International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Memory Forensics: Tools Comparison

Pooja Salave[1], Atisha Wakdikar[2]

Bharati Vidyapeeth's Institute of Management and Information Technology, Navi Mumbai, Maharashtra, India

Abstract: ***This research done to estimate the performance of different tools that acquire, analyze and recover the evidences of crime from volatile memory. Volatile memory stays for a very short period and that is why it is always tough to analyze such memory. It contains much valuable and confidential information such as passwords, usernames, running processes, etc. Acquiring, analyzing and recovering are the three major steps for memory forensics. All the tools investigated are not entirely fitted for a particular situation hence; the investigation needs to rely on many tools that can retrieve useful information from the evidences. It is important to know the usefulness of a tool before it is applied to solve a crime. Although most of the tools are successful in providing reasonable evidence, no single tool is sufficient to complete the investigation.***

Keywords: Acquisition Memory Tools, Analyzing Memory Tools, Digital Forensics, Live Analysis, Memory Forensics, Recovering Memory Tools.

1. Introduction

Digital Forensics is knowledge of investigating and recovering evidence from digital devices using different tools.[1] With the enhancement of technology, the cybercrime rate has increased drastically. To control the effects of such crimes digital forensics has gained popularity in recent years. In today's world, the dependency on computers is growing widely. Government agencies and private companies are attempting to protect themselves from cyber attacks with digital defence techniques like encryption, firewalls and heuristic or signature scanning, etc. Meanwhile, the number of attacks that include sensitive military data canters, targeting power grids and stealing trade secrets from both private and public organizations continues to increase. the detection, response and reporting of these kinds of intrusions as well as other incidents involving computer systems, are critical for cyber security professionals Just like that, if the data taken from the organizations encrypted across the network, to determine which sensitive files were stolen and that won't be recognized by traditional packet capture techniques. However, passwords and encrypted keys can often be recovered by memory forensics, or even the file's plain-text contents before they were encrypted, providing information to understand the scope of an attack.

2. Literature Review

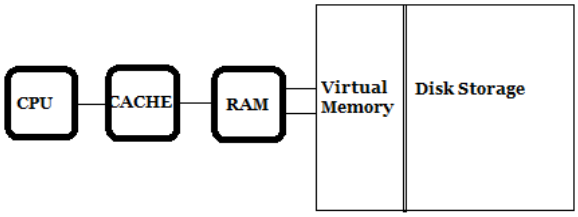

Figure 1: Flow of Memory Storage

In the world of digital forensics, memory forensics is arguably the most interesting and successful realm. Memory forensics involves analyzing the data stored in the physical memory at operating system runtime. Its primary application is in the investigation of advanced computer attacks which are quiet enough to avoid leaving data on the computer hard drive. Consequently, the memory (RAM) must be analyzed for forensic information. Each and every function performed by an application or operating system results in a special kind of change to the random access memory. These changes often stay for a long time after completion of the operation, significantly storing them. also, memory forensics provides extraordinary visibility into the runtime state of the system, such as which processes were running, open network connections, and recently executed commands. Individuals can perform an extraction of these artefacts that is totally independent of the machine being investigated. It also reduces the chance of root kits or malware preventing the investigation process. Critical data may exist exclusively in memory, such as unencrypted e-mail messages, disk encryption keys, non-cacheable internet history records, off-the record chat messages and memory-resident injected code fragments.

3. What is Memory Forensic?

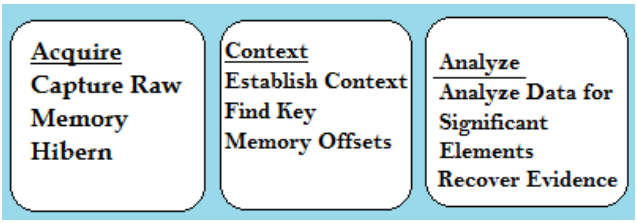

Figure: Process involved in Memory Forensics

Memory forensics is forensic analysis of a computer's memory dump. Its primary application is investigation of advanced computer attacks which are stealthy enough to avoid leaving data on the computer's hard drive. Consequently, the memory (RAM) must be analyzed for forensic information. [2]

It is about capturing the memory contents and can add an very useful resource to incident response, malware analysis, and digital forensics capabilities. Even though examination of network packet captures and hard disks can give up compelling verification, it is often the contents of the computer memory that enables the full reconstruction of events, allowing an individual to determine what has already happened, what is presently happening, and what would happen with further infection through malware or an intrusion by advanced risk factors. For example, a piece of evidence found in RAM could help to associate typical forensic artefacts that may appear different and allow for an integration which could otherwise remain unnoticed. There

are three reasons for gathering and analyzing the data contained in the physical memory.

