Orion Investigations
20th Floor, Unit 2001-2002, 29 Sukhumvit 63, North Klong Tan
Wattana, Bangkok 10110

Orion Investigations

Computer Forensics | Mobile Phone Forensics| Malware Investigations | Training |Data Recovery

Computer Forensics Services

Using Digital Evidence in Thai Courts

March 2012

Date: 05-03-2012

Author: Andrew Smith

Contents

About the Author

Andrew Smith – Director of Computer Forensic Services, Orion Investigations

Andrew is responsible for the management of the Orion Computer forensic Unit. His responsibilities include ensuring the unit operates to the highest international standards, business development and the development and delivery of training for clients and staff. Andrew is an experienced forensic investigator with extensive training and comprehensive experience in relation to criminal, corporate, malware and counter terrorism investigations within the UK and Europe. He has worked in the public sector with the South Yorkshire Police where he received his initial training in computer forensics and also in the private sector with a leading UK computer forensics company. He is also an experienced trainer having developed UK Law Society approved training courses and delivered master degree level forensic training. With nearly ten years' experience in the field of computer forensics Andrew has regularly appeared in court as an expert witness to present complex computer evidence.

Introduction

Computer forensics or digital forensics as it is now commonly called, is still in its infancy in Thailand but that is about to change. For the past two years I have regularly searched on the keywords “computer forensics Thailand”. There were always only a small number of hits but over the past several months that has begun to change. A search will now reveal companies advertising digital forensic services, training courses and blogs within Thailand dedicated to the world of forensics. If the commercial sector in Thailand wishes to compete within the global market, they will need to have in place the resources to deal with cyber-security incidents whatever form they may take. The judicial system also needs to prepare for this change. The use of digital forensics as a tool in large litigation cases and the regular production of digital evidence in Thai courts will become the norm, not the exception. As stated by Professor Peter Grabosky, Australia,

“Those who fail to anticipate the future are in for a rude shock when it arrives”

Digital Forensics

What exactly do we mean by the term digital forensics?

It is the examination of electronic data stored on computers and other digital storage devices for evidence using a forensically sound method.

A forensically sound is a method that does not alter the source evidence, except to the minimum extent necessary to obtain the evidence. The manner used to obtain the evidence must be documented and justified.

Because it is such a new field, the awareness of forensics is still quite low and there is a shortage of experienced forensic investigators in Thailand. As a result the commercial sector and the judicial system are either not utilizing the full potential of digital forensics or not using forensics at all during the course of their investigations. This is almost certainly resulting in potentially vital evidence being overlooked.

There are a number of misconceptions in relation to digital forensics.

1. Digital forensics is only relevant to criminal investigations
2. Digital evidence is very complex

Whether it is a criminal investigation, civil litigation or a private prosecution, if computers, electronic communications or electronic documents have been used by either party then digital forensics is relevant to the investigation. This includes contractual disputes between companies, employee misuse of computer, intellectual property investigations, computer hacking investigations and libel cases.

Lawyers within Thailand currently have a fear of using digital evidence in the Thai courts because they feel the evidence may be too complex and will ultimately be disallowed. This does not have to be the case. In many cases the type of digital evidence that is being produced for court consists of images, emails, electronic documents and Internet history. This type of evidence can be produced in a clear; easy to understand format that everyone can understand.

This is where the skills of the forensic investigator come into play. An experienced investigator quickly learns early in his career to stay away from using technical terms whenever possible. The investigator will work with the legal team and the client to try and achieve the following:

- Work with legal team and client to have a clear understanding of the points to prove
- Produce reports using plain language whenever possible
- Only include in the reports information that is directly relevant to the case
- When technical terms are used, provide easy to understand explanations
- Produce the exhibits in a format that is easy for everyone to access and understand

I have found from experience that by following the above guidelines I have rarely had to attend court to give my evidence in the UK. All parties will often accept my evidence because it has been laid out in such a way that it is easy for everyone to understand.

Digital Evidence

When dealing with digital evidence, there are two key issues that the court has to address, the integrity of the evidence and the authenticity of the evidence. The evidence obtained from computers or computer media is subject to the same rules of evidence as documentary evidence. The onus is on the person producing the evidence to show to the court that the evidence produced is no more and no less now than when it was first taken into possession.

When dealing with the integrity of the evidence the court needs to consider a number of key points:

- How was the electronic data handled?
- Who handled the data?
- Is the person suitably qualified to handle the data?
- What method was used to preserve the data?
- What is the likely-hood of change having occurred to the data?

