Digital Forensic

A newsletter for IT Professionals

Issue 10

I. Background of Digital Forensic

Definition of Digital Forensic

Digital forensic involves the collection and analysis of digital evidence. Any information stored on a digital media can be a piece of digital evidence to be analysed during a digital forensic process.

The purpose of digital forensic is to discover the digital evidence and ensure that they are admissible in court. Therefore, maintaining chain of custody is the most critical requirement and must be established throughout the whole process.

Definition of Chain of Custody

Chain of custody refers to the chronological documentation or paper trail, showing seizure, custody, control, transfer and disposition of evidence. As the objective of the evidence is to prove facts or to convict personnel of crimes in court, it must be handled with extreme care to avoid being altered or destroyed unauthorisedly. The ultimate purpose is to demonstrate that the alleged evidence is in fact relevant to the alleged crimes, instead of being fraudulently planted. If the chain of custody is broken, the underlying fact of the evidence will be questioned and the evidence can be no longer usable in court.

For digital evidence, the chain of custody also includes additional steps to create a binary forensic duplication of the original data and generate a digital fingerprint (i.e. hash) which can verify the data authenticity.

The Forensic Investigation Process

The forensic investigation process involves the following stages:

1. **Seizure**

   This is the preservation or ownership transfer of digital media before it is examined by forensic examiner.

Reference:
http://en.wikipedia.org/wiki/Chain_of_custody
http://www.isfs.org.hk/publications/ISFS_ComputerForensics_part2_20090806.pdf
http://en.wikipedia.org/wiki/Digital_forensics

I. Background of Digital Forensic (cont'd)

2. Acquisition and Forensic Imaging / Data Collection

After seizure, the digital media will be duplicated with a write blocking device, which creates a forensic duplication. The original digital media is then securely stored to prevent tampering.

In some case the original digital data is directly collected and examined on the digital media without duplication.

3. Analysis of Digital Media

The contents of the image files are analysed by forensic examiners with specialised tools, such as Guidance EnCase and Sleuth Kit ("TSK"), to identify evidence.

4. Reporting

This is the final stage after analysis of the digital media to convert data into a form which is suitable for non-technical individuals to become evidence in court. A "digital forensic report" should be compiled to include the following information:

- Any relevant information regarding what lead to you as the forensic examiner and when you become involved with the digital evidence;
- Detailed steps taken and people interviewed to preserve and forensically acquire the evidence, including any additional steps that you take (e.g. forensically wiping storage / examination media, etc.);
- All facts that you find during your analysis relating to the case; and
- Conclusion drawn from the forensic evidence;

International Standard for Digital Forensic

The International Organization on Computer Evidence ("IOCE") outlined principles for digital evidence collection, which include the following:

- Upon seizing digital evidence, actions taken should not change that evidence;
- When it is necessary for a person to access original digital evidence, that person should be trained for the purpose; and
- All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved and available for review.

Reference:
http://www.isfs.org.hk/publications/ISFS_ComputerForensics_part2_20090806.pdf
http://en.wikipedia.org/wiki/Computer_forensics
http://www.ioce.org/core.php?ID=5
http://en.wikipedia.org/wiki/Digital_forensic_process
http://computer-forensics.sans.org/blog/2010/08/25/intro-report-writing-digital-forensics/

I. Background of Digital Forensic (cont'd)

Common Techniques

In the digital forensic process, there are common techniques used for data collection and analysis.

- **Live Analysis** – This is the extraction of evidence from the operating system using forensic tools, or by capturing image of the system.

- **Cross-Drive Analysis** – Analysis can be performed across multiple hard disk drives without restricted to one single drive.

- **Deleted Files Recovery** – If the operating systems or the file systems "delete" data by assigning "deleted" tags on the specific sector instead of erasing it physically, the recovery of "deleted" data can still be possible.

Digital Forensic Tools

Specialist tools are developed by vendors for the forensic analysis stage and the following are common examples in the market:

- **Guidance EnCase** – It runs on Windows and provides a sophisticated graphic user interface, which allows browsing, searching and displaying devices, file systems and data files.

