

INTERNATIONAL RESEARCH JOURNAL OF **ENGINEERING & APPLIED SCIENCES**

ISSN: 2322-0821(0) VOLUME 10 ISSUE 4 ISSN: 2394-9910(P) Oct 2022 - Dec 2022 www.irjeas.org

Original Article Live Memory Forensic for Windows

*Priya Parameswarappa 问¹

¹Research Scholar, School of Information Technology, University of the Cumberland's, Kentucky, USA pparameswarappa69940@ucumberlands.edu https://orcid.org/0000-0003-2059-6043

*Corresponding Author - pparameswarappa69940@ucumberlands.edu

DOI - https://doi.org/10.55083/irjeas.2022.v10i04002

© 2022 Priya Parameswarappa

This is an article under the CC-BY license. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. https://creativecommons.org/licenses/by/4.0/

Received: 21 August 2022; Accepted: 17 October 2022

Abstract: This work describes a functional, generic, broad-scoped investigative methodology for Windows memory analysis. The methodology applies equally to functional and damaged, or corrupted memory images and relies on Volatility. It is based on the author's various memory analysis case studies. Summing it up succinctly, the methodology aids the forensic practitioner in squeezing the maximum amount of possible evidence from a memory image. The proposed methodology is suitable for analysts at all levels of investigative capability. It provides guidance in extracting maximum evidence using simple, commonplace tools and techniques familiar to digital forensic practitioners. As with all methodologies, nothing is written in stone; the forensic practitioner must be flexible and agile in responding to everchanging investigative requirements. To assess the performance of various tools for gaining, analysing, and improving criminal evidence from volatile memory. A comparison of several tools is offered in order to provide a better understanding of the tools used.

Keywords: Cyber security, Memory analysis, Memory forensic, Windows

1. INTRODUCTION

emory analysis can be complex and time consuming, particularly when done manually using command line driven. analysis frameworks (e.g., Volatility, Rekall). This is in contrast to automated or semi-automated frameworks that remove the investigator or analyst much as possible (e.g., CounterTack as ResponderPro, Mandiant Redline). Which to choose is a matter of needs vs. available resources. In situations where ample resources are available, manual analysis is an excellent manner for investigators and analysts to maintain and sharpen their skills.

Either way, there is an overreliance on automated tools. This leads to situations where investigators and analysts cannot explain the production of certain results. While such frameworks and tools certainly speed up triaging and analysis, they are unlikely to catch highly complex or stealthy malware; this has been corroborated using ResponderPro, although mileage may vary with other similar frameworks. In such cases, only a manual analysis conducted by a competent investigator can find evidence or indications of its presence.

Various memory analysis frameworks exist, including, but not limited to, free and open source software (FOSS) solutions (e.g., Volatility, Rekall.) There also exist various commercial frameworks. The primary difference between these paradigms is that the FOSS solutions usually allow an investigator or analyst to modify plugins or write new ones using high-level languages, to modify or improve their capabilities[1-2].

As there is no one-size-fits-all approach, investigators must be versatile in memory forensics, so that, when necessary, deviation from the proposed methodology will not result in the loss of analytical focus or capability. This paper attempts to combine these various case studies into a more formalized methodology although it remains qualitative in nature. Although it places much emphasis on identifying and extracting malware-specific evidence, it is sufficiently generic to allow for extracting much additional information and evidence. While it makes avid use of Volatility and its myriad plugins, broader analysis will typically maximize evidentiary extraction to better fill gaps in the investigation [3].

2. BACKGROUND

The author's initial Windows-specific investigative methodology was first proposed in the Zeus report [4]. It was later refined in Prolaco & SpyEye [5] and then further clarified in Stuxnet [7] and Tigger [8]. These early models were a first step towards a generic analytical approach. Since then, it has been vastly improved, tested and generalized. Additional revisions improved its focus for handling the complexities of malware memory investigations. However, it does not discuss Law Enforcement specific techniques or methodology. Instead, it provides a clear approach for conducting generic investigations for non-reverse engineers, computer forensic investigators and analysts [6].

Various steps are proposed in this methodology. Some are mandatory, others optional. It is broken down into ten specific steps, most of which provide an opportunity to cease the investigation and conduct a wrap-up. These steps can be readily rearranged or altered to suit the reader's needs as hey meant to be fluid. Additional processing can be applied wherever necessary. While it is aptly suited to malware, it is entirely appropriate for non-malware investigations too[7-12].

The tools and techniques described in the methodology are familiar to forensic practitioners at both ends of the knowledge/capability spectrum. Often taken for granted, they can be readily used in extended memory analysis.

3. METHODOLOGY

The process of memory forensic is majorly categorized in three distinguished processes.

- Memory Procurement
- Data Analytics
- Evidence Recuperating.
- 3.1 Memory Procurement

It's not straightforward to extract the "memory image" from a live memory. Because the data we're getting is from main memory, we must be cautious because even little relocation can result in heap deregimentation [13]. For Windows, there are a variety of tools and strategies for acquiring volatile memory and extracting harmful applications from it. Used tools are simple and can yield intriguing results.

3.1.1 Live RAM Capturer by Belkasoft

Figure 1 portrays Belkasoft's Live RAM Capturer, a free unpredictable memory measurable instrument that is utilized to catch fundamental RAM [14]. It accompanies both 32-cycle and 64-digit bit drivers, letting it to run in the most favoured portion mode. The memory dump will be saved with the mem expansion, and it will be analyzed later with the Belkasoft proof focus apparatus [15].

