I. J. Computer Network and Information Security, **2018, 5, 1-8**
Published Online May 2018 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2018.05.01

Forensics Image Acquisition Process of Digital Evidence

Erhan Akbal
Digital Forensics Engineering, Technology Faculty, Firat University, Elazig, Turkey
E-mail: erhanakbal@firat.edu.tr

Sengul Dogan
Digital Forensics Engineering, Technology Faculty, Firat University, Elazig, Turkey
E-mail: sdogan@firat.edu.tr

Received: 10 February 2018; Accepted: 18 April 2018; Published: 08 May 2018

***Abstract*—**For solving the crimes committed on digital materials, they have to be copied. An evidence must be copied properly in valid methods that provide legal availability. Otherwise, the material cannot be used as an evidence. Image acquisition of the materials from the crime scene by using the proper hardware and software tools makes the obtained data legal evidence. Choosing the proper format and verification function when image acquisition affects the steps in the research process. For this purpose, investigators use hardware and software tools. Hardware tools assure the integrity and trueness of the image through write-protected method. As for software tools, they provide usage of certain write-protect hardware tools or acquisition of the disks that are directly linked to a computer. Image acquisition through write-protect hardware tools assures them the feature of forensic copy. Image acquisition only through software tools do not ensure the forensic copy feature. During the image acquisition process, different formats like E01, AFF, DD can be chosen. In order to provide the integrity and trueness of the copy, hash values have to be calculated using verification functions like SHA and MD series. In this study, image acquisition process through hardware-software are shown. Hardware acquisition of a 200 GB capacity hard disk is made through Tableau TD3 and CRU Ditto. The images of the same storage are taken through Tableau, CRU and RTX USB bridge and through FTK imager and Forensic Imager; then comparative performance assessment results are presented.

***Index Terms*—**Forensic copy, image acquisition, digital forensics, digital evidence.

I. Introduction

Digital forensics is the discipline that deals with all the process that includes collecting digital materials from the crime scene, examining, analyzing and reporting them according to certain standards and methods [1-5]. Digital forensics consists of four main steps: preparation, collection, analysis and reporting [6,7]. Collection is about accumulating digital evidence related with information technologies from the crime scene.

Digital devices store the data in internal and external storage devices. The stored data has to be taken with certain methods. Shadow copying only the criminal part of the stored data or all of it from a device is named as image acquisition (*IA*) [8]. For coming up to judicial image standards, the data has to be taken from write-protected devices (*W-PD*) and the image must be encrypted using techniques like MD5-SHA1. When the image is not taken from *W-PD*, integrity and trueness of the evidence may be destroyed. The hash value derived at the end of the *IA* process shows the matching of the image with the data from the original device [9]. The hash value that is calculated during the evidence collection assures the integrity and determinedness of the evidence until the end of evidence investigation process. For this reason, before starting to examine the forensic copy, the hash values have to be calculated and the forensic copy must be checked against the original evidence [10,11].

Direct analysis of digital evidences isn't considered appropriate because the data storage unit of the related device can break down and investigator can make a change on the evidence. For the forensics investigator, in order to assure the integrity of the evidence, a forensic copy must be taken [12]. Since it is not possible to take forensic copies from some devices live analysis can be a necessity. Then, the analysis report has to be detailed and it has to prove there has been no change on the evidence in order to assure the evidence integrity [13].

Investigators use various software tools (*ST*) and hardware tools (*HT*) while obtaining digital evidence. Write-protected tools (*W-PT*) that have different hardware characteristics enable us to structure different software acquisition formats and characteristics. Write-protection hardware tools (*W-PHT*) like Tablaeu, CRU and Solo-III are often used. FTK, Encase, Forensic Explorer, Prodiscover and Smart are the most frequently used *ST* [14,15].

There are a lot of studies about forensics image acquisition in literature. Nikkel [16] analyzed forensic acquisition process for magnetic tape technology. In this

Copyright © 2018 MECS

study, a method was proposed for acquisition and analyzing files of tape storage media. Hirwani [17] et al presented the process of forensics image acquisition and analysis in virtual machines. They were developed a procedure to examine virtual disk images. Casey [18] presented digital forensics procedures. He showed that the forensics image acquisition process should be done as soon as possible. He pointed out that volatile data must be retrieved, then the system must be shut down and the data must be copied to permanent storage devices. Nelson [19] et al showed that a forensic copy of a storage device needs to be bit-by-bit copy. They presented that the copy could be stored as a file on another device or as a drive on a disk.

