TEKNOKOM : Jurnal Teknologi dan Rekayasa Sistem Komputer
Vol. 5, No. 1, March 2022, pp. 96 - 102
ISSN: 2686-3219, DOI: 10.31943/teknokom.v5i1.73

MEMORY FORENSIC DEVELOPMENT AND CHALLENGES IN IDENTIFYING DIGITAL CRIME : A REVIEW

Yasep Azzery[1]*, Nur Dwi Muryanto[1], Taufik Hidayat[2]
[1]Department of Electrical Engineering, Universitas Mercu Buana, Indonesia
[2]Department of Computer Engineering, Universitas Wiralodra, Indonesia

ARTICLE INFO

History of the article:
Received October 14, 2021
Revised December 28, 2021
Accepted December 29, 2021
Published March 2, 2022

Keywords:
Digital Forensic
Memory Forensic
Cybercrime
Systematic Literature Review

Correspondece:
Yasep Azzery,
Department of Electrical Engineering,
Universitas Mercu Buana, Indonesia,
Email : yasep.azzery@gmail.com

ABSTRACT

Digital forensic technology is currently advancing along with the demands to uncover various crimes using technology. Memory Forensic is one of the investigative fields in digital forensics. We use the Systematic Literature Review method to identify the developments and challenges of Forensic Memory in identifying digital crimes, analyzed from various reference papers according to the Include and Exclude Criteria and based on the specified Research Question. Authors chose from 30 reference journals from 3 online journal databases namely IEEE Explore, Sciencedirect, and Springer with themes related to forensic memory based on certain criteria for further review to determine the development of digital crime. The results of the SLR that we convey are the result of a study related to the use of Memory Forensic in identifying various digital attacks and challenges faced in the future.

INTRODUCTION

Digital crimes are increasingly rampant today, such as defacements, malware and ransomware infections, phishing, spam emails, and others. These digital crimes leave no trace at all. However, based on the Locard Exchange principle proposed by Dr. Edmund Locard who stated that "Every contact that occurs will definitely leave a trace", digital crime will also leave a digital footprint [1]. Therefore, we need a method to investigate a digital crime, namely digital forensics.

Digital Forensics is a branch of forensic science that uses science and scientific methods to search for and find digital evidence in an effort to reconstruct criminal events that occurred by going through several structured stages so that they can be accepted by the court for law enforcement. As with the disclosure of crimes in general, digital crimes also require digital evidence in an effort to uncover cases of crimes that have occurred. One of the digital artifacts is RAM or computer memory, which is a very large source of information during a computer's work since it was last turned on [2]. In the memory there may be digital evidence that is still stored. Therefore, forensic memory can be used to investigate digital crime evidence.

In this paper, information will be collected from a number of trusted journals, such as IEEE, sciencedirect and springer, then summarized so that information can be seen regarding how the developments and what challenges exist in forensic memory in an effort to identify a digital crime.

RESEARCH METHOD

Systematic Literature Review

Systematic Literature Review (SLR) method is a term used to refer to a particular research or research methodology and development carried out to collect and evaluate related research on a particular topic focus. SLR research is carried out for various purposes, including identifying, reviewing, evaluating, and interpreting all available research with topic areas of interest to phenomena, with certain relevant research questions. SLRs are also often required for setting a research agenda, as part of a dissertation or thesis, and as part of a research grant application. The application of SLR is divided into 3 main stages which must be carried out sequentially and systematically, as follows [1]:

a. Planning

At this stage, the researcher identifies the goals and needs of what will be done with this

SLR. Next is to make a Research Question (RQ), which is to prepare a series of questions related to the theme to be taken. RQ is the earliest part of the SLR process. RQ is used to guide the literature search and extraction process.

b. Conducting

The conducting stage is the stage that contains the implementation of the SLR method. Conducting has 4 (four) stages, the first is to review the related paper, the second stage is to determine whether it is included in the category or not (inclusion and exclusion), the third stage is to assess the quality of the content of the paper/journal (quality assessment), the fourth stage is to collect data (data collection).

c. Reporting

The reporting stage consists of two parts, namely reporting, to display the results of the application of SLR in related journals, and conclusion drawing, which is the stage of drawing conclusions from the entire process that has been carried out.

