Comparison of Acquisition Software for Digital Forensics Purposes

Muhammad Nur Faiz*[1], Wahyu Adi Prabowo[2]
[1,2]IT Telkom Purwokerto/Informatics
faiz@ittelkom-pwt.ac.id[*1], wahyuadi@ittelkom-pwt.ac.id[2]

Abstract

Digital Forensics, a term that is increasingly popular with internet needs and increasing cybercrime activity. Cybercrime is a criminal activity with digital media as a tool for committing crimes. The process for uncovering cybercrime is called digital forensics. The initial stage in digital forensics is an acquisition. The acquisition phase is very important because it will affect the level of difficulty and ease in investigating cybercrime. Software acquisition will affect the abandoned artefacts and even overwrite important evidence by the software, therefore investigators must use the best software for the acquisition stage. This study shows the difference in software for the acquisition of the best Random-Access Memory (RAM) such as processing time, memory usage, registry key, DLL. This research presents five acquisition software such as FTK Imager, Belkasoft RAM Capturer, Memoryze, DumpIt, Magnet RAM Capturer. Results of this study showed that FTK Imager left about 10 times more artefacts than DumpIt and Memoryze. Magnet RAM Capture the most artefacts, 4 times more than Belkasot RAM Capturer. Software acquisition with many artefacts, namely Capture RAM Magnet and FTK Imager, while for the fastest time is DumpIt and Capture RAM Magnet for software that takes a long time.

Keywords: *Acquisition, Artefacts, Digital Forensics, Software*

1. Introduction

Cybercrime can be defined as a crime committed in cyberspace with computer media. Disclosure of the cybercrime is known as digital forensics [1]. Digital forensics is a branch of forensic science pertaining to legal evidence found in computers and digital storage media such as flash drives, hard disk, or CD-ROM), electronic documents (such as email messages, video, or JPEG) or even a series of data packets in network [2]. The involvement of such a device in a computer crime is divided into three, namely: a destination computer, the computer becomes a means to make crime and computer functions to store all the information that it contains a criminal offence [3]. Digital forensics (computer forensics) is a discipline used to search digital evidence with scientific methods for the identification, preservation, extraction and documentation of digital evidence derived from digital sources to enable successful prosecution. The goal of digital forensics is to obtain legal evidence found in digital media [4]

The initial process of digital forensic namely the phase of data acquisition, which is the phase in which investigators make a perfect copy of the storage medium and Random Access Memory [5]. Investigators should be aware of all the changes data quickly. Because many of the techniques that take a long time, the software is expensive and specialized training, this makes the investigator choose a particular expertise in the field, one of which is Live Forensic. Live Forensic is a technique in the data acquisition phase need a computer that is being lit, the data that are running on that computer also called volatile data [6]. The success of the investigation depends on the quality of data collected. The quality of the copied data contains completeness of information such as information access, time and users, data quality is also affected by artefacts (Registry Key, DLL) left by the use of software acquisition [7]. Processing time, DLL, Registry Key and Memory Usage will impact to potential evidence. Data stored in RAM is data that is easy to change because data cannot be recovered after the user turns off the computer [8]. The forensics artefacts left by the web browser after the end of this session is not just a list of web visits, cookies, and downloads. These artefacts also contain the sites the user visits, the time and frequency of access, and also the search engine keywords used. When conducting a digital investigation of a system, investigators may collect evidence of the artefacts [9] . Investigators should distinguish tools that can only collect data and analyze them. There is a toolkit from the market that allows

Faiz, M., & Prabowo, W. (2018). Comparison of Acquisition Software for Digital Forensics Purposes. Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 4(1). doi:http://dx.doi.org/10.22219/kinetik.v4i1.687
Receive August 23, 2018; Revise November 04, 2018; Accepted November 09, 2018

collecting digital evidence from computers such as RAM and DISK [10]. Figure 1 shows 41 respondents in the USA about using acquisition software for digital forensics. FTK Imager ranked first with 23%, then Memoryze ranked second with 21% and ProDiscover with 16%, Belkasoft with 10%, while DumpIt and Windows Memory Reader only 7% of the total 41 respondents [7].

