ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)
https://doi.org/10.17559/TV-20210218122046
Preliminary communication

Analysing and Carving MS Word and PDF Files from RAM Images on Windows

Kubilay TAŞDELEN, Ahmet Ali SÜZEN*

Abstract: In this study, a piece of software has been developed to recover the readable data by carving MS Word and PDF files from the RAM image. String searching, signature scanning, and data carving methods are used in the design of the software. The analysis was performed on a RAM image of 14 GB by using the software that was developed. The success rate for each file was determined by comparing the recovered data to the data in the original file. It was determined that the rate of data recovery decreases as the size of the MS Word or PDF files loaded onto RAM increases. Consequently, it is aimed to be an important example of obtaining electronic evidence from volatile data in forensic informatics with the proposed study.

Keywords: electronic evidence; file carving; forensic science; image acquisition; memory analysis; memory forensics

1 INTRODUCTION

In the realm of cybercrime, data about the crime are obtained using digital evidence. The first step in cybercrime is to acquire the image of the RAM and hard disk in order to investigate it later. Particularly in regard to collecting evidence from RAM, the data must be obtained before being deleted [1]. Therefore, the data in the RAM needs to be copied by using an image acquisition software.

In the Windows operating system, only active processes in virtual memory can be accessed. Full access to RAM is only available at the kernel mode level in Windows. Therefore, RAM image acquisition software runs at the kernel mode level. There exist open source and commercial software that acquires RAM images for the Windows operating system [2-4]. The RAM images acquired by these software packages are used in RAM analysis and data carving operations.

Various data such as user passwords, images, documents, installed programs, and web addresses that have been visited can be acquired from the RAM by a RAM image analysis [3-7]. String searching, signature scanning, file carving, and data structure analysis methods are used to recover data from the RAM image. Which method is to be used in the analysis process depends on the desired data. The string search technique is used to access the user's social media or application passwords [7]. Data about the processes that are running or have been loaded in the system are kept in the data files on RAM. A data structure analysis method is used to access these data [8]. In order to obtain the data belonging to the files in the RAM, the file first needs to be recovered. The files in the image are recovered using signature search and file carving techniques, respectively [9]. Different data recovery techniques are applied depending on the file type in order to access the data in the recovered files [10-11].

In this study, a piece of software was developed to scrape readable MS Word and PDF data from RAM images. Data carving from a RAM image of 14 GB was carried out using the developed software separately for the MS Word and PDF files on a Windows 10 64 - bit operating system. At the end of the analysis, 10 MS Word files with the .doc extension were recovered in 41 minutes and 10 seconds, 10 MS Word files with .docx extension in 37 minutes 45 seconds, and 10 PDF files were recovered in 45 minutes 1 second. Each PDF and .doc file was decoded to access its data. The data in the MS Word files with .docx extension were accessed using the string search method. When the recovered data were examined, it was determined that the average success rate was 40% for MS Word files and 16% for the PDF files.

2 RELATED WORK

Digital Forensics is a multi-disciplinary scientific field that deals with the collection, examination and preservation of existing data as evidence that is given to courts. The first Digital Forensics work is understood to be the identification of when and how someone entered a system administrator's system without permission in 2001 [12]. Digital evidence, rather than physical evidence, is needed to shed light on crimes in Digital Forensics. It must be proved that the digital evidence has not been changed since it was collected. The hash signatures of the digital data can be acquired using MD5 and SHA1 algorithms. It is possible to determine whether the evidence has been changed after collection through these signatures [13].

Much of data that can be considered as digital evidence are temporarily stored in RAM. It was observed that the data stored in the RAM was not deleted for a certain period of time after the power is turned off. First, crypto keys in the RAM were found without using any special hardware by an attack scenario called Cold Boot [14].

KnTTools, which was developed in 2005, is understood to be the first RAM image acquisition from the operating system and analysis application. The search analysis for running processes and threads was carried out in the RAM image by using KnTTools [4]. Image acquisition, using external hardware, was carried out by using the application AfterLife. The system is restarted after plugging the USB memory with the AfterLife application into the system. The application that controls the system copies the content of the RAM to the free space in the USB memory during the boot. Since USB memory is used in this method, the BIOS boot settings of the target system must be changed to USB memory. In addition, the application cannot acquire RAM images greater than 4 GB [15].

Accessing RAM from the user mode in the operating system was restricted after Windows Vista [16]. Because of these restrictions, RAM image acquisition software must be run at kernel mode by a RAM driver [17].

