2016 International Workshop on Computational Intelligence (IWCI)
12-13 December 2016, Dhaka, Bangladesh

# Memory Forensics Tools: Comparing Processing Time and Left Artifacts on Volatile Memory

Khaleque Md Aashiq Kamal*, Mahmoud Alfadel* and Munawara Saiyara Munia†
*King Fahd University of Petroleum and Minerals
Dhahran, Saudi Arabia
Email: aashiqkamal@gmail.com , mahmood_1411@hotmail.com
† Ahsanullah University of Science and Technology
Dhaka, Bangladesh
Email: munawaramunia@gmail.com

***Abstract*—Digital investigation is becoming an increasing concern. Many digital forensic tools are being developed to deal with the challenge of investigating digital crimes. Acquisition of volatile memory is one of the vital steps of digital forensics process. Passwords data, indications of digital forensics methods, memory malware may be contained in volatile data which may overlooked by the investigator. The Success of memory acquisition mainly depends on the effectiveness of the memory acquisition tool. This paper compares memory forensics tools based on processing time and left artifacts on volatile memory. Furthermore, we examined how the processing time of the tools varies in terms of different volatile memory size. In order to conduct this work, we use the following tools: FTK Imager, Pro Discover,Nigilant32, Helix3(dd), OSForensics and Belkasoft RAM Capturer. The results show that Belkasoft RAM Capturer has the least amount of left artifacts, and it has also the lowest processing time. Moreover, this work concludes that tested tools are significantly different based on left artifacts on the volatile memory with 95% confidence level. Also, statistically, increasing the memory size x times does not increase the processing time x times of the tools.**

***Index Terms*—Forensics tools, acquisition tools, volatile memory, memory acquisition.**

## I. Introduction

Hacking is a critical problem in present world. Some hackers hack for their malicious goals and some do for fun. FBI reported in 2008 that Internet fraud had cost dollars 264.6 millions. So one of the major challenges in current time is the investigation of the crime in computer technology[1]. Digital forensics is an important part of approximately every investigation. Digital Forensic software tools are applied regularly by the experts in several levels. Government organizations, military forces and other public, private organizations are using these tools. Expansion in forensic study, software tools, and procedure over the last decade has been very victorious and numerous in control situation now depend on these tools on an usual basis without realizing it[2]. In addition to criminal investigation, these tools are used for the purposes of maintenance, debugging, data recovery, and reverse engineering of computer systems in private settings.

In[2] described six categories for digital forensics research: evidence modeling, network forensics, data volume, live memory acquisition, media types, and control systems. Acquisition of live memory data means RAM will allow digital investigators to get evidence that will not be found in a hard drive investigation.

This work observes present work in the acquisition of live memory artifacts and assesses the impact of using specific tools in the capturing of live memory based on left memory artifacts and processing time.

The rest of the paper is organized as follow: Section II is reviewing the background information related to our work. In section III we are describing on the impact of acquisition tools on memory. Next section is describing the related works to digital forensics tools. In section V, we will go thorough the digital forensics investigation approach. Section VI is addressing the problem statement of our research. Next section provides our research approach. Section VIII is providing our experiment and results.Finally Section IX shows statistical analysis.

## II. Background

### A. Digital Forensics

The main idea of digital forensics originated from the general forensic idea of criminal work. But it is not exactly same to the general forensic term. It needs support expertise to examine electronic data records that are not physically substantial. According to[3], Computer forensics has two steps: forensic in the occurrence area and laboratory forensic analysis . Forensic work in the occurrence area is carried out to defend what proof of the occurrence keeps from the event of the occurrence and to recognize potential evidence that may help the examination. Moreover, the proof is reserved in an evidence storage or drived to a specialized forensic lab for deeper analysis. Finally, the analyzed end results are presented to the court who are in charge for the investigation. Moreover , all forensics related to digital data belongs to the category of digital forensics. Computer forensics is the art of utilizing susceptible process and measures to keep, recognize, dig out, trace, and understand digital media facts and to analyze the basis of those proof[4].