The physical memory contains real-time data related to the operating system environment, such as the currently mounted file system and the list of processes being operated. Even the encrypted data is generally decrypted when it is stored in the physical memory.

This method adapts well to the characteristics of embedded systems. Since an embedded system is rarely turned off, the data contained in the physical memory is mostly persistent. Therefore, significant information can be obtained if analysis is performed effectively on the physical memory. The different types of information that can be extracted from memory include processes, dynamic link libraries (dll), process memory, image identification, kernel memory and objects, networking, registry, malware.

4. Tools and Techniques

0This study focuses in two phases of memory analysis: acquisition of the data and analysis of the collected data. Evidence collection-Collection of evidence focuses in obtaining digital evidence in an acceptable form. There are two approaches to acquire physical memory images: software and hardware oriented. This section presents some tools for both approaches.

1. Hardware based acquisition tools: The main idea is to avoid the operating system by means of a physical device. The dedicated hardware will open a dedicated communication port to copy the contents of the physical memory. Two main technologies are in the limelight:

Tribble.-This solution uses a dedicated PCI card. (Peripheral Component Interconnect) The PCI card requires installation before incident occurrence. The card can easily be detached after the incident. In this way the state of the system is preserved to search for digital evidence

Advantages: The ease of use and the null impact on the system.

Disadvantages: The pre-installation requirement is the major drawback. Unauthorized access to physical memory can easily be obtained through PCI cards by means of libraries .Moreover, it is possible to perform Denial of Service attacks (DoS), covering attacks, full replacing attacks by hiding system memory on the PCI bus

FireWire bus.-Also known as IEEE 1394 bus, supports among other functionalities such as high speed communication and data-transfer, physical access to the system memory.

Advantages. The FireWire port is a popular port present in many systems.
Disadvantages. For some system configurations, Fire ware bus presents problems with a region of the memory called Upper Memory Area (UMA) citeUMA.

the main advantage of hardware based acquisition tool is the absence of interaction with the operating system avoiding the risk of writing data to the target machine. However, since hardware based technologies use Direct Memory Access (DMA) to read physical memory, systems are vulnerable to attacks using this same feature.

2. Software based acquisition tools

1) Autopsy
Autopsy is a GUI-based open source digital forensic program to analyze hard drives and smart phones effectively. Autospy is used by thousands of users worldwide to investigate what actually happened in the computer.[3]

- -It's widely used by corporate examiners, military to investigate and some of the features are.
- -Email analysis
- -File type detection
- -Media playback
- -Registry analysis
- -Photos recovery from memory card
- -Extract geolocation and camera information from JPEG files
- -Extract web activity from browser
- -Show system events in graphical interface
- -Timeline analysis
- -Extract data from Android – SMS, call logs, contacts, etc.
- -It has extensive reporting to generate in HTML, XLS file format.

Alphabetical) Memory forensics tools are used to acquire and/or analyze a computer's volatile memory (RAM). They are often used in incident response situations to preserve evidence in memory that would be lost when a system is shutdown, and to quickly detect stealthy malware by directly examining the operating system and other running software in memory.
ss

2) MoonSols Windows Memory Toolkit
It supports memory acquisition from 32-bit and 64-bit versions of Windows XP, 2003, 2008, Vista, 2008 R2, 7, and 8. Version 1.4 of the software is free. At the time of this writing, the most recent version is 2.0, which is available in Consultant, Enterprise, and Enterprise Plus licensing schemes. Here are a few of the features of the

- It supports hashing with MD5, SHA-1, and SHA-256.
- It includes a server component so you can transmit memory dumps across the network, with optional RC4 encryption and/or LZNT1 compression.
- It can map memory in three different ways, including the well-known use of \Device\PhysicalMemory.
- It can convert full memory dumps to Microsoft crash dumps, which you can then analyze using one of the Microsoft debuggers.
- It can convert hibernation files and crash dumps into raw memory dumps.
- DumpIt.exe combines win32dd.exe and win64dd.exe to provide memory dumps in a single-click. You can still control options via command-line if you desire.