Belkasoft Live RAM Capturer, DumpIt, FTK Imager, and WinEn software run in the kernel mode [8-10]. These software packages have been developed as commercial or open source software. There are no studies on developing kernel mode RAM image software in the literature. In general, RAM image analysis and data recovery techniques have been used in the current studies [10-12].

The most comprehensive analysis of RAM images can be carried out with Volatility, an open source software. Data about the registry files, the running process, network, and malware detection can be accessed within the image at the end of image analysis by using Volatility [18]. In addition, digital evidence about the files is obtained by carrying out RAM image analysis. Access to images and document files within the image is carried out using the signature scanning method [19]. The image files in the RAM were accessed using signature scanning method in the studies [8].

PDF files are widely used in operating systems. At this point, many important data are stored in PDF files. PDF files have an important place in the process of obtaining digital evidence. For this reason, PDF files are also examined during the RAM image analysis. Methods for recovering PDF files from RAM have been proposed in studies [16]. The recommended methods are used with the operating systems preceding Windows Vista. PDF files from RAM cannot be accessed through the operating systems used in recent times such as Windows 7, 8, 8.1, and 10.

One of the file types used to obtain digital evidence from RAM is MS Word. Al-Sharif et al. accessed MS Word files with .docx extension in the RAM image by using string searching method in their 2017 study. This study was conducted on the Windows 7 operating system and the average success rate was 6% [17].

3. MATERIALS AND METHODS

3.1 PDF (Portable Document Format)

PDF is a digital method developed for creating portable and printable documents that are independent of software, hardware, and operating systems. The PDF file format was first developed in 1992 by Camelot, one of Adobe's founders. Today, this format is used as an open standard managed by the International Organization for Standardization (ISO). PDF files contain text, audio, video, and image data [20].

Table 1 Encryption techniques used in PDF files

FlateDecode	ASCIIHexDecode
ASCII85Decode	LZWDecode
RunLengthDecode	CCITTFaxDecode
JBIG2Decode	DCTDecode
JPXDecode	Crypt

The data in the PDF files are encrypted with the techniques given in Tab. 1. The encryption used for the PDF files is given in the reference labels in the file itself. Today, PDF programs encrypt PDF files with FlateDecode. The encrypted data in the PDF files are saved between the stream and endstream blocks [21]. As shown in Fig. 1, the algorithm used to encrypt the data is shown on the filter label.

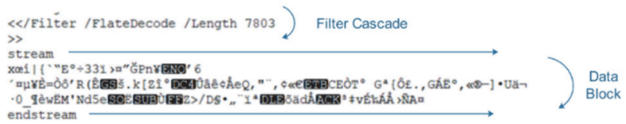

Figure 1 The structure of PDF file

3.2 Word Document File

Text, audio, image, and video data can be saved in the Word file format. .doc and .docx file formats are used in Word files. Word files with the .doc extension are in the OLE Compound Binary File (CBF) file format whose structure is shown in Fig. 2. The OLE Compound Binary File is a method for storing multiple data streams in a single file. The data in files with the .doc extension are encrypted by using codepage 1252 between WordDocument blocks. The encrypted data in the file stored between (Content_Types) and STX tags.

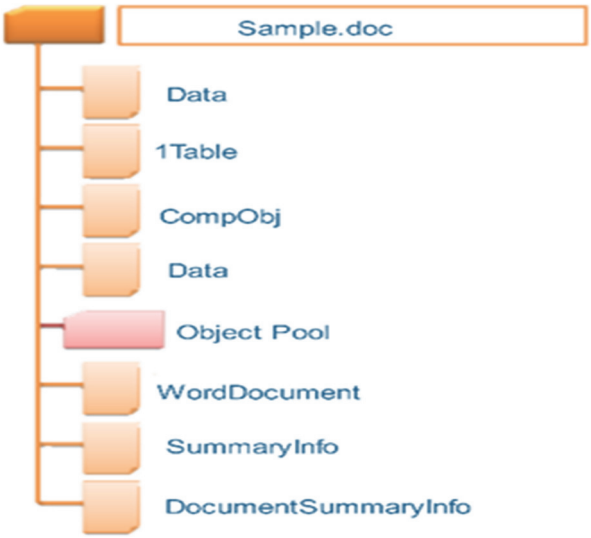

Figure 2 The parsed structure of a Word file (.doc)

Word files with the .docx extension consist of compressed XML files [22]. Data compression programs are used to parse Word files into XML format. When the Word document is parsed into XML files, the textual data is stored in a document.xml file. The image and video files used in Word are extracted into the media folder. The style and layout styles used in the document are stored in the styles.xml file [23]. Fig. 3 shows the parsed structure of a sample MS Word file with the .docx extension.

