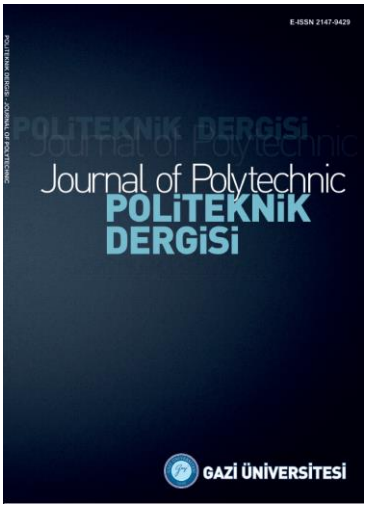

POLİTEKNİK DERGİSİ

JOURNAL of POLYTECHNIC

ISSN: 1302-0900 (PRINT), ISSN: 2147-9429 (ONLINE)
URL: http://dergipark.gov.tr/politeknik

Recovering multimedia files from a memory image

Geçici bellek yansımasından çoklu ortam dosyalarının kurtarılması

Yazar(lar) (Author(s)): *Ahmet Ali SÜZEN[1], Kubilay TAŞDELEN[2]*

ORCID[1]: 0000-0002-5871-1652

ORCID[2]: 0000-0002-2845-5643

Bu makaleye şu şekilde atıfta bulunabilirsiniz(To cite to this article): Süzen A. A. ve Taşdelen K., "recovering multimedia files from a memory image", ***Politeknik Dergisi***, 21(3): 731-737, (2018).

Erişim linki (To link to this article): http://dergipark.gov.tr/politeknik/archive

DOI: **10.2339/politeknik.417767**

Recovering Multimedia Files from a Memory Image

Araştırma Makalesi / Research Article

Ahmet Ali SÜZEN[1*], Kubilay TAŞDELEN[2]

[1]Department of Information Security Technology, Uluborlu Vocational School, Süleyman Demirel University, Isparta, Turkey

[2]Department of Electrical & Electronics Engineering, Faculty of Technology, Süleyman Demirel University, Isparta, Turkey

(Geliş/Received: 19.02.2018; Kabul/Accepted: 20.03.2018)

ABSTRACT

The widespread use of digital technologies increases the size of data stored in digital media. The increased amount of stored data also brings along data security risks. One of the most important risks in personal data security is the unauthorized or accidental data deletion. There are file recovery and carving software for recovering deleted files from the storage devices. Files must be loaded into RAM to be used in the operating system. These files are stored in RAM for a certain amount of time by the memory manager. Therefore, a file opened or deleted by the user in the operating system can be found in the RAM. File carving techniques must be applied to RAM to access these files.

In this study, the file carving and the performance values of the multimedia files carved by using different signature structures with file carving software from the RAM image were compared. In the study, carving has been performed with the header and footer signatures of the used and terminated multimedia files (JPG, PNG, GIF, BMP) used in Windows 10 operating system. In the carving process, file carving durations and carving success rates are extracted using different signature structures of the same file type. In the light of these results, the performance data of multimedia file types are evaluated according to the signature structures used. The RAM image retrieval and file carving software used in the study has been developed by us as a part of the Ph.D. project.

Keywords*:* Data recovery, file carving, multimedia files, RAM image.

Geçici Bellek Yansımasından Çoklu Ortam Dosyalarının Kurtarılması

ÖZ

Dijital teknolojilerin kullanımının yaygınlaşması, dijital ortamlarda saklanan veri boyutunu artırmaktadır. Depolanan verilerin büyümesi beraberinde veri güvenliği risklerini de getirmektedir. Kişisel verilerin güvenliğindeki en önemli risklerden biri verinin izinsiz veya yanlışlıkla silinmesidir. Depolama aygıtlarında silinmiş dosyaların kurtarılması için dosya kurtarma ve kazıma yazılımları bulunmaktadır. İşletim sisteminde dosyaların kullanılması için RAM' e yüklenmesi gerekmektedir. Bu dosyalar bellek yöneticisi tarafından belirli bir süre RAM'de saklanmaktadır. Bundan dolayı işletim sisteminde kullanıcı tarafından, açılmış veya silinmiş bir dosya RAM'de bulunabilmektedir. Bu dosyalara erişim için RAM'e dosya kazıma tekniklerinin uygulanması gerekmektedir.

