CS 978 – Legal, Ethical, and Professional Issues for the Information Society

Lecture 8 – Digital evidence

Introduction

In this lecture, we will explore further the issues around computer misuse and computer crime by considering the importance of digital evidence. The increase in cybercrime has given rise to an expanding interest in the skills of computer science in law enforcement, as the investigations are often complex and lengthy.

Digital evidence has been defined by Chisum as: “any data stored or transmitted using a computer that supports or refutes a theory on how an offence occurred or addresses critical elements of the offence such as intent or alibi” (Chisum, 1999), while Carrier and Spafford define it as “digital data that establish that a crime has been committed, can provide a link between a crime and its victim or can provide a link between the crime and the perpetrator” (Carrier and Spafford, 2003).

Revisiting the emergence of computer crime

As we discussed earlier, the emergence of the new area of cybercrime posed problems for the legal system, and new legislation had to be developed to take account of it. As well as the issues we have already highlighted in the UK, some examples from the US highlighted the global concerns of computer crime. In the 60s and 70s some US universities saw computers targeted for arson attacks as part of student protests, and the status of digital property posed problems for understanding the nature of the crime. In Florida in the mid-70s a betting scam at Flagler dog track involving computers led to a state law on computer crime to attempt to criminalise the behaviour. The first country-wide computer crime law was enacted in 1983 in Canada.

Sources of digital evidence

Casey (2004) suggests that digital evidence sources should be classified into 3 groups:

1. open computer systems, e.g. the internet;
2. communication systems, e.g. mobile phones; telephones
3. embedded computer systems, e.g. a chip in a washing machine.

All 3 types present specific challenges for investigations, and the latter category would now encompass the ever-growing area of the Internet of Things (IoT).

Digital evidence clearly differs from standard physical evidence, as it exists largely as data. This does, however, provide positive aspects for investigations, as it can be replicated to its smallest particle, the byte. In digital forensics, the focus is on ensuring a copy is made of the original data, and the analysis is done on the copy. As Stenhouse has observed, “a ballistics expert cannot make a duplicate firearm” that was central to a crime.

Challenges

Like much of the computer science field, especially around internet issues, digital forensics is a relatively new and continually expanding field. It can appear as if the investigators are always playing catch up with the cybercriminals, and new areas of investigation emerge regularly.

Other challenges exist around the time taken to investigate crimes involving computer devices. For example, in the 2006 case investigating plots to bomb transatlantic flights, the following numbers of items were seized:

- 400 computers
- 200 mobile phones
- 8000 storage devices.

With such a number of devices, all needing to be replicated and examined, we can see that computer crimes mean investigations can take several years to complete.   Tobias (2006) argues that: “The investigation, interpretation and presentation of evidence that is often derived from binary data is highly complex and usually littered with technical terms and concepts.”

Software programs that provide the means to encrypt data, or hide it, such as seen in steganography software, also provide challenges to investigators.

Criminal investigations

Casey provides an overview of the case/incident resolution process in his extensive examination of digital forensics, and it is illustrated below:

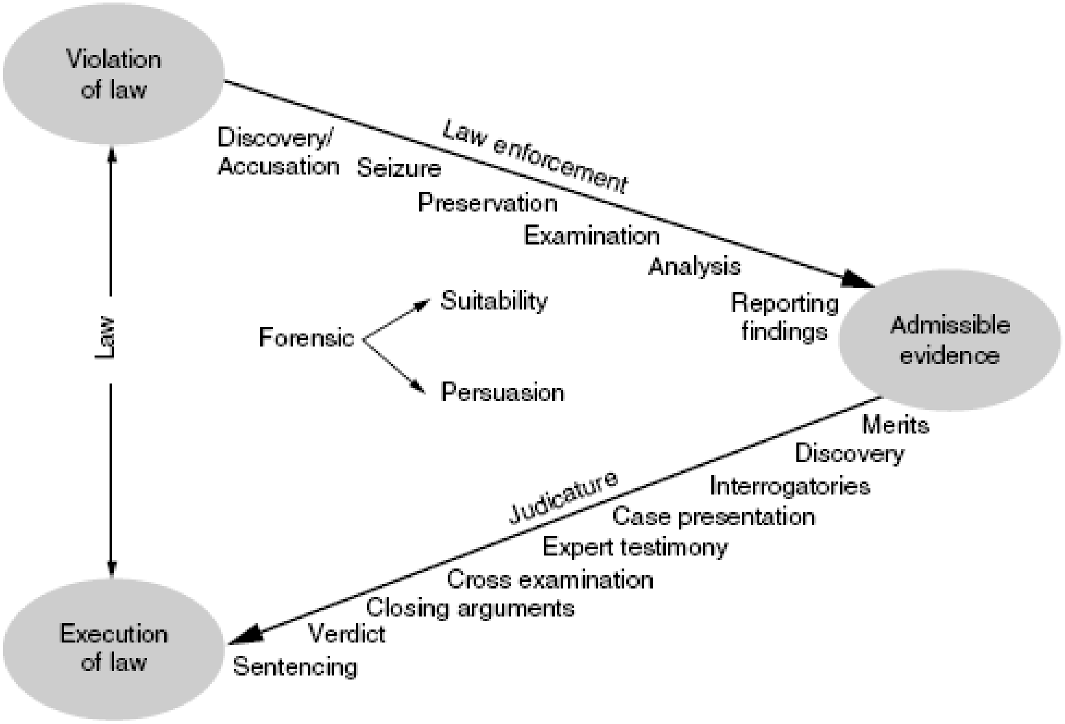

FIGURE 1 - OVERVIEW OF CASE/INCIDENT RESOLUTION PROCESS (CASEY, 2004)

