Digital Forensic Unit

Lancashire Constabulary

Digital Media Investigation Unit

BACKGROUND | NIGEL

1988 – 2000
Royal Bank of Scotland (branch staff, credit/debit cards, Cash/Bullion processing centre, Horwich Service Centre)

2000 – 2014
Lancashire Constabulary
Finance Assistant, IT Liaison Officer, 2008 transfer to High Tech Crime Unit, Computer Technician

2014 – 2018
Digital Forensic Technician, Digital Media Investigation Unit
December 2017 – completed and passed MSC in Forensic Computing and Cybercrime Investigation, University College Dublin.

2018 – present

Digital Forensic Investigator/Examiner, Digital Forensics Unit

WHAT IS DIGITAL FORENSICS?

The UK Forensic Science Regulator **DEFINES DIGITAL FORENSICS** as: *the process by which information is extracted from data storage media (e.g. devices, systems associated with computing, …), rendered into a useable form, processed and interpreted for the purpose of obtaining intelligence for use in investigations, or evidence for use in criminal proceedings*

OVERVIEW

- Digital Forensics can be used to gather evidence in many criminal investigations
- Legislations on agencies powers to access communications continues to be debated
- The forensic science regulator requires all digital forensics practitioners undertaking criminal justice work was to be accredited by 2017, but accepts this will be challenging (ISO 17025)
- Encryption and cloud storage can inhibit digital forensics investigations but offer security and flexibility to its users.
- Rapid development and adoption of technology is increasing demand for digital forensics services. Methods such a triaging are being used to address this demand.

LEGISLATION AND REGULATION

POLICE AND CRIMINAL EVIDENCE ACT 1984 (PACE)

PACE sets out to strike the right balance between the powers of the police and the rights and freedoms of the public. Maintaining that balance is a central element of PACE

COMPUTER MISUSE ACT 1990 (CMA)

The Computer Misuse Act of 1990 is a law in the United Kingdom that makes certain activities illegal, such as hacking into other people's systems, misusing software, or helping a person to gain access to protected files of someone else's computer.

NPCC GUIDELINES | The 4 Principles

PRINCIPLE 1 | *Don't change data*
"No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court"

PRINCIPLE 2 | *Be competent*
"In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of there actions."

PRINCIPLE 3 | *Keep an audit trial*
"An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result."

PRINCIPLE 4 | *SIO/OIC is in charge*
"The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to."

“IT IS ESTIMATED THAT 90% OF REPORTED CRIME HAS A DIGITAL ELEMENT”

(www.gov.uk)

TYPES OF STORAGE MEDIA

Laptops

Digital Cameras

Desktops

CCTV

iPads/ Tablets

External HDD

Sim Card

Mobile Phones

USB sticks

Memory Cards

Smart TV

Dash Cam

REMOVAL AND ACQUIRING OF DATA

Recovery of data includes;

- Data is extracted, which may involve making a copy of a hard disk, extracting data from a mobile phone, or recovering data from a remote system.
- Data is then processed to allow an examiner to work on them.
- This can include decrypting data and recovering files

EXAMINATION OF DATA

Data is analysed and interpreted, which often involves synthesising information from different sources. This may require significant expertise.

KIOSKS

A Kiosk features bespoke forensic investigation software is being trialled by the Metropolitan Police Service and other forces. It is designed to enable front-line police officers (after a day of training, for example) to collect evidence from mobile devices by following a series of on-screen instructions. Devices are plugged into the kiosk and analysed. Officers then use the software to extract relevant information and to produce a standard report on the items found.

TRIAGE

- Triage can be used to determine whether a device should be prioritised for further investigation.

- It may involve police on the scene assessing whether a device is likely to be useful before seizing it, or making a rapid search of it once seized to decide whether to pass it onto a specialist team.

- On-the-scene triage might involve officers examining computers using a USB stick with forensic software. Triaging kiosks are being piloted by some police forces as one method for triaging seized devices

DIGITAL FORENSIC CHALLENGES

ACCESSING DATA

The data required are not always readily available to investigators. They could be encrypted or stored in the cloud, making access difficult. Criminals with technical expertise may also use anti-forensics to hide their tracks.

ENCRYPTION

Encryption is a critical tool for protecting personal or commercially sensitive data. However, in some forms it may hamper digital investigations. Encryption is the process of scrambling data so that it can only be read by an authorised recipient. The original information is encoded using an encryption key and algorithm. A corresponding key and algorithm are then needed to decrypt the data.

CLOUD STORAGE

Users' data and activity records are less likely to be held locally on devices, thus a device may not yield evidence, even if forensic techniques are used. Moreover, cloud service accounts (like many online services) are often password-protected.

Data can be requested from the cloud service providers. However, these companies are often based outside the UK and the servers on which the data are stored can be anywhere in the world. Investigators use MLAT (Mutual Legal Assistance Treaties) to ask local law enforcement agencies to issue a warrant to the company to obtain the data.

ANTI-FORENSICS

Some criminals are aware of the techniques available to law enforcement and try to hide their digital activity. The processes they use, known as anti-forensics, tend only to occur in the most complex cases. Such techniques may leave traces that could alert investigators to missing evidence.
Practices include:

- Changing the dates and times associated with files to stop investigators building a reliable timeline of events
- Permanently erasing files by overwriting them
- Using encrypted digital storage with multiple passwords leading to different sections of the drive. Revealing the password to one section (which contains nothing incriminating), does not disclose whether there is a hidden section containing evidence

Man who created indecent images using AI-enabled technology sentenced to 24 years

The use of computer software and AI within online offending is an area we are noticing is growing, but my message to offenders who think creating indecent material in this way means they will not be caught out and relentlessly pursued is to think again.

[Man who created indecent images using AI-enabled technology sentenced to 24 years | Greater Manchester Police]

Hugh Nelson has been jailed

Hugh Nelson (08/01/1997) of Briggsfold Road, Bolton pleaded guilty at Bolton Crown Court last month (Friday 9 August 2024) to 11 child sexual offences, and had already pleaded guilty to another five offences in July 2023. More information on his offending can be found here.

CROWN COURTS | Lancaster & Preston

CASE STUDY | Operation Colindale

The Murder of Aya Hachem | 2020

[Seven men jailed for drive-by murder of student Aya Hachem | 5 News - YouTube]

CASE STUDY | Operation Colindale

Op Colindale, as the investigation is known, has been one of the longest-running and most complex that the Force has ever dealt with. Coupled with the added challenges that the Covid-19 pandemic brought, a special thank you and recognition has to go to all of those involved – up to 400 people from across the organisation!

3959 exhibits were generated, of which:

- 120 phones
- 180 digital storage devices
- 80,000 hours of CCTV seized
- Extensive CCTV and telephone enquiries looking at the time before, during and after the incident
- 30 vehicles seized

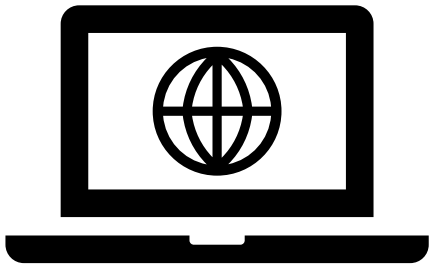
CONVICTED!!

7 Men were convicted on Tuesday 3rd August 2021

A woman was found guilty of manslaughter

They will serve a total of 216 years between them.

https://joinus.lancashire.police.uk/explore-our-roles




Caps Lock
ANY QUESTIONS
Fn