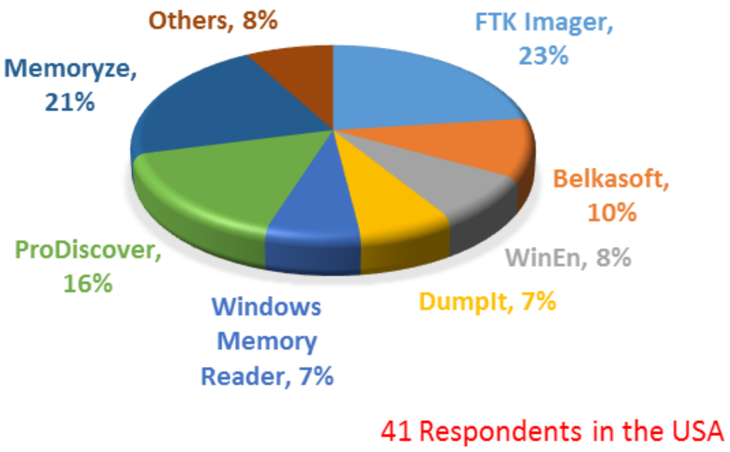


Figure 1. The Use of Software Acquisition Forensics

Information or Data can be found by analyzing RAM depending on the computer and operating system used [5]. The most valuable information: the active processes, information about open files, Registry Key, information about the activities of the network, the drivers used, user login, password and cryptographic key, hidden processes and data, malware, data temporarily, portable applications (applications that do not installed on the computer itself but only run), use etc., the session and lots of other important information [11] [12]. Windows Version uses Windows 10 operating system with 42,37% and Windows 7 with 42,14%, followed by 8,59% of Windows 8.1 and Windows XP to 3,66%. The use of the Windows Version in the world can be seen in Figure 2 [13].

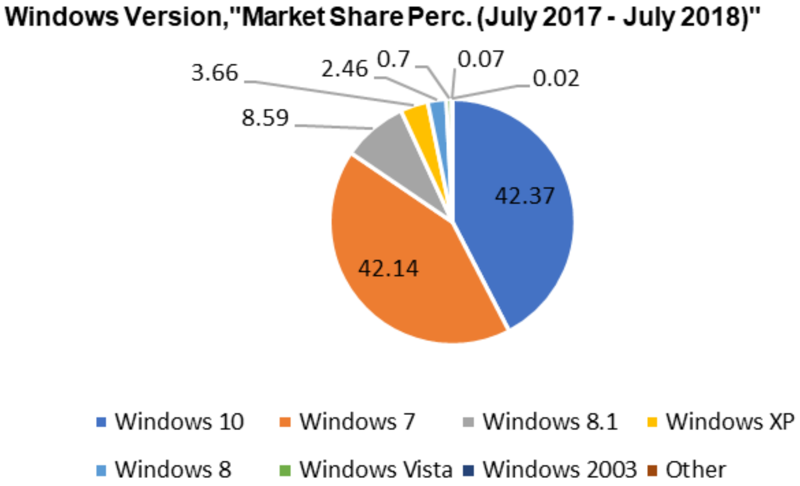


Figure 2. Windows Version Market Share 2017-2018

Forensic Toolkit Imager (FTK Imager) [14] is a forensics tool freeware developed by AccessData who have supported the researcher digital to conduct computer forensic examinations are complete of obtaining a forensic image of both the physical memory and logical, read the forensic image, decrypt the data, and reporting of digital evidence. Memoryze is a freeware forensic tool that has been developed by Mandiant. Memoryze not only can acquire physical memory from a Windows system but also can perform analysis of live memory while the computer is running. All analyses can be done either on the image that is acquired or a live system [15]. DumpIt is a freeware command-line tool developed by MoonSols. This tool allows for the acquisition of physical memory and saves the results as a raw file for later analysis [16]. Belkasoft Live Ram Capturer is a small and very powerful tool to get the memory to the operating system. An excellent feature of Belkasoft RAM Capturer Live is able to manage to acquire memory from the system with anti-debugging and anti-dumping memory enabled [17]. Magnet RAM Capture is a freeware tool designed to capture the computer's memory that allows researchers to recover and analyze valuable artefacts, as well as all the activities, are not usually stored on the local hard disk [18].