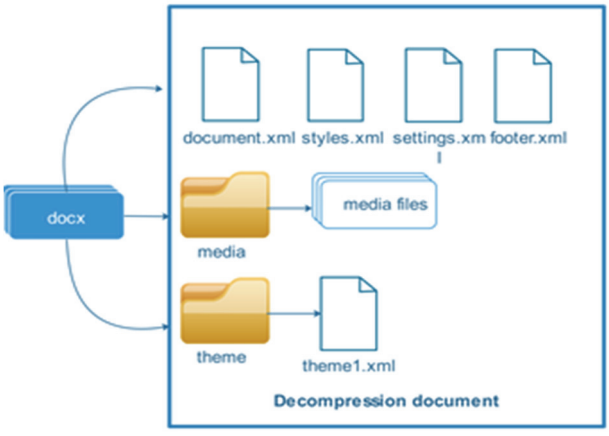

Figure 3 The parsed structure of a Word file (.docx)

3.3 File Management in RAM

When a new file is opened in the operating system, it is first loaded into RAM. The address of the opened file is kept in the EPROCESS (Executive Process) unless it is terminated. The device data, file name, and the data for the open file are kept in the FILE_OBJECT structure. FILE_OBJECT keeps the data for the file loaded into RAM in the DeviceObject, SectionObjectPointer, and Filename structures. The DataSectionObject, SharedCacheMap, and ImageSectionObject sections in the SectionObjectPointer structure are used to access readable data about the file. This situation is shown in Fig. 4.

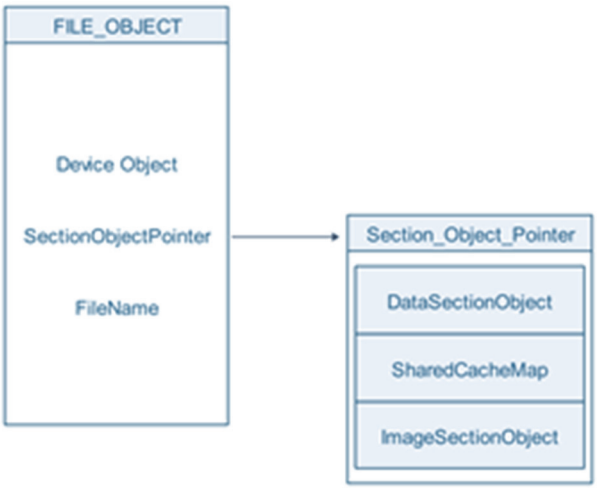

Figure 4 The structure of File_Object

When a file is loaded into RAM, the DataSectionObject structure is first triggered by the SectionObjectPointer [24]. Then the SharedCacheMap and ImageSectionObject structures are called. When the file is deleted or terminated, the record within the EPROCESS is deleted. But FILE_OBJECT keeps the deleted or terminated file until a new address is assigned [25]. Therefore, access to a file in RAM may be possible even if the process has been terminated.

3.4 RAM Image Analysis Methods

After acquiring the RAM image, various methods are then used to obtain digital evidence. The data in the divided or undivided areas of the RAM are extracted by using the signature, string, and header-footer searching methods. Applications encrypt their data using certain techniques in RAM. Some applications store their data in RAM without using encryption [26].

3.4.1 String Searching

String searching is an analysis process carried out on the RAM image. In this method, there is no need to use the data structures in the RAM image. ASCII and Unicode strings with special typing formats can be searched by selecting various search options within the RAM image [14].

The applications running on the operating system keep the user's data in RAM for a certain period of time without encryption. These data can be accessed from the RAM image by using the string searching method. The search is thus carried out by determining different string methods for each application. Sample strings created to be used for scanning for the username and password for social media accounts are given in Tab. 2 [27].

Table 2 Sample strings used for social media accounts.

Social Media	Accounts	Passwords
Gmail	&Email=	&Passwd=
Facebook	&email=	&pass=
Google+	&Email=	&Passwd=
Youtube	&Email=	&Passwd=
Twitter	&session%5Busername_or_email%5D=	&Session%5Bpassword%5D=

3.4.2 File Carving

File curving is known as a search-and-recovery process for terminated or deleted files stored as binary in RAM. The files used in the Windows operating system are stored in RAM between the header and footer signatures. The files in the RAM are extracted by scanning the header and footer signature. The header and footer signatures can be different depending on the version of the file types [28]. The header and footer signatures of various file types are given in Tab. 3.

