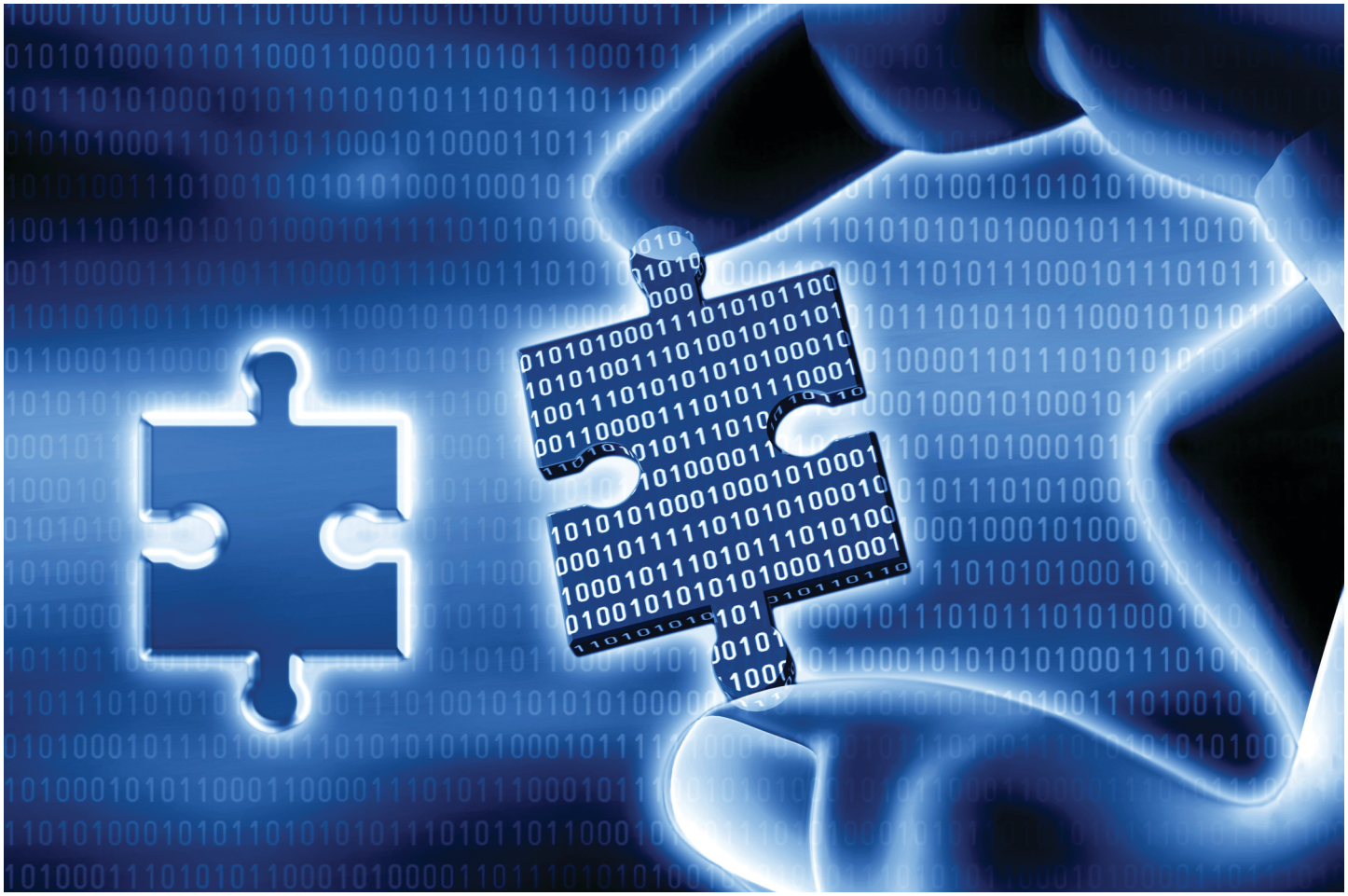
OpenLearn

The Open University

Digital forensics



About this free course

This free course is an adapted extract from the Open University course M812 *Digital forensics* www.open.ac.uk/postgraduate/modules/m812.

This version of the content may include video, images and interactive content that may not be optimised for your device.

You can experience this free course as it was originally designed on OpenLearn, the home of free learning from The Open University – www.open.edu/openlearn/science-maths-technology/computing-and-ict/digital-forensics/content-section-0

There you'll also be able to track your progress via your activity record, which you can use to demonstrate your learning.

Intellectual property

Contents

Introduction 4
Learning Outcomes 5
1 What is digital forensics? 6
2 What is forensic science? 7
- 2.1 Science, the scientific method and scientific laws 7
- 2.2 Forensic scientists 9
- 2.3 Case study: The Shirley McKie story 15
- 2.4 Summary of Section 2 17

3 The role of the forensic scientist in law 18
- 3.1 Legal decision-making 18
- 3.2 The role of the court 19
- 3.3 Contrasting scientific conclusions with court judgments 20
- 3.4 Summary of Section 3 21

4 The role of digital forensics 22
- 4.1 The digital forensic process 22
- 4.2 A brief history of digital forensics 23
- 4.3 Different types of digital forensics 24
- 4.4 Summary of Section 4 26

5 Conclusion 27
Keep on learning 28
References 29
Acknowledgements 29

Introduction

This free course, *Digital forensics*, is an introduction to computer forensics and investigation, and will give you an overview of forensic science in general, including how it works in practice. It will introduce you to the world of digital forensics, that is, applying forensic science to the digital artefacts that we create every day through our interactions with computers, mobile phones and the unseen objects around us that encompass the so-called 'internet of things'.