- **Brian Carrier's The Sleuth Kit ("TSK")** – It is a library of Unix and Windows-based utilities to perform investigations and data extraction from images of digital data from Windows, Linux and Unix platforms The TSK is normally used in conjunction with its custom front-end application, Autopsy, to provide a user friendly interface.

- **EnCase Enterprise Edition ("EEE") –** It uses the core EnCase product as the basis for examination and analysis of captured hard disk and memory images, with the added value of remote network forensic examinations of systems for large enterprises.

Do Universities Need Digital Forensics?

One may not discover the importance of digital forensic in daily operations of the systems in the university. However, it becomes very crucial when information security incidents involve regulations, litigations, crime and fraud.

The following are the major reasons for universities to spare resources on digital forensics are:

1. It gives universities a litigation and regulatory readiness and enables the universities to respond effectively to requests for information.

2. It helps to protect potential evidence to be presented in court.

3. It is required for universities for regulatory compliance purpose.

4. It provides convenience for internal investigations. For instance, it can help to detect or even prevent fraud effectively.

Reference:
http://www.guidancesoftware.com/
http://www.sleuthkit.org/

II. Risks of Digital Forensic in Universities

There are some risks of digital forensics need to be managed by universities during the process of obtaining and preserving digital evidence. These risks may affect the data authenticity and the proper documentation of the digital evidence.

- **Insufficient Knowledge and Resources**

  Very often normal backups are performed and maintained within universities. If the responsible staff is lack of proper training, or the data collection tools used are not designed specifically for forensic purposes, data collected may be altered or destroyed negligently and it may no longer represent truthful information.

- **Hidden or Tampered Evidence**

  There is a risk of deliberate hiding or tampering of information by rootkits. Rootkits are Trojan horse tools which modify the existing operating system letting an attacker to keep a secret access to the system.

  When a forensic examiner looks at the files in a directory, an application sends a request for the list to the operating system. The list passes through several pieces of software before being displayed on the screen. A filter may exist in between any software and remove the name of the file containing evidence during transfer.

- **Weak Chain of Custody**

  The logging of all the evidence and the tracking of the location of the evidence is critical to maintain the chain of custody so as to ensure the usefulness of keeping the evidence.

  However, chain of custody can be easily compromised when the documentation of tracking is not sufficient, or when IT staff checks the data on the digital media without formal documentation. This can break the chain of custody causing the evidence to be inadmissible to the court to prove any fact.

- **Security Challenge**

  Any compromise of the security of forensic software can ruin the entire forensic investigation and analysis. For example, if investigators' workstations are not adequately protected (e.g. hosted in isolated network), Denial of Service ("DoS") attack may exploit the defects of some popular forensic software and can cause crash or even allow attackers to execute malicious programs on them, which may impede the investigation, making evidence difficult or impossible to examine. Data hiding techniques can hide information in protected area of hard disks or encrypted evidence into the format un-interpretable from the forensic software.

Reference:
http://apps.americanbar.org/lpm/lpt/articles/tch11071.shtml
http://www.d.umn.edu/~schw0748/Digital%20Forensics/p56-carrier.pdf
http://www.isecpartners.com/files/iSEC-Breaking_Forensics_Software-Paper.v1_1.BH2007.pdf

III. Exploitations on Digital Forensic

Common types of exploitation on digital forensic software include data hiding, evidence corruption and analysis blocking. These exploitations adversely influence forensic investigation process in different stages.

- **Data Hiding**

  Forensic software mainly discovers and analyses evidence stored on a digital media. The software is used to detect all the information on the media. However, if vulnerability exists, exploitation can be driven by hiding evidence on the digital media.

  There are some common examples of data hiding in digital forensic software. One example is the prevention of examination of some data due to improper handling of the data partitions in Guidance Software EnCase 6.2 and 6.5.

  Another example is that EnCase Forensic Edition 4.18a does not support Device Configuration Overlays ("DCO"), which is a hidden area on many common hard disk drives. This may allow attackers to hide information without detection.