| | | Deikasuit | Evidence Center Ul | | | | | - |
|-----------------|--------------------|---|--------------------|--------------|-------|------------|---|----|
| 1 1 1 1 1 2 = 1 | | Application Tools | | х64 | | | - | |
| File Home St | are View | Manage | | | | | | ¥ |
| € · ↑ . | This PC + 16 | (6 (E) > RamCapture > x | 64 | | ~ 0 | Search x64 | | \$ |
| Name | | Date modified | Type | Size | | | | |
| 20150310.mem | | 3/10/2015 4:16 PM | MEM File | 5.240,832 KB | | | | |
| 🗟 msvcp110.dll | • | Belkasoft L | ive RAM Capturer | - | = × | | | |
| S msvcr110.dll | | | | | | | | |
| RamCapture64 | Select output fold | | | | | | | |
| RamCaptureDriv | E: Kancapure | 404 | | | | | | |
| | Loading device d | river | | | ~ | | | |
| | | Page Size = 4096 mory Size = 5118 MB | | | | | | |
| | | | | | ~ | | | |
| | | | | | | | | |
| | _ | | | | | | | |
| | | | Capturel | Cancel | Close | | | |
| | | | R | | | | | |
| | _ | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

Figure 1- Procurement of Memory

| 2 A | ccessData FTK Imager 3.1.0.1514 | | | - | |
|---------------------------|-----------------------------------|-----------|-----------|------|---------------|
| ACCURATE A DESIGNATION OF | View Mode Help | | | | |
| ۵ | Add Evidence Item | | 🖻 🐱 😹 🦹 🕴 | | |
| 6 | Add All Attached Devices | File List | | | |
| • | Image Mou <u>n</u> ting | Name | Size | Туре | Date Modified |
| | Remove Evidence Item | | | | |
| ŝ | Remove All Evidence Items | | | | |
| | <u>Create Disk Image</u> | | | | |
| | Export Disk Image | | | | |
| | Export Logical Image (AD1) | | | | |
| 42 | Add to Custom Content Image (AD1) | | | | |
| 9 | Create Custom Content Image (AD1) | | | | |
| | Decrypt AD1 image | | | | |
| =0 | Verify Drive/Image | | | | |
| | Capture Memory | | | | |
| | Obtain Protected Files | | | | |
| 8 | Detect EFS Encryption | | | | |
| D | Export Eiles | | | | |
| | Export File Hash List | | | | |
| | Export Directory Listing | | | | |
| | Exit | | | | |

Figure 2- Choose the "Capture memory"

3.1.2 Ftk Imager

The Ftk Imager22 produces a bit-by-bit image with unused and slack space. As seen in Figure 2, it assists in the capture of active RAM, but it is unable to inspect the memory dump obtained. It stores the memory dump as memextentions (as seen in Figure 3), which may then be analysed using the wxHexEditor tool or another tool [16].

| Ele View Mode Help | | | · 盐 愁 ? . | | |
|---|-----|---------------|--|---------------|---|
| Evidence Tree | | : List ame | Size Type | Date Modified | > |
| | | | C:\Projects\memdump.mem 2GB/SGB [48%] | | |
| Custom Content Sources Evidence:File System/Path/File Option | × | | Cancel | | |
| | . [| | | | |
| III New Edit Remove Remove Al Create Image | | | | | |

Figure 3- FtkImager Tool for procurement of memory

3.1.3 Madiant Memoryze

MadiantMemoryz23 is a free memory forensics tool that helps first responders find evil in real-time memory. It has the ability to both acquire and analyse memories. As seen in Figure 4, this programme can capture all processes that are in running condition, all drivers, and the entire memory image dependent system [17].

3.1.4 DumpIt

It's a fascinating tool which provides the facility to the people wishing to record the RAM of a suspicious or under surveillance individual [18-20]. The live RAM may be acquired in less than a minute with this utility, which can be stored on a pen drive. Just an affirmation question (i.e., asking yes or no) is provoked when the pen drive is joined and DumpIt24 is run on that individual's PC, as displayed in Figure 5, and a mem document of that individual's live RAM is put away on the pen drive.

3.2 Acquired Memory Dump Analysis

Following the obtaining of the memory picture, the memory picture will be surveyed. The evidences must be thoroughly examined during this step.

10

| D:\memoryze\Memoryze.exe |
|---|
| nstalling and starting MIR Agent driver. dding service Mandiant_Tools. reating service: Mandiant_Tools, Mandiant_Tools, Mandiant_Tools, D:\memoryze\mk pols.sys |
| he install has completed. Larting service falled (timeout). ervice start has completed. |
| pading the script from 'D:\memoryze\out.txt'. eginning local audit. udit started 10-13-2011 21:18:20 |
| hecking if 'D:\memoryze\Audits\NETPWN\20111013191820' exists aving batch result to 'D:\memoryze\Audits\NETPWN\20111013191820\'. atch results written to 'D:\memoryze\Audits\NETPWN\20111013191820\'. uditing (w32memory-acquisition) started 10-13-2011 21:18:20 xecuting command for internal module w32memory-acquisition, 1.3.22.2 |
| issue number="2" level="Error" summary="Unable to open a handle to the device. he system cannot find the file specified." context="OpenDevice"/> |
| lssue number="6" level="Warning" summary="The handle is invalid." context="Star Audit"/> |
| issue number="6" level="Error" summary="Unable to determine physical device mem ry." context="StartAudit"/> |

Figure 4- Mediant Memoryze Tool Demonstration

| C:\Users\a555114\Downloads\ | DumpIt.exe | |
|---|--|-----------------|
| Copyright (c) 2007 - 201 | - One click memory memory dumper 1, Matthieu Suiche <http: www.msuich<br="">1, MoonSols <http: th="" www.moonsols.com<=""><th></th></http:></http:> | |
| Address space size: Free space size: | 9099542528 bytes (8678 Mb) 210422509568 bytes (200674 Mb) | |
| <pre>* Destination = \??\C:</pre> | \Users\a555114\Downloads\A555114-2015 | 0211-092913.raw |
| > Are you sure you w + Processing | ant to continue? [y/n] y | |
| | | |
| | | |
| | | Ŧ |

Figure 5- DumpIT memory procurement

3.2.1 Evidence Centre at Belkasoft

Belkasoft21 is highest intriguing applications available today. This application reads the mem file created by the Belkasoft LIVE Ram capturer, which allows it to swiftly analyse the memory dump. It's simple to understand and use, and it doesn't require any special understanding to use [21]. The technique for presenting the gathered memory file connected to photographs from Belkasoft live RAM capturer is shown in Figure 6. Figure 7 illustrates how to import the necessary data sources for carving. Finally, as shown in Figure 8, the carved data of the acquired memory image is analysed [22].