978-1-5090-5769-6/16/$31.00 ©2016 IEEE

### B. Digital Evidence

Conventional forensics depends on proof, the accurate data employed in criminal events, to verify that the defendant consign a crime. There are mainly three types evidence: (1) evidence based on observation, (2) evidence based on object (3) evidence based on document[3]. Moreover, Digital evidence is totally different to traditional evidence. We can not examine digital evidence using only open eye. We depend on electronic technology to understand the evidence. Most of the important evidence might be included in the RAM memory.

### C. Importance of RAM data analyzing

To understand the importance of examining RAM , it is essential to explain wherever this information are to be originated and what data does it contain. According to K. Hausknecht et al.[5], all the information of computer system necessary to visit the ram at any time of process. Data will be kept in RAM as well as on the systems HDD. But the key distinction is that RAM shows us what was occurred on the PC at any fix point of time. It is essential to remark that there is enormous of data which are never stored on the HDD but it is available in RAM such as internet data. According to the same authors, we can get a lot of information from RAM data. It mainly depends on the system and the OS. Most significant information are: processes data, network data, information on open files, user data , registry entries, drivers used, processes and data which are hidden, temporal data, used dlls, information about opened session etc.

### D. Memory Artifacts

Memory artifacts mean footprint on the memory. While any application runs on a machine, it occupies a portion of memory. During the run time of the application, it leaves footprint on volatile memory.

### E. Memory acquisition methods

To analyze a RAM, an investigator should have a tool to acquire the RAM image. There are mostly two methods used for capturing RAM: software and hardware method. According to authors[5] Software method is a commonly used to seize the RAM and it is advised to do if the system is live. The main problem of software method is that delinquent can cover its information from such acquisition tools while it is enabled. Another problem is that when these tools are run , they left artifacts on the memory. It can violate important information of the RAM. To recover these issues, investigator can use hardware methods but this a very expensive way to acquire RAM image.

### F. Tools for memory acquisition

There are commercial tools for acquiring RAM such as ProDiscover, Helix3 , FTK Imager. There are non-business software tools such as dd, memdump or Dumpit etc. According to authors [2],among computer forensics expertises, the most excellent way for resolving the reporting issue is to purchase any of these tools from market. But, this just works for financed associations. And there are numerous conditions in where business commercial software tools get failed and specialist needs to depend on open source software. While some of these tools are of very good quality, other tools are poorly recognized, out dated, and even discarded.

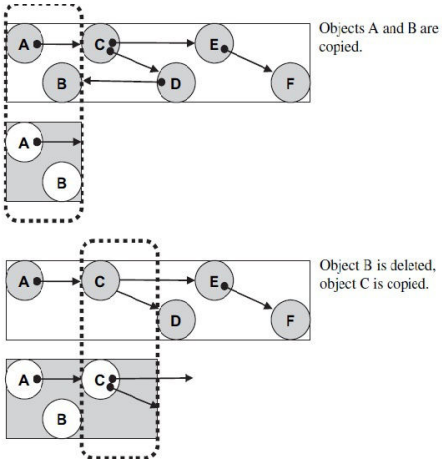


Fig. 1. Acquisition of the memory image from a live system

## III. Impact of acquisition tools on memory

Any tool cannot guarantee that other systems act would get leave for the period of capture a memory ; it means system action is essential for the software to implement. According to [6] while the image of memory is captured, it is as well altered by other processes which are running parallelly and self-sustainability is hampered because of the chronological character of the memory capturing process. Moreover, there is a chance that the suspected executor may have a process in execution to destroy information in memory with parallel by the dump of memory.

As a result, we can say that a dump of memory is captured in parallel with the system action as a technique that produce non-self-sustainability data, and potentially loses data of interest. While this data may expose valuable information, it is less useful from a forensic point of view than data that is self-consistent and therefore more readily interpreted.

Fig 1 shows that how the memory image is captured in a live system and new processes effect the acquisition technique.

As forensics tools executing on the live machine under examination will change the content of the memory whose condition is being acquiesced, their use is error in terms of proof acceptability. So, measuring the extent of the volatile memory changes by causing of running a live forensic tools becomes more and more important.