Bu çalışmada geliştirilen dosya kazıma yazılımı ile farklı imza yapıları kullanılarak multimedya dosyalarının RAM imajından kazınmasına ve performans değerlerinin karşılaştırılması gerçekleştirilmiştir. Çalışmada Windows 10 işletim sisteminde kullanılmış ve sonlandırılmış multimedya dosyalarına (jpg, png, gif, bmp) ait header ve footer imzaları ile kazıma işlemi yapılmıştır. Kazıma işleminde aynı dosya türüne ait farklı imza yapıları kullanılarak, dosya kazıma süreleri ve kazıma başarı oranları çıkartılmıştır. Bu sonuçlar doğrultusunda multimedya dosya türlerinin, kullanılan imza yapısına göre performans verileri değerlendirilmiştir. Çalışma kapsamında kullanılan RAM imajı alma ve dosya kazıma yazılımları doktora projesi kapsamında tarafımızdan geliştirilmiştir.

Anahtar Kelimeler: Dosya kazıma, çoklu ortam dosyaları, ram imajı, veri kurtarma

1. INTRODUCTION

Along with the improvement of the digital technology, users now store their data in digital media. Therefore, the size of the stored data has been rapidly increasing [1].

The increase in the amount of the stored data also creates the risks of personal data security. The most important of these risks is the unauthorized or accidental deletion of the data [2]. There are file recovery and carving software for recovering deleted files from the storage devices [3].

When the user wants to open a file, the operating system first loads the file into RAM before opening it. The requested file is displayed to the user via RAM [4]. These files are stored in RAM for a certain amount of time. Therefore, a file opened or deleted by the user in the operating system can be found in the RAM [5]. To access these files, file carving techniques are utilized on RAM. In order to perform file carving on the RAM, firstly, a

**Sorumlu yazar (Corresponding Author)*
e-mail: ahmetsuzen@sdu.edu.tr

copy of the file must be taken. Carving process is carried out on this copy.

In order to acquire RAM image used in the study, Kernel Mode RAM software is utilized. Kernel Mode image acquisition software provides the image of RAM in Windows 8, 8.1, and 10 operating systems. The fact that the size of the memory acquisition in RAM is low prevents the data losses caused by address conflicts in RAM. This is why Kernel Mode RAM image acquisition software, which occupies 156 KB of RAM, has been preferred. The software used has been developed as a part of the Ph.D. project.

In this study, the comparison of the performance values of the carving software used to scrape multimedia files from a RAM image of 14GB is performed. In the carving process, file carving durations and recovery success measurements are conducted using different signature structures of the same file type. At the same time, the carving durations of different multimedia files are compared. With these results, multimedia file types and carving durations to be obtained from RAM have been presented.

2. RELATED WORK

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 [5-7]. String searching, signature scanning, file carving, and data structure analysis methods are used to recover data from the RAM image [7-8]. 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 [8]. 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 [9].

3. BACKGROUND

3.1. File Carving

The file carving is known as the process of searching and extracting the files loaded into RAM by the operating system to the disk. In the Windows operating system, the files are stored between the header and the footer signatures when they are loaded to RAM [10]. Therefore, the header and footer signatures are used to carve the files in the RAM. There can be different header and footer signatures depending on the versions of the file types used by the operating system [11]. All the signatures of the requested file need to be known in order to perform the carving process. Sample header and footer signatures of different file types are shown in Table 1 [12].

Table 1. Signature samples for PNG, JPG and GIF files

File	Header	Footer
PNG	89 50 4E 47 0D 0A 1A 0A	49 45 4E 44
JPG	FF D8 FF	FF D9
GIF	00 00 3B	47 49 46 38 39 61

It is necessary to know the structures of the RAM in order to extract the multimedia files from the image with the file scraping technique. File size information is written along with signature labels when visual elements are loaded into RAM in the operating system. This size information is used to identify the last addresses of files that are not footer-signed or deleted in RAM. Figure 1 shows the structural view of JPG file in RAM.