3.2.2 wxHexEditor

wxHexEditor25 can be used to examine the memory dump captured by the FtkImager. It's a free programme that analyses memory dumps. It is divided into two sections: right side and the left side. The information string values are displayed on the right side, while the string hex values are displayed on the left side. Figure 9 shows the FtkImagercaptured memory image being loaded into wxHexEditor for processing.

| - 8 × | * | ource | Add data | <u>P</u> | | <u>.</u> |
|--------------------------|-------------|------------|---|--|-----------------------|---|
| | | | arve? | What would you like to ca | | File Edit View Tools Help |
| | | | data types below | Select from supported of | Z 🔍 | 12 🖆 💾 🗶 🎍 |
| - × | | | | | a x | Case Explorer |
| ¥ | 4 | | en Live RAM Live RAM Mi He RAM Sames Live RAM Games Live RAM Live RAM | Constant Measuring Constant Measuri | Com Pe Ty Tr | Cher Bekauft care (215 0.00 1/657 29) Cher Bekauft care (215 0.00 1/657 29) Cher Bekauft care (210) Cher Bekauft care (210) |
| 4 c | Select none | Select all | | | Task | |
| Time Bagsed | | | | Search in metadata Search in metadata SugFit SugFite Enable BekaCarving | Та | |
| Cancellaria Vew tesk log | Cancel | Fnish | < Back | | Run | |

Figure 6- Access of Procured Memory with Belkasoft

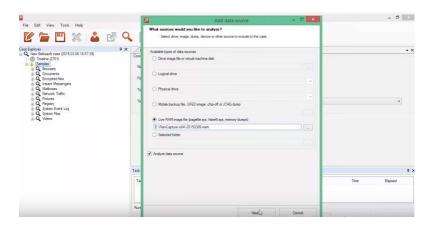


Figure 7- Updation of Data Source

| 2 💽 🐂 🛈 | | | | | | |
|----------------------------------|--|---|---|---|--|--|
| X File system item list Prop | perties Data List | | | | - | |
| URL | | Location | Offset | Length | _ | |
| http://camava2008ctos.com.d | in 501 net locks con SOURCE H4DIGR | H w64\20150306 mem | 37663993 | 77 | | |
| http://nt.malwantor.com/stat.ph | p?func+instalirun&d+%s | H/w64\20150306.mem | 49232105 | 66 | | |
| http://www.footbal.skype.com/ | | H:\x64\20150306.mem | 59641533 | 40 | | |
| http://down.namepics.info/insta | Il pho Thame+ | H:vs64\20150305.mem | 145257097 | 53 | | |
| http://d.laiyba.com/ | | H:\x64\20150306.mem | 159770497 | 31 | | |
| http://www.rysiologger.yoyo.pl/8 | tentibia txt | H \x64\20150306.mem | 168137685 | 54 | | |
| http://www.sysiologger.yoyo.pl/k | dibia.bt | H \x64\20150306 mem | 52 | | | |
| http://www.rysiologger.yoyo.pl/y | 9g bd | H:\x64\20150306.mem | 168137793 | 47 | | |
| http://super-tds.info/ | | H.'x64\20150306.mem | 176984877 | 32 | | |
| http://la1a11i.mfo/ | | H:\x64\20150306.mem | 33 | | | |
| http://1i1i1i11.com/ | | H:\x64\20150306.mem | 176984941 | 32 | | |
| http://uTlui1il.ws/ | | H \x64\20150306.mem | 176984973 | 31 | | |
| http://xep.ru/ | | H/x64\20150306.mem | 176985005 | 24 | | |
| http://www.microsoft.com/provi | sioning/Branding | H:\x64\20150306.mem | 200958085 | 56 | 56 77 | |
| http://www.microsoft.com/provi | sioning/BaseEapConnectionPropertiesV1 | H/x64\20150306.mem | 200958485 | 77 | | |
| http://www.microsoft.com/provi | sioning/EapConnectionProperties\/1 | H:\x64\20150306.mem | 200958869 | 73 | | |
| http://www.microsoft.com/provi | sioning/MsChapV2ConnectionPropertiesV1 | H.\x64\20150306.mem | 200959253 | 78 | | |
| http://www.microsoft.com/provi | soning/MsPeapConnectionPropetiesV1 | H:\x64\20150306.mem | 200959677 | 76 | | |
| Task Manager | | | | | | |
| Task | % completed Status | | Time | Bapsed | | |
| | | | | | | |
| | File system item list Pro URL URL Hold Communication Hold Communication | File system item list Properties Data List UR UR Tork Tor | File system item list Properties Data list URL Location Hgb //server/2008/bits care af-e/021 mit Acade acom/2008/021, MADOIS H 546/20150006 mem Hgb //server/2008/bits care af-e/021 mit Acade acom/2008/021, MADOIS H 546/20150006 mem Hgb //server/2008/bits care af-e/021 mit Acade acom/2008/021, MADOIS H 546/20150006 mem Hgb //server/2008/bits care af-e/021 mit Acade acom/2008/021, MADOIS H 546/20150006 mem Hgb //server/2008/bits care af-e/021 mit Acade acom/2008/021, MADOIS H 546/20150006 mem Hgb //server/2008/bits care af-e/021 H 546/2015006 mem Hgb //server/2008/bits care af-e/021 H 546/20150006 mem Hgb //server/2008/bits care af-e/021 H 546/20150006 mem Hgb //server/2008/bits care af-e/02018 H 546/20150006 mem Hgb //server/2008/bits care af-e/02006 mem H 546/20150 | File system item list Properties Data List Location Offset 198. Location Offset 199. 1 | Set Data Let Location Offset Length 10% Location Offset Length Location Offset Length 10% Location Offset Location Offset Length 10% Location Offset Location Offset Length 10% Location Offset Location Offset Length 10% Location If Visit 2015000 nem 42021500 66 100 1 | |