Data Source Journal

The paper/journal search that the author did was obtained from the Scopus indexed paper database site for international and reputable papers, this is so that the papers obtained from the search results are papers that have high quality. The search data for papers/journals and their websites can be seen in Table 1.

Table 1. Journal Database

Database Journal	Link Journal
IEEE Explore	https://ieeexplore.ieee.org/Xplore/home.jsp
Sciencedirect	https://www.sciencedirect.com/
Springer Link	https://link.springer.com/

The search site in Table 1 is a popular site and its credibility can be trusted so that it can be used as a reference in the application of the SLR method with the keyword Memory Forensic. The paper/journal search process was selected based on 2015 to 2020 and the following journals were produced which are shown in Table 2.

Table 2. Result Journal Form 2015-2020

Digital Online Journal Library	Total Journal	
	Keyword: Digital Forensic	Keyword: Memory Forensic
IEEE Explore	1.315	130
Sciencedirect	7.263	4.810
Springer Link	8.171	6.694

Based on the data in Table 2, the search results obtained according to keywords and filters based on the specified year. Search results vary according to the keywords typed on the site. For Digital Forensic keywords, Springer Link displays the most search results with 8,171 papers. As for the Memory Forensic keyword, the Springer Link site also displays the most results with 6,694 papers/journals. From the search results, it will still be re-selected to answer the Research Question (RQ) and determine the quality of the content of the paper being sought, whether it is in accordance with the criteria determined by the author. Overall, the Springer Link site displays the most search results, it will be studied further whether the search results are relevant to the contents of the paper.

Selection Criteria Journal

Based on the search data, we took 30 reference journals related to the theme of Memory Forensic to analyze a form or potential of digital crime. The determination is based on titles and abstracts that are relevant to the theme and research studies on Memory Forensic. Journals were obtained from 3 online journal databases to conduct SLR studies, the general criteria were determined. First, the year of the paper/journal starting from 2015 to 2020, the second being a Scopus indexed paper/journal, and the third discussing the topic of Forensic Memory technology and its applications. From these criteria, 30 papers/journals were taken, which are shown in table 3 below. The contents of the paper are related to the discussion of Memory Forensic and its application in analyzing digital crimes.

Table 3. Source Journal for Analysis

Title Journal	Year	Reference
Analyzing and searching process of internet username and password stored in Random Access Memory (RAM)	2018	[2]
Reliable and Trustworthy Memory Acquisition on Smartphones	2018	[3]
Acquisition and analysis of compromised firmware using memory forensics	2018	[4]
The impact of GPU-assisted malware on memory forensics A case study	2018	[5]

Computer forensic analysis model for the reconstruction of chain of evidence of volatile memory data	2018	[6]
Framework for Live Forensics of a System by Extraction of Clipboard Data and Other Forensic Artefacts from RAM Image	2018	[7]
Forensic reconstruction of executables from Windows 7 physical memory	2019	[17]
Memory forensics: tools Comparing processing time and left artifacts on volatile memory	2019	[19]
Detecting objective-C malware through memory forensics	2019	[8]
Robust bootstrapping memory analysis against anti-forensics	2019	[9]
An Efficient Approach for Advanced Malware Analysis Using Memory Forensic Technique	2019	[10]
Gaslight: A comprehensive fuzzing architecture for memory forensics frameworks	2019	[11]
Linux memory forensics Dissecting the user space process heap	2019	[12]
Hidden process offline forensic based on memory analysis in windows	2020	[13]
Memory Forensic: Challenges Under Misused Architectural Features	2020	[14]

The journal was analyzed by SLR, because it has relevant and interesting themes and materials for further study. There is no search for national papers/journals, because the authors limit the search to only international journal sites [15].