2. Related Work

Some results from the research were given by Aljaedi, et.al in [19] shows the effect of implementing Live Response forensic toolkit, which changed significantly volatile data environment in some cases and can override the potential evidence. memory image analysis is also used as an alternative approach that helps reduce the risk of losing evidence volatile. This comparative analysis calls attention to the ability of both methods of retrieving and recovering volatile data. Hausknecht, et.al in [12] that shows and explains the importance of the data live forensic and artefacts that can be found as well as the methods and tools used to extract and analyze data from RAM. Moreover, it also shows that sometimes the forensic investigation, the data contained in RAM can contain sufficient evidence to settle the whole case. Mcdown, et al. in [7] Acquisition software selection greatly affects the quality of the data when copying. The results of research analyzing the memory depth at seven acquisition software that runs on Windows 7 that FTK Imager, Belkasoft RAM Capturer, ProDiscover, Windows Memory Reader, WinEn, DumpIt and Memoryze. RAM usage when software is being run showed different results. Relics artefacts in FTK Imager Pro 10 times more compared with Belkasoft and Windows Memory Reader, 8 times more than WinEn, and 5 times more than DumpIt and Memoryze. These artefacts can overwrite important forensic content in RAM, which will negatively affect the investigation. Campbell in [20] the other four tested software is Windows Memory Reader, WinPmem, FTK Imager and DumpIt) were tested against two criteria (impact and completeness). WMR and DumpIt found to have the least impact, and also showed the greatest accuracy throughout the experiment.

Belsare and Sinha in [21] showed Software and Hardware for acquisition and storage of memory Live in getting the processes that occur during a system to turn widely available. the use of hardware does not have an impact on the data acquired but the price for this method is too expensive, while the use of methods of software will have an impact on the data obtained. the purpose of this research is the algorithm to make the collected data is authentic and can be accepted in court. Meera, Isaac and Balan in [22] that cybercrime will thrive on the virtual machine and the techniques used must be appropriate, such as acquisition technique in obtaining VMware via live internal file and analyzes the files obtained from the raw data stored in various grains.

Kolhe and Ahirao in [23] research examined tools for acquisition in live and dead forensics. This Live or dead method depends on the target. this research produces the advantages and disadvantages of both methods with acquisition tools as a comparison. the results of this study are recommended to use the live forensics method because this method is the best way to investigate in a short time because it takes data only on RAM that is running, it is far more effective than dead forensics

Based on previous research, it can be concluded that research on comparison of acquisition software has been done by McDown, Varol, Carvajal, Chen, but the software tested was different from this study. The results of this study are expected to help investigators in determining the best acquisition software so as not to leave many artifacts because it impacts on important evidence.

3. Methodology

The method used to compare the acquisition of five tools that run on Live forensics Image Acquisition Proposed, as seen Figure 3.

This research begins with a device that lights up then the acquisition and completion stages. In the acquisition phase, things are examined such as the use of Memory, Processing time, DLL, Registry Key, because this will determine the artefacts left behind. Experiments performed on a physical device by using the Laptop Intel (R) Core (TM) i3-2350M CPU @ 2.30GHz, RAM 4 GB DDR3 SO-DIMMs, 250 GB hard disk, HD Seagate 1,5 TB the operating system 64-bit Windows 10 with tools FTK Imager_Lite_3.1.1, DumpIt v1.3.2.20110401, Belkasoft RAM Capturer, RAM

Magnet Capture V1, Memoryze Version 3.0.0. This experiment is not connected to the Internet to prevent the computer may change the data in memory that can be caused by Internet services.