Figure 8- Data Analytics from Procured Memory

| File Edit View Tools D | evices Options I | Help | | | | | | | | | | |
|-----------------------------|------------------|---------|----|----|----|----|----|-----|----|----|------------|---|
| 🗔 胡 🗔 🖾 | 1 🖻 🖉 🚭 | | | | | | (| | | ţ. | 0 👁 | |
| DataInterpreter | K memdump. | mem | 6 | _ | | | | | | _ | | |
| 🕅 Unsigned 🔄 Big Endian | Offset | | | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 012345678 | |
| Binary 00101110 | E 0020459241 | 2E | 61 | 64 | 26 | 26 | 61 | 2 E | 73 | 65 | .ad&&a.se | A |
| | | 74 | 28 | 22 | 61 | 64 | 6B | 22 | 2C | 74 | t("adk",t | |
| 8 bit 46 | 0020459259 | 68 | 69 | 73 | 2E | 67 | 2E | 61 | 64 | 29 | his.g.ad) | |
| 16 bit 24878 | 0020459268 | 3B | 61 | 2E | 73 | 65 | 74 | 28 | 22 | 6E | ;a.set("n | |
| | 0020459277 | 75 | 6D | 5F | 61 | 64 | 73 | 22 | 2C | 61 | um_ads",a | |
| 32 bit 644112686 | 0020459286 | 59 | 28 | 74 | 68 | 69 | 73 | 29 | 29 | 3B | Y(this)); | |
| 64 bit 8299677979771167022 | 0020459295 | 61 | 2E | 73 | 65 | 74 | 28 | 22 | 63 | 68 | a.set("ch | |
| | 0020459304 | 61 | 6E | 6E | 65 | 6C | 22 | 2C | 77 | 6B | annel",wk | |
| Float 7.9235093539929e-016 | 0020459313 | 61 | 28 | 74 | 68 | 69 | 73 | 29 | 29 | 3B | a(this)); | |
| Double 6.6378421675694e+246 | 0020459322 | 61 | 2E | 73 | 65 | 74 | 28 | 22 | 6F | 75 | a.set("ou | |
| | 0020459331 | 74 | 70 | 75 | 74 | 22 | 2C | 22 | 78 | 6D | tput", "xm | |
| | 0020459340 | 6C | 5F | 76 | 61 | 73 | 74 | 33 | 22 | 29 | l_vast3") | |
| InfoPanel | 0020459349 | 3B | 74 | 68 | 69 | 73 | 2E | 62 | 2E | 73 | ;this.b.s | |
| Name: | 0020459358 | 6D | 26 | 26 | OA | 61 | 2E | 73 | 65 | 74 | m&&Ba.set | |
| memdump.mem | 0020459367 | 28 | 22 | 61 | 64 | 74 | 65 | 73 | 74 | 22 | ("adtest" | |
| Path: C:\Projects | 0020459376 | 2C | 22 | 6F | 6E | 22 | 29 | 3B | 56 | 50 | ,"on");VP | |
| Size: 5.0 GB | 0020459385 | | 26 | 61 | 2E | 73 | 65 | 74 | 28 | 22 | &&a.set(" | |
| Access: Read-Only | 0020459394 | 10000 C | | 61 | 73 | 68 | 22 | 2C | 73 | 4E | flash", sN | |
| Device: FILF | 0020459403 | 29 | 3B | 51 | 58 | 28 | 22 | 61 | 6C | 74 |);QX("alt | - |

Figure 9- FtkImager Screenshot with procured memory

This tool allows you to look for a pattern by typing some words into the search box. Figure 10 depicts the results of a search for the term "gmail." Figure 11 shows the result of enquiring for the word gmail. The terms that match "gmail" will be shown as shown in Fig. 11 and can then be evaluated. As demonstrated in Figure 12, the wxHexEditor can be used to extract users and passwords.

3.3.3 Autopsy

Autopsy26 is a free utility that analyses the RAM that has been recorded. It's used to examine disc images and do in-depth file system analysis. Figure 13 depicts the Autopsy tool in action.

3.4 Recovering Data using FtkImager

In order to protect the system, the attacker may remove some sensitive information or photos. However, data that has been deleted can be recovered. Although it is a taxing process that needs complete concentration, the outcomes are occasionally fascinating. Assume the attacker utilised a puppy image and then erased it from the machine. The image can now be retrieved using FtkImager22, as illustrated in the screenshots in Figures 14, 15, 16 and 17. The assailant stores the photograph before deleting it from the file as well as the recycle bin. The FtkImager application is launched, and deleted files are searched in the unallocated region. Because FtkImager does not include a searching tool, each file must be opened individually

| | individually. |
|----------------------------------|--|
| wxHexEditor 0.23 Beta fo | or Windows |
| File Edit View Tools | Devices Options Help |
| | 3 🛯 🖉 🔿 🗇 🥐 📄 🗊 🖏 😭 🗶 👘 |
| DataInterpreter | X memdump.mem |
| Unsigned 🔄 Big Endian | Offset 00 01 02 03 04 05 06 07 08 012345678 |
| Binary 00101110 | E 0020459241 2E 61 64 26 26 61 2E 73 65 .ad&&a.se * |
| 8 bit 46 | 0020459250 74 28 22 61 64 6B 22 2C 74 t("adk",t 0020459259 68 69 73 2F 67 2F 61 64 29 bis g ad) |
| 16 bit 24878 | Find |
| 32 bit 644112686 | Find |
| 64 bit 829967797977116702 | Search: gmail |
| Float 7 9235093539929e-01 | Find All |
| | Match Caro Find Some Bytes |
| Double 6.6378421675694e+24 | 6 Hex Search backwards Cancel |
| | |
| InfoPanel | × Wrap around |
| Name: | As UTF-8 |
| memdump.mem Path: C:\Projects | Finding matches |
| | Search Speed : 24.00 MB/s |
| | |
| | Densities in 0.0112 |
| | Remaining time: 0:04:13 |
| | Cancel |
| | |

