Digital Forensics: New Opportunities

Generally, digital forensics is considered as the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data. Digital forensic tools are used to respond to an event by investigating suspect systems, gathering and preserving evidence, reconstructing events, and assessing the current state of an event. It can also be used for operational troubleshooting, log monitoring, data recovery, data acquisition, due diligence/regulatory compliance. The process for performing digital forensics comprises the four basic phases; viz., collection, examination, analysis and reporting. Read on to know more…

Dr. Onkar Nath

The author is an Information Security Strategist. He can be reached at dronkar@yahoo.com

Introduction

According to the Oxford dictionary, the word forensic is defined as *"relating to or denoting the application of scientific methods to the investigation of crime"* and *"or relating to courts of law"*. The first definition is that scientific methods are used in the investigation, and the second definition emphasises the fact that forensic activity usually relates to courts

Over the last decade, there has been an increase in the number and variety of crimes that involve computers. Computer crime investigators and law enforcement is using computer-based evidence to determine who, what, where, when, why and how for crimes. Digital forensic tools are used to respond to an event by investigating suspect systems, gathering and preserving evidence, reconstructing events, and assessing the current state of an event.

of law. But not all cases investigated end up in court. It is important that when a forensic investigation is launched it is conducted in a scientific way, and with a legal base as support.

In the organisations there are various data sources, hence, the digital forensic techniques can be used for many purposes, such as investigating crimes and internal policy violations, reconstructing information security incidents, troubleshooting operational problems, and recovering from accidental system damage. The organisation investigating the suspicious behaviour often lacks the tools and skills required to successfully gather evidence. The organisation needs to have the capability to perform digital forensics without such a capability; an organisation will have difficulty determining what events have occurred within its systems and networks.

What is Digital Forensics?

As per NIST (National Institute for Standards and Technology, USA), digital forensics is considered as the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.

Techopedia defines digital forensics as the process of uncovering and interpreting electronic data for use in a court of law. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past events.

Digital Forensic Research Workshop has defined digital forensics as *"The use of scientifically derived and proven methods toward the preservation, 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 unauthorised actions shown to be disruptive to planned operations."* This definition is comprehensive and encompasses all the practical aspects of digital forensics.

The Need for Digital Forensics

Over the last decade, there has been an increase in the number and variety of crimes that involve computers. Computer crime investigators and law enforcement is using computer-based evidence to determine who, what, where, when, why and how for crimes. Digital forensic tools are used to respond to an event by investigating suspect systems, gathering and preserving evidence, reconstructing events, and assessing the current state of an event. However, digital forensics is also useful for the following:

- **Operational Troubleshooting:** Digital forensic tools and techniques can be applied to troubleshooting operational issues, such as resolving a functional problem with an application, recording and reviewing the OS and application configuration settings for a host.
- **Log Monitoring:** Digital forensic tools can assist in log monitoring, such as analysing log entries and correlating log entries across multiple systems. This can also assist in incident handling, identifying policy violations, auditing, and other efforts.
- **Data Recovery:** Digital forensic tools can recover lost data from systems, including data that has been accidentally or purposely deleted or otherwise modified. The volume of data that can be recovered varies on a case-by-case basis.
- **Data Acquisition:** Digital forensic tools are used to acquire data from hosts or remote systems such as in the event of a user leaves an organisation, the data from the user's systems can be acquired and stored in case it is needed in the future. The system's media can then be sanitised to remove all of the original user's data.
- **Due Diligence/Regulatory Compliance:** The laws of the land or regulations require many organisations to protect sensitive information and maintain certain records for audit purposes. In the event of protected information is exposed to other parties, organisations may be required to notify other agencies or impacted individuals. Forensics can help organisations exercise due diligence and comply with such requirements.

Process of Digital Forensics

As per the National Institute of Standards and Technology (NIST), the process for performing digital forensics comprises the four basic phases:

1. **Collection:** Identifying, labeling, recording, and acquiring data from the possible sources of relevant data, while following procedures that preserve the integrity of the data.
2. **Examination:** Use manual and automated methods to assess and extract data of particular interest, while preserving the integrity of the data.
3. **Analysis:** Use legally justifiable methods and techniques to derive useful information.
4. **Reporting:** Describe actions used, explain how tools and procedures were selected, and determine what other actions need to be performed, recommend improvements to policies, guidelines, procedures, tools and other aspects of the forensic process.