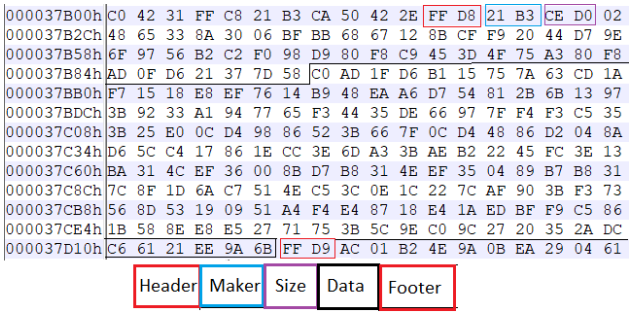

Figure 1. Structure in RAM of JPG files

3.2. File Carving Software

The file carving software is a digital forensics software developed to recover files from RAM images by string search and data extraction techniques in Windows operating systems. In order for this software to perform the carving process, a binary-format image file obtained from RAM is used. The format of this image file has the extension of "raw". The file carving software has been developed by us as a part of our Ph.D. study.

Windows operating system does not provide access to the terminated file. The Windows memory manager needs to be stopped in order to erase the finished file. Therefore, it is necessary to take an image of RAM for scraping and scanning. The developed software installs a RAM driver on the system to acquisition the RAM image. The driver provides access to all addresses of the RAM. Image acquisition software copies the entire contents of RAM to disk via this driver. All the addresses and addresses in the image file are bit-for-bit scanned. Blocks matching the header and footer tags of the multimedia files in the signature database are inserted into the temporary memory. After the carving process is finished, the data blocks stored in the memory are converted to file formats and recorded in a disk. Figure 2 shows the model of RAM image taking and scratching process in Windows operating system.

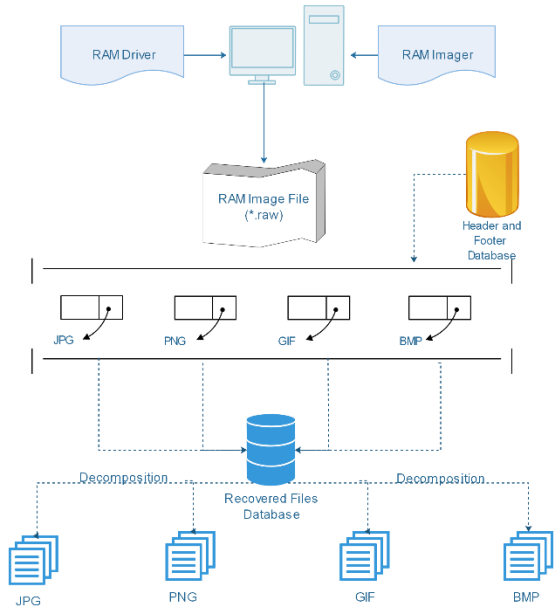

Figure 2. A process modeling of file carving

4. IMPLEMENTING FILE CARVING PROCESS

4.1. Defining the Carving Parameters

To start the process with the file carving software, the image file to be to be scraped should be obtained. The image file used in the study is obtained from the system whose specifications are given in Table 2. The size of the obtained image file is 14 GB. The RAM image was taken from the computer that was actively used for about 2 hours.

Table 2. The information of the system where the image was obtained.

System Used	
OS System	Windows 10 (64 Bit) Version 1709
RAM	12 GB
Pagefile.sys	2 GB
CPU	Intel i7 7300U 2.90 Ghz

Header and footer signatures of the multimedia files used in the carving process are given in Table 2. It is mandatory to have a header tag in the signatures of multimedia files. However, not all the files have footer signatures. In such cases, the estimated size value is entered according to the file type by using the header address as the beginning point. The end of the footer address of the file is estimated according to the defined size. In the study, the size of 3 MB was taken in the files without footer signatures in the carving process.

In the carving process, as shown in Table 3, 5 different signature structures are used for the files with "PNG, JPG, and BMP" extensions, and 4 different signature structures are used for the files with "GIF" extension.

Table 3. Signatures used in file carving

Dosya	Header	Footer
PNG	**(1)** 89 50 4E 47 0D 0A	49 45 4E 44
	(2)1A 0A	-
	(3) 89 50 4E 47	-
	(4) 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D	-
	(5) 49 48 44 52	-
JPG	**(1)** FF D8 FF	FF D9
	(2) FF D8 FF E0	FF D9
	(3) FF D8 FF E0 00 10	
	(4) FF D8 FF E1 4E D8	
	(5) 45 78 69 66 00 00 49 49	
GIF	**(1)** 00 00 3B	47 49 46 38 39 61
	(2) 47 49 46 38	00 3B
	(3) 47 49 46 38 39 61	00 00 3B
	(4) 47 49 46	-
BMP	**(1)** 42 4D	-
	(2) FF FF 00 01 64 00	-
	(3) 00 00 03 00	-
	(4) 02 00 00 00	-
	(5) 42 41	-