Figure 10- Evidence-based procured memory analytics

| wxHexEditor 0.23 Beta for Win | ndows | x |
|--|---|---|
| File Edit View Tools Devi | ces Options Help | |
| 🔓 🚚 🗖 🗖 😂 | S 2 📀 🛸 🐑 🗋 🗇 🐒 🕤 🐲 | |
| Datainterpreter X | memdump.mem | Ŧ |
| 🕅 Unsigned 🔄 Big Endian | Offset 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 0123456789ABCDEF01234567 | _ |
| Binary 00110010 | 0791789112 48 6F 6C 64 65 72 31 24 54 65 78 74 32 28 42 61 6E 67 61 6C 6F 72 65 20 Holder1\$Text2(Bangalore 0791789136 4F 6E 6C 79 29 28 62 61 6E 67 61 6C 6F 72 65 20 6F 6E 6C 79 29 53 80 94 Only)(bangalore only)\$Çõ | ^ |
| 16 bit 29490 | 0791789160 DA 53 81 FD 03 2A 81 03 08 07 HB 61 61 04 04 01 63 74 6C 30 30 24 43 67 r ⁵⁰¹⁴⁸¹ Ume ⁻ Kaae+Oct1005Co 0791789184 6E 74 65 6E 74 50 6C 61 63 65 48 6F 6C 64 65 72 31 24 54 65 78 74 31 53 mtentPlaceHolder15Text13 0791789206 56 6C 65 63 74 20 49 53 20 57 65 62 20 61 70 70 6C 69 63 61 74 69 6F 6E elect 15 Web application | |
| 32 bit 1919447858 64 bit 3342085875103724338 | 0791789232 73 2D 2D 3E 54 72 61 76 65 6C 20 53 79 73 74 65 6D 73 65 6C 65 63 74 20 =->Travel Systemselect 0791789256 69 73 20 77 65 62 20 61 70 70 6C 69 63 61 74 69 6F 6E 73 2D 2D 3E 74 72 is web applications>tr | |
| Float 4.6041462314324e+030 | 0791789280 61 76 65 6C 20 73 79 73 74 65 6D 53 80 94 DA 53 81 FD 0A 2A 3E 07 07 15 avel systemSÇ6 ₁ Sü*8+>••€ 0791789304 37 37 04 04 01 61 73 5F 71 61 63 63 65 6E 74 75 72 65 20 6F 6E 6C 69 6E 77++0as_gaccenture onlin | |
| Double 2.8109210151678e-085 | 0791789328 65 20 74 65 73 74 61 63 63 65 6E 74 75 72 65 20 6F 6E 6C 69 6E 65 20 74 e testaccenture online t 0791789352 65 73 74 53 5C AF D2 53 5C AF D2 01 30 06 07 17 27 27 04 04 02 15 60 61 est5\a_BS\a_000+1'***€ | |
| InfoPanel X | 0791789376 <mark>13 60 34 60 34 60 34 60 34 60 32 67 61 35 72 53 62</mark> 73 68 72 65 79 61 22 67 61 <u>3 10 hore ya opur</u> [Bhreya.ga 07917893400 75 72 32 32 52 66 75 28 57 F3 CD 5D 01 AD 19 05 07 17 11 11 04 04 01 45 ur22Rfu+W=10;] * 1 * 1 * 1 0791789342 [6D 61 66 6C 73 68 73 68 53 7Σ D8 D8 53 75 F8 E8 50 71 70 40 71 70 67 04 mailshehsh= ¹ 5 4 07 i* 100 | |
| Name: memdump.mem | 0791789148 [0 61 65 60 73 68 73 68 73 78 13 76 44 58 54 9 E0 7F 08 33 02 01 17 2B 2B •OEmailssister 10 + 0 + 1 + 1 + 0 + 0 + 0 + 0 + 0 + 0 | |
| Path: C:\Projects Size: 5.0 GB Access: Read-Only Device: FILE | 0791789496 61 74 79 61 79 61 6E 69 2E 6E 69 73 68 69 52 66 6B E5 53 9B 39 4D 04 2F atyayani.nishiRfko369Me/ 0791799520 01 07 17 27 27 04 04 01 45 6D 61 69 6C 61 6E 6E 75 70 61 77 61 72 31 39 0+ ***0Emailannupawar19 0791795941 93 16 16 E6 67 57 06 17 76 17 23 13 93 93 15 26 67 55 55 28 C2 3D 80 4 91annupawar1991Rturk] | |
| Showing Page: 1736379 | Cursor Offset: 791789390 Cursor Value: 50 Selected Block: 791789373 -> 791789390 Block Size: 18 | Ŧ |

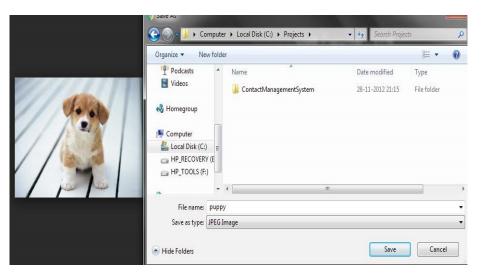
Figure 11- Analytics of Procured Gmail Details

