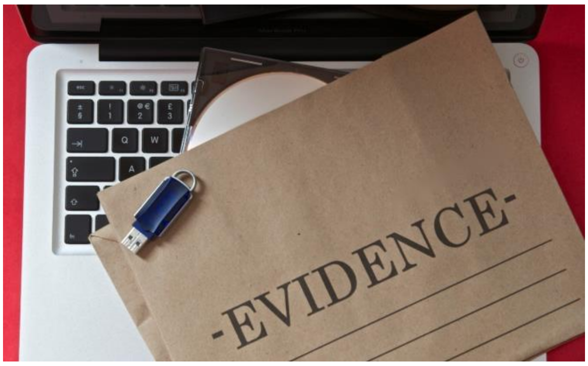
HOUSES OF PARLIAMENT
PARLIAMENTARY OFFICE OF SCIENCE & TECHNOLOGY

POSTNOTE

Number 520 March 2016

Digital Forensics and Crime



Digital forensic science is the process of obtaining, analysing and using digital evidence in investigations or criminal proceedings. Digital evidence ranges from images of child sexual exploitation to the location of a mobile phone. This note looks at how evidence is obtained, legislation and regulation, and efforts to address challenges faced by practitioners.

Overview

- Digital forensics can be used to gather evidence in many criminal investigations.
- Legislation on agencies' powers to access communications is being debated.
- The Forensic Science Regulator requires all digital forensics practitioners undertaking criminal justice work to be accredited by 2017, but accepts this will be challenging.
- Encryption and cloud storage can inhibit digital forensic investigations, but offer security and flexibility to users.
- Rapid development and adoption of technology is increasing demand for digital forensic services. Methods such as triaging are being used to address this demand.

Background

The ubiquity of digital devices means that digital evidence may be present in almost every crime.[1] This offers new opportunities for police investigations. However, the proliferation of devices is increasing demand for digital forensic techniques (Box 1).[2] This increase is compounded by rapid growth in the volume of data stored on devices, further adding to forensic workloads. Some police forces have delays of up to 12 months for the analysis of devices,[3] and policing organisations have identified a need to develop their digital investigation capabilities.[4]

Law enforcement and intelligence agencies undertake large numbers of digital forensic analyses (Box 2). These can provide evidence of criminality (e.g. by finding plans for a terrorist attack), exonerate suspects (e.g. by corroborating an alibi), or generally aid an investigation (e.g. locating a missing person). Commercial companies may also use digital forensic techniques in internal investigations, such as examining an information security breach. This note looks at the use of digital forensics by UK law enforcement agencies.

Agencies may conduct digital forensic analyses in-house or contract them out to commercial forensic service providers. This is often done through a tendering process, as the Government-run national forensic procurement framework does not extend to digital forensics.[5] Agencies can also seek support from the National Technical Assistance Centre,[1] a part of GCHQ.[6] Publicly available information about agencies' spending on forensic services is limited.[5]

Traditionally, digital forensics mainly involved extracting data from PCs and laptops.[7] Now, other devices are also important: the Metropolitan Police examines around 40,000 devices annually, almost three quarters of which are mobile phones.[2] Data sources include smart phones, WiFi routers, GPS equipment, CCTV, building access recorders, smart TVs, games consoles and fitness watches.[8] The diversity of sources is growing as the number and variety of devices that store data and connect to networks increase (POSTnote 423).[9-11]

Information about the use of devices may also be available from service providers, for example determining a mobile phone's location from the cell masts it connects to.[13] Publicly available data such as Facebook or Twitter profiles can also provide evidence.[1] With lawful authority, evidence may be captured 'in transit' by intercepting voice calls, emails or other communications.

Box 1. Defining Digital Forensics

There is no standard definition, but 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.*[12]

Box 2. Examples of Using Digital Evidence
Agencies using digital forensics include police forces, intelligence agencies, the National Crime Agency, HMRC, the Financial Conduct Authority (FCA), Border Force, the Serious Fraud Office and others.