4.2. Files Carving

The image file and the signature database must be entered as parameters for the file carving software to start the scraping process with the signature structures. The required sequence for the scraping software to run through the command line is given in the number 1 notation.

filecarving.exe /-test.raw /-database.a2s (1)

The process of extracting multimedia files from the image as shown in Figure 3; Reading the contents of the image file, finding the addresses of files based on the signature ranges, copying the data within the addresses and extracting them according to the extension of the files. However, in order to shorten the period of carving; each file type is executed synchronous on separate threads.

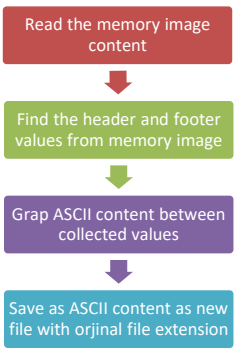

Figure 3. Processing model of file carving software

File carving software scans the image file in memory for each header signature. The addresses that correspond to the signature are kept in generic according to the formula shown in Equation 2 for the footer scan. File types with the footer signature are identified by the file address range, which is mapped to header addresses and added to the queue. For file types with no footer signature, a closing address is made with a 3MB displacement over the header address reference. At the last stage, the data between all the address ranges in the queue is scraped from the image file.

$$\forall x \in [0, l] \rightarrow y = y_0 + x \quad (2)$$

l = the total image file length.

x = the file offset.

y_0 = coordinate.

4.3. Extracting Multimedia Files

The carving process is performed after the entry of the parameters required for running the software. The carving software is used on the system given in Table 2. 532 multimedia files were accessed at the end of carving process for various file types within the 14 GB image file by using the file carving software in 38.23 minutes. Carving to determine carving times according to file types; performed synchronous with 4 threads. The sample files that are carved are shown in Figure 4.

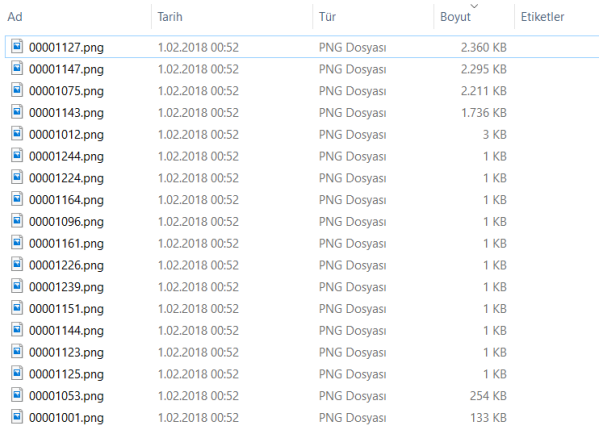

Figure 4. Files acquired at the end of carving process

4.4. Evaluation of Carving Results

It is observed that the different signature structures used for multimedia file types do not affect the carving duration. The carving times obtained during the carving process for the different signature types of the multimedia files are given in Table 4.

Table 4. Carved files according to signature types

	Used Signature Types					
	1	**2**	**3**	**4**	**5**	**Total**
JPG	78	2	16	24	0	120
PNG	1	3	14	0	0	18
GIF	127	122	78	11	---	338
BMP	12	24	1	8	11	56
				∑ Total		**532**

At the same time, the carving by using different signature structures different to the file in the carving process increases the result as seen in Table 5. In the carving process, the last number of threads in T3 is ended. The end time of thread T3 is 38.23 min. During this time, the software provides the total carving time. Because of the difference in the sizes of the files obtained through carving, the carving times also differentiate. Increasing the carving period positively affects the increase of the number of carved files and the file size.

Table 5. Carving durations according to signature types

	ID	Used Signature Types					
		1	**2**	**3**	**4**	**5**	**∑ m**
JPG	P1	14,12	2,33	3,45	8,66	0,40	28,96
PNG	P2	0.20	0.4	10	0,36	0,37	10.73
GIF	P3	14,54	15,22	5,01	3,46	---	38,23
BMP	P4	6,02	14,11	0,18	3,51	2,48	26,30

In the study, 10 PNG, JPG, GIF, and BMP files were taken as samples from 532 files in order to determine the recovery success rate of files carved from the RAM image. The sample files were selected among the multimedia files whose original files were detected. The success rates for accessing PNG files from the image file are given in Table 6. Accordingly, an average of 98% success rate has been achieved in PNG files. As shown in Table 7, a 95% success rate has been achieved for JPG files. Since the GIF files are usually small in size within the operating system, it resulted in 99% success rate as shown in Table 8. Finally, the success rate of BMP files is 95% as given in Table 9. As a result, the overall success rate of the multimedia files is 96.99%.