## IV. Related work

All the digital forensic tools that will be used during any investigation should be tested before using them due to the potential changes that can occur in original data. Several works have been done by the forensics researchers to evaluate or

illustrate the features, quality ,drawbacks of the forensics tools. The study of [7] highlighted a number of usability issues which needs to be considered for comparing forensics tools. User interface,level of expertise, training needs ,reporting and documentation etc. According to them, people are more comfortable with GUI interface than to command line interface tools.

Seo et al.[8] has described several dumping techniques like WinDD, process dump using task manager for windows, dd(linux) , MDD etc. It is very difficult to dump pure memory using WinDD and a collection of more than 4GB of RAM can not be done by MDD.

Okolica et al.[9] has introduced a self contained tool named CMAT(Compiled memory analysis tools). It can extracts environmental and activity data from the live memory. CMAT parses a memory dump to find active, inactive and hidden processes as well as system registry information. It then compiles live response of forensic information from these processes and registry files and assembles it into a format suitable for data correlation.

On the other hand, Wazid et al. in[1] has categorized the tools in several field. Computer forensics tools,memory forensics tools, Network forensics tools, mobile phone forensics tools, database forensics tools. They categorized windowsSCOPE and memoryze as memory forensic tools. Both are used for windows. Memoryze is used for live system and windowsSCOPE performs network wide live memory forensic.

Manson et al.[10] ,has compared another three tools-FTK imager,Encase,Autopsy. According to them, Encase imports image fastest but it is difficult to use for almost all. On the other hand, FTK Imager is easy to use to basic computer user and autopsy is easier to linux user. And according to the author[7],FTK is similar to the windows classic tree view. Thus it has more intuitive interface than other tools.

In[11] Carvajal et al. have focused on digital forensic tools that collect evidence from RAM which contains volatile data such as network connections, logged users, processes, etc. In their paper they compared six forensic tools including: FTK Imager, Pro Discover, Win32dd, Nigilant32, Memoryze, and Helix3 (dd).They evaluated tools based on user interface, reporting, processing time, training, and leaving fingerprints or artifacts. They investigated GUI types of tools leaves more artifacts than the command line types of tools.

The authors of[12] have focused on digital forensic tools that collect evidence from RAM by using fmem and dd tool. But According to the authors Fmem and dd tools are successful in linux but in android, its performance is poor. This is mainly due to some of the android kernel security mechanism that prevent the kernel to load external code.They introduced a tool named lime. It is an open source tool to capture memory from android phones. It can capture through the local SD card.

Another method of capturing android memory is DDMS. Leppart et al.[13] used DDMS. But, it can not acquire complete physical memory. It only can dump single process heap contents. That's why it uses a lot of memory data. To overcome the drawback, Zhou et al.[14] used lime to capture the full memory.

However software method is comparatively cheaper and easier to other imaging process, the method has some drawback. According to[15] while these tools are executed on the machine, valuable forensics information might be deleted before it is preserved.

## V. Digital Forensics Investigation Approach

Digital forensics investigation follows an idle approach for effective result. Mostly investigation process follows the phases as mentioned below[16]. These phases are not restricted to follow but following those phases might bring efficient result of investigation.

- ***Collection***
  - This step handles the gathering of a variety of possible basis of digital proof e.g. RAM data, Mobile data,Hard Disk information etc.
- ***Identification***
  - This step focuses on the identification of digital proof. The evidence are labeled in this step.
- ***Acquisition***
  - Decode to the origin of e-proof evidence from the different sources which are acquiesced.
- ***Preservation***
  - In this step, It gives emphasis of using the satisfactory procedures that make sure the reliability and the genuineness of proof evidence.
- ***Examination and Analysis***
  - It involves the actions such as search, filter, detection and investigation/assessment for relevant weight of the acquiesced e evidence.
- ***Reporting***
  - In this step, the final result and finding of investigation process is reported in details.

In this work our focus is on third phase of digital forensics investigation process which is acquisition.