Counter-terrorism: Operation Rhyme[14]
In 2006, Dhiren Barot was convicted of conspiracy to murder for planning terrorist attacks on the UK and US. Investigators at the Metropolitan Police examined 274 computers and 1,785 external storage media devices in what was then the largest counter-terrorist investigation launched in the UK.[14,15] Some of the material had been deleted or encrypted but was forensically recovered and demonstrated the extent of his planning.[16]

Child Sexual Abuse Images: Dominic Stone, October 2011
Dominic Stone was working as a clergyman when he downloaded hundreds of images of child sexual abuse. Although he suggested someone else may have downloaded them, digital forensic techniques revealed that the computer had been used for purposes related to his church work while the images were being downloaded.[17,18]

Insider Dealing: Operation Saturn, July 2012
The FCA prosecuted an insider dealing ring that had been profiting from buying and selling shares using leaked confidential information. Two print-room employees were sharing confidential documents detailing takeover bids involving the companies they worked for. The FCA was able to implicate the ring by gathering multiple sources of digital information including telephone records, computer log files (Box 3), and office entry and exit records. It compiled these to create timelines tracing the documents and the actions of the ring.

The Digital Forensics Process
Though investigations vary, the process is likely to include:

- Recovery – data are extracted, which may involve making a copy of a hard disk, downloading data from a mobile, or recovering data from a remote system.[1,12] Data are then processed to allow an examiner to work on them. This can include decrypting data and recovering files (Box 3).
- Interpretation – data are analysed and interpreted, which often involves synthesising information from different sources. This may require significant expertise.
- Presentation – findings from the analysis are communicated; for instance verbally to the investigation team, as a written report, or perhaps eventually in court.

Legislation and Regulation
Data on a device can be searched if the device has been lawfully seized, such as under the Police and Criminal Evidence Act 1984.[19] Law enforcement and security agencies may, with a warrant, intercept the content of communications for the most serious investigations. They may also acquire information about communications (such as who contacted whom and when) from communications service providers. These powers are currently governed by the Regulation of Investigatory Powers Act 2000,[20] the Data Retention and Investigatory Powers Act 2014,[21] and other legislation (HoC Library briefing SN06332). Investigators can also acquire data via equipment interference (such as bugging or hacking a device). Police may either do this using physical equipment (Police and Crime Act 1997),[22] or software that allows remote access to the device (Serious Crime Act 2015,[23] which grants certain exemptions from the Computer Misuse Act 1990).[24]

Parliament is currently considering the Investigatory Powers Bill.[25] The Government intends the Bill to consolidate the powers available to security, intelligence and law enforcement agencies to obtain communications and data about communications.[26] It aims to provide a more transparent basis for seeking the warrants required for interception and equipment interference, and to enhance safeguards by introducing judicial oversight. However, there has been considerable opposition to the Bill (HoC Library briefing CBP-7371). A draft version of the Bill has been examined by three Parliamentary Committees.[27-30] Six new draft codes of practice, including two providing guidance on equipment interference and the interception of communications, were published alongside the Bill.[31]

Evidence is subject to the Criminal Procedure Rules 2015,[32] and there are best practice guidelines for law enforcement personnel dealing with digital evidence.[1] These include the principles that data should not be changed by an investigation and that records should be kept of all of the processes applied to data. The Forensic Science Regulator (FSR) is responsible for upholding the quality of digital forensic services within the UK Criminal Justice System (CJS),[33] although she currently has no statutory powers to ensure compliance.[5] The FSR says that the risk of errors occurring in digital forensics is significant.[34] By October 2017, all digital forensic practitioners working for the CJS will need to be accredited to ISO 17025 for most of their work. However, the FSR says that meeting the 2017 deadline will be challenging. Based on this standard, she has published codes of practice and conduct, which include analyst competence, the validation of methods, and the handling and storage of test items.[35]

Digital Forensics 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. It is a cornerstone of electronic security technologies, used by businesses, governments and individuals.[36] However, in some forms it may hamper digital investigations.[37] Encryption is the process of

Box 3. Recovering Files

Deleted Files
When a user deletes a file, it is rarely erased from the system. Computers create tables that tell the system where to look for the file's data. When deleting a file, the system merely removes the reference from the table; the data remain until overwritten by something else. Until then, the data can be extracted and reconstructed.