Potential Sources of digital forensics are hard disks, tapes, external/removable media, network infrastructure logs (Firewall, IDS, proxy, *etc.*), application, audit log files, e-mail, other server content (Windows shares, web servers, databases, *etc.*) and Captured network traffic.

eDiscovery

eDiscovery, also known as electronic discovery, is the aspect of identifying, collecting and producing Electronically Stored Information (ESI) in response to a request for production in a law suit or investigation. ESI includes, but is not limited to, emails, documents, presentations, databases, voicemail, multimedia files, social media, and web sites. The processes of eDiscovery are often complex because of the sheer volume of electronic data produced and stored. Additionally, electronic documents are more dynamic and often contain metadata such as time-date stamps, author and recipient information, and file properties. Preserving the original content and metadata for electronically stored information is required in order to have acceptability in the court of law.

Pre-requisite for Digital Forensics *(Policy, Standard, Procedures and Guidelines)*

Organisation should have digital forensics policy duly approved by the appropriate authority and disseminated to the concerned audience. Digital forensic policy should clearly define the roles and responsibilities of all people performing or assisting with the organisation's forensic activities. The policy should include all internal and external parties that may be involved and should clearly indicate who should contact which parties under different circumstances. The organisation should adopt some standard to have consistency and acceptability digital evidences in the court of law and develop supporting procedures and guidelines to implement digital forensics policy.

Tabletop exercises that focus on how forensic tools and techniques can be used in various scenarios provide an effective way of building and maintaining skills and identifying problems with guidelines, procedures, and policies.

Digital Forensic Tools

Digital forensic tools are being developed at a brisk pace in response to the ever increasing variety of forensic targets. Most tools are created for specific tasks—file system analysis, memory analysis, network analysis, *etc.* and make little effort to interoperate with one another. Following are the commonly used digital forensics tools. Some of them are freeware too.

- Forensic Disk Controller
- SANS SIFT
- AccessData
- ProDiscover Basic
- EnCase
- FTK Imager
- PTK Forensics
- The Sleuth Kit
- CAINF
- Xplico

The admissibility of digital evidence in the court of law relies on the tools used to extract it. In the US, forensic tools are subjected to the Daubert standard, where the judge is responsible for ensuring that the processes and software used were acceptable.

DFF (Digital Forensics Framework) is a free and Open Source computer forensics software built on top of a dedicated Application Programming Interface (API). It advertises that the capability to be used both by professional and non-expert people in order to quickly and easily collect, preserve and reveal digital evidences without compromising systems and data. Following are some of the digital forensics frameworks are DFF, PyFlag, FACE, DIALOG, and FORZA.

Apart from the computer/cyber crime investigation, there are several financial forensic engagements which extensively use the digital forensics. Some of the engagements are: 'economic damages calculations whether suffered through tort or breach of contract post-acquisition disputes such as earn outs or breaches of warranties,' 'bankruptcy, insolvency, and reorganisation,' 'securities fraud,' 'business valuation,' 'computer forensics/e-discovery,' etc.

Guidelines for Effective and Efficient Digital Forensic Activities

- Organisations should ensure that their policies contain clear statements addressing all major digital forensics considerations, such as contacting law enforcement, performing monitoring. There should be regular reviews of forensic policies and procedures.
- Organisations should create and maintain procedures and guidelines for performing forensic tasks, based on the organisation's policies and all applicable laws and regulations.
- Organisations should ensure that their policies and procedures support the reasonable and appropriate use of forensic tools.
- Organisations should ensure that their IT professionals are prepared to participate in forensic activities.

Challenges in Digital Forensics

The leading challenge for digital forensic investigations is that of scale. This has a significant impact on digital forensics. However, a deeper and more significant implication of recent trends is the escalating complexity of scenarios of digital investigations. As the capabilities of individual applications, the size of forensic targets, and the number of networked systems all increase, the number of possible interactions and possible outcomes of forensic interest grows exponentially. Some of the commonly faced problems in digital forensics are as under:

Hard to get

- Duplicating or preserving the digital evidence is very difficult, without knowing the duplication itself inherently changed the data?
- Time lines are critical for showing who did what, and when. But digital time stamps are absent, can easily be spoofed, in digital data or the digital time provided by NTP (Network Protocol Server) is incorrect.
- In order to be able to state conclusively that action A caused result B, the concept of repeatability must be introduced. This is very difficult with digital forensics.
- Anti-forensic activity may prevent collection.