- **Evidence Corruption**

  Buffer overflow occurs when data written to a memory address corrupts data in the adjacent memory address due to insufficient boundary checking. Programming errors such as buffer overflow can cause code execution vulnerability.

  This may allow an attacker to overwrite control information in the program and provide new malicious codes to be executed in the vulnerable program.

  This kind of vulnerability in forensic software can cause the forensic image to be corrupted and hide or destroy the evidence captured by the forensic image.

  One example of evidence hiding attack is by changing the checksums of the evidence files. This causes the forensic software to ignore the evidence without obvious counting.

- **Analysis Blocking**

  Denial of Service ("DoS") may not cause significant destruction but temporary inconvenience to users in most of the systems in universities.

  However, if it happens to forensic software, it will disturb or stop the forensic analysis service, affecting the forensic investigation process or even making the evidence impossible to examine.

Reference:
http://www.isecpartners.com/files/iSEC-Breaking_Forensics_Software-Paper.v1_1.BH2007.pdf
http://www.cvedetails.com/cve/CVE-2007-4201/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-1578
http://en.wikipedia.org/wiki/Buffer_overflow

III. Exploitations on Digital Forensic (cont'd)

Buffer overflow can let the system analyse a maliciously crafted evidence file which frustrates the forensic analysis, or even execute code on the forensic examiner's machine.

Exploitations of Remote Acquisition

The following three types of exploitation are possible for forensic software with the function of remote acquisition of evidence. This functionality is usually useful in large enterprises as well as universities to perform investigations of their production or employee systems from time to time.

These attacks rely on specific configurations of the network upon which the forensic software is used. It is based on the insufficient authentication of the target system that running the forensic software.

- **IP Address Takeover**

  Remote acquisition of evidence relies on the network configurations. Hence it is possible that a malicious user builds a virtual machine with incriminating evidence and assigns it to another user's IP address.

  The forensic examiner will inspect the deliberately built machine and find evidence when examining another user's IP address.

- **Address Resolution Protocol ("ARP") Spoofing**

  ARP spoofing can be achieved by intercepting all the network traffic between a forensic examiner's machine, the forensic system and another user. A virtual machine with incriminating evidence is set up by the malicious user, which intercepts all the traffic from the forensic system to another user.

- **Dynamic Host Configuration Protocol ("DHCP") Spoofing**

  Another attack is DHCP spoofing, which assigns another user a new IP address, with the malicious attacker's machine as his or her gateway. Then the malicious user's machine can perform network translation and forward network traffic from the forensic system to the incriminating virtual machine.

Reference:
http://www.isecpartners.com/files/iSEC-Breaking_Forensics_Software-Paper.v1_1.BH2007.pdf

IV. Hardening Steps for Digital Forensic

A few hardening steps are listed below, which are useful to enforce a higher level of security protection during the forensic process performed by forensic examiners.

Initial Registration

The forensic system can be modified to perform a registration procedure when it is used for the first time in the universities' campus networks. This can generate unique key pair and create hardware ID per each machine in the campus network.

By deploying initial registration, secured mapping between the keypair and the machine's IP address can be established to detect any potential frauds or exploitations.

Utilise Existing Authentication

A secured communication with the remote systems is important for remote forensic examination of digital media.

Utilising the Active Directory's identification facilities can provide mutual authentication between the target machine and the forensic examiner's machine.

Enable Logging

Some forensic software provides an audit function to generate crash dump logs. This ensures that it is possible to recover critical information before the system crashed. The forensic examiners can investigate the logs after the crashes to identify any suspicious attempts or evidence of malicious exploitations. EnCase is an example of forensic software with a logging function.

Upgrade Regularly

Forensic software vendors usually develop new versions or patches of forensic software to address already-discovered vulnerabilities.

Universities are recommended to upgrade their forensic software timely and regularly to ensure that the vulnerabilities to public known exploitations are remediated. This process can be integrated with the patch management procedures to increase the overall security level of the forensic investigation process.