This OpenLearn course provides a sample of postgraduate study in Maths.

Learning Outcomes

After studying this course, you should be able to:

- explain the origins of forensic science
- explain the difference between scientific conclusions and legal decision-making
- explain the role of digital forensics and the relationship of digital forensics to traditional forensic science, traditional science and the appropriate use of scientific methods
- outline a range of situations where digital forensics may be applicable
- identify and explain at least three current issues in the practice of digital forensic investigations.

1 What is digital forensics?

Digital forensics is an exciting area, often glamorised (and its capabilities exaggerated) in films and television shows like *CSI*, *NCIS* and *Spooks*. You may have heard the area described using slightly different words, each of which may bring to mind different activities.

Activity 1

(Allow 10 minutes)

Let's get started with a simple activity. Write down all the topics that you can think of that might be encompassed by the term 'digital forensics and investigations'.

Discussion

Here are some of the names I thought of; your list should include at least some of these:

- computer forensics
- forensic computing
- forensic science
- network forensics
- ICT forensics
- forensic investigations
- digital investigations
- business continuity
- incident response
- computer policing
- high-tech crime investigation
- computer security
- incident management
- cloud security.

2 What is forensic science?

At first sight, the answer to this question seems straightforward. The Higher Education Academy offers the following definition:

> Forensic science is the application of science to matters of law.
>
> (Higher Education Academy, 2010)

A more careful examination, however, yields some extremely important insights. The 'science' part alludes to scientific method and how it might apply both generally and in terms of a specific investigation. The 'forensic' element refers to how courts make their decisions. One of the most important lessons is that forensic scientists acting as witnesses are not allowed to usurp the authority and role of the court in reaching its decision. As we will see later, this has a considerable impact on how forensic scientists go about their business, how they write reports for court use, and how they give evidence.

Scientific fact-finding and decision-making are very different to legal fact-finding and decision-making. You need to know the difference, not just because it is an interesting area to think about, but also because it goes to the heart of how forensic investigators generate evidence for use in court. The cultures and expectations of each are different, as is their impact and how each is likely to affect the lives of others.

You need to begin by considering what is meant by science and the scientific method, and then see how it operates within the domain of forensic science.

2.1 Science, the scientific method and scientific laws

The aim of science is to make order out of chaos by producing explanations for what we see around us. These explanations come in the form of rules or laws, which we hope, once described, are universally true. For example, objects of whatever weight, dropped from a tower or other high point, will always fall at the same rate (assuming the same air resistance) – and that rate can be described by a scientific formula. We can also say that this is part of a more general phenomenon known as gravity and that we can produce broader explanations which, among other things, show why the earth orbits the sun in a particular way and that the sun in turn has positional relationships with other stellar bodies.

Typically we are able to derive a scientific law by:

- making an initial observation
- giving a provisional hypothesis which explains what is being observed
- providing a means of testing the hypothesis
- actually testing the hypothesis – the experiment
- examining and analysing the results of the testing to see that they conform with expectations, or some revision thereof
- saying that the hypothesis is now a scientific law that holds good for a given range of the phenomenon – and which can be published as such.

This process is known as the scientific method. The end result of the application of the scientific method is a scientific law.

If we have carried out the exercise properly, we can now predict what will happen for all activities within that range of the phenomenon – and anyone else will be able to do the same. **Universality** and **repeatability** are key features of scientific laws. You should also be aware that scientists generally agree that nothing can be proven in absolute terms, but we can say a scientific law holds good until it is proven false.

Although findings may be written up in academic journals using a structure rather like the bullet points above, in practice, scientific endeavour is often much more complex than this. Indeed, the actual process may be much more intuitive and haphazard, showing strong elements of creativity and imagination. Here are a few issues that impact on scientific advances:

- It is not unusual for the initial hypothesis to be substantially wrong. It may, for example, be recognised part way through testing that the initial hypothesis is misconceived, in which case a new, preferably more reliable, hypothesis may be produced.
- One of the key features of the scientific method is testing, but what constitutes a test? Experimental activities must be carefully designed to test the precise hypothesis and nothing else. Controls are usually needed to examine and isolate observations of changes under various conditions. Perhaps the single biggest area of dispute within science is that of testing methodology; the second is allegation of falsifying results.
- Real-life formulation of scientific laws is often an iterative process towards fuller and more reliable understanding. Once the researcher is satisfied with the test results, they may be published in an appropriate scientific journal, thereby adding to the pool of scientific knowledge. Before publication takes place, the work will be peer-reviewed for flaws (and originality).

It is also the case that, at any one time, there is a dominant view of how things work, within which most scientific endeavour in a particular field takes place. Every so often that dominant view turns out to be misconceived and/or there is a major discovery and a paradigm shift occurs. It is therefore possible to distinguish between normal science, which is the vast majority of work that is carried out, and the much rarer paradigmatic work.

Established scientific law does change through time, and through agreement and convention of the scientific community. For example, Einstein's theories on relativity now extend understanding formed by Newton's ideas on gravity. The same applies in legislation, as new ideas, experiences and, often, criminal practices emerge. As well as considerable improvements in methods of detection, advances such as fingerprints have enhanced the proof allowed in law (although even this has been subject to revision in light of new data, as you will soon see).

