Digital Forensic Investigation Webinar – Teacher Notes

Introduction

This webinar was recorded with the staff and students from Barnsley College and Fareham College on 3rd March 2021.

The speaker is Stu Richards who is now the Course Leader for the Masters Degree programme in Digital Forensic Investigation at the University of Gloucestershire having been invited to set up one of the UK's first Masters programmes in this discipline because of his background as a Digital Forensic Investigator for Gwent Police.

Paul discusses his experiences both in the private and public sectors, giving examples of cases he's worked on and challenges he has met along the way.

Students were asked to contribute some questions in advance and others were asked throughout the video by students using the chat function. These are introduced as they occur.

Discussion topics/group exercises include:

- The role of the digital forensic investigator
- Examples of tools and techniques used in digital forensic investigation
- Routes into the industry

Video length: approximately 51 minutes

Questions are set at the points shown below:

00:00	Introduction Stu provides an overview of his career to date and explains how this brought him into the role of the Digital Forensic Investigator.
02:53	What do you do with the evidence you gather to make it usable in court? Are there any particular processes?
07:56	What is the best route to get into computer forensics? In this section Stu describes his personal reasons for wanting to get into digital forensics and describes routes to access jobs with organisations such as Tesco and Vodafone. Stu describes a disciplinary case he was involved with where an employee was accused of 'being on Facebook all day'.
14:51	Which element of computing do you really need to understand to work in investigation? Hardware, software or both? In the video Stu mentions 'chip-off extraction'. This 1 minute video from YouTube demonstrates the chip-off technique in a short film from the Canadian Police: https://www.youtube.com/watch?v=5EAFDciA3d4
17:28	**Live Student Question:** Can you learn cyber forensics in the armed forces?

	Stu explains how cyber units work in the armed forces explains how cyber specialists are used in military operations and patrols. He also shows a typical civilian cyber kit (cost about £6,000), explaining that a military version would be much more sophisticated and expensive (circa £28,000).
20:18	When you join the army do you join a specific regiment or do you just join the army and the unit comes later?
22:22	**Live Student Question:** Have you ever used the Parrot Operating System? For students who might be interested in following up on the Parrot OS question, here is a useful link: https://www.parrotsec.org/ Stu also mentions Santoku software: https://santoku-linux.com/ for any student who may wish to follow up. Please note – both of these also have videos on YouTube.
25:29	**Live Student Question:** What operating system do you find you use the most? Stu mentions Cellebrite UFED software: https://www.cellebrite.com/en/ufed-ultimate/ for any student who may wish to follow up. In this section, Stu also mentions Regular Expressions, or Regex. An article on Regex was included in the Spring Student Newsletter. A copy has been placed on the provider site in the Understanding the Industry -> Key and emerging technologies folder.
27:34	Is real computer investigation anything like what you see on programs such as CSI?
30:45	What is the most difficult recovery task you have been involved with? Stu describes a number of cases he was involved with and some of the forensic challenges he faced.
38:12	Is there a lot of pressure when you are working in forensics? Stu is very open and honest about the downsides of working in forensic investigation, including how it can impact on your mental health.
43:42	**Live Student Questions:** a) Have you ever had to compromise your own values and morals for your job? and b) How do you go from the work mindset, under all that pressure, to your home life?
51:14	Thank you and webinar close.

Digital Forensic Investigation Webinar – Teacher Notes

Teacher suggestions:

You could use the whole, or parts of the video using the time stamps above.

To set the scene you could ask students whether they think that files, chats and media that they store on their mobile devices can ever be completely deleted?

Below are some useful background articles and videos you could use to stimulate discussion:

Digital Forensic Investigation (publication date and author unknown): https://digitpol.com/digital-forensic-investigation/ This article is a brochure for an organisation called Digitpol. Stu talks specifically about mobile forensics, but the digital forensic investigative space does have facets such as drone and WiFi forensics. This website lists a wide range of applications for forensics.

Computer and Cyber Forensics BSc (Hons) at University of Gloucestershire (accessed 11th March 2021): https://www.glos.ac.uk/courses/course/computer-and-cyber-forensics/bsc-hons-computer-and-cyber-forensics-flex-pt/ has been included to show students the range of skills and techniques they would learn on a digital forensics programme.

Inside the FBI's digital forensics laboratory (published 21st August 2020): https://www.youtube.com/watch?v=lA_flSH-FrU is a 2 minute video which may surprise you.

Top 10 free tools for digital forensics (published 30th July 2014): https://www.youtube.com/watch?v=zjK-JThLg_Y introduces a range of free digital tools in a 2.5 minute video.

Below is a small group or pair activity which can be carried out in class or given as homework.

Activity: Chain of Custody

During the video Stu talks about the need to prepare digital forensic evidence for court cases. But what are the UK regulations?

Work with a partner or small group and use your research to answer the following questions:

- What are the main processes in the chain of custody for digital evidence?
- How can the chain of custody be assured?

Create one or two PowerPoint slides with the results of your research.

Digital Forensic Investigation Webinar – Teacher Notes

Teacher: The following links could be issued to students to support the activity, but will largely provide the answer.

What is the Chain of Custody in Digital Forensics? (publication date and author unknown): https://www.linealservices.com/what-is-the-chain-of-custody-in-digital-forensics/ provides an overview of the main processes and examines how the chain of custody can be assured.

Computer Evidence and Legal Proceedings by Athena Forensics (published 29th October 2018): https://athenaforensics.co.uk/computer-evidence-and-legal-proceedings/ provides similar information to the first link, but also includes an example of what can go wrong in the chain of evidence.

Chain of Custody – Digital Forensics (published 2nd June 2020, author unknown): https://www.geeksforgeeks.org/chain-of-custody-digital-forensics/ is a very readable overview which also includes bulleted lists and a useful diagram.