In this study, hardware images are taken by means of CRU Ditto and Tableau TD3. Software images are also taken through CRU Ultradock, CRU RTX, and Tableau Bridge; then acquisition time, connection type and average transfer speed are presented comparatively. In the study both compressed and uncompressed hardware and software images are taken through the FTK Imager and Forensic Imager in E01 and DD raw format. The aims of this study:

- Comparing the *IA* times of CRU Ditto with Tableau TD3, the tools used for software *IA*.
- *IA* by the means of FTK Imager and Forensic Imager through the write-protection hardware (*W-PH*) and showing the effect of the software to the time of *IA*.
- Presenting the effect of hardware write-protected (*W-P*) bridge tools to the duration of *IA*.

II. Forensic Acquisition Process

For a digital material taken from the crime scene to be used as evidence, its integrity has to be protected. In legal laws of countries, there are clear issues about this point. The common feature of these substances is that the evidence for clarify the crime must be obtained in accordance with the law. It is also stated that the evidence obtained without the law will not be accepted by the legal authorities. Compliance with laws can only be fulfilled through proving that the evidence is examined as it was in its original situation and there has been no fabricating on it. For this, the image of the output taken from the acquisition tool during collection of digital evidences has to be identical with the original material. Besides, any fabricating evidence has to be detectable when wanted. Especially the *HT* satisfying the above-stated characteristics protect integrity of evidence.

A quantitative verification score is used during the acquisition process for testing the trueness of the evidence. This is a one-way function constituted by algorithms. During acquisition, the data and this value is signed together and thus in the event of any change in the data the value of this function also changes. Thus, the integrity and trueness of the data can be checked through comparing the first verification score with the following ones. One-way function provides irreversibility. Commonly used verification algorithms are MD (Message-Digest) series and SHA (Secure Hashing Algorithm) series.

Forensic copies are taken according to acquisition formats that are accepted in literature [20]. Image formats determine how the data derived from the evidence will be stored. DD, AFF, E01, NUIX, ProDiscover, SafeBack, Smart, XWays are some different image formats that are being used [20-22].

A. Hash Functions

Hash functions are used to assure the irreversibility and integrity of digital evidences. Hash functions derive a fixed-length hash value from the given data through mathematical methods that are contained in itself. The obtained hash value is unique and if there is a change in the data that is to be sent to the function, then the newly calculated hash value will also change. Hash value is stamp of the given data.

HT and *ST* of forensic image can calculate file, section, index and disk based hash values through using hash functions. Frequently used hash functions are MD2 (Message-Digest), MD4, MD5, SHA-0, SHA-1, SHA-256/224, SHA-384 and SHA-512 series algorithms [20,23].

- *MD series algorithms:* MD series algorithm is an algorithm series that produces 128-bit result. Passing the given data through algorithms that make mathematical transactions, MD series algorithms produces a 128-bit value. The algorithm is only one-way and the derived value is irreversible. There are three type of this algorithm: MD2, MD4 and MD5 [21,23].
- *SHA series algorithms:* SHA series algorithm is an encryption algorithm series that is developed by National Security Agency (NSA). It makes one-way encrypting. The process of algorithm is similar to MD series algorithms. The value it produces is 160 bit in SHA-0 and SHA-1; 224 bit in SHA-224; 256 bit in SHA-256, 384 bit in SHA-385 and 512 bit in SHA-512 [20,21]. It is commonly used in data integrity and authentication processes. While the data is divided to 512 bit pieces SHA-0 and SHA-1 algorithms, in other versions hash outputs are derived from 1024 and 512 bit pieces [20].

B. Forensic Acquisition Types

During forensic acquisition, type of the final output file has to be determined. *ST* and *HT* are compatible with different file types. The most commonly used file types DD (RAW), E01, AFF and SMART. Software and hardware tools are compatible with certain types. In the conclusion part of this study, compatibility of acquisition types with hardware and software is given in comparative form [24-26].

- *DD:* DD is also named as raw image type. It is means copying the data from the hardware bit by bit

Copyright © 2018 MECS

without being doctored. The copy size and the disk copied are equal. Besides, it doesn't store any metadata from the copy. Its file extension is DD.