Forensic science uses the scientific method too, but we need to distinguish between at least two instances of it:

1. the discoveries of phenomena that we can put rules to and that appear to have a value within an investigation that might end in legal proceedings (such as particular qualities of fingerprints and DNA)
2. the development and proper use in the relevant instances of specialist tools and standard operating procedures based on the above.

Arguably there is also a third instance: when a forensic technician examines a specific item of evidence and reports the findings. This must be ‘scientific’ to the extent that it is repeatable by others. In criminal law procedure, the repeatability should be accessible to an expert instructed by the defence. This requirement to be scientific implies, among other things, having the original material (or some acceptable duplicate) available for inspection and having detailed reporting of what was done.

Activity 2

(Allow 30 minutes)

Perform a simple internet search for college or university courses with the word ‘forensic’ in their title. See if you can find two or three that would fit our definition of forensic science and two or three that do not.

Discussion

Your findings may vary, but most of the natural sciences can easily apply the forensic adjective and still qualify by our definition. Perhaps forensic psychology fits, but what about forensic geography? How about forensic literature study? This is something you could discuss with other students in the forums.

2.2 Forensic scientists

Professionals who work in this field are known as forensic scientists or ‘archaeologists of the recent past’. Forensic scientists work in hospitals, police departments, laboratories, universities, morgues and corporate organisations.

The profession has gained huge popularity all over the world mainly due to TV drama series (such as *CSI* and *Silent Witness*) and forensic documentaries, but progress in forensic science has not been uniform throughout the world.

The different specialisms of forensic science include:

Forensic Pathology – the study of problems relating to unnatural death and various types of trauma to the living. It is a specialty of medicine and a sub-speciality of pathology.

Figure 1 Fingerprint

Forensic DNA – the use of biological science to identify individuals by their DNA profile, using genetic samples such as blood, semen and saliva. The concept was first designed by Sir Alec Jeffreys at the University of Leicester in 1985.

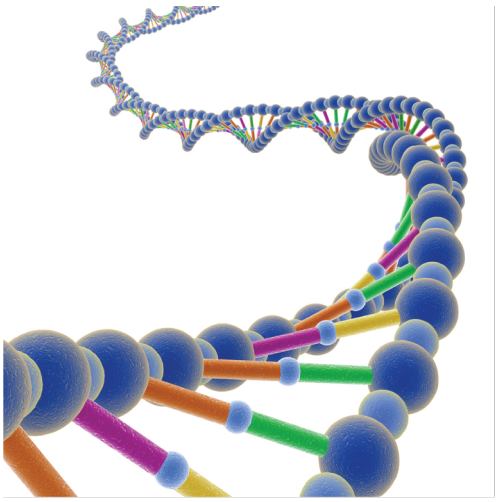


Figure 2 DNA strand

Forensic Engineering – the investigation of accidents involving vehicle, aircraft, fire, electrical or metal fatigue by applying engineering principles to solve how they were caused.

Figure 3 Burning vehicle

Digital Forensics – digital forensics is the area of forensics in which professionals analyse and gather data from a computer or other form of digital media.

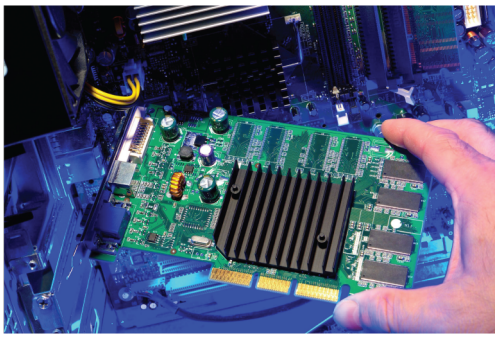


Figure 4 Inside a computer

Forensic Accounting – to trace any financial inconsistencies within a company's account.

Figure 5 Money

Forensic Dentistry – the use of information through examination of teeth and dental prostheses to assist in identifying human remains and evaluating bite marks.

Figure 6 Teeth

Forensic Anthropology – the study of human beings in relation to their physical character. The specialist answers questions on gender, age, ethnicity, stature, nutritional status, existence of disease processes, and the presence and character of skeletal trauma.

Early pioneers of forensic anthropology included Thomas Dwight, whose book *The Identification of the Human Skeleton: A Medico-Legal Study* (1878) was used successfully in a court case in 1897.

Figure 7 Bones

Forensic Toxicology – the detection, identification and quantification of drugs, other poisons or toxins in body tissues and fluid, including blood.

Figure 8 Test tube of liquid

Activity 3

(Allow 15 minutes)

Using search engines or other resources, name two other areas of forensic science and write a short paragraph describing each.

Provide your answer...

If you would like to know more about some of the other forensic science disciplines, the book *Crime Scene to Court* (White, 2016) provides a good overview of many of them.

Activity 4

(Allow 30 minutes)

Write your thoughts on one or more of the following topics. You don't have to spend much (if any) time performing research to answer the questions.

a. How do you think fictional crime dramas have affected the public perception of forensic science? How do you think they have affected criminals? Which dramas do you think give the most accurate and least accurate portrayals of forensic scientists?

b. Why do you think an electrician who helps to determine the source of a fire is not a forensic scientist? Why is education alone not sufficient for one to become a forensic scientist?

Provide your answer...