Table 3 The signatures of header and footer

File Type	Header	Footer
PNG	89 50 4E 47 0D 0A 1A 0A	49 45 4E 44
JPEG	FF D8 FF	FF D9
JPG	FF D8 FF E0 00 10	FF D9
GIF	47 49 46 38 39 61	00 00 3B
PDF	25 50 44 46	25 25 45 4F 46
WORD	D0 CF 11 E0 A1 B1 1A E1 00 00	D0 CF 11 E0 A1 B1 E1 00 00
MP3	57 41 56 45	00 00 FF
XML	3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D 22 31 2E 30 22 3F 3E	-

Some file types do not leave footer signatures in RAM. For files that lack a footer signature, during the RAM image analysis, termination is performed by entering the maximum size after the header signature [29].

4 IMPLEMENTATION OF THE SOFTWARE

The software implementation is composed of two parts. In the first part, binary scanning is carried out using signature traces in RAM. The address ranges of the files are determined at the end of this scan. The files whose addresses in the RAM have been specified are then extracted to the disk through file carving. In the second part, the content is extracted from the recovered files. The XML string search method is used for MS Word files with the.docx extension, and the stream decode method is used for the files with .pdf and .doc extensions to extract content. The operating model of the implemented software is given in Fig. 5.

The RAM image used in the analysis process was acquired using the image acquisition software developed within the scope of this study. The study was carried out for a RAM image of 14 GB in the system given in Tab. 4. The address range of the image is 0 × 000000000000 h and 0 × 36EFFF904 h.

Table 4 System data about RAM image

Experimental System	
OS	Windows 10 64 Bit
RAM	12 GB
Page File	2 GB
CPU	Intel i7 7300U 2.90 Ghz

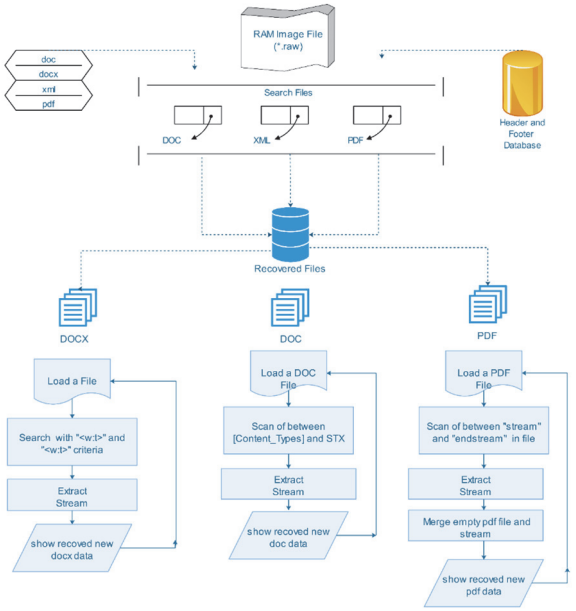

Figure 5 The operating model of the software

4.1 Signature Database

MS Word and PDF files can leave different signatures in RAM depending on their versions. For a complete scanning of the RAM image, all signatures of MS Word and PDF files need to be scanned. The textual data of the MS Word files with .docx extension is saved in *document. xml* file. Therefore, xml files were also added to the signature scan. As shown in Fig. 6, all signatures for the files with .doc, .xml, and .pdf extensions are collected in the source database named source.a2s. The signatures to be scanned when the software is running are loaded into the system.

```
// ----Word Files Header and Footer---
Header:50 4B 03 04/Footer:
Header:50 4B 03 04 14 00 06 00 Footer:D0 CF 11 E0 A1 B1 1A E1 00 00
Header:D0 CF 11 E0 A1 B1 1A E1 00 Footer: 00 D0 CD 11 E0 A1 B1 1A E1 00 00
// ----PDF Files Header and Footer—
Header:25 50 44 46 Footer:25 25 45 4F 46
// ----XML Files Header and Footer---
Header:3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D 22 31 2E 30 22 3F 3E Footer:
Header:3C 3F 78 6D 6C Footer:
Header:FF FE 3C 00 52 00 4F 00 4F 00 54 00 53 00 54 00 55 00 42 Footer:
```

Figure 6 The signatures for MS Word, XML and PDF files

4.2 File Carving

The header and footer signatures in the signature file loaded into the system are used to identify the structure of the files and their addresses in the RAM. The developed software searches for signatures in each byte of the RAM image file. The beginning address for the header signature and the end address for the footer signature are specified. As in the scanning result given in Fig. 7, the data between the beginning and the end addresses are transferred to the file generated in binary structure.

