An Optimized Technique for Digital Forensic Investigation

Esan P. Panchal[1] Dr. B.K. Sharma[2]
[1]Research Scholar (Ph.D.) [2]HOD
[1]Rai University, Ahmedabad, Gujarat [2]R.B. Institute of Management Studies, Ahmedabad, Gujarat

Abstract— Several digital forensic investigation techniques are available in market. Digital forensic investigators use these techniques to solve digital crime. They use different forensic tools and techniques to find suspicious computer. Different digital forensic tools have their limitations. Therefore, Digital forensic investigators have to work with these limitations. Even increased digital data is a biggest challenge for investigators. Thus, traditional digital forensic investigation techniques waste resources to solve digital crime. Thus, there is a need of a technique which saves resources of digital forensic investigator.

Key words: Digital Forensic Investigation, Cyber Forensic Tools

I. Introduction

Traditional technique of digital forensic investigation performs different steps to analyze evidence. In order to analyze digital evidences it should be back up in any digital storage devices. As digital data size growing very rapidly that lead to need of more back up storage devices. Therefore, it will take more time to back such large data and also need more storage devices. Cost, Human Resource, Time is wasted to back up of data. An optimized technique for Digital Forensic Investigation would help digital forensic investigator to optimize resource utilization in solving the digital crime.[1]

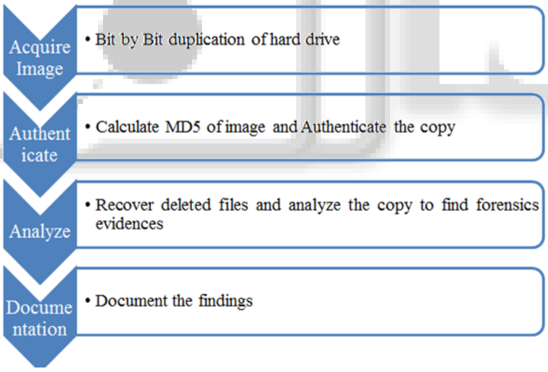

Acquire Image
• Bit by Bit duplication of hard drive
Authent icate
• Calculate MD5 of image and Authenticate the copy
Analyze
• Recover deleted files and analyze the copy to find forensics evidences
Docume ntation
• Document the findings

Fig. 1: A traditional technique of digital forensic investigation

II. Traditional technique

As shown in fig- 1, a traditional technique performs bit by bit duplication of hard drive for digital forensic investigation. To authenticate a copy it uses MD5 hashing technique. Digital forensic investigator performs investigation on authenticated copy hard drive and proves suspicious computer. A limitation of traditional technique is it needs time to get authenticated copy of in proportional to size of digital data. Thus, 1 TB size of each 10 hard disk needs 10 TB backup storage devices. A time needed is 10 times of each of hard disk to backup data.

A. *Cyber forensic Tools that follows Traditional Technique*

- Vinetto
- Pasco
- Encase
- FTK Access Data
- The Sleuth Kit(TSK)
- Nmap
- Helix
- Advanced Registry Tracer[21]
- Windows Registry Analyzer[22]
- The Volatility Framework: Volatile memory artifact extraction utility framework[23]
- Computer Online Forensic Evidence Extractor (COFEE)[24]
- Memoryze™[25]
- The Pmem Memory acquisition suite[26]
- Windows Memory Reader™[27]
- Paraben[28]
- Dd[30]
- Safe Back Version 2.0[31]
- SnapBack DatArrest Version 4.12
- Portable Evidence Recovery Unit
- Rapid Action Imaging Device

B. *Limitations of Traditional Technique*

- It needs larger storage media to back up digital data
- Waste more time to back up larger digital data
- Need more manpower
- Possibility of breach of privacy of private data[2]

III. An optimized technique

An optimized technique concentrates on identifying most probable suspicious computer system instead of taking image copy of every computer system.