## VI. Problem Statement

This work is trying to investigate which memory acquisition tools leave less memory artifacts while it is executed. Moreover, the relation between the size of volatile memory and the processing time of capturing volatile memory image will be evaluated. Some tools like: FTK Imager, Pro Discover, Nigilant32,Helix3 (dd),OSForensics,Belkasoft RAM Capturer will be used in this work to investigate this relation. Through this research work we are trying to answer the following questions:

- Can we differentiate those tools based on the amount of left artifacts in the volatile memory and processing time of capturing ?

- What is the relation between the size of volatile memory and the processing time of capturing volatile memory image?

- What is the statistical influence of multiple runs of tools in multiple environments ?

Finally, we will evaluate our investigation result based on statistical analysis.

From our research questions we formulate two set of hypothesis to be tested.

- $\mathbf{H_a0}$: The difference of left artifacts amount on volatile memory of the tools is not significant statistically.

  $\mathbf{H_a1}$: The difference of left artifacts amount on volatile memory of the tools is significant statistically.

- $\mathbf{H_b0}$: Increasing the memory size x times increases the processing time of the tools x times.
  $\mathbf{H_b1}$: Increasing the memory size x times does not increase the processing time of the tools x times.

## VII. Approach

To come up with the solution of our problems, we need a dependable approach to implement our work. To test our experiment, two different environments setup were needed to gather deeper data from the variation of source. Here, we can divided our work in two steps:

- Experimental phase: It starts with the installlation of selected tools and ends with recording our desired data. Fig 2 shows all the steps of our experimental phase.
- Statistical Analysis: In this phase, we will evaluate our experimental results based on statistical analysis.

## VIII. Experiment and Results

In this section we are describing how we have done our experiment. Moreover, our experiment results will be illustrated. To formulate the experiments, our examined tools are collected from the authentic sources and minimum requirement, characteristic has been observed.

The acquisition of RAM using tools is the first goal of this work. Six tools have been used to acquire memory image from the two differnt experimental setup. Table I shows the list of the tools. We used windows 7 operating system as a guest on virtual machine named oracle virtual box. For finding the memory artifatcts by the acquisition tools, we used all the listed tools in the virtual environment which has memory of 1024 MB.

We have run all the tools three times to observe the variation of result.During the capturing of memory, all variates values of physical and virtual memory have been recorded. The detail of both of the examined environment is given below.

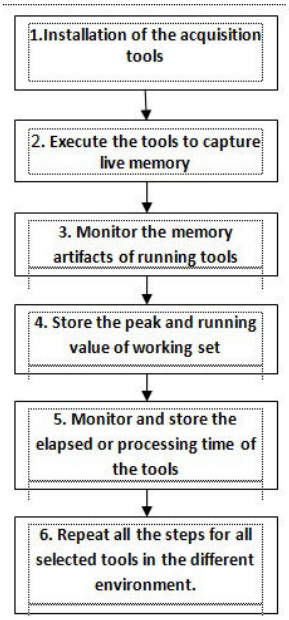


Fig. 2. Steps of the experimental phase

TABLE I
The List of examined tools

| Name of the tools | Developer | Type |
|---|---|---|
| FTK Imager | Access Data | Commercial |
| Nigilant32 | Agile Risk Management | Commercial |
| ProDiscover | Technology Pathway | Commercial |
| Helix3(dd) | E-fense Commercial | Commercial |
| OSForensic | PassMark Soft | Commercial |
| Belkasoft RAM Capturer | Belkasoft Forensics | Commercial |

- ***Experimental Setup 1***
  - Model: HP NOTEBOOK PC
  - Operating System (guest): Windows 7
  - Operating System (host machine): Windows 7
  - RAM : 1024 MB
  - Processor: INTEL PENTIUM DUAL CORE 2.40 GHZ
  - Internet Status : Not Connected
- ***Experimental Setup 2***
  - Model: HP NOTEBOOK PC
  - Operating System (guest): Windows 7
  - Operating System (host machine) : Windows 7
  - RAM : 512 MB
  - Processor: INTEL PENTIUM DUAL CORE 2.40 GHZ
  - Internet Status : Not Connected

There are varieties of artifatcts in KB size between the tools. The peak and the average value are given in Table II.