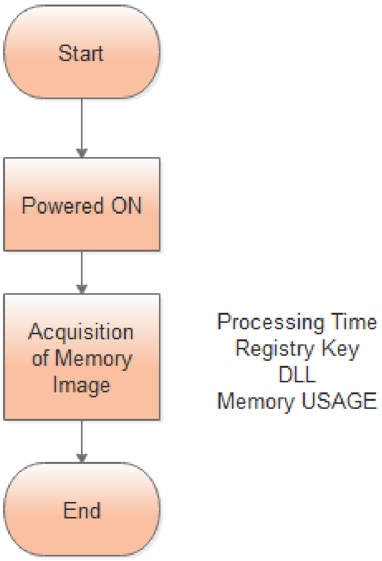
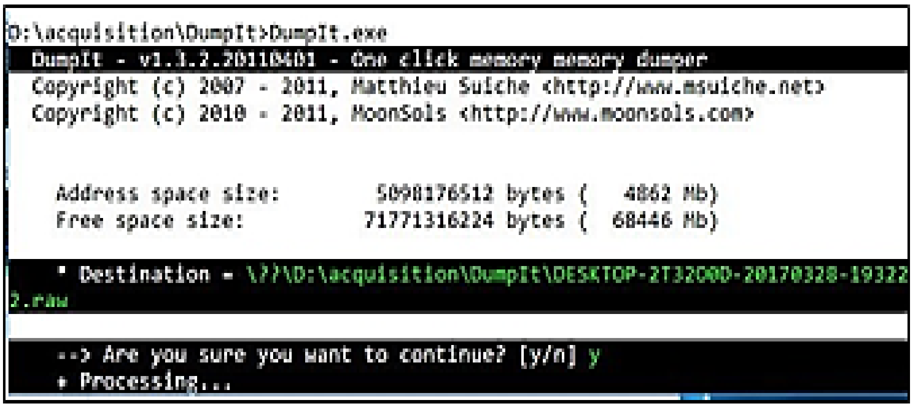


Figure 3. Live Forensics Image Acquisition Proposed

4. Results and Discussion

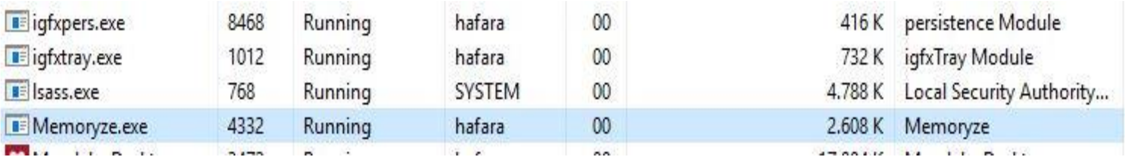
Experiments carried out at the research aims to determine the memory usage, the use of DLL, the processing time and changes in the Registry Key when running these tools. The acquisition process on the RAM is very important because the data must be clean of tools used investigator.

Figure 4 shows acquisition process with tools DumpIt run via command line on windows and then point DumpIt layout and imaging processes. The capacity of the RAM of 4862 MB and all data on it will be recorded on the acquisition process with the file extension RAW. Memoryze is tools acquisition and RAM usage showed in 2600k in Figure 5. It can be seen the use of RAM on the Windows task manager. Process Explorer also shown application use of RAM and showed in Figure 6.



