The Chartered Society of Forensic Sciences

Component Standard - Digital Forensics

Purpose

To equip students with an understanding of the theory and application of analytical methods commonly used in digital evidence examination, recovery & preservation. In addition to equip them to provide justified evaluation and interpretation of the results of analysis for the purposes of intelligence, investigation including those reaching the justice system.

General Outcomes

Students should be equipped to identify and recover a range of digital devices from typical crime scenes appropriate to the course. They should also be able to produce "forensically sound" copies of stored data using appropriate tools and techniques.
Extra Info[1]: By range we mean this may include mock crime scenes but this is not mandatory provided the skills are acquired.

The course should be designed to enable the student to:

A. Understand what we find in the world.

1. Understand the foundations of computer science principles including data structures and algorithms, common physical and network digital architectures, network layers and protocols.

2. Demonstrate[2] a detailed understanding of common physical and logical digital data storage formats including their operation and interfaces.
Extra Info: Considering the logical structure of the NTFS file system, for example we argue a detailed knowledge of this is not required on a day to day basis in the real world. However the ability to recognise anomalies from normal behaviour and to understand the evidential implications, or to prepare for questioning in court, coupled with the ability to 'deep dive' to investigate is more useful.

3. Identify, categorize and describe the basic function of typical embedded, wearable, carry-able, desktop and rack mounted digital devices.
Extra info: This means that students should be able to identify contemporary computing devices in whatever form they may take and understand what data they may store and/or transmit elsewhere in order to determine whether or not the device may be relevant in an investigation. (*They should be able to identify a rack mounted server and differentiate it from a rack mounted network switch for example)*

4. Demonstrate understanding of current operating systems and commonly used application software, where their relevant forensic artefacts may be found and what network traffic they may generate.
Extra Info: This means that students should be competent basic users of the 3 major operating systems (but not necessarily be able to do forensics examinations on all 3, they should be competent on Windows) and be aware of the major office suite software including email and browsers

5. Demonstrate awareness of the basic principles, operation and applications of relevant wireless and

[1] *Extra info: this information may be updated over time as the world of digital technology changes while the key component standard remaining fairly constant.*

[2] *Demonstrate does not necessarily mean students have to be observed performing this in a laboratory but the teaching and assessment must show that this has been achieved.*

physical networking technologies, how to identify and locate them, and the artefacts they produce and retain.
Extra Info: This means being aware of major wireless computing technologies and standards as well as wired standards. This does not mean a Cisco qualification is required, but students should be able to capture live network data and be able to recognize network devices.

6. Demonstrate an understanding of the current digital communication technologies being used for individuals and groups to communicate, such as social media, and where to legally find and acquire the artefacts they produce.
Extra info: This will change over time as different technologies come and go, currently this would include being aware of Skype, Facebook, Twitter, Whats App, and Viber and knowing how to find artefacts relating to these as well as the legal situation with asking providers or other social media witnesses for data.

B. Explain how we acquire and analyse what we find within the context of legal and regulatory standards *- this includes the Forensic Science Regulators Standards - Codes of Practice and conduct, ACPO[3] Good Practice Guide for Digital Evidence.*

1. Demonstrate evaluation, selection and use of appropriate tools and techniques for legal acquisition and analysis, safely handling and archiving digital evidence from storage and network devices in both a dead and live environment, including hashing and cryptographic techniques.
Extra Info: This includes being able to take a strategic approach to minimise cost and/or time to complete a job adequately with limited resources.

2. Understand the importance of validation / verification and evaluation, selection and use of toolsets for data recovery and analysis.
Extra info: There should be an awareness the Forensic Regulator's Code of Practice although this is covered in the IEPE component standard.

3. Demonstrate awareness of common security features and vulnerabilities across typical portable and non-portable digital devices and systems.
Extra info: This includes both file and whole disk encryption techniques.

4. Understand typical threat actors and threat vectors for current digital systems and how they may affect the interpretation of artefacts collected.
Extra info: This includes malware, keylogers and DDOS attacks on systems. Notes:

https://www.russharvey.bc.ca/resources/isthedesktopdead.html

http://www.wired.com/2015/07/death-pc-not-greatly-exaggerated/

5. Understand current anti-forensics techniques including range and applicability in both a local and network context.

6. Demonstrate how to explain the impact of an investigator's actions on the evidence in both a dead and live investigation including the legal ramifications.
Extra info: This covers UK and a wider international audience, it is about the awareness of ACPO Principle 2 and how to mitigate the effects of the investigator when live interaction with data is required.

***Black font** are the fixed standards and can only change with review*
***Red font** are the explanations – which can be changed as the industry develops.*

[3] ACPO – these ACPO principles are still valid and will be transferred across to the National Police Chiefs' Council (National Policing Council)

© The Chartered Society of Forensic Sciences