| File Edit View Tools Dev | | Help | | | | | | | | | | | | | |
|---------------------------------|------------|------|----|-----|----|----------|----|----|----|----|----|----|----|--|-------------------------------------|
| 📑 🗐 🗖 🖓 🚱 | 3 2 3 | | 9 | 6 | | | | | | 6 | | ዏ | | | |
| DataInterpreter × | memdump. | теп | 1 | _ | _ | _ | _ | _ | | _ | _ | _ | _ | Ŧ | Search Results |
| 🔲 Unsigned 🛛 🕅 Big Endian | Offset | 00 | | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | OA | 0B | 0123456789AB | 1. Offset 44952 |
| Binary 01100111 | 0018966516 | 6F | 70 | 61 | 69 | 6E | 74 | 65 | 64 | 63 | 69 | 74 | 69 | opaintedciti * | 2. Offset 18966 3. Offset 24377 |
| 8 bit 103 | 0018966528 | 7A | 65 | 6E | 49 | 20 | 64 | 6F | 6E | 27 | 74 | 72 | 65 | zenI don'tre 📃 | 4. Offset 33444 |
| 5 DIE 103 | 0018966540 | | 72 | 65 | 61 | 74 | - | 20 | 53 | | | 65 | | treat. Some | 5. Offset 33445 |
| 6 bit 28007 | 0018966552 | | 77 | | | | | | | | | | | ww."); Boombi | 6. Offset 33559 |
| 2 bit 1767992679 | 0018966564 | | | | | | | | | | | | | ngmailto:mad | 7. Offset 33559 |
| | 0018966576 | | | | 6E | | | 4D | | | | | | e in. Many c | 8. Offset 33727: |
| 34 bit 4210712185587985767 | 0018966588 | | 72 | 0.7 | | 65 | 73 | 70 | 70 | 7B | 7D | 3B | | arries {};w | 9. Offset 33743 |
| Float 1.703280921091e+025 | 0018966600 | | | 6F | | 6B 65 | - | 6F | | 74 | | 6E | | iwork ofsyno nymdefeatsfa | 10. Offset 3382 11. Offset 3383 |
| | 0018966624 | | 6F | | | 64 | 6F | 70 | | | | | | voredoptical | 12. Offset 3383 |
| ouble 3.1761210390033e-027 | 0018966636 | 1 | 61 | | 65 | | | 61 | | | | | | pageTraunles | 13. Offset 3383 |
| | 0018966648 | | 20 | | | | | 69 | | | | | | s sendinglef | 14. Offset 3400 |
| | 0018966660 | | | | 3C | | | | | | | | | t"> <comscora< td=""><td>15. Offset 3400.</td></comscora<> | 15. Offset 3400. |
| nfoPanel X | 0018966672 | | | | 74 | | | 64 | | 75 | | | | 11 the Ouerv | 16. Offset 3400 |
| lame: | 0018966684 | 2E | 74 | 6F | 75 | 72 | 69 | 73 | 74 | 43 | 6C | 61 | 73 | touristClas | 17. Offset 3460. |
| nemdump.mem | 0018966696 | 73 | 69 | 63 | 66 | 61 | 6C | 73 | 65 | 22 | 20 | 57 | 69 | sicfalse" Wi | 18. Offset 3460. |
| ath: C:\Projects ize: 5.0 GB | 0018966708 | 6C | 68 | 65 | 6C | 6D | 73 | 75 | 62 | 75 | 72 | 62 | 73 | lhelmsuburbs | 19. Offset 3485. 20. Offset 6013 |
| Access: Read-Only | 0018966720 | | | | 75 | | | | 62 | | | | | genuinebisho | 20. Onset 6013. |
| Device: FILE | 0018966732 | 70 | 73 | 2E | 73 | 70 | 6C | 69 | 74 | 28 | 67 | 6C | 6F | ps.split(glo _ | Clear |