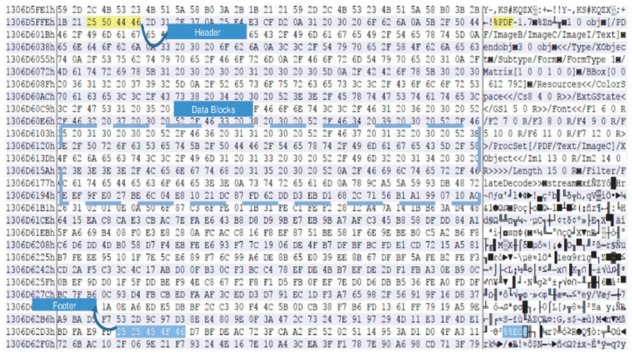

Figure 7 Signature scan for a PDF file

Some of the files do not have a footer signature. In this case, the address range is determined by specifying the maximum size after the header signature.

Since there are losses in the structures of the MS Word and PDF files which are recovered by file scraping method, the recovered files cannot be open. Stream decode method should be used for the files with pdf and doc extensions and string search method should be used for the files with docx extension.

4.3 DOC Stream Decoder

A Word file with .doc extension is encrypted by dividing it into 7 parts. The data in the file is located in the WordDocument section. The WordDocument block in the file begins with the (Content_Types) tag. As shown in Fig. 8, the encrypted data in the file is extracted from the addresses between the beginning and the STX tag.

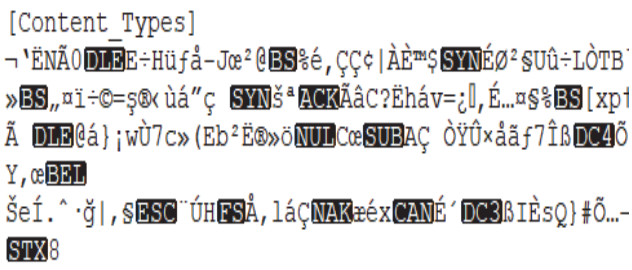

Figure 8 An encoded MS Word file with doc extension

The encrypted data blocks in the scraped MS word file with doc extension are decoded by using Codepage 1252 in the C# programming language. The code block used for the decoding operation is shown in Fig. 9.

```
doc_Stream.Read(fib, 0, 1472);
byte[] bytes_Text = new byte[cb];
doc_Stream.Read(bytes_Text, bytes_Text.Length, finish_offset);
Encoding encoding = Encoding.GetEncoding(1252);
text += encoding.GetString(bytes_Text);
```

Figure 9 Decoding operation for encrypted data by using Codepage1251

4.4 DOCX String Searching

The textual data in the recovered MS Word and XML files from the RAM image are stored in <x:w> and <w:tbl>

tags in the XML tree structure. The data stored between the tags are not encrypted. Separate string searches are carried out for all the files some of which are shown in Fig. 10.

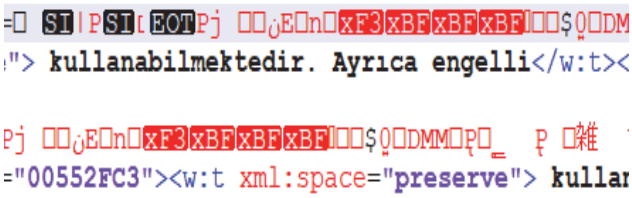

Figure 10 The text view of the scraped file

At the end of this scan, the resulting data is also transferred to the text files. The comparison of the original file to the recovered data is given in Fig. 11.

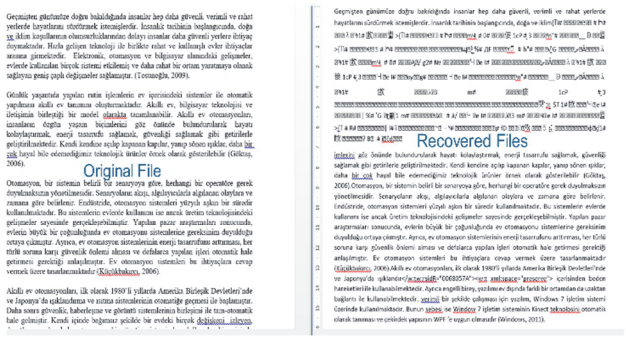

Figure 11 The comparison of the original MS Word file to the recovered MS Word file

4.5 PDF Stream Decoder

When the PDF files are loaded into the RAM, the data in them are encoded by using digital encryption techniques. In order to collect the contents of the recovered PDF files, the encryption method applied to the file needs to be known.