RESULTS AND DISCUSSION

Result Extraction Data

The stages of extracting data are divided into several parts, starting with making a Research Question (RQ), determining the Inclusion/Exclusion Criteria, making a Quality Assessment (QA), analyzing the data, and ending with answering the RQ that has been made.

Research Question

RQ is used to guide the literature search and extraction process. The selection of RQ in a journal study on Forensic Memory analysis with the SLR method is as follows.

Table 4. Research Question

RQ1	**Does the paper cover the major themes of Memory Forensic analysis and its application?**
RQ1.1	What technology does the investigation using Memory Forensic do?
RQ1.2	What problems can be solved with the application of Memory Forensic?
RQ1.3	What types of digital crimes are analyzed with the application of Memory Forensic?
RQ2	**Can Memory Forensic be applied to be able to provide solutions to existing problems?**
RQ2.1	Can the use of Memory Forensic provide a solution to the problem?
RQ2.2	Do you propose any new Memory Forensic tools/methods?

Inclusion and Exclusion Criteria

At this stage, the feasibility of a paper is determined for further analysis. If it meets the Incussion, it means that the journal is worthy of being used as a reference, otherwise if it is in the Exclusion category, the journal is not used.

a. Inclusion Criteria

1. Paper/journal used in the 2015-2020 period.
2. Scopus indexed papers/journals.
3. Research themes related to Memory Forensic.
4. The topics discussed are only related to Memory Forensic and its application in solving problems.

b. Exclusion Criteria

1. The paper/journal does not specifically discuss Memory Forensic.
2. Papers/journals are not published in the period 2015 - 2020.

Quality Assessment (QA)

QA is used to assess the quality of the topic of the paper related to Memory Forensic as determined. I determined QA and divided based on the following questions:

Table 5. Quality Assesment List

Code	Question	Category
QA1.	Does the paper/journal discuss topics related to Memory Forensic technology and its application?	Y / N
QA2.	Does the paper/journal discuss theoretical studies related to the mechanism of Forensic Memory analysis?	Y / N
QA3.	Has the application of Memory Forensic been successfully applied in the research in that paper/journal?	Y / N

Y = Yes, it means that it is in the QA category
N = No, it means that it does not fall into the QA category

Based on the QA, an assessment was produced from 30 reference journals which are shown in the following table.

Tabel 6. Quality Assessment (QA) Paper/Journal

Title Journal	QA 1	QA 2	QA 3	Result
Analyzing and searching process of internet username and password stored in Random Access Memory (RAM)	Y	Y	N	OK
Reliable and Trustworthy Memory Acquisition on	Y	Y	Y	OK
Acquisition and analysis of compromised firmware using memory	Y	Y	Y	OK
The impact of GPU-assisted malware on memory forensics A	Y	Y	N	OK
Computer forensic analysis model for the reconstruction of chain of evidence of volatile	Y	Y	N	OK
Framework for Live Forensics of a System by Extraction of Clipboard Data and	Y	Y	Y	OK
Forensic reconstruction of executables from Windows 7 physical	Y	Y	Y	OK
Memory forensics: tools Comparing processing time and left artifacts on	Y	Y	N	OK
Detecting objective-C malware through memory forensics	Y	Y	N	OK
Robust bootstrapping memory analysis against anti-forensics	Y	Y	N	OK
An Efficient Approach for Advanced Malware Analysis Using Memory	Y	Y	Y	OK
Gaslight: A comprehensive fuzzing architecture for memory	Y	Y	N	OK
Linux memory forensics Dissecting the user space process heap	Y	Y	Y	OK
Hidden process offline forensic based on memory analysis in	Y	Y	N	OK
Memory Forensic: Challenges Under Misused Architectural	Y	Y	N	OK

OK : Included in the reference paper for research because it meets QA
NOK : Not included in the reference paper because it does not meet QA (Not OK)

Reseacrh Question (RQ)

Of the 15 reference papers/journals studied, an extraction will be carried out regarding the discussion of Forensic Memory in the literature used.