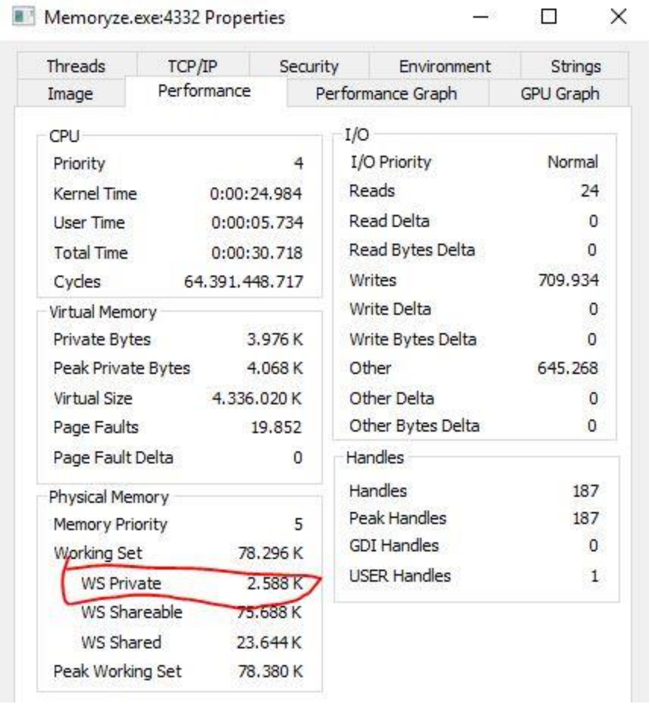
```
D:\acquisition\DumpIt>DumpIt.exe
  DumpIt - v1.3.2.20110401 - One click memory memory dumper
  Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
  Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>


    Address space size:        5098176512 bytes (   4862 Mb)
    Free space size:          71771316224 bytes (  68446 Mb)

    * Destination = \??\D:\acquisition\DumpIt\DESKTOP-2T32O0D-20170328-19322
2.raw

    --> Are you sure you want to continue? [y/n] y
    + Processing...
```

Figure 4. Acquisition Process Using DumpIt



igfxpers.exe	8468	Running	hafara	00	416 K	persistence Module
igfxtray.exe	1012	Running	hafara	00	732 K	igfxTray Module
lsass.exe	768	Running	SYSTEM	00	4.788 K	Local Security Authority...
Memoryze.exe	4332	Running	hafara	00	2.608 K	Memoryze

Figure 5. RAM Usage of Memoryze by Windows Task Manager



CPU

Priority	4
Kernel Time	0:00:24.984
User Time	0:00:05.734
Total Time	0:00:30.718
Cycles	64.391.448.717

Virtual Memory

Private Bytes	3.976 K
Peak Private Bytes	4.068 K
Virtual Size	4.336.020 K
Page Faults	19.852
Page Fault Delta	0

Physical Memory

Memory Priority	5
Working Set	78.296 K
WS Private	2.588 K
WS Shareable	75.688 K
WS Shared	23.644 K
Peak Working Set	78.380 K

I/O

I/O Priority	Normal
Reads	24
Read Delta	0
Read Bytes Delta	0
Writes	709.934
Write Delta	0
Write Bytes Delta	0
Other	645.268
Other Delta	0
Other Bytes Delta	0

Handles

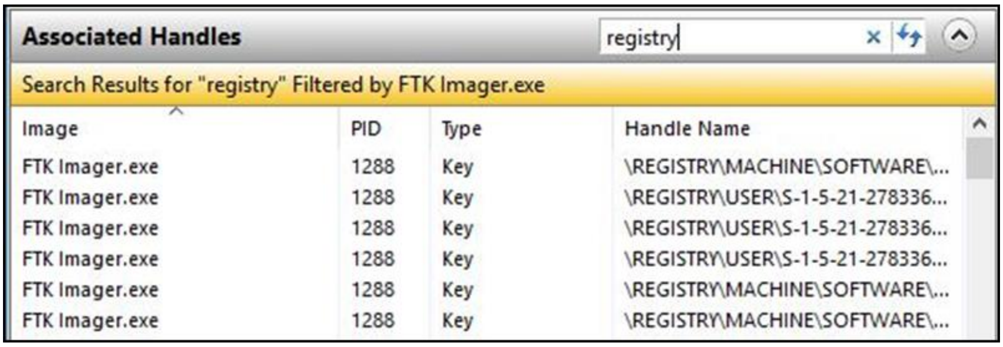
Handles	187
Peak Handles	187
GDI Handles	0
USER Handles	1

Figure 6. RAM usage of Memoryze by Process Explorer

Figure 7 can be seen all of the keys that are used to run the FTK Imager so that this key will turn on the RAM which will be useful for a forensic process. Registry Key will record all log the use of programs including access time, walking and even modify the program. Tools FTK Imager 13.736 Kb of RAM, this is because FTK Imager multithread resulting takes a lot of RAM. In DumpIt tools using the smallest RAM is equal to 692 Kb, this happens because DumpIt runs on the command line so it takes up little RAM shown in Figure 8.