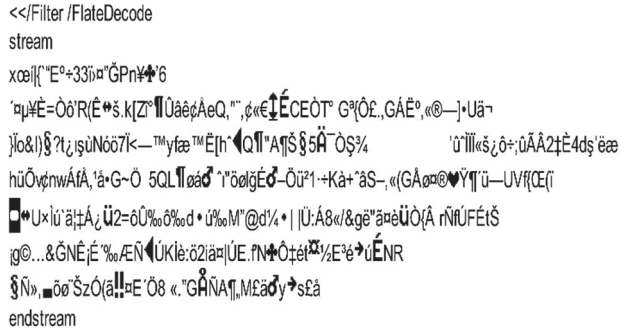

Figure 12 An encoded PDF file

As seen in Fig. 12, the applied method can be accessed by using the Filter tag. The data in the PDF file are encoded between the *stream* and *endstream* blocks. The recovered data in the study are placed in data blocks in a blank PDF file to be decoded. When the PDF file is opened in Windows, the data are automatically decoded and the content is displayed.

5 RESULTS

Four different image files were used by the implemented software. The MS Word and PDF files were scraped from these image files. As seen in Tab. 5, the PDF files were recovered in a period between 23 and 37 minutes, depending on the size of the image file. The scanning time for MS Word files was between 17 and 45 minutes. Since XML files are also included in the scanning process, the duration of scanning MS Word files is longer.

Table 5 Period of scraped PDF and Word files

	Elapsed Time		
Total Image File Size	PDF	Word (.docx)	Word (.doc)
4 GB	23 m 17 s	32 m 25 s	17 m 03 s
6 GB	28 m 54 s	36 m 25 s	30 m 52 s
10 GB	32 m 03 s	39 m 23 s	39 m 12 s
14 GB	37 m 45 s	45 m 01 s	41 m 10 s

The files scraped from the 14 GB RAM image are used in recovering data in the MS Word and PDF files. This image file was acquired by using the developed RAM image acquisition software. 10 files for each of the .doc, .docx, and .pdf extensions which were previously opened and terminated in the operating system have been included in the analysis. The analysis process is carried out by the software developed by using the C# programming language.

The data in the Word files with the .doc extension were decoded by using codepage1252. The comparison of the recovered data with the original file is given in Tab. 6. The success rate was over 50% for the files under the size of 300 KB. As the file size increases, the recovery rate of the data decreases. In the end, the recovery rate of the data in 10 MS Word files with the .doc extension was 35.6%.

Table 6 Recovery analysis for the Word (.doc) files

Document	Total Size / KB	Recovered File Size / KB	Recovered Text Size / KB	%
DOC1	100	56	50	50.0
DOC2	180	160	120	66.7
DOC3	205	200	110	53.7
DOC4	270	201	140	51.9
DOC5	490	350	143	29.2
DOC6	672	600	300	44.6
DOC7	730	540	103	14.1
DOC8	750	590	130	17.3
DOC9	840	400	102	12.1
DOC10	1.205	900	201	16.7
			Avg / %	35.6

The comparison of the data recovered by string searching in the scraped file with the .docx extension to the original file is given in Tab. 7. The average success rate in the recovery of the data in the MS Word files.

The data in the PDF files are encrypted by FlateDecode. The date was accessed by decoding each block in the recovered data. The recovery rates for the 10 PDF files can be seen in Tab. 8. According to these figures, the recovery rate for the PDF files under the size of 250 KB is over 50%. The recovery rate for the data in the files over the size of 250 KB ranges between 8.6% and 17.4%.

MS Word and PDF files in the operating system that have been terminated continue to stay in RAM data structures. However, the addresses of newly opened files may conflict with the addresses of previous MS Word and PDF files. This conflict causes the deletion of the data belonging to terminated MS Word and PDF files.

Each paragraph within PDF files is encrypted in a separate data block by FlateDecode. The loss of 1 byte in the encrypted data blocks during the carving process

prevents the recovery of the data in the block. The losses in the encrypted blocks result in a lower recovery rate for PDF file data.

Table 8 Recovery analysis for the PDF files

Document	Total Size / KB	Recovered File Size / KB	Recovered Text Size / KB	Rate / %
PDF1	158	149	60	38.0
PDF2	244	200	76	31.1
PDF3	298	290	52	17.4
PDF4	305	251	40	13.1
PDF5	561	352	43	7.7
PDF6	630	427	54	8.6
PDF7	728	549	103	14.1
PDF8	757	520	67	8.9
PDF9	900	630	102	11.3
PDF10	1.056	900	107	10.1
			Avg / %	16.0

Different methods are applied to the files with .doc and .docx extensions during data recovery. The data in the files with .docx extension is stored in the XML structure without encryption. Therefore, the data in the scraped files are accessed through string searching. The data blocks in the files with the ,doc extension are encrypted by codepage1252. Therefore, encrypted data needs to be decoded to recover data in the files with the .doc extension.

