Types of Investigation

MODULE

Contents

Types of Investigation

4.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Explain various types of investigations
- Classify techniques of digital forensics
- Understand volatile data
- Discover the importance of volatile data
- List order of volatility of digital evidences

4.2 TYPES OF INVESTIGATION

There are four main types of investigation performed by digital forensics specialists[1]. The first three are broadly similar in the activities they involve, but differ in terms of the legal restrictions and guidelines imposed as well as the type of digital evidence and form of report.

4.2.1 Criminal forensics

The largest form of digital forensics and falling under the remit of law enforcement (or private contractors working for them). Criminal forensics is usually part of a wider investigation conducted by law enforcement and other specialists with reports being intended to facilitate that investigation and, ultimately, to be entered as expert evidence before the court. Focus is on forensically sound data extraction and producing report/evidence in simple terms that a lay man will understand.

4.2.2 Intelligence gathering

This type of investigation is often associated with crime, but in relation to providing intelligence to help track, stop or identify criminal activity. Unless the evidence is later to be used in court forensic soundness is less of a concern in this form of investigation, instead speed can be a common requirement.

4.2.3 Electronic discovery (eDiscovery)

Similar to "criminal forensics" but in relation to civil law. Although functionally identical to its criminal counter part, eDiscovery has specific legal limitations and restrictions, usually in relation to the scope of any investigation. Privacy laws (for example, the right of employees not to have personal conversation intercepted) and human rights legislation often affect electronic discovery.

4.2.4 Intrusion investigation

[1] https://en.wikibooks.org/wiki/Introduction_to_Digital_Forensics/Types

The final form of investigation is different from the previous three. Intrusion investigation is instigated as a response to a network intrusion, for example a hacker trying to steal corporate secrets. The investigation focuses on identifying the entry point for such attacks, the scope of access and mitigating the hackers activities. Intrusion investigation often occurs "live" (i.e. in real time) and leans heavily on the discipline of network forensics.

VIDEO LECTURE

4.3 TECHNIQUES OF DIGITAL FORENSICS

A number of techniques are used during computer forensics investigations and much has been written on the many techniques used by law enforcement in particular[1].

4.3.1 Cross-drive analysis

A forensic technique that correlates information found on multiple hard drives. The process, still being researched, can be used to identify social networks and to perform anomaly detection.

4.3.2 Live analysis

The examination of computers from within the operating system using custom forensics or existing *sysadmin* tools to extract evidence. The practice is useful when dealing with Encrypting File Systems, for example, where the encryption keys may be collected and, in some instances, the logical hard drive volume may be imaged (known as a live acquisition) before the computer is shut down.

VIDEO LECTURE

> Volatile data

Live analysis

The examination of computers from within the operating system using custom forensics or existing sysadmin tools to extract evidence.

4.3.2.1 Volatile data

Volatile data is a data that is lost if the power is switched off. Computer requires some memory space where it could store most frequently used data, intermediately results of an operation, etc. which could be access by the CPU of a computer at faster rate. Some of the examples of fast memory are CPU registers, Cache memory, Random Access Memory(RAM), etc. The access time to these memory devices is low but they are volatile in nature. RAM contains wealth of information like system registries, passwords, browsing history, information about open processes and ports, uses profile of the system i.e. who logged into the computer, what are the hardware attached to the system, remote login details, IP address, etc. which could be very useful for the forensics investigator.

As discussed earlier, there are many volatile memory units present in system like CPU register, Cache memory, RAM, etc. with different order of volatility. Order of volatility specifies the how sensitive the memory is towards the loss of data. Higher is the order of volatility, higher are the chances of data being lost/change/modified. Therefore, the forensics investigator must follow the order of volatility to capture data from different memory devices. The order of volatility of various digital storage devices or digital evidences is shown in the figure below. The higher is the level of memory in the pyramid, higher is the order of volatility.