Discussion

a. Crime dramas tend to oversimplify forensic science, which is often necessary to move a plot along. Results that may take days or weeks take hours because it would be boring to watch a protagonist twiddle their thumbs or get on with other jobs while they wait for results to come back. Digital forensics tends solve impossible tasks in crime dramas or give the impression that a digital forensics expert can (or would!) hack into any system. Criminals are certainly more forensically aware and will know to avoid leaving DNA or wiping or destroying digital devices that may contain evidence. Almost all the dramas we have seen take great liberties with the speed at which digital forensics, or triage, can be carried out, although the recent series *Mr Robot* has some of the most accurate portrayals of forensics and security tools.

b. While an electrician may find that poorly insulated electrical cables allowed arcing to cause a fire, she may not be trained to look for tool marks on cabinets, which might indicate tampering. She may not have studied examples of arson committed by consumer unit tampering or recognise residue from an explosive device or firearm, and will not have been independently examined in the practical and legal frameworks surrounding an investigation. A forensics scientist needs both education and experience to deal with the unique characteristics that each crime scene presents. Life rarely matches textbook situations.

2.2.1 Pioneers of forensic science

Modern forensic science has its roots in the work of several 19th century pioneers. Some of the 'fathers' of forensic science include:

Alphonse Bertillon (1853–1914) was a French police officer and a biometrics researcher who created the first scientific system used by police to identify criminals based on physical measurements, including the invention of the police 'mug shot'. His technique of anthropometry cannot actually uniquely identify a person and is no longer used.

Bertillon also wrote a famous paper, 'Les empreintes digitales' (1912) on the uniqueness of 16 ridge points on fingerprints to identify people. In 1999 the paper was found to have contained altered images and fingerprints are now considered as opinion evidence, not proof a person was there. This finding was recently reported by Miller (2013) in his law blog.

August Vollmer (1876–1955) was the chief of police in Berkeley in 1909 and the lead figure in the development of the field of criminal justice in the USA. He pioneered the system of fingerprinting and handwriting evidence, the use of polygraph and the application of forensic science to investigations.

Dr Edmund Locard (1877–1966) was a French criminalist who wrote several pieces with his most famous, *Traite de criminastique* (Treaty of Criminalistics), in the 1920s postulating that microscopic examination of clothing and other physical evidence could reveal information about the history of the wearer. He is best known for Locard's Exchange Principle which can be summarised as 'every contact leaves a trace'

Locard's Exchange Principle states: 'Wherever two surfaces come into contact, a transfer of minutiae, however slight, occurs.' Kirk described this as follows:

> Wherever he steps, whatever he touches, whatever he leaves – even unconsciously – will serve as silent evidence against him. Not only his fingerprints and his shoeprints, but also his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects – all these and more bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong; it cannot perjure itself; it cannot be wholly absent. Only in its interpretation can there be error. Only human failure to find, study, and understand it can diminish its value.
>
> (Kirk, 1953)

Silent Witness (1996–), which takes its name from Locard's Exchange Principle, is one of many recent TV series to include forensics as a major plot element. Although professionals usually advise the script writers, the portrayal of forensics in these series is often adjusted for dramatic effect and gives the general public a distorted view of the field (cf. The *CSI* effect).

Figure 9 Dr Edmund Locard

Locard's Exchange Principle is really about physical evidence and the question arises as to how far his ideas apply to digital evidence where concepts of touch and contact may require some reinterpretation.

Activity 5

(Allow 30 minutes)

Based on your current understanding of the various types of digital evidence, how far do you think Locard's Exchange Principle can be made to apply?

Discussion

No matter what your level of technical sophistication, you will probably realise that most events involving a computer leave some trace of the behaviour. A log of every action is recorded somewhere, whether the action is email passing through, the act of logging into a computer or visiting a web page. The more difficult thing to verify is who committed a given act, since the use of a password does not guarantee that the password holder is the person typing it.

2.2.2 Further reading

A discussion of Locard's Exchange Principle and other theories can be found in ' Evidence dynamics: Locard's Exchange Principle & crime reconstruction' (Chisum and Turvey, 2000).

2.3 Case study: The Shirley McKie story

In February 1997, a British policewoman, Shirley McKie, was charged with perjury after testifying at a murder trial that she had not been in the victim's house, where her thumbprint was supposedly found. McKie's house was searched and she was taken back to the police station where she was strip-searched and detained because of the controversial thumbprint.

The Scottish Criminal Record Office produced four fingerprint experts who certified that the thumbprint definitely belonged to McKie. However, she maintained her innocence and was acquitted, saved from a potential eight years' imprisonment, after two American fingerprinting experts endorsed that the thumbprint did not belong to her.

After much media activity, legal action and controversy, Michael Russell, a member of the Scottish parliament, asked fingerprinting experts from around the world to verify the ownership of this thumbprint and had 171 certifications from 18 different countries that the thumbprint did not belong to McKie.

The main concern with the entire issue was not only about its effect on McKie's career, but also about the accuracy of the Scottish Criminal Record Office's earlier assertions. A civil trial against the Scottish Executive was due to be heard in early 2006. On the morning of the trial, the Executive offered McKie a settlement of £750,000 without admitting liability. She accepted the offer and the trial did not go ahead. Following the end of legal proceedings, the Scottish Parliament held an inquiry during 2006, which identified fundamental weaknesses in the Scottish fingerprinting service. Before the inquiry reported, the Scottish Criminal Record Office offered early retirement to four of its fingerprint officers, three of whom accepted the offer. The officer who refused early retirement was subsequently sacked, but later won a case for unfair dismissal.