Log Files
Log files, or event logs, are files that a system writes to record significant events. These include information such as when a user logs onto the system,[34] the hardware used with the system (such as printers or removable storage), and data about network connections.

scrambling data so that it can only be read by an authorised recipient.[38] The original information is encoded using an encryption key and algorithm. A corresponding key and algorithm are then needed to decrypt the data.[39]

Stored data, drives and devices can be encrypted, as can online communications such as emails and instant messages. Some email providers encrypt data in transit,[40] and users may be able to apply stronger encryption to their emails if desired. For example, end-to-end encryption – where only the sender and receiver can decrypt and read the communication – is being offered by some providers.[41,42] To date, the optional encryption on most computers and mobiles can be activated by the user.[43] However, major manufacturers are now supplying devices with encryption turned on by default, for which they may not have the key.[44-48] Such developments could lead to digital evidence becoming less accessible to investigators.

Cloud Storage

Increasing use of cloud computing (which involves online access to shared computing resources, such as data storage, processing and software) presents a challenge to digital forensic practitioners. Data can change quickly, and anything deleted by one user may be rapidly overwritten by another. This can result in the loss of relevant information and can make later verification of the data (for example by the defence) difficult.[49] 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.[50]

Law enforcement agencies can request data stored in the cloud from the cloud service provider. 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 Mutual Legal Assistance Treaties to ask local law enforcement agencies to issue a warrant to the company to obtain the data. Law enforcement agencies say that this strategy can be extremely slow.[19]

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.[51] Some of these practices are used legitimately, not as anti-forensics tools, but by those seeking to protect data and privacy. 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.[52,53]

Rapidly Changing Technology

The rapid pace of technological change presents a significant challenge to digital forensic practitioners.[1] New hardware, operating systems and applications must be studied to discover how to reliably find information of forensic value.[54,55] This requires the development and testing of new techniques, which can leave digital forensic practitioners playing catch-up.[56] Another problem faced by investigators is the high and increasing volume of data stored on devices. Processing data can take a long time, and increases in data storage and in the number of devices associated with crimes have led to increased pressure on forensic services.[2] Large volumes of data can also make it difficult for investigators and prosecutors to fulfil their obligations under the Criminal Procedure and Investigations Act 1996. According to the Act, a 'disclosure officer' has a duty to inspect, view or listen to all relevant material in the investigation.[1,57] The Attorney General's Guidelines on Disclosure 2013 suggest that it might be reasonable to examine digital material by, for instance, using software search tools.[58] Budgetary constraints will be a key factor in responding to technological change.[4]

Skills

Anecdotal reports suggest that skills retention is a problem in some police forces, although data on this are not currently collected. Skilled individuals are highly sought after and companies can often offer higher salaries for similar work.

Addressing the Challenges

Accessing Data

Cracking Cryptography and Hacking Devices

Data on encrypted devices or in the cloud can be accessed if an investigator has the user's encryption key or password. These might be found in the volatile memory of the device (the part of memory that is erased when the machine switches off), or might have been written down by the user. If the user will not disclose the password or key, an official (such as a District Judge)[59] can serve a notice requiring them to,[60] with a penalty of up to five years in jail for failing to comply.[61,62] An investigator may also try to crack the encryption (Box 4) or access the account by brute force. However, in the case of modern, well-implemented encryption, this will generally fail.[63]

Investigators might use equipment interference to access remotely (hack) a computer while it is still in use, to obtain passwords and encryption keys. Hacking exploits vulnerabilities that could be used for either legal or criminal purposes.[65] This may result in a tension for law enforcement between using vulnerabilities and disclosing them to