5. CONCLUSION

In the study, carving by using a file carving software and assessment of carving performance for various multimedia files have been performed. JPG, PNG, GIF, and BMP files, which are more commonly used by the users in Windows operating system, have been selected. The carving results have been compared by using different signature structures of these multimedia files. In total, 532 files were extracted from the RAM image in 38.23 minutes. The following conclusions have been drawn from the data obtained from this study. Each multimedia file is carved on average 4.31 second from the 14 GB image file.

- Using different signature structures for each file increases the total number of carved files.
- Different signature types do not affect the file carving duration.
- Increasing the estimated size of the files that do not have footer signatures affects the recovery rate of files positively.

- Different signatures of file types do not affect the success rate of file recovery.
- The total carving time can be reduced by increasing the number of simultaneous operations in the carving software.

The number of carving obtained from the developed software is compared with the commercial software's used in the field of computer forensics. Comparison of software is made using their signature files and the same image file. The resulting carving numbers are given in Table 10.

Table 10. Comparison of file carving counts

Used Software	Image Size	Carved Files	Rates (%)
Forensic Explorer	14 GB	610	98.34
Carving Software	14 GB	532	96.99
EnCase	14 GB	497	95.09
X-Ways Forensics	14 GB	451	87.27

To increase the success rate obtained from file carving software; Smart carving, Bifragment Gap carving, Encrypted Volume carving methods must be implemented. To increase the number of files that are excavated, the signatures used for multimedia files need to be increased. In the next study, the implementation of methods and techniques to improve the performance of the software will occur. Thus, the developed software is intended to demonstrate the same performance as commercial 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.

REFERENCES

[1] Law, Frank Y.W., K.P. Chow, Michael Y.K. Kwan, and Pierre K.Y. Lai., "Consistency Issue on Live Systems Forensics", ***IEEE Future Generation Communication and Networking (FGCN)***: 136–40, (2007).

[2] (KJ) Kuchta and Kelly J., "Forensic Methodologies: A Computer Forensic Professional's Compass!", ***Information Systems Security*** 10(6): 42–49, (2002).

[3] Zanoni, M., Perin, F., Fontana, F. A., and Viscusi, G., "Pattern detection for conceptual schema recovery in data-intensive systems", ***Journal of Software: Evolution and Process***, 26(12), 1172–1192, (2014).

[4] Povar, D., and Bhadran, V. K., "Forensic data carving. In Lecture Notes of the Institute for Computer Sciences, ***Social-Informatics and Telecommunications Engineering***, 53:137–148, (2011). https://doi.org/10.1007/978-3-642-19513-6_12

[5] Al-sharif Z. A, Bagci H and Asad A., "Towards the Memory Forensics of MS Word Documents", ***Information Technology - New Generations***, 558: 179–85, (2018). doi:10.1007/978-3-319-54978-1.

[6] Burdach, M., "Digital forensics of the physical memory" ***Journal of the National Cancer Institute. Monographs***, 2013(47): (2013). https://doi.org/10.1093/jncimonographs/lgt036

[7] Hejazi, S. M., Talhi, C., and Debbabi, M., "Extraction of forensically sensitive information from windows physical memory", ***Digital Investigation, 6(SUPPL.)***, (2009). https://doi.org/10.1016/j.diin.2009.06.003

[8] Quina GN, Diaz J, Park SGY and Piccirilli D., "Data restoration and file carving [Restauración de datos y el File Carving]" ***Iber Conf Inf Syst Technol Cist,*** (2017). doi:10.23919/CISTI.2017.7976035.XXX

[9] Vömel, S., and Freiling, F. C., "A survey of main memory acquisition and analysis techniques for the windows operating system" ***Digital Investigation,***8:3-22,(2011). https://doi.org/10.1016/j.diin.2011.06.002

[10] Bui, S., Enyeart, M., and Luong, J., "Issues in Computer Forensics", ***Santa Clara University Computer*** Retrieved from http://www.cse.scu.edu/~jholliday/COEN150sp03/projects/Forensic Investigation.pdf, (2003).