A public inquiry into the case was held in 2009, with the report being published in 2011. The inquiry blamed human error and inadequate procedures for the misidentification of McKie's thumbprint. It found no evidence of a conspiracy by the police against McKie, nor did it find any weaknesses in the theory of identification using fingerprints. However, it warned:

> Practitioners and fact-finders alike require to give due consideration to the limits of the discipline.
>
> (Report of The Fingerprint Inquiry Scotland, 2011, p. 630)

Among its recommendations, the inquiry said 'fingerprint evidence should be recognised as opinion evidence, not fact' (p. 741).

Shirley McKie received a full personal apology from Strathclyde Police Chief Constable Stephen House in April 2012, more than 14 years after the murder of Marion Ross. Ross's murder has never been solved.

Activity 6

(Allow 10 minutes)

Based on your current knowledge of digital forensics, what lessons do you think the McKie case has for digital forensic investigations?

Discussion

Digital evidence can only show what a computer did, not what a person did, and the conclusions of a digital forensics investigators need to distinguish clearly between facts and opinion. It is also important to know what your assumptions are based on. The fingerprint experts assumed that Bertillon's claim about 16 ridge points making a print unique was true, but it turned out not to be.

2.4 Summary of Section 2

In this section you saw that forensic science uses various branches of knowledge such as science, medicine or technology to assist the courts in legal proceedings.

Forensic science is the collection and analysis of physical evidence generated by criminal activity or relating to a civil matter. The physical evidence may include drugs, firearms, tool marks, fingerprints, footwear, blood, glass, paint, bones, soil, accounting records and other material. All the analysis is conducted in a forensic laboratory, following strict evidence handling procedures laid down by professional bodies and regulators.

3 The role of the forensic scientist in law

The end result of many forensic investigations is their use to prove guilt or innocence in a criminal trial, establish liability in a civil trial, reach an internal disciplinary decision in a company, or arrive at a result in an employment tribunal.

Activity 7

(Allow 30 minutes)

Perform a search on UK internet news and legal websites for reports about Professor Sir Roy Meadow, a child welfare specialist widely believed to have misunderstood statistical material in cases involving mothers accused of killing their children. As a result of his testimonies a number of women were imprisoned and only later released. Who do you think is to blame for what happened?

Discussion

You will, of course, have your own opinion, but you should consider how much blame should fall on Professor Meadow and how much should fall on the courts and lawyers for not testing his evidence with sufficient rigour.

3.1 Legal decision-making

This takes us neatly to the next issue to explore: the relationship between a 'finding' by a forensic scientist, and the decision of the court. Put bluntly: if a forensic scientist were to state in evidence that there is a probability of 1 in 1 million that a DNA sample found at a scene of crime matches the DNA profile of an accused, then would the court be bound to accept his finding?

Activity 8

(Allow 1 hour)

One case where forensic evidence was crucial to the prosecution is known as *R v Adams* [1996] (R in this case stands for Regina and is used where the Crown Prosecution Service brings a case to court). Use the Wikipedia entry for *R v Adams* [1996] case as a starting point for research to answer the question:

What position does the court take regarding Adams and the statistical value of evidence?

As with all Wikipedia entries, you should only use the article as an initial jumping-off point and check what is being said against other sources.

Discussion

The position the court takes is quite clear. In the appeal case, Adams was accused of rape but the only evidence against him was DNA. Later Court of Appeal guidelines said that the judge's directions to the jury about the statistical value of the evidence in effect usurped their role.

The Court of Appeal said that the jury should have been told:

> Suppose the match probability is 1 in 20 million. That means that in Britain (population about 60 million) there will be on average about 2 or 3 people, and certainly no more than 6 or 7, whose DNA matches that found at the crime scene, in addition to the accused. Now your job, as a member of the jury, is to decide on the basis of the other evidence, whether or not you are satisfied that it is the person on trial who is guilty, rather than one of the few other people with matching DNA. We don't know anything about the other matching people. They are likely to be distributed all across the country and may have been nowhere near the crime scene at the time of the crime. Others may be ruled out as being the wrong sex or the wrong age group.
>
> Court of Appeal Guidelines

You can read the short article mentioned on the Wikipedia page: Donnelly, P. (2005) 'Appealing statistics', *Significance*, vol. 2, no. 1, pp. 46–8 to see the view of Professor Donnelly, who took part in the appeal.

If you have access to a legal database, you can find analysis of the *R v Adams* case in a system such as Westlaw, which is an authoritative source of case reports. Once in the database select Cases from the menu and enter ***R v Adams*** in the Party Names box and search. You should see a result from 1996 and can select the Case Analysis to read.

3.2 The role of the court

The case of *R v Adams* in Activity 8 illustrates that scientists and the courts have entirely different functions. You have already seen what scientists do: they try to produce a universal explanation using a set of procedures, which are capable of replication and testing. The court's job is to adjudicate on specific issues between the parties, or in the criminal courts, determine whether the prosecution has shown on the basis of evidence presented and accepted to a sufficient standard that a specific, identified crime has been committed.

It is fundamental to the operation of the courts that once it reaches its decision, that decision is final. This is true unless there are profound and obvious grounds for appeal. There is a sound policy reason for this. It would be unfair to the participants in a civil case, and even more unfair to someone accused of a crime, if a court could, several months or years after reaching its decision, be allowed to say: 'Sorry, we have done a bit more thinking and we have now changed our mind'. This is sometimes referred to as the fiction of certainty.