Reference:
http://www.encaseenterprise.com/support/articles/whenencasecrashes.aspx
http://www.isecpartners.com/files/iSEC-Breaking_Forensics_Software-Paper.v1_1.BH2007.pdf

IV. Hardening Steps for Digital Forensic (cont'd)

Chain of Custody

- **Protect All Evidence Equally**

  A sloppy or nonexistent chain of custody may end up being sufficient for a simple internal investigation of an employee. But it is better not to take the chance. Instead, universities should always protect all evidence equally so that it will hold up in court.

- **Enforce Comprehensive and Accurate Documentation**

  To prove chain of custody, universities should document in detail regarding how the evidence is handled. The documentation should answer the following questions:

  - What is the evidence?
  - How did you get it?
  - When was it collected?
  - Who has handled it?
  - Why did that person handle it?
  - Where has it travelled, and where was it ultimately stored?

  Every single time the evidence is handed off, the chain of custody documentation needs to be updated.

- **Secure the "Best Evidence"**

  The first image of a storage media (e.g. hard drive) that forensic examiners take is usually known as the "best evidence," because it is closest to the original source. The chain of custody documentation should be always attached to the best evidence and stored under lock and key. In addition, it is also highly recommended to create a secondary image of the "best evidence" as working copy.

Confidentiality (new added content)

Like all sciences, there is a potential for abuse of digital forensic science and confidentiality is paramount since many types of digital evidence may involve sensitive information such as personal data, patent, financial information, etc. Adequate steps should be taken to tackle the confidentiality issues that forensic examiners may bring to the universities.

Reference:
http://www.csoonline.com/article/220718/how-to-keep-a-digital-chain-of-custody
http://www.ehow.com/about_5999274_confidentiality-important-forensic-science_.html#ixzz1Y2GyVedn

IV. Hardening Steps for Digital Forensic (cont'd)

- **Outside Law Enforcement**

  It has been always a controversial topic between preservation of sensitive information (e.g. privacy) and law enforcement's need to search and seize digital evidence.

  When digital forensic work is going to be performed by the law enforcement agencies, universities should first seek advice from their legal advisors to determine whether there are sufficient legal documents (e.g. warrant) stating the purpose for accessing the sensitive information. In addition, with the assistance of legal advisors, universities should also determine if the disclosure of sensitive information to the law enforcement will violate any statutory or regulatory requirements (e.g. Personal Data (Privacy) Ordinance).

- **Third Party Digital Forensics Contractors**

  Universities should only engage contractors with sufficient controls and equipments to allow digital forensic work to be conducted in a secured manner. For example, secured office / laboratory premises, encryption of data storage, and proper information disposal policy and mechanism.

  In addition, universities should always enter into confidential agreements with contractors in order to provide the necessary peace of mind. This agreement can be commenced at the outset of forensic work and therefore guarantees complete security of sensitive information.

- **Internal Digital Forensic Specialist**

  For internal digital forensic specialists, universities should clearly define the requirement on maintaining confidentiality in their job descriptions. A non-disclosure agreement ("NDA") should be signed by each internal digital forensic specialist upon commencing his or her position in the universities.

  Employee background check is highly recommended to be performed by the human resources departments of the universities before hiring the internal digital forensic specialists.

Reference:
http://www.ccl-forensics.com/About-CCL-Forensics/confidentiality-agreement.html
http://peninsuladigitalforensics.co.uk/confidiality.htm
http://euro.ecom.cmu.edu/program/law/08-732/Evidence/RyanShpantzer.pdf

V. Summary

In order to present the digital evidence in court, universities must maintain the chain of custody with the help of established digital forensic procedures. Various digital forensics tools are available to aid the data collection and analysis process so as to ensure the preservation of evidence in digital regime.

Due to the importance of the data processed by digital forensics software, a higher security requirement is required since it is used to examine evidence from suspected computer criminals or from computers which may already be compromised by an attacker. This means the evidence may be under the control of someone who is capable to frustrate or distract the investigation against them, not to mention that such evidence must be admissible to court.

Hence, owners and administrators of the digital forensics software in universities should pay close attention to the latest vulnerabilities of the digital forensics software, and react with appropriate hardening actions so as to avoid possible exploitations that compromise the relevant digital evidence.