Easy to destroy

- Starting a PC/Server, updates hundreds of timestamps and modifies many files
- Attaching a hard disk or USB stick will modify file system timestamps
- Volatile memory is lost when a machine is powered off

Support and Awareness

Support from top management for digital forensics set up in the organisation is of paramount importance. There should be defined and established process of escalation and additional support. It should be included in the work flow and the business processes. Awareness must take place at all levels in the organisation; rather it should be beginning with top management. The awareness may take place online or off-line. If awareness campaign is linked with performance, then it will work like catalyst.

Supporting Forensics in the Information System Life Cycle

NIST has stated in its special publication 800-86 "*Guide to Integrating Forensic Techniques into Incident Response*" that many incidents can be handled more efficiently and effectively if forensic considerations have been incorporated into the information system life cycle. Examples of such considerations are as follows:

- Performing regular backups of systems and maintaining previous backups for a specific period of time.
- Enabling auditing on workstations, servers, and network devices.
- Forwarding audit records to secure centralised log servers.
- Configuring mission-critical applications to perform auditing, including recording all authentication attempts.
- Maintaining a database of file hashes for the files of common OS and application deployments, and using file integrity checking software on particularly important assets.

- Maintaining records (*e.g.*, baselines) of network and system configurations.
- Establishing data retention policies that support performing historical reviews of system and network activity, complying with requests or requirements to preserve data relating to ongoing litigation and investigations, and destroying data that is no longer needed.

Use of Digital Forensic by Practicing CAs

Apart from the computer/cyber crime investigation, there are several financial forensic engagements which extensively use the digital forensics. Some of the engagements are:

- Economic damages calculations, whether suffered through tort or breach of contract
- Post-acquisition disputes such as earn outs or breaches of warranties
- Bankruptcy, insolvency, and reorganisation
- Securities fraud
- Business valuation
- Computer forensics/eDiscovery.
- Investigate network intrusions to determine the cause and extent of the breach

Standard for Digital Forensics

ISO/IEC 27037:2012 provides guidelines for specific activities in the handling of digital evidence, which are identification, collection, acquisition and preservation of potential digital evidence that can be of evidential value. It provides guidance to individuals with respect to common situations encountered throughout the digital evidence handling process and assists organisations in their disciplinary procedures and in facilitating the exchange of potential digital evidence between jurisdictions.

Certifications for Digital Forensics

Following are the International standard certifications considered for digital forensics:

- Certified Forensic Computer Examiner (CFCE)

The need for effective and efficient digital forensics analysis has been a major driving force in the development of digital forensics. Presently it is supported by ISO standard and guidelines issued by several internationally recognised agencies. Large number of digital forensics tools is available to support in-depth analysis of digital evidence.

- Certified Hacking Forensic Investigator (CHFI)
- Global Information Assurance Certification (Forensics Certifications)
- Certified Cyber Forensics Professional (CCFP)
- Certified Computer Forensics Examiner (CCFE)

Conclusion

The need for effective and efficient digital forensics analysis has been a major driving force in the development of digital forensics. Presently, it is supported by ISO standard and guidelines issued by several internationally recognised agencies. Large number of digital forensics tools is available to support in-depth analysis of digital evidence. The success of digital forensics depends upon the admissibility of digital evidences in the court of law.

Key Words:

Anti-Forensic: *A technique for concealing or destroying data so that others cannot access it.*

Daubert standard: *The Daubert standard provides a rule of evidence regarding the admissibility of expert witnesses' testimony during United States federal legal proceedings.*

Forensic Disk Controller: *A forensic disk controller or hardware write-block device is a specialised type of computer hard disk controller made for the purpose of gaining read-only access to computer hard drives without the risk of damaging the drive's contents.*

References:

1. "Guide to integrating forensic techniques into incident response", National Institute of Standards and Technology Special Publication 800-86 (August 2006).

2. Andrew Cristina, Lodovico Marziale, Golden G. Richard and Vassil Roussev, "FACE: Automated digital evidence discovery and correlation Andrew Case", Digital Investigation 5 (2008), S65-S75.

3. http://cdslegal.com/knowledge/the-basics-what-is-e-discovery/ accessed on 10 October 2014.

4. http://www.formalforensics.org/publications/thesis/chapter3.pdf accessed on 10 October 2014.

5. http://icsa.cs.up.ac.za/issa/2006/Proceedings/Full/101_Paper.pdf accessed on 10 October 2014.