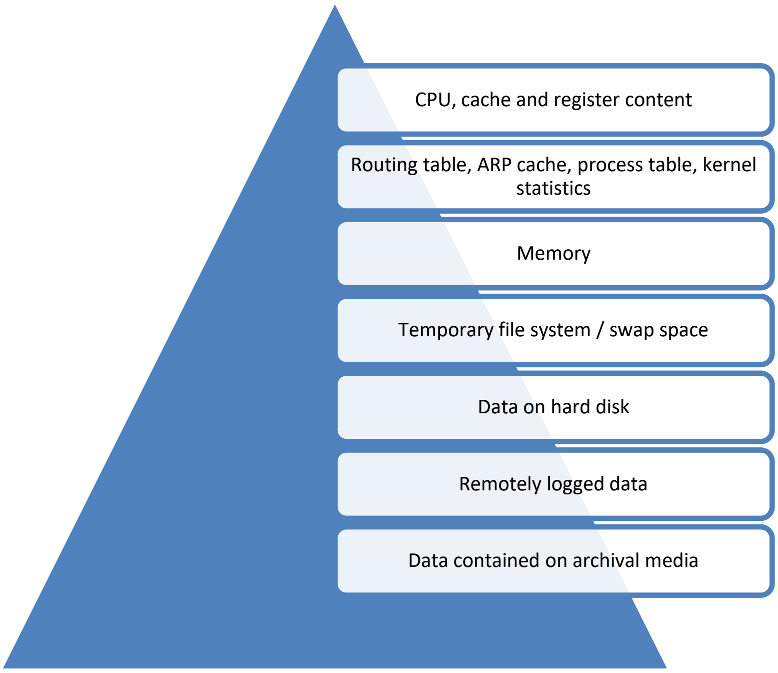
CPU, cache and register content
Routing table, ARP cache, process table, kernel statistics
Memory
Temporary file system / swap space
Data on hard disk
Remotely logged data
Data contained on archival media

Figure 2: Order of volatility of digital evidences

4.3.3 Recovery of Deleted files

A common technique used in computer forensics is the recovery of deleted files. Modern forensic software have their own tools for recovering or carving out deleted data. Most operating systems and file systems do not always erase physical file data, allowing investigators to reconstruct it from the physical disk sectors. File carving involves searching for known file headers within the disk image and reconstructing deleted materials.

4.3.4 Stochastic forensics

A method which uses stochastic properties of the computer system to investigate activities lacking digital artifacts. Its chief use is to investigate data theft.

4.3.5 Steganography

One of the techniques used to hide data is via steganography, the process of hiding data inside of a picture or digital image. An example would be to hide pornographic images of children or other information that a given criminal does not want to have discovered. Computer forensics professionals can fight this by looking at the hash of the file and comparing it to the original image (if available.) While the image appears exactly the same, the hash changes as the data changes. In Forensic examination, Steganalysis is used to get the details of Steganographic contents.

4.4 SUMMARY

1. It is advisable to take the photograph of the computer, cabling and the devices that are attached to the victim's computer, which are as important as victim's computer.

2. Only forensically clean storage devices should be used to store the logs and other important digital information from the victim's system.

3. The examination of the digital evidence should be done by a trained person as mishandling of digital devices may corrupt the data.

4. The Investigator look for document properties, file signatures, browser history, chat history, emails, printer spools, cache files, registry files, timeframe, ownership information, etc. to find clues.

5. Do not shut-off or reboot the machine. This will erase all the valuable data present in the volatile devices.

6. A common technique used in computer forensics is the recovery of deleted files.

4.5 CHECK YOUR PROGRESS

1. Fill in the blanks

i. _______________is a forensic technique that correlates information found on multiple hard drives.
ii. _______________ analysis is useful when dealing with Encrypting File Systems.
iii. _______________ data is a data that is lost of the power is switched off.
iv. _______________ is the process of hiding data inside of a picture or digital image.

2. State True or False

i. Original media can be used to carry out digital investigation process.
ii. By default, every part of the victim's computer is considered unreliable.
iii. Encrypted data can be impossible to view without the correct key or password.
iv. Cache memory is an example of volatile memory.

4.6 ANSWERS TO CHECK YOUR PROGRESS

1. Fill in the blanks

i. Cross-drive analysis
ii. Live
iii. Volatile
iv. Steganography

2. True or False

i. False
ii. True
iii. True
iv. True

4.7 FURTHER READING

Bunting, S., & Wei, W. (2006). *The Official EnCE: EnCase Certified ExaminorStudy Guide.* Wiley Publishing Inc.