Acquisition tools on Figure 9 shows the time difference in the acquisition process of the five tools, from five tools, can be seen that DumpIt has the fastest time is 184.54s compared to other tools and Magnet RAM Capture lowest time is 220.24s. Different uses of the DLL and change the Registry Key for running software, can be obtained Magnet RAM Capture uses the highest DLL that is 285 to change the Registry Key for 98. At DumpIt tools using the smallest DLL by 44 and Registry Key as 4. this makes the best DumpIt on heritage artifacts in the operating system shown in Figure 10.

In the Table 1, are known to the software with the use of a memory with a small size that is DumpIt, Memoryze, Belka RAM Capturer. FTK Imager on the memory usage using the highest memory is 117 Mb, while the lowest with 10.9 Mb DumpIt. At Magnetic RAM Capture processing time takes a lot for the acquisition of 4 Gb of RAM memory that is 220.24 s while Memoryze only takes 184.54 s. The use of RAM Capture Key Registry Majority Magnet by using 98 keys and DumpIt only need 4 key. RAM usage Magnet Capture DLL for use with the highest DLL 285 and DLL little DumpIt use only 44



Search Results for "registry" Filtered by FTK Imager.exe

Image	PID	Type	Handle Name
FTK Imager.exe	1288	Key	\REGISTRY\MACHINE\SOFTWARE\...
FTK Imager.exe	1288	Key	\REGISTRY\USER\S-1-5-21-278336...
FTK Imager.exe	1288	Key	\REGISTRY\USER\S-1-5-21-278336...
FTK Imager.exe	1288	Key	\REGISTRY\USER\S-1-5-21-278336...
FTK Imager.exe	1288	Key	\REGISTRY\MACHINE\SOFTWARE\...
FTK Imager.exe	1288	Key	\REGISTRY\MACHINE\SOFTWARE\...