Like any other kind of investigation, the first question a digital forensic investigator has to ask is, has a crime been committed. Evidence may point to a crime, but analysis may prove otherwise, or inconclusive. Casey cites two examples:

1. The person accused of computer misuse who denies it and is discovered on investigation to be truthful, with errors in computer logs as the source of accusation
2. A suicide note left on a computer with a date after the suicide supposedly took place. After examination, it was found that the computer clock was malfunctioning

Trawling through data can be time-consuming, but it is usually the only way that such discrepancies can be discovered.

In traditional forensics, *Locard's Exchange Principle* posits the notion that contact between two items will leave a trace. For instance, anyone or anything entering a crime scene leaves something of themselves, and also takes something from the scene. It is represented below:

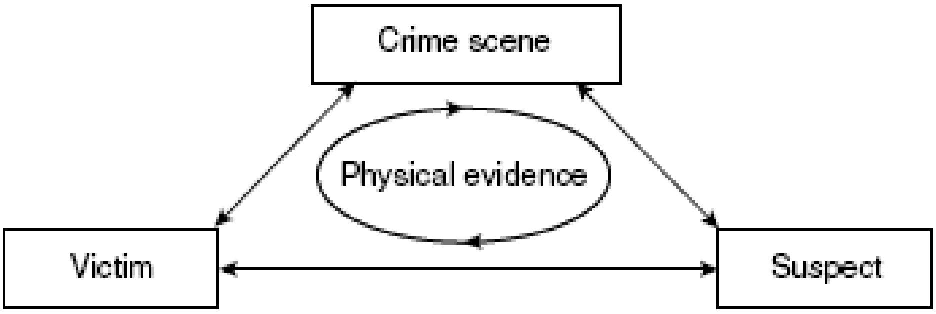

FIGURE 2 - LOCARD'S EXCHANGE PRINCIPLE

In the digital realm Locard's Exchange Principle is also valid, for instance:

- The harasser who uses email will leave a trace of that action
- The paedophile using Usenet groups or other transfer services will leave a trace of his/her presence
- The hacker improperly accessing a computer system will leave a trace of their intrusion
- Unique characteristics of software or hardware can be used to prove a specific machine produced something

Therefore while digital forensics does raise new areas for the forensics investigators, traditional forensic theories still apply.

Controversies

A major international investigation called Operation Ore is to date perhaps the highest profile case in digital forensics. The aim of the initiative, which began investigations in 1999 in Texas, was to discover and prosecute individuals accessing child pornography. In terms of statistics there were:

- 7250 suspects identified
- 4283 homes searched
- 3744 arrests
- 1848 charged
- 1451 convictions
- 39 suicides as a result of pressure of investigation

The investigation focussed on Landslide Productions, which was a company involved in processing credit card payments for other sites, including some distributing child pornography. As it turned about, many people accused in the operation were completely innocent, as it was discovered that Landslide productions had been the victim of credit card fraud, with over 50,000 fraudulent transactions. This meant that many arrests were made of individuals who had not been customers of any of the sites but instead had seen their card details stolen.

Conclusions

The emergence of digital evidence in terms of crime investigations continues to pose challenges for investigators and the wider criminal justice system. Nevertheless, the area presents some excellent possibilities for new computer scientists in an expanding and vitally important area.

References

Carrier, B. and Spafford, E. (2003), "Getting physical with the digital forensics investigation", *International Journal of Digital Investigation*, Winter.

Campbell, D. (2007) "Operation Ore flawed by fraud" *The Guardian.* 19th April. Available from: http://www.guardian.co.uk/technology/2007/apr/19/hitechcrime.money

Casey, E. (2004), *Digital Evidence and Computer Crime; Forensics Science, Computers and the Internet*, 2nd ed., Elsevier Academic Press, San Diego, CA*. (Available as e-book via library catalogue)*

Chisum, W.J. (1999), "An introduction to crime reconstruction", in Turvey, B. (Eds),*Criminal Profiling: An Introduction to Behavioural Evidence Analysis*, Academic Press, London

Irons, A. (2006) “Computer forensics and records management – compatible disciplines” *Records Management Journal* 16 (2) pp.102-112.

Kennedy, I. (2006) *Presenting digital evidence to court*. Available from: http://www.bcs.org/server.php?show=ConWebDoc.7372

Kessler, G. (2004) An Overview of Steganography for the Computer Forensics Examiner. *Forensic Science Communications* 6 (3) Available from: http://www.fbi.gov/hq/lab/fsc/backissu/july2004/research/2004_03_research01.htm

Tobias, J. (2006) *Are criminals going free?* Available from: http://www.bcs.org/server.php?show=ConWebDoc.3253

DMcM/10-2017