Studies can be carried out to improve the performance and data recovery success rates of developed forensic software. Extending the signature database used in the proposed software will enable more MS Word and PDF files to be engraved. In addition, by increasing the features of the hardware where the engraving process is performed, accelerating the processes performed on the GPU will reduce the engraving times. The decoding of compressed data blocks in data recovery software can be strengthened with character-based reverse-engineering algorithms. As a result, it can be expected that the data recovery success rate will increase.

Table 7 Recovery analysis for the Word (.docx) files

Document	Total Size / KB	Total Text Blocks	Total Paragraphs	Recovered File Size / KB	Recovered Text Size / KB	Rate / %
DOCX1	38	22	20	23	12	52.2
DOCX2	47	31	27	28	14	50.0
DOCX3	58	42	32	45	21	46.7
DOCX4	87	46	34	28	17	60.7
DOCX5	120	51	45	34	19	55.9
DOCX6	145	76	65	66	32	48.5
DOCX7	236	89	71	80	21	26.3
DOCX8	350	91	75	120	29	24.2
DOCX9	3.512	156	130	320	80	25.0
DOCX10	5.200	280	213	824	120	14.6
					Avg / %	40.4

6 CONCLUSION

When a process is terminated in the Windows operating system, the address information of the process is deleted. However, data belonging to the process are not deleted in RAM data structures. It is possible to access these data by file scraping and data recovery methods to be made in the RAM image. The software has been developed for scraping MS Word and PDF files from the RAM image to be used in forensic informatics. Because the small size of the image file to be scraped reduces the access rate to deleted files, a 14 GB image file was selected. With the proposed software, 10 PDF, DOC, and DOCX files randomly selected from the 14 GB RAM image were compared with the data in their original files. As a result of the comparison, the recovery success rate was obtained for each file.

For future studies, it is planned to increase the success rate of the recovered data by applying different carving techniques and algorithms in the developed software.

Acknowledgments

I would like to express my greatest gratitude to Süleyman Demirel University Scientific Research Projects Coordination Unit Board of Management, who supported this study with the project numbered 5035-D1-17.

7 REFERENCES

[1] Varol, A. & Sönmez, Y. Ü. (2017). Review of evidence collection and protection phases in digital forensics process. *International Journal of Information Security Science*, *6*(4), 39-46.

[2] Al-Sharif, Z. A., Bagci, H., & Asad, A. (2018). Towards the memory forensics of ms word documents. *Information Technology-New Generations*, 179-185. https://doi.org/10.1007/978-3-319-54978-1

[3] Ali, R. R., Mohamad, K. M., Jamel, S. A. P. I. E. E., & Khalid, S. K. A. (2018). A review of digital forensics methods for JPEG file carving. *Journal of Theoretical and Applied Information Technology*, *96*(17), 5841-5856.

[4] Joseph, P. & Norman, J. (2019). Forensic corpus data reduction techniques for faster analysis by eliminating tedious files. *Information Security Journal: A Global Perspective*, *28*(4-5), 136-147. https://doi.org/10.1080/19393555.2019.1689319

[5] Lewis, N., Case, A., Ali-Gombe, A., & Richard III, G. G. (2018). Memory forensics and the Windows Subsystem for Linux. *Digital Investigation*, (26), S3-S11. https://doi.org/10.1016/j.diin.2018.04.018

[6] Case, A. & Richard III, G. G. (2017). Memory forensics: The path forward. *Digital Investigation*, (20), 23-33. https://doi.org/10.1016/j.diin.2016.12.004

[7] Didier, S. (2017). See: https:// blog. didierstevens.com /2008 /05 /19 /pdf-stream-objects/

[8] Dolan-Gavitt, B. (2007). The VAD tree: A process-eye view of physical memory. *Digital Investigation*, *4*, 62-64. https://doi.org/10.1016/j.diin.2007.06.008

[9] Halderman, J. A., Schoen, S. D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J. A., & Felten, E. W. (2009). Lest we remember: cold-boot attacks on encryption keys. *Communications of the ACM*, *52*(5), 91-98. https://doi.org/10.1145/1506409.1506429