3.3 Contrasting scientific conclusions with court judgments

A trial process is not an enquiry into the truth or into hypothetical issues; it is testing various versions of relevant evidence to see whether 'on the balance of probabilities' (in civil cases) or the higher standard of 'beyond a reasonable doubt' (in criminal matters) it is possible to reach a particular decision for that set of circumstances. In a famous US case, *Daubert v Merrell Dow Pharmaceuticals* [1993], the judge said: 'Scientific conclusions are subject to perpetual revision. Law, on the other hand, must resolve disputes finally and quickly ... Rules of Evidence [are] designed not for the exhaustive search for cosmic understanding but the particularized resolution of legal disputes.' (The quote is from section 39.)

Two Oxford philosophers, Herbert Hart and Antony Honoré, put the matter thus: 'The lawyer and historian are both primarily concerned to make causal statements about particulars, to establish that on some particular occasion some particular occurrence was the effect or consequence of some other particular occurrence ... whereas for the scientist the focus of attention is the discovery and the construction of theories.'

In the case of unauthorised access to a computer, the court isn't asking a generalised question along the lines of: 'where a computer disk's directory says that a file was first created, does it always mean that this is the date on which the file first appeared on that hard disk?' Rather, the court is trying to decide if a party has made unauthorised access to a computer, contrary to Section 1 of the Computer Misuse Act 1990. To prove this has indeed happened, there are a set of tests, each of which must be satisfied, before the court can be satisfied that a person has had unauthorised access to a computer. In the case of the offence just mentioned, the tests must show that:

1. a computer was involved
2. it was accessed

3. it was accessed by the accused
4. such access was unauthorised
5. at the time of the offence the accused knew that the access was unauthorised.

You will realise that each of these five steps or tests raises several subsidiary questions, which also need to be answered.

3.4 Summary of Section 3

This section illustrated the fact that although forensic investigations may use the scientific method, the objective of the investigation is markedly different from scientific research. A forensic investigation aims to make a clear determination of fact in a specific case that is acceptable to a court of law and which is not subject to revision.

You also saw that there are significant issues with the presentation of forensic evidence to courts; not only must any limitations on the evidence be made clear, but also evidence must be tightly constrained so that it does not mislead participants.

4 The role of digital forensics

Digital forensics is a branch of forensic science and is recognised as such by most courts. One definition from the first Digital Forensic Research Workshop (DFRWS) is:

> The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.
>
> (Palmer, 2001, p. 16)

In the UK the professional body for forensic scientists, The Chartered Society of Forensic Sciences, includes digital forensics as one of its sub-disciplines and the process for digital forensics is much the same as for the traditional areas of forensic science.

4.1 The digital forensic process

The digital forensic process has the following five basic stages:

1. **Identification** – the first stage identifies potential sources of relevant evidence/ information (devices) as well as key custodians and location of data.
2. **Preservation** – the process of preserving relevant electronically stored information (ESI) by protecting the crime or incident scene, capturing visual images of the scene and documenting all relevant information about the evidence and how it was acquired.
3. **Collection** – collecting digital information that may be relevant to the investigation. Collection may involve removing the electronic device(s) from the crime or incident scene and then imaging, copying or printing out its (their) content.
4. **Analysis** – an in-depth systematic search of evidence relating to the incident being investigated. The outputs of examination are data objects found in the collected information; they may include system- and user-generated files. Analysis aims to draw conclusions based on the evidence found.
5. **Reporting** – firstly, reports are based on proven techniques and methodology and secondly, other competent forensic examiners should be able to duplicate and reproduce the same results.

A crucial activity that accompanies the first four steps is **contemporaneous note-taking**. This is the documentation of what you have done immediately after you have done it in sufficient detail for another person to reproduce what you have done from the notes alone.

Activity 9

Optional (Allow 1 hour)

This activity is for the technically minded or curious only who would like a preview of the digital forensics process: watch the YouTube video

A Geek's Guide to Digital Forensics (2011) (you may want to use the fast-forward feature to skip some sections).

Digital forensics is not solely about the processes of acquiring, preserving, analysing and reporting on data concerning a crime or incident. A digital forensic scientist must be a scientist first and foremost and therefore must keep up to date with the latest research on digital forensic techniques. They may also contribute to the discipline through their own research and publish it in peer-reviewed journals.

4.2 A brief history of digital forensics

Until the late 1990s, what became known as digital forensics was commonly termed 'computer forensics'. The first computer forensic technicians were law enforcement officers who were also computer hobbyists. In the USA in 1984 work began in the FBI Computer Analysis and Response Team (CART). One year later, in the UK, the Metropolitan Police set up a computer crime unit under John Austen within what was then called the Fraud Squad.

A major change took place at the beginning of the 1990s. Investigators and technical support operatives within the UK law enforcement agencies, along with outside specialists, realised that digital forensics (as with other fields) required standard techniques, protocols and procedures. Apart from informal guidelines, these formalisms did not exist but urgently needed to be developed. A series of conferences, initially convened by the Serious Fraud Office and the Inland Revenue, took place at the Police Staff College at Bramshill in 1994 and 1995, during which the modern British digital forensic methodology was established.

In the UK in 1998 the Association of Chief Police Officers (ACPO) produced the first version of its *Good Practice Guide for Digital Evidence* (Association of Chief Police Officers, 2012). The ACPO guidelines detail the main principles applicable to all digital forensics for law enforcement in the UK.

As the science of digital forensics has matured these guidelines and best practice have slowly evolved into standards and the field has come under the auspices of the Forensic Science Regulator in the UK.

Activity 10

(Allow 1 hour)

Part 1

Search the internet for no more than five minutes for the series of ISO standards relating to digital forensics and list each of the standards you think applies.