Authenticity of the evidence refers to the ability to assess the integrity of the evidence and the courts need to consider the following key points:

- Has the data been produced in its entirety?
- Is it possible to demonstrate that no change has occurred to the data?
- Is there a complete audit trail for the handling of the data through to the production of exhibits?
- Would an independent third party be able to reproduce the steps taken and achieve the same results?

Digital Forensic Guidelines

Digital forensics is well established in many countries around the world and as a result the use of digital evidence in a wide range of court cases is common place. The unique issues surrounding digital evidence are well documented and the integrity and authenticity of the evidence has been thoroughly tested in numerous stated cases around the world. As a result various guidelines have been produced in order to develop best practice when conducting digital forensic examinations and to allow the courts to be able to make an assessment in relation to the integrity of the evidence.

Good Practice Guide for Computer Based Electronic Evidence (UK)

In the UK, a good practice guide has been agreed by the Association of Chief Police Officers (ACPO) called **Good Practice Guide for Computer Based Electronic Evidence**. Within the guidelines are four principles that are applied to computer based evidence.

Principle 1: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

Principle 2: In circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Principle 3: An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4: The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

The four principles represent best practice in relation to computer forensic investigations, whether it is a criminal, civil or corporate investigation. By adhering to the principles, it will help ensure that no questions are raised in relation to the integrity of the evidence produced from digital data.

Federal Rules of Evidence (United States)

In the United States the admissibility of digital evidence is covered by the Federal Rules of Evidence.

In the case **Lorraine v. Markel American Insurance Company**, the judge noted that in order for electronically stored information (ESI) to be properly admitted into evidence, counsel needed guidance to avoid electronic evidence being disallowed.

He summarized that whenever ESI is offered as evidence either the judge or jury can make a preliminary determination regarding the admissibility of evidence. If the jury decides, then the Federal Rules of Evidence still apply, however when the judge makes the decision, they do not apply anymore.

He identified that the following evidential hurdles must be overcome for ESI to be admitted into evidence.

- The relevance of the evidence.
- The authenticity of the evidence.
- The issue of Hearsay.
- The original writing rule.
- Balance of probative value with unfair prejudice.

In 2006 the Supreme Court approved amendments to the Federal Rules of Civil Procedure. The new rules directly address the issue surrounding the use and production of electronic evidence in civil cases. The four key areas are:

- **Scope of discovery** – The new changes have been interpreted as meaning a thorough search of all active and stored data, as opposed to all available data, which would include the recovery of deleted documents.
- **Early review and production** – The new rules now require extremely quick production of electronic evidence. A comprehensive search must be done of the electronic data prior to the first pre-trial conference.
- **Native production** – Allows for the parties to discuss the form in which electronic data is produced.
- **Sanctions –** The new rules allows for sanctions against the parties in the event the data is not produced in a timely manner or has been deleted.

Council of Europe Convention on Cybercrime (International)

In 2001 the Convention on Cybercrime came into force. The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing in particular with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

Its main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.

As of the 27th February 2012, 47 countries have signed up to the convention of which 32 countries have ratified the convention.

Thai Legislation

There is already in place in Thailand, legislation for dealing with computer crime and the production of digital evidence for court.

Electronic Transaction Act B.E 2544 (2001)

The act applies to all civil and commercial transactions performed by using a data message. Data message means information generated, sent, received, stored or processed by electronic means, such as emails, telegram, telex or facsimile.

Section 7 of the act states the following:

"Information shall not be denied legal effect and enforceability solely on the ground that it is in the form of a data message".

Section 11 of the act states the following:

"*The admissibility of a data message as evidence in the legal proceedings shall not be denied solely on the grounds that it is a data message.*

In assessing the evidential weight of a data message whether it is reliable or not, regard shall be had to the reliability of the manner in which or the method by which the data message was generated, stored or communicated, the manner or the method by which the completeness and the integrity of the information was obtained, the manner or the method by which the originator was identified or indicated, including all relevant circumstances".

It can be seen from the above that when assessing the admissibility of the digital evidence it again comes down to the two key issues, the integrity and the authenticity of the evidence.

Copyright Act B.E. 2537 (1994)

The use of electronic evidence for IP investigations is still quite low compared to many other countries. The potential importance of the electronic data may often be overlooked when conducting searches on office or factory premises. The focus will often be on the physical goods found on the premises; however the computers and often the mobile phones may provide additional information such as contacts, electronic transactions and email messages.