Box 4. Breaking Encryption

Encrypted data cannot be read without the appropriate key. Finding this can be a matter of brute force – randomly generating keys and applying them to the encrypted data to see if they produce a meaningful result. Longer keys require more computing power and time to crack them, as there are more possible combinations to try. A 128-bit key consists of a string of 128 0s and 1s, offering 340 trillion trillion trillion possible keys. This is effectively uncrackable; estimates suggest a brute force attack would take over a billion billion years.[64]

software manufacturers for fixing.[66] Privacy campaigners have raised concerns about the integrity of evidence obtained from a device that has been subject to equipment interference.[65] For example, a piece of malware that sends passwords to the investigator might in theory modify or deposit evidence.

Encryption Backdoors and Key Escrow

The Investigatory Powers Bill seeks to grant the Secretary of State the power to oblige service providers to remove any “electronic protection” that they (the service provider) have applied to communications or data.[27] There is ambiguity over what this term might cover.[63,67] Privacy advocates have suggested that this requirement might be incompatible with some services, such as end-to-end encryption, and that this would introduce information security risks.[68,69] It has also been suggested that the obligation to remove electronic protection could require the building of “backdoors” or vulnerabilities into encryption systems, which could be used by law enforcement to access data.[63]

Debates around the use of encryption have also included the idea that all encryption keys could be held by a trusted third party, accessible to law enforcement when required. This is a form of key escrow. A type of key escrow featured in the 1999 Draft Electronic Communications Bill, but was dropped and has not been considered in legislation since.[70]

The deployment of key escrow or backdoors would require keeping the keys secure and knowledge of the backdoors secret, as their release could render vulnerable all data ever encrypted with that system.[71] Some security experts argue that providing such access to law enforcement alone would be unworkable and could increase security risks for users.[72] In recent evidence to the Joint Committee, the Home Secretary denied that the Government is looking to service providers to provide agencies with a backdoor or key.[73]

Addressing the Digital Forensic Workload

Some police forces are outsourcing cases to commercial companies, which can help clear backlogs.[2,74] New approaches are being adopted to address the disparity between the demand for services and available resources.

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. There are many triage tools. For example, on-the-scene triage might involve officers examining computers using a USB stick with forensic software.[75] Triaging kiosks are being piloted by some police forces as one method for triaging seized devices (Box 5).

Triaging requires front-line officers to have some understanding of potential evidence sources, and police are building digital awareness into probationer training.[4]

Box 5. Triaging Kiosks

A triaging kiosk featuring 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.

However, front line-officers will not typically have detailed knowledge of how triaging software works. If a tool were to overlook evidence, the officer may not realise. Police training highlights this risk and the potential need to escalate the investigation to specialist colleagues, particularly should officers not find what was expected. Nevertheless there are concerns that using investigating officers for this work may potentially conflict with the Regulator’s requirement for digital forensic practitioners to be independent and impartial.[76] Police say it might be possible to reduce this risk, for example by ensuring that officers do not interpret triage results and only use them as factual evidence.[77]

Streamlined Forensic Reporting

Streamlined Forensic Reporting (SFR) is being used to deliver DNA and fingerprint evidence to UK courts, to reduce the time and cost of gathering forensic evidence.[78] SFR involves police investigators preparing a short report early in an investigation, detailing the key forensic evidence the prosecution intend to rely on. The aim is to achieve early agreement with the defence on forensic issues, or to identify the contested issues. The Crown Prosecution Service says that SFR is also appropriate for digital evidence.[79]

Police and Government Strategy

In December 2015, the Government announced £4.6m of police force funding for digital policing reform.[80] The College of Policing, National Crime Agency and National Police Chiefs’ Council have recognised a need to develop digital investigation and intelligence capabilities. In April 2015, they highlighted priority areas that include:

- developing partnerships with academia and industry
- enhancing awareness of digital evidence among officers
- developing career paths for digital specialists.[4]

In 2013, the House of Commons Science and Technology Committee noted a shortage of UK funding for forensic science research, and renewed recommendations that the Government develops a strategy for forensics.[5,81,82] The Home Office is planning to publish this in 2016. The Home Office is also beginning to collect statistics from police forces in England and Wales on their use of digital forensics. The Government Chief Scientific Adviser’s 2015 annual report examined forensic science, including digital forensics, and its many applications.[83]

POST is an office of both Houses of Parliament, charged with providing independent and balanced analysis of policy issues that have a basis in science and technology. POST is grateful to Kathryn Boast for researching this briefing, to the Science and Technology Facilities Council for funding her parliamentary fellowship, and to all contributors and reviewers. For further information, please contact the co-author, Dr Lydia Harriss. Parliamentary Copyright 2016. Image Copyright Grumpy59.

Endnotes

[1] ACPO Good Practice Guide for Digital Evidence, Association of Chief Police Officers (2012)

[2] Information for Prospective Bidders, Metropolitan Police Service – Digital Cyber and Communications Forensics Unit (2015)

[3] Online and on the edge: Real risks in a virtual world, HM Inspectorate of Constabulary (2015)

[4] Digital Investigation and Intelligence, College of Policing, National Crime Agency, National Police Chief's Council (2015)

[5] The Home Office's Oversight of Forensic Services, National Audit Office (2014)

[6] NTAC – What Is It?, Inside Time (2015)

[7] An Examination of Digital Forensic Models, Reich *et al* (2002)

[8] Digital Forensics, Innovate UK (2015)

[9] Alternate Data Storage Forensics, A. Schroader & T. Cohen (2007)

[10] Internet of Things Forensics, Champlain College Computer & Digital Forensics Blog (2015)

[11] Digital forensics in the age of the Internet of things: Challenges and opportunities, Samuel Liles (2014)

[12] Forensic Science Regulator Newsletter No. 26, Forensic Science Regulator (2015)

[13] What is Cell Site Analysis, LGC Group

[14] Terrorist jailed for life for conspiracy to murder in the UK and US, Metropolitan Police Service (2006)

[15] The Government's Counter–Terrorism Proposals, HoC Home Affairs Committee (2007)

[16] Operation Rhyme Terror Convictions, Metropolitan Police Service (2007)

[17] Vicar walks free after child porn conviction, The Independent (2010)

[18] Vicar 'accessed child porn while working', BBC News (2010)

[19] E-crime, HoC Home Affairs Committee (2013)

[20] Regulation of Investigatory Powers Act, UK Government (2000)

[21] Data Retention and Investigatory Powers Act 2014, UK Government (2014)

[22] Police and Crime Act 1997, UK Government (1997)

[23] Serious Crime Act 2015, UK Government (2015)

[24] Computer Misuse Act 1990, UK Government (1990)

[25] Investigatory Powers Bill, UK Government (2016)

[26] Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny, UK Government (2016)

[27] Draft Investigatory Powers Bill, Home Secretary (2015)

[28] Draft Investigatory Powers Bill Report, HoC HoL Joint Committee (2016)

[29] Report on the Draft Investigatory Powers Bill, Intelligence and Security Committee of Parliament (2016)

[30] Investigatory Powers Bill: Technology Issues, HoC Science and Technology Committee (2016)

[31] Investigatory Powers Bill: codes of practice, Home Office (2016)

[32] The Criminal Procedure Rules 2015, UK Government (2015)

[33] About Us, Forensic Science Regulator

[34] Annual Report, Forensic Science Regulator (2015)

[35] Codes of Practice and Conduct Appendix: Digital Forensic Services, Forensic Science Regulator (2014)

[36] Cryptography for Network and Information Security, Microsoft TechNet

[37] The growing impact of full disk encryption on digital forensics, Casey *et al* (2011)