Computer Forensics: Investigation Procedures and Response. EC-Council Press.

Cowen, D. (2013). *Computer Forensics: A Beginners Guide.*

ENISA, & Anderson, P. (2014). *Electronic evidence - a basic guide for First Responders.* European Union Agency for Network and Information Security.

Godbole, N., & Belapure, S. (2011). *Cyber Security (with CD): Understanding Cyber Crimes, Computer Forensics and Legal Perspectives.* Wiley.

Kent, K., Chevalie, S., Grance, T., & Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response.* Special Publication 800-86, National Institute of Standard and Technology, U.S. Department of Commerce.

Mukasey, M. B., Sedgwick, J. L., & Hagy, D. W. (2008). *Electronic Crime Scene Investigation:A Guide for First Responders Second Edition.* Special report, National Institute of Justice .

Nelson. (2013). *Guide to Computer Forensics and Investigations.*

Nelson, B., Phillips, A., & Steuart, C. (2009). *Guide to Computer Forensics and Investigations.* Cengage Learning.

Nolan, R., O'Sullivan, C., Branson, J., & Waits, C. (2005). *First Responders guide to Computer Forensic.* CERT Training and Education.

Nolan, R., O'Sullivan, C., Branson, J., & Waits, C. (2005). *First Responders Guide to Computer Forensics.*

Schneier, B. (1994). *Applied Cryptography.* Wiley.

Vacca, J. (2009). *Computer Forensics: Computer Crime Scene Investigation.*

Wolfe, H. B. (2007). Electronic Forensics: A Case for First Responders. *19th Annual FIRST Conference on Computer Security Incident Handling.* Spain.

4.8 MODEL QUESTIONS

1. What are the various technical, legal and administrative issues faced by computer forensics?

2. What are the main types of investigation performed by digital forensics specialists?

3. What are the different techniques of digital forensics?

4. What is volatile data? What is order of volatility of digital evidences? Explain.

REFERENCES, ARTICLE SOURCE & CONTRIBUTORS

Digital evidence. (2015, Aug. 20). Retrieved Oct. 11, 2015, from Wikipedia: https://en.wikipedia.org/wiki/Digital_evidence

Introduction to computer forensics. (n.d.). Retrieved Oct. 11, 2015, from forensic control: https://forensiccontrol.com/resources/beginners-guide-computer-forensics/

Krause, M., & Tipton, H. F. (Eds.). (1993). *Handbook of Information Security Management.* AUERBACH.

Lawton, D., Stacey, R., & Dodd, G. (2014). *eDiscovery in digital forensic investigation.* CAST publication number 32/14 available under the Open Government Licence v3.0 https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/.

Locard's Exchange Principle. (2005, April 10). Retrieved Oct. 11, 2015, from Project Gutenberg Self-Publishing Press: http://self.gutenberg.org/article/whebn0001722373/locard

Morton, T. (2013, Sep. 13). *Types of investigations.* Retrieved Oct. 11, 2015, from Wikibooks: https://en.wikibooks.org/wiki/Introduction_to_Digital_Forensics/Types

EXPERT PANEL

Dr. Jeetendra Pande, Associate Professor- Computer Science, School of Computer Science & IT, Uttarakhand Open University, Haldwani

Dr. Ajay Prasad, Sr. Associate Professor, University of Petroleum and Energy Studies, Dehradun

Dr. Akashdeep Bharadwaj, Professor, University of Petroleum and Energy Studies, Dehradun

Mr. Sridhar Chandramohan Iyer, Assistant Professor- Universal College of Engineering, Kaman, Vasai, University of Mumbai

Mr. Rishikesh Ojha, Digital Forensics and eDiscovery Expert

Ms. Priyanka Tewari, IT Consultant

Mr. Ketan Joglekar, Assistant Professor, GJ College, Maharastra

Dr. Ashutosh Kumar Bhatt, Associate Professor, Uttarakhand Open University, Haldwani

Dr. Sangram Panigrahi, Assistant Professor, Siksha 'O' Anusandhan, Bhubaneswar

UTTARAKHAND OPEN UNIVERSITY

This MOOC has been prepared with the support of

C·O·L

CEMCA