3) MANDIANT Memoryze

MANDIANT Memoryze, formerly known as MANDIANT Free Agent, is a memory analysis tool. Memoryze can not only acquire the physical memory from a Windows system but it can also perform advanced analysis of live memory while the computer is running. All analysis can be done either against an acquired image or a live system.[4] some of the features are.

- Image the full range of system memory (no reliance on API calls).
- Image a process' entire address space to disk, including a process' loaded DLLs, EXEs, heaps and stacks.
- Image a specified driver or all drivers loaded in memory to disk.
- Enumerate all running processes (including those hidden by rootkits), including:
- Report all open handles in a process (including all files, registry keys, etc.)

4) Belkasoft Evidence Center

Belkasoft Evidence Center makes it easy for an investigator to acquire, search, analyze, store and share digital evidence found inside computer and mobile devices. The toolkit will quickly extract digital evidence from multiple sources by analyzing hard drives, drive images, memory dumps, iOS, Blackberry and Android backups, UFED, JTAG and chip-off dumps. Evidence Center will automatically analyze the data source and lay out the most forensically important artifacts for investigator to review, examine more closely or add to report. some of the features are,

- Mobile and Computer device examination. Supporting all major desktop and mobile operating systems, Belkasoft Evidence Center is suitable for mobile and computer forensics. It can parse real and logical drives and drive images, virtual machines, mobile device backups, UFED images, JTAG and chip-off dumps.
- Smart and Comprehensive Analysis. The product looks everywhere on the device completely automatically and can successfully identify over 700 types of digital artifacts. Convenient Evidence Search feature helps to narrow down the findings using filters, pre-defined search, or other options.
- Powerful Carving.Data carving allows to locate evidence that was deleted, destroyed, or never stored on the hard drive at all (page file, hibernation file, RAM contents). Besides, advanced carving mode called BelkaCarving™ is available, making it possible to reconstruct fragmented chunks into contiguous pieces of information that would otherwise not be accessible at all.
- Native SQLite Parsing.Recovers corrupted and incomplete SQLite databases, restores deleted records and cleared history files. Processes freelists, write-ahead logs and journal files, and SQLite unallocated space.
- Live RAM Analysis.Evidence Center can extract potentially crucial information from volatile memory, such as: in-private browsing and cleared browser histories, online chats and social networks, cloud service usage history, and much more. Belkasoft Live RAM Capturer is a powerful tool for creating memory dumps, and it is complimentary.
- Handy Built-in Tools.PList, Registry, and SQLite viewers allow you to work more thoroughly with particular types of data and find even more evidence than automatic search was able to discover.[5]

5) wxHexEditor

wxHexEditor is an open source cross-platform hex editor written in C++ and wxWidgets. It can work as low level disk editor too. It uses 64 bit file descriptors (supports files or devices up to 264 bytes). It does not copy the whole file to your RAM. This makes it faster and lets it open very large files. some of the features are,

- It uses 64 bit file descriptors (supports files or devices up to 2^64 bytes , means some exabytes but tested only 1 PetaByte file (yet).).
- It does NOT copy whole file to your RAM. That make it FAST and can open files (which sizes are Multi Giga < Tera < Peta < Exabytes)
- You can work with delete/insert bytes to file, more than once, without creating temp file!.
- Could open your devices on Linux, Windows or MacOSX.
- Memory Usage : Currently ~25 MegaBytes while opened multiple > ~8GB files.
- Could operate with file thru XOR encryption.
- Has multiple views to show multiple files in same time.
- Has x86 disassembly support (via integrated udis86 library) to hack things little faster.
- Has colourfull tags to make reverse engineering easier and more fun.
- You can copy/edit your Disks, HDD Sectors with it.(Usefull for rescue files/partitions by hand.)
- Sector Indication on Disk devices, also has Go to Sector dialog...
- Formated CopyAs! It's easy to copy part of a file in HEX format for C/C++ source, ASM source, also supports HTML,phpBB and Wiki page formats with TAGs!!