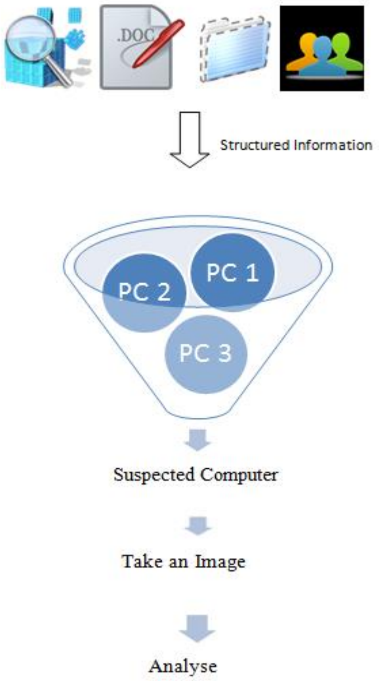


Fig. 2: An Optimized Technique for digital forensic investigation

As shown in Fig-2, An optimized technique for digital forensic investigation takes multiple computer system as an input and analyze forensic information of computer system not data. After filtration process digital forensic investigator can conclude on specific computer system which can be proved as a suspicious and would be used as a culprit in court. Digital forensic investigators have to take an image copy of specific computer system. Thus, Time and other resources needed are minimized and digital crime can be solved very easily.

A. Extraction of Digital Forensic Information from Computer System

- File metadata such as Creation, Modification and Accessed Data and Time
- History of Browsed Websites by user
- Installed/Uninstalled Programs
- Recently Executed programs
- Hidden files and directories
- Recently Attached USB Devices
- Logged on users
- Open ports
- Running processes
- Hidden files inside another file (ADS)
- Network connections
- File with different header
- Details of Temp Folder
- Unusual files, Processes
- Suspicious Accounts
- Log files[3]

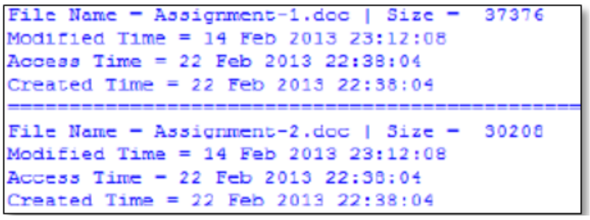
Above digital forensic information can be used as an evidence to prove a computer system as suspicious computer.

B. Probable areas of Digital Forensic Evidences

- DOSKEY/History – Displays command history
- Windows Registry – Different Key/Value pair also used as digital forensic evidence.
- Internet Browsing history –
- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedUrls
- Last user logged on user information-
- HKLM\SOFTWARE\Microsoft\Windows\Current Version\Authentication\LogonUI
- Command Entered by user in RUN command utility-
- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
- Download Directory for Internet Explorer- HKCU\Software\Microsoft\Internet Explorer\Download Directory
- Windows Task Manager also shows Process ID, Process Name, Username, Memory usage

C. A demo on Optimized Technique to fetch Digital Information

1) To gather File attributes of file

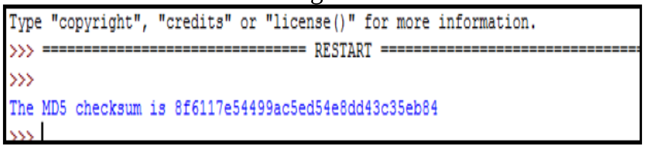


```
File Name - Assignment-1.doc | Size -  37376
Modified Time = 14 Feb 2013 23:12:08
Access Time = 22 Feb 2013 22:38:04
Created Time = 22 Feb 2013 22:38:04
==============================================
File Name - Assignment-2.doc | Size -  30208
Modified Time = 14 Feb 2013 23:12:08
Access Time - 22 Feb 2013 22:38:04
Created Time = 22 Feb 2013 22:38:04
```

Fig. 3: File attributes as digital forensic information

As shown in Fig-3, it fetches file name, size, Last Modified Time, Created Time, Last Access Time of all files of computer system. Even Hidden files and directories can also be analyzed.

Authentication of Fetched Digital Forensic Information



```
Type "copyright", "credits" or "license()" for more information.
>>> ============================== RESTART ==============================
>>>
The MD5 checksum is 8f6117e54499ac5ed54e8dd43c35eb84
>>> |
```

Fig. 4: MD5 Checksum for Authentication

As shown in Fig-4, It fetches md5 hashing algorithm to authenticate a copy.

IV. CONCLUSION

All tools extract information by using proprietary format and there is no interoperability between those tools to analysed data. Extract data of all system is time and space consuming task so instead of follow this process there is a pre-process which is used to identify suspicious system. This technique can remove space complexity and time complexity in process of digital forensic investigation.

ACKNOWLEDGEMENT

I would like to express my heartily gratitude towards my guide Dr. B.K. Sharma for this guidance on various aspects of this document and his contribution on the betterment of my work. I appreciate the thoughtful contributions that he has made to my efforts. It has been a great privilege to work under him. With his guidance and persistent help this research becomes possible. Lastly I would also like to give a special thanks to my friends, colleagues and Parents for playing an important role in strengthening my approaches in this work.