[11] van Baar, R. B., Alink, W., and van Ballegooij, A. R., " Forensic memory analysis: Files mapped in memory", ***Digital Investigation***, 5(SUPPL.), 5:S52-S57, (2008). https://doi.org/10.1016/j.diin.2008.05.014

[12] Garcia, G. L., "Forensic physical memory analysis: an overview of tools and techniques", ***In TKK T-110.5290 Seminar on Network Security***, 207:305–320, (2007).

APPENDIX

Table 6. Recovery success rates of PNG files

	File Carving Software			Commercial Software		
	Original Files (KB)	**Carving Files (KB)**	**Rates (%)**	**Forensic Explorer**	**EnCase**	**X-Ways**
PNG 1	2.360	2.359	99,95762712	97,23	92	70,44
PNG 2	2.295	2.290	99,78213508	98,12	94,13	75,75
PNG 3	2.211	2.001	90,50203528	98,65	98,11	90,12
PNG 4	1.736	1.700	97,92626728	98,11	92,73	86,08
PNG 7	254	254	100	96,96	89,23	86,66
PNG 8	135	133	98,51851852	94,74	98,1	93,4
PNG 5	3	3	100	98	97,22	95
PNG 6	1	1	100	100	97,19	87
PNG 9	1	1	100	100	96,13	90
PNG 10	1	1	100	100	97,17	91
		AVG	**98,66865833**	**98,181**	**95,201**	**86,545**

Table 7. Recovery success rates of JPG files

	File Carving Software			Commercial Software		
	Original Files (KB)	**Carving Files (KB)**	**Rates (%)**	**Forensic Explorer**	**EnCase**	**X-Ways**
JPG 1	1.251	1.200	95,92326139	99,23	91,5	68,12
JPG 2	1.100	1.000	90,90909091	100	93	69,23
JPG 3	980	900	91,83673469	96,65	98,11	71,34
JPG 4	950	920	96,84210526	98,01	92,73	86,08
JPG 5	125	120	96	97,65	88,1	90
JPG 6	90	89	98,88888889	100	97,1	96,19
JPG 7	50	47	94	100	96,62	96,09
JPG 8	10	10	100	100	95,16	86,67
JPG 9	5	4,89	97,8	100	96,3	90,16
JPG 10	5	4	80	100	95,12	90,68
		AVG	**94,22000811**	**99,154**	**94,374**	**84,456**

Table 8. Recovery success rates of GIF files

	File Carving Software			Commercial Software		
	Original Files (KB)	**Carving Files (KB)**	**Rates (%)**	**Forensic Explorer**	**EnCase**	**X-Ways**
GIF 1	10	10	100	91,23	92	87,45
GIF 2	8	7,8	97,5	98,12	94,13	86,33
GIF 3	8	7,6	95	100	96,15	87,21
GIF 4	7	7	100	93,01	92,73	87,43
GIF 5	6	6	100	96,76	89,23	89,34
GIF 6	6	6	100	97,34	98,1	87,43
GIF 7	5	5	100	100	95,96	95,1
GIF 8	1	1	100	100	98,12	90,18
GIF 9	1	1	100	100	98,11	86,9
GIF 10	1	1	100	100	97,17	91,9
		AVG	**99,25**	**97,646**	**95,17**	**88,927**

Table 9. Recovery success rates of PNG files

	File Carving Software			Commercial Software		
	Original Files (KB)	**Carving Files (KB)**	**Rates (%)**	**Forensic Explorer**	**EnCase**	**X-Ways**
BMP 1	2.370	2.360	99,57805907	94,23	96,65	90,12
BMP 2	2.337	2.290	97,98887463	98,12	94,13	87,34
BMP 3	229	220	96,069869	100	97,67	90,5
BMP 4	175	173	98,85714286	98,06	90,12	80,68
BMP 5	144	140	97,22222222	97,06	92,65	86
BMP 6	135	133	98,51851852	96,34	98,1	90,12
BMP 7	12	10	83,33333333	100	96,56	96
BMP 8	11	10	90,90909091	100	97,19	88,28
BMP 9	10	10	100	100	96,13	92,65
BMP 10	10	9,6	96	100	97,17	90
		AVG	**95,84771105**	**98,381**	**95,637**	**89,169**