6) Xplico

Xplico is an open source network forensic analysis tool. It is basically used to extract useful data from applications which use Internet and network protocols.[6] It supports most of the popular protocols including HTTP, IMAP, POP, SMTP, SIP, TCP, UDP, TCP and others. Output data of the tool is stored in SQLite database of MySQL database. It also supports IPv4 and IPv6 both. some of the features are,

- Protocols supported: HTTP, SIP, IMAP, POP, SMTP, TCP, UDP, IPv6, …;
- Port Independent Protocol Identification (PIPI) for each application protocol;
- Multithreading;
- Output data and information in SQLite database or Mysql database and/or files;
- At each data reassembled by Xplico is associated a XML file that uniquely identifies the flows and the pcap containing the data reassembled;
- Realtime elaboration (depends on the number of flows, the types of protocols and by the performance of computer - RAM, CPU, HD access time, …-);
- TCP reassembly with ACK verification for any packet or soft ACK verification;

7) HELIX3

HELIX3 is a live CD-based digital forensic suite created to be used in incident response.[7] It comes with many open source digital forensics tools including hex editors, data carving and password cracking tools. If you want the free version, you can go for Helix3 2009R1. After this release, this project was overtaken by a commercial vendor. So, you need to pay for most recent version of the tool.

This tool can collect data from physical memory, network connections, user accounts, executing processes and services, scheduled jobs, Windows Fegistry, chat logs, screen captures, SAM files, applications, drivers, environment variables and Internet history. Then it analyzes and reviews the data to generate the complied results based on reports. some of the features are,

- SIM Card Reader
- SIM Card Clone
- Mobile Phone Logical Examination
- Mobile Phone Physical Examination
- Chinese Phone Logical Examination
- Chinese Phone Physical Examination
- Backup File importing and Decoding
- Security Code Detection and Bypass
- Hex Data Viewing and Carving
- Hash Algorithms
- File Signature Analysis
- Watch List Matching

Tool	Autopsy	MoonSols Windows Memory Toolkit	MANDIANT Memoryze	Belkasoft Evidence Center	wxHexEditor	**Xplico**	**HELIX3**
Features							
1.Easy to use	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.Support Computer	Yes	Yes	Yes	Yes	Yes	Yes	Yes
3.support smart phones	Yes	No	No	Yes	Yes	Yes	No
4.information security	Yes	Yes	Yes	Yes	No	Yes	Yes
5.support image format	Yes	Yes	Yes	Yes	Yes	Yes	No
6. memory acquisition	Yes	Yes	Yes	Yes	Yes	Yes	Yes
7. memory analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes
8.fast operation	Yes	Yes	Yes	Yes	Yes	No	No
9.cost effective	Yes	Yes	Yes	Yes	Yes	Yes	No

5. Conclusion

The next generation of digital forensic tools for memory should use more sophisticated data analysis techniques to sufficient to the sophistication techniques of malware. Moreover, new developed tools should integrate different approaches. This field has a very bright potential even with fast growth in digital forensics in last decade. The focus towards memory forensics is a major step towards decrease cybercrime at fast pace. This paper has discussed some of the available tools for volatile memory. The observation in features of tools for performing three major operations of memory forensics, there are many tools investigated depending on their features usability of tool, use for computer or phones , information security, memory operations, performance speed. Seven tools are investigated depending on their features two tools Autopsy and Belkasoft Evidence Center fulfill most of the requirement.

References

[1] Dave R, Mistry NR, Dahiya MS. Volatile Memory Based Forensic Artifacts and Analysis. International Journal for Research in Applied Science and Engineering Technology. 2014
[2] https://en.wikipedia.org/wiki/Memory_forensics
[3] https://geekflare.com/forensic-investigation-tools/
[4] https://www.fireeye.fr/content/dam/fireeye-www/services/freeware/ug-memoryze.pdf
[5] https://belkasoft.com/ec
[6] https://declara.com/collection/5209ea3f-8d17-4483-8f3f-62e3452757d6/post/853dd6ee-8f89-482b-b89e-d674d01fa01f
[7] http://resources.infosecinstitute.com/computer-forensics-tools/#gref