Question RQ1.1 focuses on technologies that can be analyzed using forensic memory to uncover a digital crime.

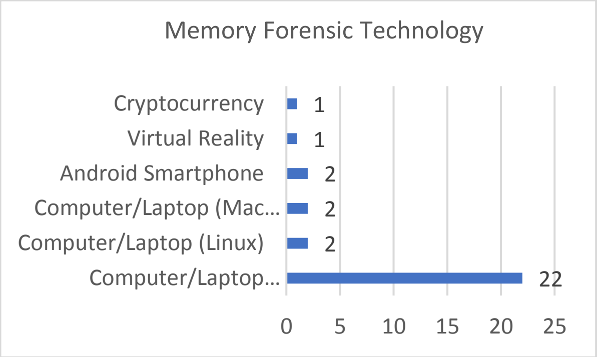

Figure 1. Memory Forensic Technology

Based on the data in Figure 1, it can be seen that the majority of Memory Forensic usage is still aimed at computers/laptops with Windows operating systems. However, what is interesting is the implementation of forensic memory analysis on virtual reality and cryptocurency technology. This shows that the development of forensic memory also follows the development of existing technology.

The question in RQ1.2 aims to see the problems that want to be solved using memory forensics.

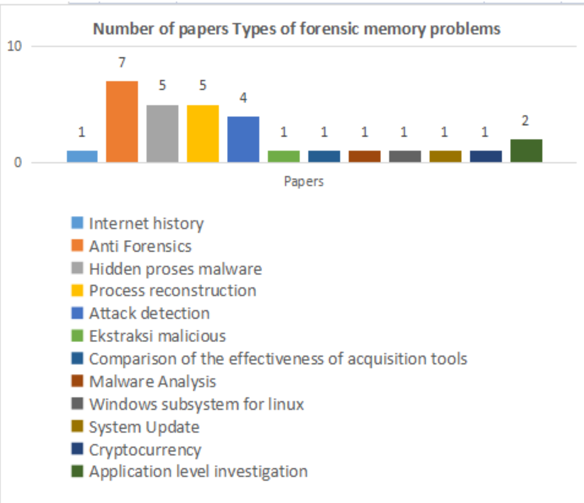

Figure 2. Memory Forensic Problem

Based on Figure 2, it can be seen that the problems faced in research related to memory forensics are mostly crimes that use antiforensics in their actions, hidden malware processes, process reconstruction/evidence chains, and attack detection problems. The interesting thing is that there are problems when updating the system, due to the possibility that when updating the system there is a massive change in the system which results in changes in the system parameters used. In addition, the existence of the Windows Subsystem for Linux that allows running Linux applications on Windows is also a problem in forensics.

Questions in RQ1.3 were used to extract the types of digital crimes that were analyzed using Memory Forensic.

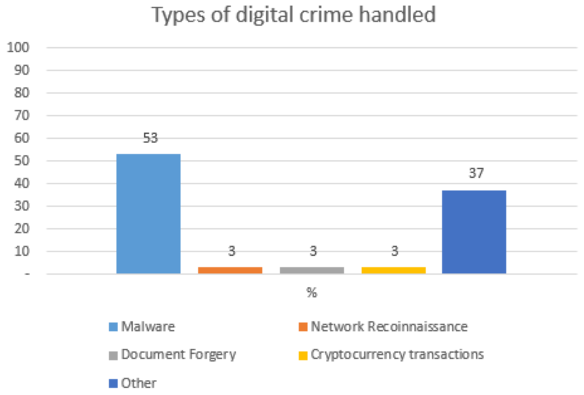

Figure 3. Digital crimes handled

Based on the data in Figure 3, the majority of the literature used shows the use of forensic memory to analyze the presence of malware in a system, which is 53.3%.