Figure 7. Analysis Key of FTK Imager

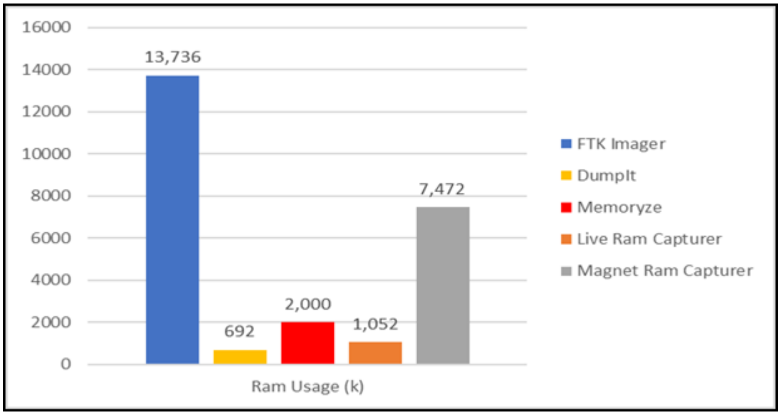


Figure 8. RAM Usage Acquisition Tools

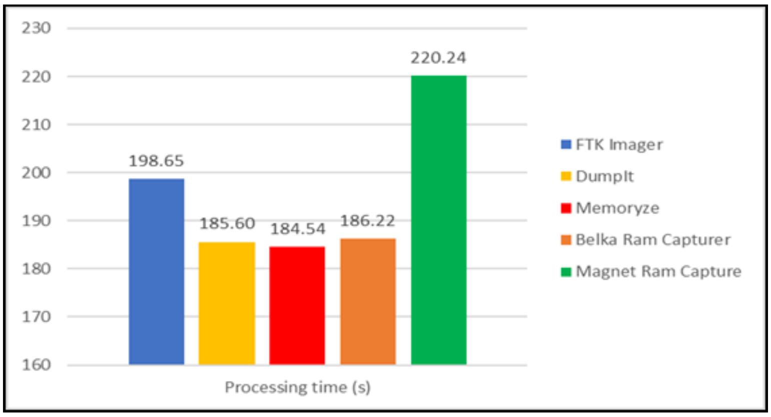


Figure 9. Processing Time Acquisition Software

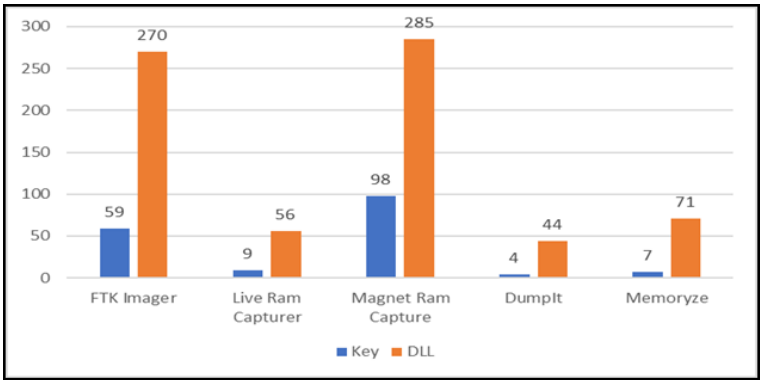


Figure 10. DLL and Registry Key of Acquisition Software

Table 1. Comparison Acquisition Software

Tools	Memory Usage (Mb)	Processing Time (second)	Registry Key	DLL
FTK Imager	117	198.65	59	270
Belka RAM Capturer	18	186.22	9	56
Magnet RAM Capture	76	220.24	98	285
DumpIt	10	185.6	4	44
Memoryze	13	184.54	7	71

5. Conclusion

Volatile data on RAM is very important in the process of digital forensic investigation because errors in turbulent data acquisition can potentially overwrite evidence and tool selection is also a determinant of the investigator's success in obtaining the first evidence. This research presents five acquisition software with a fast process, leaving little artifacts and RAM usage. The five forensic acquisition software analyzed were FTK Imager, Memoryze, Belkasoft RAM Capturer, Magnet RAM Capturer, DumpIt. As a result of this study, the FTK Imager left around 10 times more artifacts from DumpIt and Memoryze. Magnet RAM Capture artifacts at most, four times more than Belkasot RAM Capturer. Software acquisition with many artifacts, namely Capture RAM Magnet and FTK Imager, while for the fastest time is DumpIt and for software that takes a long time, namely RAM Capture Magnet. Suggestions for future research is to compare with hardware, other operating systems with software commonly used by digital forensics investigators.

References

[1] Sindhu. K. K and B. Meshram, *“Digital Forensic Investigation using WinHex Tool,”* International Journal of Computer Science and Technology, Vol. 3, No. 1, Pp. 1-7, 2012.

[2] N. R. Syambas and N. El Farisi, *“Two-Step Injection Method for Collecting Digital Evidence in Digital Forensics,”* Journal of ICT Research Applications, Vol. 8, No. 2, Pp. 141–156, 2014.

[3] F. Gianni and F. Solinas, *“Live digital forensics: Windows XP vs Windows 7,”* 2013 2nd International Conference Informatics Applications (ICIA), Pp. 1–6, 2013.

[4] M. M. Nasreldin, M. El-hennawy, H. K. Aslan, and A. El-hennawy, *“Digital Forensics Evidence Acquisition and Chain of Custody in Cloud Computing,”* in IJCSI International Journal of Computer Science Issues, Vol. 12, No. 1, Pp. 153–160, 2015.