[38] What is encryption?, Microsoft

[39] Data Encryption, Parliamentary Office of Science and Technology (2006)

[40] Transparency Report: Protecting emails as they travel across the web, Google (2014)

[41] User-Focused Security: End-to-End Encryption Extension for Yahoo Mail, Yahoo (2015)

[42] An Update to End-To-End, Google (2014)

[43] How does Android Lollipop's encryption affect me?, Android Central (2015)

[44] iPhone 6 specifications, Apple

[45] iOS Security Guide, Apple (2015)

[46] New Android Marshmallow devices must have default encryption, Google says, Naked Security by Sophos blog (2015)

[47] Government Information Requests, Apple

[48] Helping to protect your files with device encryption, Microsoft

[49] NIST Cloud Computing Forensic Science Challenges, NIST Cloud Computing Forensic Science Working Group (2014)

[50] How to Safely Store your Data in the Cloud, Boston University

[51] Anti-Forensics: Techniques, Detection and Countermeasures, S. Garfinkel (2007)

[52] Anti-forensic Techniques, Forensics Wiki (2015)

[53] Hidden Volume, Codeplex.com (2014)

[54] Digital Forensics Research: The Next 10 Years, S. Garfinkel (2010)

[55] Digital Forensic Reverse Engineer and Researcher (UK Based), ADF Solutions (2015)

[56] Forensic science standards in fast-changing environments, P. Sommer (2010)

[57] CPS Disclosure Manual, Crown Prosecution Service

[58] Attorney General's Guidelines on Disclosure, Attorney General (2013)

[59] Regulation of Investigatory Powers Act 2000: Schedule 2, UK Government (2000)

[60] Regulation of Investigatory Powers Act 2000: Section 49, UK Government (2000)

[61] Regulation of Investigatory Powers Act 2000: Section 53, UK Government (2000)

[62] Annual Report, Office of Surveillance Commissioners (2015)

[63] Oral evidence: Investigatory Powers Bill: technology issues, HoC Science and Technology Committee (2015)

[64] How secure is AES against brute force attacks?, EE Times (2012)

[65] Draft Equipment Interference Code of Practice Submission, Open Rights Group (2015)

[66] Liberty and Security in a Changing World, The President's Review Group on Intelligence and Communications Technologies (2013)

[67] Apple raises concerns over UK's draft surveillance bill, BBC News (2015)

[68] Privacy International Submission In Response To Science & Technology Committee Call For Evidence On The Draft Investigatory Powers Bill (2015)

[69] Investigatory Powers bill will remove ISPs' right to protect your privacy, The Conversation (2015)

[70] Research Briefing: The Electronic Communications Bill (revised edition), HoC Library (1999)

[71] The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption, H. Abelson *et al* (1998)

[72] Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications, MIT Computer Science and Artificial Intelligence Laboratory Technical Report (2015)

[73] Oral evidence: Draft Investigatory Powers Bill: Home Secretary, Joint Committee on the Draft Investigatory Powers Bill (2016)

[74] Outsourcing Forensic Analysis, Evidence Technology Magazine (2010)

[75] One example of this is http://www.adfsolutions.com/products/triage-responder

[76] Codes of Practice and Conduct, Forensic Science Regulator (2014)

[77] Personal communication with Mark Stokes, Head of Digital, Cyber and Communications Forensic Unit, Metropolitan Police Service

[78] Streamlined Forensic Reporting Guidance and Toolkit, Crown Prosecution Service (2015)

[79] National Streamlined Forensic Reporting Guidance Section 2 – The Toolkit, Crown Prosecution Service (2015)

[80] Police Grant Report England and Wales 2016/17, Minister of State for Policing, Crime and Criminal Justice (2015)

[81] Forensic Science, HoC Science and Technology Committee (2013)

[82] The Forensic Science Service, HoC Science and Technology Committee (2011)

[83] Forensic science and beyond**,** Government Chief Scientific Adviser (2015)