REFERENCES

[1] First Responders Guide to Computer Forensics By Richard Nolan, Colin O'Sullivan, Jake Branson, Cal Waits

[2] M. Reith, C. Carr, & G. Gunsch: An examination of digital forensic models, International Journal of Digital Evidence, 1, pp. 1-12 (2002).

[3] M. Alazab, S. Venkatraman & P. Watters: Digital forensic techniques for static analysis of NTFS images, Proceedings of ICIT2009, Fourt International Conference on Information Technology, IEEE Xplore (2009).

[4] B. Carrier: File system forensic analysis, Addison-Wesley Professional, USA, (2008).

[5] C. V. Marsico and M. K. Rogers, “ipod forensics,” International Journal of Digital Evidence, vol. 4, no. 2, 2005.

[6] M. Kiley, T. Shinbara, and M. K. Rogers, “ipod forensics update,” International Journal of Digital Evidence, vol. 6, no. 1, 2007.

[7] S. Willassen, “Forensic analysis of mobile phone internal memory,” In Advances in Digital Forensics, 2005, pp. 191–204.

[8] J. Sammes, Anthony and B. Jenkinson, “The treatment of pcs,” inForensic Computing. London: Springer, 2007, pp. 277–299.

[9] W. H. Allen, “Computer forensics,” Security & Privacy, IEEE, vol. 3,no. 4, pp.59–62, 2005.

[10] F. Adelstein, “Live forensics: Diagnosing your system without killing itfirst,” Communications of the ACM, vol. 49, no. 2, pp. 63–66, 2006.

[11] C. Hargreaves and H. Chivers, “Recovery of encryption keys from memory using a linear scan,” in Availability, Reliability and Security,2008. ARES 08. Third International Conference on, 2008, pp. 1369–1376.

[12] B. Carrier, “Risks of live digital forensic analysis,” Communications of the ACM, vol. 49, no. 2, pp. 56–61, 2006.

[13] R. McKemmish, “When is digital evidence forensically sound?” inAdvances in Digital Forensics IV, 2008, pp. 3–15.

[14] E. Casey, “What does "forensically sound" really mean?” Digital Investigation, vol. 4, no. 2, pp. 49–50, 2007.

[15] J. Haggerty and M. Taylor, “Forsigs: Forensic signature analysis of the hard drive for multimedia file fingerprints,” in New Approaches for Security, Privacy and Trust in Complex Environments, ser. IFIP International Federation for Information Processing, H. Venter, M. Eloff, L. Labuschagne, J. Eloff, and R. von Soims, Eds. Boston: Springer,2007, vol. 232, pp. 1–12.

[16] V. Roussev, “Hashing and data fingerprinting in digital forensics,” Security & Privacy, IEEE, vol. 7, no. 2, pp. 49–55, 2009.

[17] D. Byers and N. Shahmehri, “Contagious errors: Understanding and avoiding issues with imaging drives containing faulty sectors,” Digital Investigation, vol. 5, no. 1-2, pp. 29–33, 2008.

[18] J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten, Lest We Remember: Cold Boot Attacks onEncryption Keys, Proc. 2008 USENIX Security Symposium.

[19] Mariusz Burdach, Physical Memory Forensics, Black Hat 2006

[20] Timothy Vidas, The Acquisition and Analysis of Random Access Memory,Journal of Digital Forensic Practice, Volume 1 Issue 4 December 2006.

[21] http://www.elcomsoft.com/art.html

[22] http://www.wilderssecurity.com/showthread.php?t=56267

[23] https://www.volatilesystems.com/default/volatily

[24] https://cofee.nw3c.org/

[25] http://www.mandiant.com/resources/download/memoryze/

[26] https://volatility.googlecode.com/svn/branches/scudette/docs/pmem.html

[27] http://cybermarshal.com/index.php/cyber-marshal-utilities/windows-memoryreader

[28] http://www.forensicswiki.org/wiki/Category:Disk_imaging

[29] http://www.moredata.com/home/computer-forensic-imaging-tools.html

[30] http://www.forensicswiki.org/wiki/Dd

[31] http://www.sans.org/reading_room/whitepapers/incident/overview-diskimaging-tool-computer-forensics_643