[10] Hejazi, S. M., Debbabi, M., & Talhi, C. (2008). Automated windows memory file extraction for cyber forensics

investigation. *Journal of Digital Forensic Practice*, *2*(3), 117-131. https://doi.org/10.1080/15567280802552829
[11] Hejazi, S. M., Talhi, C., & Debbabi, M. (2009). Extraction of forensically sensitive information from windows physical memory. *Digital Investigation*, *6*, S121-S131. https://doi.org/10.1016/j.diin.2009.06.003
[12] Hu, L., Zhang, X., Wang, F., Wang, W., & Zhao, K. (2012). Research on the Architecture Model of Volatile Data Forensics. *Procedia Engineering*, *29*, 4254-4258. https://doi.org/10.1016/j.proeng.2012.01.653
[13] Microsoft. See: https://support.office.com/tr-tr/article/Open-XML-Bi%C3%A7imleri-ve-dosya-ad%C4%B1-uzant%C4%B1lar%C4%B1-5200d93c-3449-4380-8e11-31ef14555b18
[14] Okolica, J. & Peterson, G. L. (2011). Extracting the windows clipboard from physical memory. *Digital investigatio*n, *8*, S118-S124. https://doi.org/10.1016/j.diin.2011.05.014
[15] Pena, A. J. & Balaji, P. (2014). Toward the efficient use of multiple explicitly managed memory subsystems. *2014 IEEE International Conference on Cluster Computing (CLUSTER*), 123-131. https://doi.org/10.1109/CLUSTER.2014.6968756
[16] Petroni Jr, N. L., Walters, A., Fraser, T., & Arbaugh, W. A. (2006). FATKit: A framework for the extraction and analysis of digital forensic data from volatile system memory. *Digital Investigation*, *3*(4), 197-210. https://doi.org/10.1016/j.diin.2006.10.001
[17] Poisel, R., Tjoa, S., & Tavolato, P. (2011). Advanced file carving approaches for multimedia files. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *2*(4), 42-58.
[18] Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. (2016). Current challenges and future research areas for digital forensic investigation.
[19] Quina, G. N., Díaz, J., Park, S. G. Y., & Piccirilli, D. (2017, June). Data restoration and file carving. *12th Iberian Conference on Information Systems and Technologies (CISTI*), 1-5. https://doi.org/10.23919/CISTI.2017.7976035
[20] Ravi, A., Kumar, T. R., & Mathew, A. R. (2016). A method for carving fragmented document and image files. *2016 International Conference on Advances in Human Machine Interaction (HMI)*, 1-6. https://doi.org/10.1109/HMI.2016.7449170
[21] Thongjul, S. & Tritilanunt, S. (2015). Analyzing and searching process of internet username and password stored in Random Access Memory (RAM). *12th International Joint Conference on Computer Science and Software Engineering (JCSSE)*, 257-262. IEEE. https://doi.org/10.1109/JCSSE.2015.7219806
[22] Van Baar, R. B., Alink, W., & Van Ballegooij, A. R. (2008). Forensic memory analysis: Files mapped in memory. *Digital investigation*, *5*, S52-S57. https://doi.org/10.1016/j.diin.2008.05.014
[23] Vidas, T. (2007). The acquisition and analysis of random access memory. *Journal of Digital Forensic Practice*, *1*(4), 315-323. https://doi.org/10.1080/15567280701418171
[24] Adobe (2017). See: https://acrobat.adobe.com/tr/tr/why-adobe/about-adobe-pdf.html
[25] Vidas, T. (2010). Volatile memory acquisition via warm boot memory survivability. *43rd Hawaii International Conference on System Sciences*, 1-6. https://doi.org/10.1109/HICSS.2010.439
[26] Vömel, S. & Freiling, F. C. (2011). A survey of main memory acquisition and analysis techniques for the windows operating system. *Digital Investigation*, *8*(1), 3-22. https://doi.org/10.1016/j.diin.2011.06.002
[27] Vömel, S. & Stüttgen, J. (2013). An evaluation platform for forensic memory acquisition software. *Digital Investigation*, (10), S30-S40. https://doi.org/10.1016/j.diin.2013.06.004
[28] Zhang, L., Zhang, D., & Wang, L. (2010). Live digital forensics in a virtual machine. *International Conference on Computer Application and System Modeling (ICCASM 2010)*, *4*, V4-328. https://doi.org/10.1109/ICCASM.2010.5620364

Contact information:

Kubilay TAŞDELEN, PhD, Assistant Professor
Department of Electrical Electronics Engineering,
Isparta University of Applied Sciences,
32050, Isparta, Turkey
E-mail: kubilaytasdelen@isparta.edu.tr

Ahmet Ali SÜZEN, PhD
(Corresponding author)
Department of Information Security Technology,
Isparta University of Applied Sciences,
32050, Isparta, Turkey
E-mail: ahmetsuzen@isparta.edu.tr