The Copyright Act section 67 states the following:

*"**Section 67** For the benefit of operation under this Act, the officials shall be the officials according to the Penal Code and have the following authorities:*

(1) To enter a building, office, factory or warehouse of any person during sunrise and sunset or during the working hours of such place or to enter a vehicle to search or examine the merchandise when there is a reasonable suspicion that an offence under this Act is committed,

(2) To seize or forfeit documents or materials relating to the offence for the benefit of proceeding a litigation when there is a reasonable suspicion that an offence under this Act is committed,

(3) To order any person to testify or submit accounting books, documents or other evidences when there is a reasonable suspicion that the testimony, accounting books, documents or such evidences shall be useful for the finding or the use as evidence for proving the offence under this Act.

Any person concerned shall provide suitable convenience for the operation of the officials".

We can see from section (3) that the *"or other evidences"* opens up the opportunity to potentially secure the data from computer systems, digital storage devices and mobile phones.

Computer Crime Act B.E 2550 (2007)

Offences under this act can be grouped into two categories, offences committed against computer systems or computer data and content offences committed via computers.

Examples of offences committed against computer systems or computer data, include:

- Illegally accessing computer data for which there is a specific access prevention measure not intended for their own use.
- Illegally damages, destroys, corrects, changes or amends a third party's computer data.
- Sending computer data or electronic mail to another person and covering up the source of such aforementioned data in a manner that disturbs the other person's normal operation of their computer system.

- Illegally commits any act that causes the working of a third party's computer system to be suspended, delayed, hindered or disrupted to the extent that the computer system fails to operate normally.

Examples of content offences committed via computers, include:

- Any person, who imports to a computer system that is publicly accessible, computer data where a third party's picture appears either created, edited, added or adapted by electronic means or otherwise in a manner that is likely to impair that third party's reputation or cause that third party to be isolated, disgusted or embarrassed.
- Any person commits any offence of the following acts:
    - (1) that involves import to a computer system of forged computer data, either in whole or in part, or false computer data, in a manner that is likely to cause damage to that third party or the public;
    - (2) that involves import to a computer system of false computer data in a manner that is likely to damage the country's security or cause a public panic;
    - (3) that involves import to a computer system of any computer data related with an offence against the Kingdom's security under the Criminal Code;
    - (4) that involves import to a computer system of any computer data of a pornographic nature that is publicly accessible;
    - (5) that involves the dissemination or forwarding of computer data already known to be computer data under (1) (2) (3) or (4);

Conclusions

Many people here in Thailand are just waking up to the true potential of using digital forensics as a tool for their investigations. We cannot get away from the fact that the majority of transactions, communications and documentation are now in electronic format. That fact alone means that investigators and the judicial system should be looking at the importance of digital evidence.

There is still a fear of using digital evidence in Thailand, either due to a lack of awareness of what can be achieved through forensics, because there are no formal guidelines in Thailand for the handling of digital evidence or because they feel the evidence will be far too complex for the investigation in question.

Nevertheless the use of digital evidence in Thai courts will continue to increase and the judicial system needs to prepare for the changes. In order to assess the integrity and authenticity of the digital evidence, take note of the guidelines and the fundamental forensic principles that have been developed in other countries. These principles have been well tested in various courts and are accepted throughout the forensic community.

Because the use of digital evidence is still so new, there will be challenges and evidence may be disallowed. This is not a bad thing. It will force people to gain an understanding of the issues surrounding digital evidence, raise standards and help to formalize a set of guidelines for Thailand.

It is vital to find forensic investigators / experts to work with who have a good depth of experience and the ability to explain and present the evidence in a clear easy to understand manner. It doesn't matter how good the evidence is if the expert cannot present the evidence in a way that will be understood by all concerned.

People who have to deal with digital evidence need to:

- Undergo training in relation to forensic techniques, digital evidence and the issues surrounding the collection, preservation and production of digital evidence.
- Identify suitably qualified forensic investigators / experts who they can work with.
- Look at working together to put in place guidelines for the handling of digital data / evidence.

Taking the above steps will ensure that the judicial system is well placed to handle the issues surrounding digital evidence.

References

Good Practice Guide for Computer Based Electronic Evidence (UK)
http://7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence_v4_web.pdf

Lorraine v. Markel American Insurance Company
http://www.lexisnexis.com/applieddiscovery/LawLibrary/whitePapers/ADI_WP_LorraineVMarkel.pdf

Council of Europe Convention on Cybercrime (International)
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp

Electronic Transaction Act B.E 2544 (2001)
http://thailaws.com/law/t_laws/tlaw0073.pdf

Copyright Act B.E. 2537 (1994)
http://www.stop.in.th/webdatas/download/copyright_act_2537.pdf

Computer Crime Act B.E 2550 (2007)
http://www.thailawforum.com/database1/thailand-computer-crime-law.html