Discussion

You may have found the ISO27001 information security website in your search results. This lists various standards relevant to digital forensics some of which are draft:

- ISO/ IEC 27037:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence
- ISO/ IEC 27041 Assurance for digital evidence investigation methods
- ISO/ IEC 27042 Guidelines for the analysis and interpretation of digital evidence
- ISO/ IEC 27043 Incident investigation principles and processes.

You may have looked at the ISO website for these too. You can browse standards by the relevant technical committee (ISO/IEC JTC1 – Joint Technical Committee) and this shows both published and draft standards. (The abbreviation ISO/IEC/DIS stands for International Organization for Standardization/International Electrotechnical Commission/Draft International Standard.)

British Standards has a standards development site which you can search and has a link to their Draft standards review site.

Part 2

Search the internet for the current UK Forensic Science Regulator's Codes of Practice and Conduct (Forensic Science Regulator, 2011). Read Section 21 and say why a digital forensic scientist might have difficulty complying with this item.

Answer

A forensic scientist may have difficulty complying with Section 21 of the Forensic Science Regulator's Codes of Practice and Conduct because software rarely (if ever) comes with a certification from the manufacturer as to its validity (or for that matter, fitness for purpose to do anything).

4.3 Different types of digital forensics

Digital forensics is a constantly evolving scientific field with many sub-disciplines. Some of these sub-disciplines are:

1. **Computer Forensics** – the identification, preservation, collection, analysis and reporting on evidence found on computers, laptops and storage media in support of investigations and legal proceedings.
2. **Network Forensics** – the monitoring, capture, storing and analysis of network activities or events in order to discover the source of security attacks, intrusions or other problem incidents, i.e. worms, virus or malware attacks, abnormal network traffic and security breaches.
3. **Mobile Devices Forensics** – the recovery of electronic evidence from mobile phones, smartphones, SIM cards, PDAs, GPS devices, tablets and game consoles.
4. **Digital Image Forensics** – the extraction and analysis of digitally acquired photographic images to validate their authenticity by recovering the metadata of the image file to ascertain its history.
5. **Digital Video/Audio Forensics** – the collection, analysis and evaluation of sound and video recordings. The science is the establishment of authenticity as to whether a recording is original and whether it has been tampered with, either maliciously or accidentally.
6. **Memory forensics** – the recovery of evidence from the RAM of a running computer, also called **live acquisition**.

In practice, there are exceptions to blur this classification because the grouping by the provider is dictated by staff skill sets, contractual requirements, lab space, etc. For example:

- Tablets or smartphones without SIM cards could be considered computers.

- Memory cards (and other removable storage media) are often found in smartphones and tablets, so they could be considered under mobile forensics or computer forensics.
- Tablets with keyboards could be considered laptops and fit under computer or mobile forensics.

The science of digital forensics has a seemingly limitless future and as technology advances, the field will continue to expand as new types of digital data are created by new devices logging people's activity. Although digital forensics began outside the mainstream of forensic science, it is now fully absorbed and recognised as a branch of forensic science.

Activity 11

(Allow 15 minutes)

a. Based on your current understanding of the various types of digital evidence, how far do you think Locard's Exchange Principle can be made to apply?

b. Forensic data stored in electronic media differs in one important aspect from most physical evidence: how can this make the digital forensic scientist's job easier than scientists dealing with blood or fibres?

Discussion

a. In visiting a website a visitor will leave a trace in the log file of the web server which includes the IP address that accessed the server. However some traces may only be transient; most routers do not store details of the packets passing through them (unless the NSA or GCHQ have tapped the router!). Data stored in electronic media differs from physical evidence in that a perfect copy (called an image) can be created and an investigator can perform tests on the copy without affecting the original. If the copy is destroyed or altered a new copy can be made at no cost. Physical evidence is usually irreparably altered or destroyed by testing.

b. Locard's Exchange principle applies even though there is no physical contact when computers connect to each other, but the trace may be transient and the trace easily lost, for example a packet passing through a router.

Activity 12 *The Case of the Stolen Exams*

(Allow 30 minutes)

There is a crisis for The Open University. Exam papers are circulating on eBay! Can our fearless forensic investigators find the source of the leak and ensure a successful prosecution?

Watch the short video *The Case of the Stolen Exams*, taking notes of what you see so that you can answer the following question:

Can you see any problems with the investigation?

Write down all the issues that you think might be a problem for securing a conviction.

Video content is not available in this format.

Activity 13 *The Case of the Stolen Exams – Revisited*

(Allow 30 minutes)

Now watch the video *The Case of the Stolen Exams – Revisited* and see how many issues you spotted in the original investigation.

Video content is not available in this format.

4.4 Summary of Section 4

In this section you saw that digital forensics is an obvious development of existing forensic procedures brought about by the introduction of new technology. What began almost as an ad hoc set of procedures rapidly became formalised as guidelines for investigators (ACPO, 2012). These guidelines offer procedures for securing and studying digital evidence in a way that does not compromise its integrity so that it can be used in a court of law.

Such is the scope of digital technology that digital forensics is further subdivided into specialised areas. An investigation may require specialists from several areas to understand all of the evidence.

5 Conclusion

This free course, *Digital forensics*, which is an introduction to computer forensics and investigation, has given you a taster for the full course, which is M812. It has given you a broad view of the scope of digital forensics, including topics which are covered in greater depth in M812. As you have seen, both forensics (in general) and digital forensics (in particular) encompass a wide range of distinct disciplines.

You have learned something of the history of forensics from the 19th century onwards and seen how many of the principles laid down by early investigators can be applied to modern technologies. You have also been introduced to some of the guidelines used by digital forensic investigators.

