Device Forensics (A14032)

Short Title: Device Forensics
Department: Computing and Mathematics
Credits: 5 **Level:** Advanced

Description of Module / Aims

This module aims to provide students with the skills to uncover information that is found in mobile digital devices. Such devices may include phones, tablets, IoT devices, medical devices, automotive systems. These devices can hold vast amounts of data that can be used in a multitude of environments to recreate a persons movements in online and real world environments.

Programmes

		stage/semester/status
COMP-0495	BSc (Hons) in Computer Forensics and Security (WD_KCOFO_B)	4 / 8 / M
COMP-0495	BSc (Hons) in Applied Computing (WD_KCOMP_B)	4 / 8 / E

Indicative Content

- Mobile Device Forensics
- Acqusition Issues
- Android Forensics
- iOS Forensics
- Connected Devices: Wearable Devices; Internet of Things; Medical Devices; Automotive Industry

Learning Outcomes

On successful completion of this module, a student will be able to:

1. Collect digital evidence from a mobile device.
2. Analyse digital evidence from a mobile device.
3. Reconstruct device usage patterns.
4. Appraise potential issues relating to forensic analysis.

Learning and Teaching Methods

- This module will be presented by a combination of lectures and practicals. The lectures will be used to introduce new topics and their related concepts. The practical element allows the student to put into practice the theoretical concepts covered in the lectures.

Assessment Methods

	Weighting	Outcomes Assessed
Continuous Assessment	100%	
Assignment	50%	1,2,3
Assignment	50%	4

Assessment Criteria

<40%: Unable to perform investigations of mobile digital devices.

40%–49%: Able to perform basic tasks of digital investigations relating to mobile devices.

50%–59%: All of the above and in addition can reason as to the benefits/limitations of surrounding technologies. Can use tools to analyse different data sources associated with mobile devices.

60%–69%: In addition, be capable of discussing the relative merits of associated technologies.

70%–100%: All above to an excellent level. Be able to critically review new and emerging technologies and tools. Be able to discuss their effect on forensic examinations.

Learning Modes

Learning Type	**F/T Hours**	**P/T Hours**
Lecture	12	
Lab	36	
Independent Learning	87	

Essential Material(s)

- Hoog, A. *Android Forensics.* 21 July: Syngress, 2011.

Supplementary Material(s)

- "Digital Investigation Journal." http://www.sciencedirect.com/science/journal/17422876
- "I am the Calvary." https://www.iamthecavalry.org/
- "forensicfocus." www.forensicfocus.com
- Drake, J, Z Lanier, C Mulliner, P Fora, S Ridley and Wicherski G. *Android Hacker's Handbook.* United States: Wiley, 2014.
- Hoog, A and K Strzempka. *iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices.* United States: Syngress, 2011.
- Miller, C, D Blazakis, D DaiZovi, S Esser, V Iozzo and Weinmann R. *iOS Hacker's Handbook.* United States: Wiley, 2012.

Requested Resources

- Computer Lab: BYOD Lab