- *E01:* E01 is the acquisition type used as Expert Witness Format (EWF) by Encase. This format allows segmented copy from the disk. During acquisition, the data is divided into segments. A control value is calculated for the segmented pieces and added to the data. Along with copied file, control value and verification scores are also obtained.
- *FF:* FF is known as Advanced File Format. The data to be duplicated and the header information that defines the data are stored together.
- *SMART:* It is the acquisition type derived by SMART, Linux based open-source software. It stores the data to be duplicated, header information and verification score altogether.

C. Forensic Acquisition Methods

During forensic *IA* different copy types can be taken by using hardware, software or firmware. Image types vary by the characteristics of the used *ST* or *HT*. In judicial cases, the type of acquisition may also vary by the legal arrangements of related countries. Certain countries demand copying certain parts instead of duplicating the whole storage unit considering the privacy of personal information. Besides, in order to examine the device related to the crime easier and more quickly it is possible not to take whole copy of the storage, case specifically. Forensic image formats being used for this purpose are Physical Driver, Logical Drive, Image File, Contents Folder and Fernico (CD/DVD). Physical driver image is copying the whole disk. Logical drive image is copying the logical parts (C, D, etc.) in the disk that are constituted during configuration of it. As for contents folder, it is acquisition of a certain part within the logical drive.

D. Forensic Acquisition Hardware and Software Methods

ST and *HT* are needed for *IA* of digital materials. It is features of *ST* and *HT* that provide judicial credibility. In order to conserve the integrity of the evidence, no typing can be done on it during acquisition process. For this reason, *W-PHT* have to be used. Certain *W-PHT* allow acquisition directly through the related hardware. Companies like Tableau, CRU and Solo have products that can only provide acquisition through hardware. Yet this kind of products cannot always be used because of their high costs. In such cases, *HT* that provide *W-P* interconnection and *ST* that provide *IA* from these *HT* are used all together. Thus, the cost is decreased to a large extent. MountImagepro, Encase Forensic Imager, Access Data FTK Imager and Xways Imager are the most frequently used *ST* for this purpose. *IA* is possible also without using physical hardware. A certain storage can be duplicated using just software and computer. However, the copies obtained via this method aren't generally considered judicially valid. If acquisition is done directly through computer's related connection interface without using *W-PH*, integrity of the evidence can be destroyed because the software will make reading and writing on the disk during acquisition operation. However, if judicial authorities can't get access to the certain examinations, software acquisition method is also being used.

Table 1. Classification of ST Frequently used in Digital Forensics

Software/Command		Programs
Licensed		Accessdata FTK Imager
		Encase Forensic Imager
		Xways Imager
		ProDiscover
		Forensic Imager
		Macrium Reflect
Open Sources	Programs	Clonezilla
		Guymager
		AIR – Automated Image and Restore
		Advanced Forensic Format Library (afflib)
	Commands	dd
		dcfldd
		sdd
		dd_rescue
		dc3dd

Copyright © 2018 MECS

- *Image Acquisition HT:* Forensic image acquisition *HT* are divided into two parts as embedded and bridges. It is possible to take the forensic copy directly through the hardware with the help of embedded devices. Copies of judicial devices that are properly connected to the hardware's connection interface can be taken with the help of configurations that are made from the web interface or those on the hardware. In this type of *IA*, there is no need to a computer or a separate software. As for *W-PHT* that are used as bridge, they vary by the type of proper connection interface that belongs to the device from which the copy is going to be taken. A computer and a hardware that will ensure the configuration of copy properties is a must for acquisition. Costs of integrated hardware are much higher than of bridge *HT*.
- *Image Acquisition ST:* Image acquisition *ST* provide an opportunity to operate depending on characteristics of *HT*. Many *ST* that are used for forensic purposes are developed in an attempt to communicate among *HT* in the lowest level. Thus, all the data on the evidence can be properly taken. *ST* that are developed close to the machine language level can interfere in all operating units of *HT*. Since this kind of *ST* are generally used by investigators or law enforcers, they are developed target-oriented. Acquisition *ST* can be examined in two groups as licensed and open source. Frequently used *ST* are shown in Table 1.

