk analyses in computer forensics, Encase and FTK are used.
- In oder to conduct memory forensics, many forensics examiners’ choice of tools would be Volatility and redline.

What is Cyber-Law:

- Cyberlaw is the area of law that deals with the Internet’s relationship to technological and electronic elements, including computers, software, hardware and information systems (IS).
- Cyberlwas is also known as Cyber Law or Internet Law.

How Cyberlaw works:

- Increase in Internet traffic has led to a higher proportion of legal issues worldwide.
- Cyberlaws helps to prevent large scale damage from cybercriminal activities.
- It reduces criminal activities by protecting information access, privacy, communications, intellectual property (IP) and freedom of speech related to the use of the Internet, websites, email, computers, cell phones, software and hardware, such as data storage devices.
- Cyberlaws vary by jurisdiction and country, enforment is challenging, and restitution ranges from fines to imprisonment.

Modules details:

- Introduce the foundational legal concepts and terminologies relevant to digital forensics, with an emphasis on evidence and proof.
- Outline the relevant global legal and regulatory environment, including the GDPR and the obligations it imposes.
- Discuss cyber harms and digital rights.
- Introduce ethics in cyber work.
- Examine the challenges and opportunities of regulating and policing cyberspace.
- Explain different types of evidence and evidence collection and the underlying principles of verifiability, continuity and presentation.
- Examine the range of investigations cybersecurity professionals carry out and the challenges of investigation.

Module Outcomes:

- Critically appraise the global legal and regulatory environment as it applies to cyberspace, and compliance requirements, including the GDPR and the obligations it imposes.
- Critically appraise ethical considerations and the rights that people may or may not have in cyberspace, and understand the debates in this area.
- Explore the challenges and opportunities of regulating and policing cyberspace.
- Critically evaluate different types of evidence and collection and presentation techniques, underpinned by the principles of continuity of evidence and reliability of analytical tools and techniques.

Module content:

Unit 6: Mid-Module Assignment 1 – Presentation (19 September 2022)

Unit 9: Mid- Module Assignment 2 – Blog Post (10 October 2022)

Unit 12: End of Module Assignment – Expert Report (31 October 2022)

Seminar:

- Attendance is optional; however, you will benefit from attending these sessions as it's a good opportunity to speak to you tutor and fellow students directly.
- Theses seminars are activities that should attempt prior to each seminar.
- You will find links to recordings in the Module Announcements on the Home page.

E-Portfolio & Discussion Forum:

- Opportunity to use discussion form
- Need of creating a E-Portfolio section