TABLE II
MEMORY ARTIFACTS ON PHYSICAL MEMORY

| Name of the tools | Physical Memory(Peak Value in KB) | Physical Memory(Average Value in KB) |
|---|---|---|
| FTK Imager | 33660 | 32981 |
| Nigilant32 | 28316 | 25485 |
| ProDiscover | 30984 | 28181 |
| Helix3(dd) | 24584 | 23541 |
| OSForensic | 32380 | 29531 |
| Belkasoft RAM Capturer | 5248 | 4934.2 |

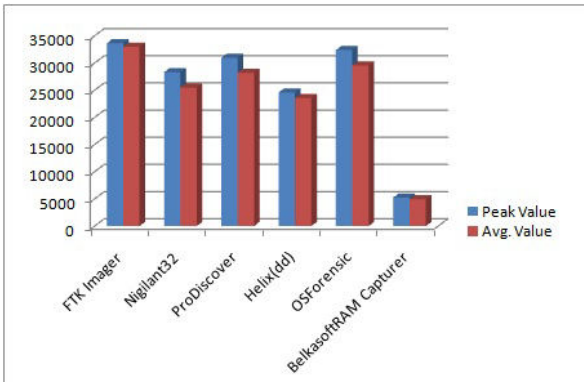


Fig. 3. Physical Memory peak and average value(KB)

Fig 3 graphically displays the differences between acquisition tools based on the left artifacts criteria in physical memory.

Also,the utilization of virtual memory (peak and average value) during execution has been listed in Table III.

From Table II, we can say Belkasoft RAM Capturer has the least memory artifacts while FTK Imager has the most. In addition, Table IV shows the processing time of the tools on both experimental environment. As we notice, Belkasoft RAM Capturer tool has the lowest processing time to capture the memory. Our second goal is to find the relationship between the processing time of memory acquisition and the memory size of the machine. We run those tools on the two different environment by changing the virtual machines memory size.

Table IV is showing the ratio of processing time in both environment. Moreover, Its shows the average of the ratio

TABLE III
MEMORY ARTIFACTS ON VIRTUAL MEMORY

| Name of the tools | Virtual Memory(Peak Value in KB) | Virtual Memory(Average Value in KB) |
|---|---|---|
| FTK Imager | 17428 | 17250 |
| Nigilant32 | 15628 | 12994 |
| ProDiscover | 15836 | 14106 |
| Helix3(dd) | 19244 | 18949 |
| OSForensic | 152808 | 149606 |
| Belkasoft RAM Capturer | 1804 | 1762.5 |

TABLE IV
PROCESSING TIME OF THE COMAPARED TOOLS

| Name | Processing time (seconds) 512MB | Processing time(seconds) 1024MB | Ratio |
|---|---|---|---|
| FTK Imager | 58 | 70 | 1.206 |
| Nigilant32 | 85 | 101 | 1.188 |
| ProDiscover | 95 | 177 | 1.86 |
| Helix3(dd) | 45 | 80 | 1.77 |
| OSForensic | 49 | 70 | 1.438 |
| Belkasoft RAM Capturer | 37 | 56 | 1.51 |
| Average of Ratio | | | 1.494 |

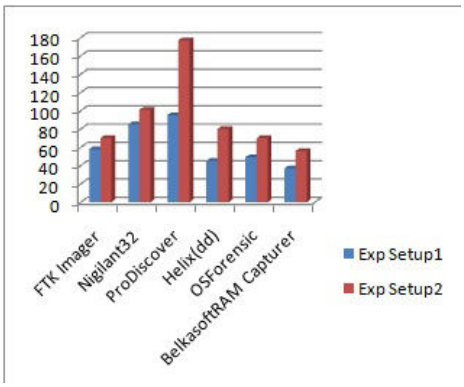


Fig. 4. Processing time in the both experimental setup(in seconds)

of processing time in experimental setup 1 and experiment setup 2 which is 1.494. But, the ratio of memory size in both set up is exactly 2 (1024/512=2). From this relation we can say, increasing the memory size x times does not increase the processing time x times. Fig 4 is graphically shows the processing time in both experimental setup.