A clear distinction between scientific investigations for research purposes and forensic investigations using scientific methods has been made. It is vital to remember this distinction. Scientific research is always subject to revision whereas forensic investigations should result in a clear-cut result and any limitations on that result made clear to a court.

You also had your first chance to experience a forensic investigation. In *The Case of the Stolen Exams*; you saw how a poor investigation could compromise any subsequent trial, and how proper investigative techniques help to preserve evidence for further investigations.

This OpenLearn course is an adapted extract from the Open University course M812 *Digital forensics*.

Keep on learning

Study another free course

There are more than **800 courses on OpenLearn** for you to choose from on a range of subjects.

Find out more about all our free courses.

Take your studies further

Find out more about studying with The Open University by visiting our online prospectus.

If you are new to university study, you may be interested in our Access Courses or Certificates.

What's new from OpenLearn?

Sign up to our newsletter or view a sample.

For reference, full URLs to pages listed above:

OpenLearn – www.open.edu/openlearn/free-courses

Visiting our online prospectus – www.open.ac.uk/courses

Access Courses – www.open.ac.uk/courses/do-it/access

Certificates – www.open.ac.uk/courses/certificates-he

Newsletter – www.open.edu/openlearn/about-openlearn/subscribe-the-openlearn-newsletter

References

Association of Chief Police Officers (ACPO) (2012) *Good Practice Guide for Digital Evidence*, 5th version [Online]. Available at http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf (Accessed 28 January 2014).

Bertillon, A. (1912) 'Les empreintes digitales'. *Archives d'Anthropologie Criminelle, Médecine Légale et Psychologie Normale et Pathologique*, vol. 27, pp. 36–52.

Campbell, A. (2011) *Report of the Fingerprint Inquiry Scotland* [Online]. Available at http://www.thefingerprintinquiryscotland.org.uk/inquiry/21.html (Accessed 17 December 2013).

Chisum, W. J. and Turvey, B. E. (2000) 'Evidence dynamics: Locard's Exchange Principle & crime reconstruction', *Journal of Behavioral Profiling*, vol. 1, no. 1 [Online]. Available at http://www.profiling.org/journal/vol1_no1/jbp_ed_january2000_1-1.html (Accessed 2 December 2013).

Daubert v Merrell Dow Pharmaceuticals (92-102), 509 U.S. 579 [1993].

Dwight, T. (1878) *The identification of the human skeleton*. Boston, Massachusetts Medical Society [Online]. Available at https://archive.org/details/identificationof00dwig (Accessed 20 February 2014).

Forensic Science Regulator (2011) *Codes of Practice and Conduct* [Online]. Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118949/codes-practice-conduct.pdf (Accessed 5 December 2013).

Higher Education Academy (2010) 'What is forensic science?' [Online] Available at http://www.heacademy.ac.uk/forensic_careers/what_is_forensic_science (Accessed 22 March 2014).

Kirk, P. L. (1953) *Crime Investigation: Physical Evidence and the Police Laboratory*, New York, Interscience.

Miller, C. G. (2013) 'Fingerprint identification not infallible, nor scientific & based on fraud', *cliffordmillerlaw*, 8 March [Online]. Available at http://cliffordmillerlaw.wordpress.com/2013/03/08/fingerprint-identification-not-infallible-nor-scientific-based-on-fraud/ (Accessed 2 December 2013).

Palmer, G. (2001) *A Road Map for Digital Forensic Research: Report from the First Digital Forensic Research Workshop (DFRWS)*, Digital Forensic Research Workshop, DTR – T001-01 FINAL [Online]. Available at http://www.dfrws.org/2001/dfrws-rm-final.pdf (Accessed 3 December 2013).

R v Adams [1996] EWCA Crim 22.

White, P. C. (ed) (2016) *Crime Scene to Court*, London, Royal Society of Chemistry.

Acknowledgements

This free course was written by Peter Sommer and Blaine A. Price.

This free course is adapted from a former Open University course Digital forensics (M812).

The material acknowledged below is Proprietary and used under licence (not subject to Creative Commons Licence). Grateful acknowledgement is made to the following sources for permission to reproduce material in this free course:

Images

Course image: © nmedia/Shutterstock.com

Figure 1: Public Domain. Taken from Wikipedia

Figure 2: © Benjamin Albiach Galan/Dreamstime.com

Figure 3: © Andre Schaerer/Shutterstock.com

Figure 4: © Oliver Le Queinec/123RF.com

Figure 5: © Slallison/123RF.com

Figure 6: *** © Dozenist. This file is licensed under the Creative Commons Attribution-Share Alike Licence http://creativecommons.org.licenses/by-sa/3.0/

Figure 7: © PÃ©ter Gudella / 123RF.com

Figure 8: © Jag_CZ/Shutterstock.com

Figure 9: *** Reproduced with permission from Bibliothèque municipale de Lyon. This file is licensed under the Creative Commons Attribution-Noncommercial-NoDerivatives Licence http://creativecommons.org/licenses/by-nc-nd/2.0/fr/

Keep on Learning Image: © Konstantin Chagin/iStockphoto.com

Every effort has been made to contact copyright owners. If any have been inadvertently overlooked, the publishers will be pleased to make the necessary arrangements at the first opportunity.

Don't miss out

If reading this text has inspired you to learn more, you may be interested in joining the millions of people who discover our free learning resources and qualifications by visiting The Open University – www.open.edu/openlearn/free-courses.