- RQ2 discussion

RQ2. Can Memory Forensic be applied to be able to provide solutions to existing problems?.

In RQ2, it is a form of analytical question related to the application of Memory Forensic to solve the problem solution in the paper/journal. The results of the RQ2 analysis are poured into the answers for RQ2.1, RQ2.2, and RQ2.

RQ2.1	Can the use of Memory Forensic provide a solution to the problem?	Results	%
	Yes	30	100
	No	0	0

From the results of the discussion of RQ2.1 it can be converted to the following graph:

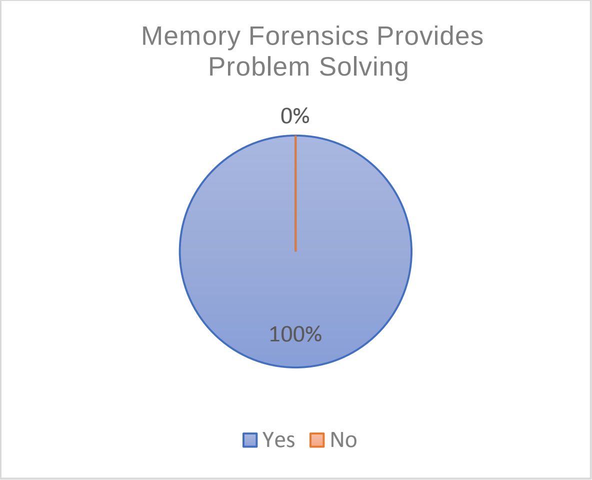

Figure 4. Discussion of RQ2.1

Figure 4 shows that memory forensics always provides solutions to the problems raised in the paper/journal.

RQ2.2	Does it generate new technology ideas/methods after a Memory Forensic simulation has been carried out?	Results	%
	Yes	15	50
	No	15	50

From the results of the discussion of RQ2.2, it can be converted into the following graph:

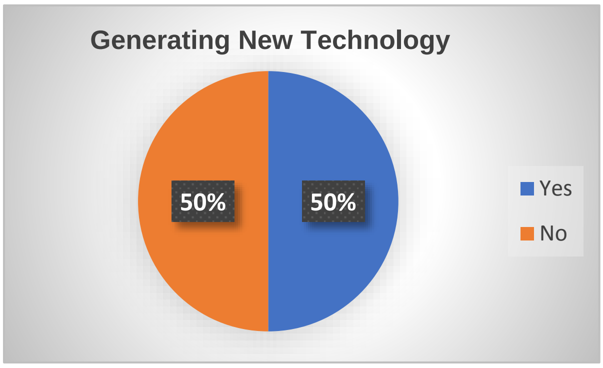

Figure 5. Discussion of RQ2.2

Figure 5 explains that there are 50% of papers/journals that propose new methods in applying memory forensics, and half of them are still using existing methods.

CONCLUSION

The SLR study on the development of Memory Forensic technology taken from 30 reference journals from 3 online journal databases namely IEEE Explore, Sciencedirect, and Springer Link provides an overview of the development of Memory Forensic analysis and its application in identifying crimes by analyzing storage devices, operating systems, and smartphones. The challenges of technological development are increasingly difficult for law enforcement and to reveal increasingly sophisticated and complex digital crimes. By writing this study on SLR, the author hopes that various studies on Memory Forensic can develop following technological advances.

REFERENCES

[1] Romi Satria Wahono, “A Systematic Literature Review of Software Defect Prediction: Research Trends, Datasets, Methods and Frameworks,” Andi Offset, vol. 1, no. 1, pp. 1–16, 2015.

[2] V. Ravindra Sali and H. K. Khanuja, “RAM Forensics: The Analysis and Extraction of Malicious Processes from Memory Image Using GUI Based Memory Forensic Toolkit,” Proc. - 2018 4th Int. Conf. Comput. Commun. Control Autom. ICCUBEA 2018, pp. 1–6, 2018, doi: 10.1109/ICCUBEA.2018.8697752.