## IX. STATISTICAL ANALYSIS

This section is describing the statistical analysis on our experimental results. To validate our results we have done statistical analysis techniques. For $\mathbf{H_a}$, we have applied Analysis of Variance technique(ANOVA), and Confidence Interval(CI) for $\mathbf{H_b}$.

### A. Statistical Analysis of Left Artifacts on Volatile Memory

Anova is a technique that is used to differentiate multiple factors in order to conduct analysis of variance. The main objective of Anova is to find statistically that one alternative is better than to other alternative or not. In this work,we analyze the results of left memory artifacts of the acquisition tools. Anova does the work as following:

- it separates total variation observed in a set of measurements into:
  - (1) Variation **within** one system.
    - Due to random measurement errors
  - (2) Variation **between** systems
    - Due to real differences + random error

TABLE V
OUTCOME OF ANOVA ANALYSIS

| Name | Value |
|---|---|
| F-tabulated | 2.437692635 |
| F-calculated | 6.816682225 |

The main idea behind Anova is to check the variation(2) if it is statistically>variation(1)?
To get much deeper understanding on how to use and apply Anova, we looked in the book published in 1991 by Jain's [17]. The book(The Art of Computer Systems Performance Analysis) explains thoroughly how to use Anova and calculate these two variations. Here, we show the basic measurements we need to come up with Anova analysis technique. The technique applied in this work uses F-test which is decompressed to F-computed and F-table. F-table is obtained from a specific table as mentioned in the book. F-computed needs to be calculated as follows:

$$F = \frac{S_a^2}{S_e^2}$$

Where in general :

$$S_x^2 = \frac{SS_x}{df}$$

$df$ =degrees of freedom
$Sa$ =the mean square value for SSA
$Se$ =the mean square value for SSE
$\alpha$ =the significant level needed to be obtained
$SS_e$ =calculated by variation due to errors in measurements
$SS_a$ =calculated by variation due to effects of alternatives.

After calculating the previous part(F-computed and F-table), we need to compare between both of the values in order to take such the following decisions:
If F-computed is greater than F-table, we have $(1 - \alpha) * 100\%$ confidence that differences among alternatives(modes) are statistically significant.

As shown in Table V, F-calculated(it is calculated based on our experimental results of Table II and III) is clearly greater than the F-tabulated.

As a result, we can come to say that our tested acquisition tools are significantly different with 95% confidence interval based on left artifacts on the volatile memory. So, we reject $H_a0$ and accept $H_a1$ .

### *B. Statistical Analysis of Processing Time*

According to the experiment, increasing the memory size x times do not increases the processing time x times. To validate it we have done confidence interval(CI) [17] for the average accuracy. As shown in Table VI, the mean of processing time ratio(1.49) is located between upper bound(C1) and lower bound(C2). Consequently, $\mathbf{H_b0}$ is rejected, and $\mathbf{H_b1}$ is accepted. The outcome of the statistical analysis validates the stated results previously.

TABLE VI
CONFIDENCE INTERVAL OF PROCESSING TIME RATIO

| Confidence Interval for the Average Ratio | |
|---|---|
| Mean | 1.495 |
| SD | 0.279 |
| Confidence Coefficient | 1.96 |
| Error Margin | 0.223 |
| Upper Bound C1 | 1.72 |
| Lower Bound C2 | 1.27 |

## X. CONCLUSION

The field of digital forensics is progressing day by day to enrich the area of security domain. New advance forensics tools are existence to investigate occurrence. But the threat to forensics is also becoming equipped with anti forensics tools which can remove digital evidence or can make delay in the evidence capturing process.As a result , efficient forensics tools are necessary to maintain a proper investigation process. This research examined six highly used memory forensics tools based on left artifacts and processing time. According to our experiment result and analysis, we can conclude that BelkasoftRAMCapturer has least memory artifacts while it is executed on any machine. As a result, it will erase less system information from the volatile memory which are very much important for digital forensics investigation. On the other hand, FTK Imager has the highest memory artifacts which may erase valuable evidence from the volatile memory. For processing time, BelkasoftRAM Capturer has the lowest while ProDiscover has the highest to capture memory for the digital investigation process. Moreover, we can say that if the memory size is increased then the processing time of capturing memory of those acquisition tools may not be increase rationally.