[5] M. Kaur, N. Kaur, and S. Khurana, *“A Literature Review on Cyber Forensic and its Analysis tools,”* International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, No. 1, Pp. 23–28, 2016.

[6] M. N. Faiz, R. Umar, and A. Yudhana, “Analisis Live Forensics Untuk Perbandingan Keamanan Email Pada Sistem Operasi Proprietary,” Jurnal Ilmiah ILKOM, Vol. 8, No. 3, Pp. 242–247, 2016.

[7] R. J. Mcdown, C. Varol, L. Carvajal, and L. Chen, *“In-Depth Analysis of Computer Memory Acquisition Software for Forensic Purposes,”* Journal of Forensic Sciences, Vol. 61, No. January, Pp. 110–116, 2016.

[8] S. Thongjul and S. Tritilanunt, *“Analyzing and Searching Process of Internet Username and Password Stored in Random Access Memory (RAM),”* in 2015 12th International Joint Conference on Computer Science and Software Engineering (JCSSE), Pp. 257–262, 2015.

[9] U. Rusydi, A. Yudhana, and M. N. Faiz, *“Experimental Analysis of Web Browser Sessions Using Live Forensics Method,”* International Journal of Electrical and Computer Engineering, Vol. 8, No. 5, Pp. 5, 2018.

[10] P. Lallement, *“The Cybercrime Process : An Overview of Scientific Challenges and Methods,”* International Journal of Advanced Computer Science & Applications, Vol. 4, No. 12, Pp. 72–78, 2013.

[11] M. H. Ligh, A. Case, J. Levy, and Aa. Walters, *"The Art of Memory Forensics,"* Indianapolis: Wiley Publishing, Inc., 2013.

[12] K. Hausknecht, D. Foit, and J. Burić, *“RAM Data Significance in Digital Forensics,”* in 38th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2015 - Proceedings, Pp. 1372–1375, 2015.

[13] StatCounter Global Stats, *“Windows Version,"* Market Share Perc. (July 2017 - July 2018), 2018.

[14] AccessData, *"FTK Imager,"* Lindon: AccessData Group, 2016.

[15] P. Hazel, *“User Guide Memoryze Mandiants.”* Mandiant, Cambridge, Pp. 1–33, 2008.

[16] A. Borges, *“Memory Acquisition,”* 2015.

[17] R. Dave, N. R. Mistry, and M. S. Dahiya, *“Volatile Memory Based Forensic Artifacts & Analysis,”* International Journal for Research in Applied Science and Engineering Technology, Vol. 2, No. I, Pp. 120–124, 2014.

[18] T. Willett, *“Forensic Image Acquisition Process – Windows,”* 2017.

[19] A. Aljaedi, D. Lindskog, P. Zavarsky, R. Ruhl, and F. Almari, *“Comparative Analysis of Volatile Memory Forensics,”* IEEE International Conference Privacy, Security, Risk and Trust IEEE International Conference on Social Computing, Pp. 1253–1258, 2011.

[20] W. Campbell, *“Volatile Memory Acquisition Tools – A Comparison Across Taint And Correctness,”* Australian Digital Forensics Conference, Pp. 9–19, 2013.

[21] J. Belsare and A. Sinha, *“Live Memory Forensic Analysis,”* International Journal on Recent and Innovation Trends in Computing and Communication, Vol. 3, No. 5, Pp. 2775–2778, 2015.

[22] V. Meera, M. M. Isaac, and C. Balan, *“Forensic Acquisition and Analysis of VMware Virtual Machine Artifacts,”* Proc. - 2013 IEEE International Multi-Conference Automation, Computing, Communication, Control and Compressed Sensing, iMac4s 2013, Pp. 255–259, 2013.

[23] M. Kolhe and P. Ahirao, *“Live Vs Dead Computer Forensic Image Acquisition,”* International Journal of Computer Science and Information Technologies, Vol. 8, No. 3, Pp. 455–457, 2017.