Figure 12- Retrieval of Credentials

| 😸 Close Case 🐈 Add Image 📓 Generate Report | | | A | • Keyword | Usts - Search | | | Q |
|---|---|---|--|--|--|----------|------------|----------|
| ♦ ⇒ | Directory Listing | | | | | | | |
| | \xp-sp3-v4.001\vol2 | | | | | | | 25 Resul |
| - Images xp-sp3-v4.001 | Table View Thumbnail View | | | | | | | |
| vol1 (Unalocated: 0-62) | Name | Mod. Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flag |
| vol2 (NTPS (0x07): 63-8193149) \$Extend | \$Boot | 2012-01-20 12:09:03 | 2012-01-20 12:09:03 | 2012-01-20 12:09:03 | 2012-01-20 12:09:03 | 8192 | Allocated | Alloca |
| | SExtend | 2012-01-20 12:09:03 | 2012-01-20 12:09:03 | 2012-01-20 12:09:03 | 2012-01-20 12:09:03 | 344 | Allocated | Alloca |
| Documents and Settings | SLogFile | 2012-01-20 12:09:03 | 2012-01-20 12:09:03 | 2012-01-20 12:09:03 | 2012-01-20 12:09:03 | 23085056 | Allocated | Alloca |
| Program Files System Volume Information | SMFT | 2012-01-20 12:09:03 | 2012-01-20 12:09:03 | 2012-01-20 12:09:03 | 2012-01-20 12:09:03 | 15859712 | Allocated | Alloca |
| WINDOWS | SMFTMirr | 2012-01-20 12:09:03 | 2012-01-20 12:09:03 | 2012-01-20 12:09:03 | 2012-01-20 12:09:03 | 4096 | Allocated | Alloca |
| SOrphanFiles | \$Secure: \$SDS | 2012-01-20 12:09:03 | 2012-01-20 12:09:03 | 2012-01-20 12:09:03 | 2012-01-20 12:09:03 | 0 | Allocated | Alloca |
| e vol3 (Unallocated: 8193150-10485215) | \$UpCase | 2012-01-20 12:09:03 | 2012-01-20 12:09:03 | 2012-01-20 12:09:03 | 2012-01-20 12:09:03 | 131072 | Allocated | Alloca |
| Views | SVolume | 2012-01-20 12:09:03 | 2012-01-20 12:09:03 | 2012-01-20 12:09:03 | 2012-01-20 12:09:03 | 0 | Allocated | Alloca |
| E - B Fle Types | AUTOEXEC.BAT | 2012-01-20 17:20:49 | 2012-01-20 17:20:49 | 2012-01-20 17:20:49 | 2012-01-20 17:20:49 | 0 | Allocated | Alloca |
| Images Videos | boot.ini | 2012-01-20 17:19:25 | 2012-01-20 17:20:54 | 2012-01-20 17:19:25 | 2012-01-20 12:10:10 | 211 | Allocated | Alloca |
| Audio | CONFIG.SYS | 2012-01-20 17:20:49 | 2012-01-20 17:20:49 | 2012-01-20 17:20:49 | 2012-01-20 17:20:49 | 0 | Allocated | Alloca |
| Occuments | Documents and Settings | 2012-03-22 19:29:54 | 2012-03-22 19:29:54 | 2012-03-10 14:40:46 | 2012-01-20 12:10:41 | 56 | Allocated | Alloca |
| E Recent Files | IO.SYS | 2012-01-20 17:20:49 | 2012-01-20 17:20:49 | 2012-01-20 17:20:49 | | 0 | Allocated | Alloca |
| - Final Day | MSDOS.SYS | 2012-01-20 17:20:49 | 2012-01-20 17:20:49 | 2012-01-20 17:20:49 | 2012-01-20 17:20:49 | 0 | Allocated | Alloca |
| Pinal Day - 1 Final Day - 2 | NTDETECT.COM | 2008-04-13 22:13:04 | 2012-01-20 12:11:07 | 2012-01-20 12:10:07 | | 47564 | Allocated | Alect |
| Final Day - 2 Final Day - 3 | ntidr | 2008-04-14 00:01:44 | 2012-01-20 12:11:07 | 2012-01-20 12:10:07 | 2008-04-14 00:01:44 | 250048 | Allocated | Allocz |
| Final Day - 4 | pagefie.svs | 2012-03-10 14:44:29 | 2012-01-20 12:11:07 | 2012-01-20 12:10:07 | 2012-01-20 12:09:08 | 20971520 | Allocated | Alloca |
| 🕑 Final Day - 5 | Program Files | | | | | 56 | | Alloca |
| Final Day - 6 | | 2012-03-20 19:25:02 | 2012-03-20 19:25:02 | 2012-03-10 14:40:46 | 2012-01-20 12:11:01 | | Allocated | |
| E Results | System Volume Information | 2012-01-20 17:21:37 | 2012-01-20 17:21:37 | 2012-03-10 14:40:46 | 2012-01-20 12:10:41 | 56 | Allocated | Alloca |
| Extracted Content Bookmarks (174) | WINDOWS | 2012-03-05 19:12:38 | 2012-03-05 19:12:38 | 2012-03-10 14:40:46 | 2012-01-20 12:09:08 | 56 | Allocated | Alloca |
| - Goodeliands (174) | \$OrphanFiles | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0 | Allocated | Alloca |
| Web History (1218) | • | m | | | | | | ×. |
| Downloads (30) | Result View Hex View Media Vie | String View Text Vie | | | | | | |
| | Page: 1 of 3 P | age 🗧 🔶 Go to l | Page: | | | | | |
| Becer Document (2) Motada forgane (2) Device Attached (9) Govern Attached (9) | 0x00000: 66 55 66 39 0x000010: 7D CO 66 39 52 0x000010: 7D CO 66 39 52 04 0x000010: 7D CO 66 39 52 04 0x000040: 66 39 52 04 04 04 0x000040: 66 39 52 04 04 04 0x000060: 30 53 04 06 7 02 04 07 72 04 04000 04000 04000 04000 04000 04000 04000 04000 04000 040000 040000 0400000 0400000 0400000 0400 | 66 39 4E 0C 66 39 6E 1C 66 57 66 56 C9 66 33 D2 26 00 00 66 00 00 00 00 57 53 60 42 C6 47 01 58 C6 57 07 30 | FF FF 00 00 E9 04 52 CB 00 00 52 D1 66 39 76 10 7D D0 66 53 66 51 66 53 66 51 66 53 57 68 52 66 00 00 00 00 66 83 85 66 00 00 00 00 66 83 96 67 00 00 00 00 00 66 83 90 77 77 08 50 77 78 60 45 06 | 1E 06 66 53 03 C1 7D D8 30 0E 04 00 66 39 7E 14 06 0 00 00 66 33 C0 66 33 FF E8 B7 58 07 1F 66 00 00 00 00 CD 15 53 39 47 03 30 4F 0A 5B 5F 5E 06 6E 08 39 | fug.f fvfm f.f.f f.vf.N.f.v.f f.vf.N.f.v.f fugRimtvrojsf3 g.g.f3_f3_f3_f3 f.d_f_f_f f.vf_g_frf u.vws.N. v.d_X.g.d_ v.v.N. v.v.N. | ~. | | |