## REFERENCES


[1] M. Wazid, A. Katal, R. Goudar, and S. Rao, "Hacktivism trends, digital forensic tools and challenges: A survey," in *IEEE Conference on Information & Communication Technologies (ICT),2013*. IEEE, 2013, pp. 138–144.

[2] S. L. Garfinkel, "Digital forensics research: The next 10 years," *digital investigation*, vol. 7, pp. S64–S73, 2010.

[3] I.-L. Lin, Y.-S. Yen, and F.-Y. Leu, "Research on comparison and analysis of the defsop, nist cell sop, and iso27037 sop," in *Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS),2014*. IEEE, 2014, pp. 511–516.

[4] I.-L. Lin, H.-C. Chu, W.-N. Wu, and C.-P. Chang, "To construct the digital evidence forensics standard operation procedure and verification on real criminal cases-take linux/unix system as an example," *The 10th Cyberspace2008 Cybersecurity, Cybercrime and Cyberlaw*.

[5] K. Hausknecht, D. Foit, and J. Buric, "Ram data significance in digital forensics," in *38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO),2015*. IEEE, 2015, pp. 1372–1375.

[6] E. Huebner, D. Bem, F. Henskens, and M. Wallis, "Persistent systems techniques in forensic acquisition of memory," *Digital Investigation*, vol. 4, no. 3, pp. 129–137, 2007.

[7] H. Hibshi, T. Vidas, and L. Cranor, "Usability of forensics tools: a user study," in *Sixth International Conference on IT Security Incident Management and IT Forensics(IMF),2011*. IEEE, 2011, pp. 81–91.

[8] J. Seo, S. Lee, and T. Shon, "A study on memory dump analysis based on digital forensic tools," *Peer-to-Peer Networking and Applications*, pp. 1–10, 2013.
[9] J. Okolica and G. Peterson, "A compiled memory analysis tool," in *Advances in Digital Forensics VI*. Springer, 2010, pp. 195–204.
[10] D. Manson, A. Carlin, S. Ramos, A. Gyger, M. Kaufman, and J. Treichelt, "Is the open way a better way? digital forensics using open source tools," in *40th Annual Hawaii International Conference on System Sciences, 2007. HICSS 2007.* IEEE, 2007, pp. 266b–266b.
[11] L. Carvajal, C. Varol, and L. Chen, "Tools for collecting volatile data: A survey study," in *International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE), 2013*. IEEE, 2013, pp. 318–322.
[12] J. Sylve, "Android mind reading: memory acquisition and analysis with dmd and volatility," *Retrieved from*, 2012.
[13] J. Sylve, A. Case, L. Marziale, and G. G. Richard, "Acquisition and analysis of volatile memory from android devices," *Digital Investigation*, vol. 8, no. 3, pp. 175–184, 2012.
[14] F. Zhou, Y. Yang, Z. Ding, and G. Sun, "Dump and analysis of android volatile memory on wechat," in *IEEE International Conference on Communications (ICC), 2015*. IEEE, 2015, pp. 7151–7156.
[15] S. Vömel and F. C. Freiling, "A survey of main memory acquisition and analysis techniques for the windows operating system," *Digital Investigation*, vol. 8, no. 1, pp. 3–22, 2011.
[16] O. K. Appiah-Kubi, S. Saleem, and O. Popov, "Evaluation of some tools for extracting e-evidence from mobile devices," 2011.
[17] R. Jain, *The art of computer systems performance analysis*. John Wiley & Sons, 2008.