[3] Y. Otsuki, Y. Kawakoya, M. Iwamura, J. Miyoshi, and K. Ohkubo, “Building stack traces from memory dump of Windows x64,” Digit. Investig., vol. 24, pp. S101–S110, 2018, doi: 10.1016/j.diin.2018.01.013.

[4] N. Lewis, A. Case, A. Ali-gombe, and G. G. Richard, “Memory forensics and the Windows Subsystem for Linux,” Digit. Investig., vol. 26, pp. S3–S11, 2018, doi: 10.1016/j.diin.2018.04.018.

[5] A. M. Muniz Soares and R. T. de Sousa Junior, Forensic Analysis of Android Runtime (ART) application heap objects in emulated and real devices, vol. 867. Springer International Publishing, 2018.

[6] C. B. Leopard, N. C. Rowe, and M. R. McCarrin, “Memory forensics and the Macintosh OS X operating system,” Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng. LNICST, vol. 216, pp. 175–180, 2018, doi: 10.1007/978-3-319-73697-6_13.

[7] F. Olajide, T. Al-Hadrami, and A. James-Taylor, Forensic use case analysis of user input in windows application, vol. 843. Springer International Publishing, 2019.

[8] A. Kazim, S. Al Ali, and K. Al-hussaeni, “Memory Forensics : Recovering Chat Messages and Encryption Master Key,” 2019 10th Int. Conf. Inf. Commun. Syst., pp. 58–64, 2019.

[9] E. Qawasmeh, M. I. Al-Saleh, and Z. A. Al-Sharif, “Towards a Generic Approach for Memory Forensics,” ITT 2019 - Inf. Technol. Trends Emerg. Technol. Blockchain IoT, pp. 94–98, 2019, doi: 10.1109/ITT48889.2019.9075122.

[10] P. Casey, R. Lindsay-decusati, I. Baggili, and F. Breitinger, “Inception : Virtual Space in Memory Space in Real Space e Memory Forensics of Immersive Virtual Reality with the HTC Vive,” Digit. Investig., vol. 29, pp. S13–S21, 2019, doi: 10.1016/j.diin.2019.04.007.

[11] F. Block and A. Dewald, “Windows Memory Forensics : Detecting (Un) Intentionally Hidden Injected Code by Examining Page Table Entries,” Digit. Investig., vol. 29, pp. S3–S12, 2019, doi: 10.1016/j.diin.2019.04.008.

[12] N. R. Mistry and M. S. Dahiya, “Signature based volatile memory forensics: a detection

based approach for analyzing sophisticated cyber attacks," Int. J. Inf. Technol., vol. 11, no. 3, pp. 583–589, 2019, doi: 10.1007/s41870-018-0263-4.

[13] T. Thomas, M. Piscitelli, I. Shavrov, and I. Baggili, "Forensic Science International : Digital Investigation Memory FORESHADOW : Memory Forenensics of HerDware CryptOcurrency wallets e A Tool and Visualization Framework," Forensic Sci. Int. Digit. Investig., vol. 33, p. 301002, 2020, doi: 10.1016/j.fsidi.2020.301002.

[14] D. Uroz and R. J. Rodríguez, "Forensic Science International : Digital Investigation On Challenges in Verifying Trusted Executable Files in Memory Forensics," Forensic Sci. Int. Digit. Investig., vol. 32, p. 300917, 2020, doi: 10.1016/j.fsidi.2020.300917.

[15] L. Campanile, M. Gribaudo, M. Iacono, F. Marulli, and M. Mastroianni, "Computer Network Simulation with ns-3: A Systematic Literature Review," Electronics, vol. 9, no. 2, p. 272, Feb. 2020, doi: 10.3390/electronics9020272.