Figure 13- Evidence Finding using Image Analytics





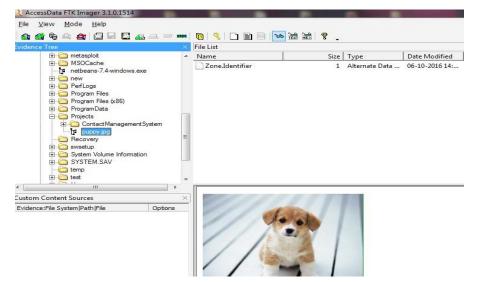


Figure 15- FtKImager based image

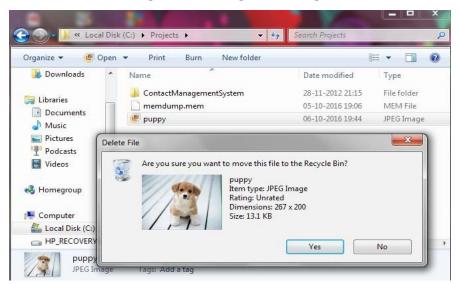


Figure 16- Destroy the Image

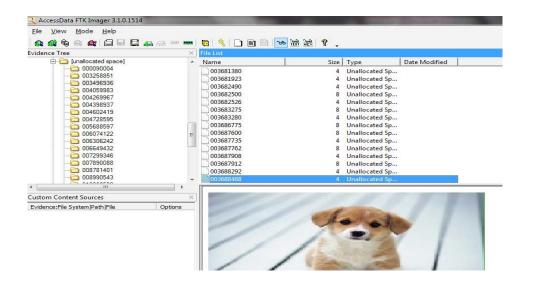


Figure 17- Recovery of Deleted File

4. **DISCUSSION**

Memory forensics is a large field with a lot of work done so far. Researchers used to focus on hardware acquisition although software acquisition has become increasingly prominent in the recent decade, while unstable memory legal sciences are still in its outset. Despite the fact that there are various free devices accessible to support the examination of impermanent memory, there are as yet a couple of holes that should be filled. Looking at the information recovered turns into a troublesome and tedious methodology since the information to be broke down is seen as a tree with many branches in FtkImager and Belkasofttools. It also does not guarantee hundred percent successes, which can result in fruitless searches. The tools examined in this study are solely designed to locate a specific piece of evidence, not to aid in the inquiry; as a result, the investigation takes a long time to complete. This essentially means that the investigator must use his or her brains to locate evidence, as the technology does not supply intelligent data. Another key issue in the field of forensics is that numerous tools are required to obtain results, and one instrument is insufficient throughout the entire process. The instruments take a long time to retrieve and restore information that is sensitive, which may result in excessive harm, and critical evidence could be destroyed because information does not last long in memory.

5. CONCLUSION

A very new discipline that has a lot of promise emerged as a Memory forensics. Although different technologies exist to tackle cybercrime, their efficacy and effectiveness are insufficient to deal with the tremendous increase in cybercrime. Regardless of the explosive growth of digital forensics over the last decade, this field has a promising future. The increased attention on memory forensics is a significant step in quickly combating cybercrime. There are lot of tools available for volatile memory. Some of them have been discussed in this study. The limitations and benefits of tools for executing the three key memory forensics activities of acquisition, analysis, and recovery have been examined. There is a lot of future potential in the field of memory forensics. Some tools provide a tree-like structure that can be adjusted to save time and offer improved results. Additionally, the focus should be on developing a single tool capable of acquiring and analysing memory.

REFERENCES

- Reith M, Carr C, Gunsch G. An examination of Digital Forensics Models. International Journal of Digital Evidence. 2002; 1(3):1–12.
- [2] Hay B, Nance K, Bishop M. Live analysis: Progress and Challenges. IEEE Security and Privacy. 2009:7(2):30–7.
- [3] Wang L, Zhang R, Zhang S. A model of computer live forensics based on physical memory analysis. Proceedings of 1st IEEE International Conference on Information Science and Engineering (ICISE). 2009. p. 4647–9.
- [4] Aljaedi A, Lindskog D, Zavarsky P, Ruhl R, Almari F. Comparative Analysis of Volatile Memory Forensics: Live Response vs. Memory Imaging. Proceedings of 3rd IEEE International

Conference on Privacy, Security, Risk and Trust. 2011.p. 1253–8.

- [5] Petroni NL, Walters A, Fraser T, Arbaugh WA. FATKit: A Framework for the Extraction and Analysis of Digital Forensic Data from Volatile System Memory. Digital Investigation. 2006;3(4): 197–210.
- [6] Gianni F, Solinas F. Live Digital Forensics: Windows XP vs Windows 7. Proceedings of 2nd IEEE International Conference on Informatics and Applications (ICIA). 2013. p. 1–6.
- [7] Balogh S, Pondelik M. Capturing encryption keys for digital analysis. Proceedings of 6th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS). 2011. 2, p. 759–63.
- [8] Savold A, Gubian P. Towards the virtual memory space reconstruction for windows live forensic purposes, Proceedings of 3rd IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering. 2008. p. 15–22.
- [9] Carrier BD. Risks of live digital forensic analysis. Communications of the ACM. 2006; 49(2): 56–61.
- [10] Meera V, Isaac MM, Balan C. Forensic acquisition and analysis of VMware virtual machine artifacts. Proceedings of IEEE Automation, Computing, Communication, Control and Compressed Sensing (iMac4s). 2013. p. 255–9.
- [11] Chhikara RR, Sharma P, Singh L. A hybrid feature selection approach based on improved PSO and filter approaches for image steganalysis. International Journal of Machine Learning and Cybernetics. 2015; 7(6):1195–206.
- [12] Shenbagarajan A, Ramalingam V, Balasubramanian C, Palanivel S. Tumor diagnosis in MRI brain image using ACM Segmentation and

ANN-LM classification techniques, Indian Journal of Science and Technology. 2016 Jan; 9(1): 1–12.

- [13] Sajana T, Sheela Rani CM, Narayana KV. A Survey on clustering techniques for Big Data mining. Indian Journal of Science and Technology. 2016 Jan; 9(3):
- [14] Hamid HM S, Shafie AL M, Yahaya C, Muhammad A S. An appraisal of meta-heuristic resource allocation techniques for IaaS Cloud. Indian Journal of Science and Technology.
- [15] Deevi R. R, Sk. Nazma S, Pasala L. S. Challenges of Digital Forensics in Cloud Computing Environment, Indian Journal of Science and Technology. 2016 May; 9(17):1–7.
- [16] Sungjin L, Sunghyuck H. Analysis of Time Records on Digital forensics. Indian Journal of Science and Technology. 2022 Apr; 8(S7):365–72.
- [17] Belkasoft tool. 2022March 03. Available from: https:// belkasoft.com/ec.
- [18] Ftkimager tool. 2022March 24. Available from: https://accessdata.com/product-download/digitalforensics/ftk-imager-version-3.2.0.
- [19] Memoryze tool. 2022March17. Available from: https:// www.fireeye.com/services/freeware/memoryze.ht ml.
- [20] Dumpit tool.2022April 27. Available from: http://qpdownload.com/dumpit.
- [21] Wxhexeditor tool.2022March 25. Available from: https:// sourceforge.net/projects/wxhexeditor/.
- [22] Autopsy tool. 2022March 25. Available from: http://www.sleuthkit.org/autopsy/download.php.

Conflict of Interest Statement: The author declares that there is no conflict of interest regarding the publication of this paper.

Copyright © 2022 Priya Parameswarappa. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

This is an open access article under the CC-BY license. Know more on licensing on https://creativecommons.org/licenses/by/4.0/