III. Method

In this study, performance of the used programs is evaluated through analyzing software and hardware *IA* processes. The examination is made on a PC with Intel I5-4460 CPU 3.2 GHz processor, 4 GB RAM and Windows 7 Professional 64 operating system. The hard disk of which image is taken is Western Digital 200 GB. In the image, there are

- Windows 7 Professional 64 bit
- Office Professional Plus 2010 64 bit
- Web browsers: Google Chrome, Internet Explorer, Safari, Opera, Mozilla Firefox
- Constant websites for all web browsers
- Chatting Software: WhatsApp Desktop, Viber Desktop, Facemessenger, Tictoc, Line
- Standard texts for chatting *ST*

In Figure 1 analysis environment image acquisition is given.

Fig.1. Analysis Environment

The image of this hard disk is taken through the following steps by using Tableau TD3, CRU Ditto and hardware RTX, CRU, Tableau bridges with the help of FTK Imager v3.4.2.6 and Forensic Imager v1.1.0. The hardware and software process steps are as follows.

Hardware image acquisition:

Step 1: Link the forensic device to Tableau/CRU Ditto through its Write-Blocked interface
Step 2: Link the storage unit in which the image is going to be saved to the device through the "Read-Write" interface
Step 3: Check whether both devices are identified by Tableau/CRU Ditto devices.
Step 4: Specify the settings during image acquisition
Step 5: Enter case specific cookies (case information, date, browser)
Step 6: Specify the image format (DD, E01)
Step 7: Choose the HASH type of the image (MD5, SHA1)
Step 8: Start the procedure

Hardware-Software image acquisition:

Step 1: Link the forensics tool to the device through RTX, CRU, Tableau bridges using "Write-Blocked" interface, and the "Read-Write" interface to the PC.
Step 2: Specify the image acquisition software and run (FTK Imager, Forensic Imager)
Step 3: Choose the image format with the image acquisition software (DD, E01, AFF, Smart)
Step 4: Enter the case information (case information, date, browser)
Step 5: Specify the key settings.
Step 6: Determine how many regions the image is going to be segmented.
Step 7: Determine zip settings of the image.
Step 8: Determine verify operation settings
Step 9: Start the procedure

The process of Hardware *IA* and Hardware-Software *IA* is given for definition 1-2, in Table 2 and 3, respectively.

Copyright © 2018 MECS

Table 2. The Bases Process of Hardware *IA* in Digital Forensics

	Definition 1
1/	*Determine the W-P SOFTWARE → depending on the physical type of the forensic device*
2/	*Link the device → WRITE-BLOCK interface*
3/	*Link the storage → READ-WRITE interface*
4/	*Check the storage unit*
5/	*Choose IA settings → General, Device Properties, etc.*
6/	*Enter the case information → Examiner, Case Number, etc.*
7/	*Choose the image format → DD, E01, etc.*
8/	*Choose the hash type → MD5, SHA1, etc.*
9/	*Start IA process*

Table 3. The Bases Process of Hardware-Software *IA* in Digital Forensics

	Definition 2
1/	*Specify the W-P HARDWARE → The physical type of the forensic device*
2/	*Determine IA SOFTWARE*
3/	*Link the device → WRITE-BLOCK interface (source)&&READ-WRITE interface (target)*
4/	*Start IA HARDWARE and SOFTWARE*
5/	*Choose the format of IA SOFTWARE*
6/	*Choose hash type → MD5, SHA1, etc.*
7/	*Enter the case information → Examiner, Case Number, etc.*
8/	*Decide encryption of image*
9/	*Decide segmented of image*
10/	*Decide compression of image*
11/	*Decide verification of image*
12/	*Start IA process*

IV. Results

Whenever there are a lot of digital materials that can be a crime, image acquisition times are very important. For investigators, the most important parameter is to start the analysis process by acquisition the forensic copy without the integrity and accuracy of the evidence. The time becomes a much more important parameter for digital investigation when the forensic copy needs to be taken from the crime scene. Therefore, selecting fast image acquisition tools will shorten the process considerably. In addition, the connection ports version on the device greatly affect duration of acquisition process. It is important to use the USB3.0 connection interface for this process.

In this study, image acquisition times of widely used tools are shown. In the first step of the running, a comparison among the talents of FTK, Forensic, Encase and Xway Imager is made and the results are given in Table 4.

Table 4. Comparison of *IA* HT

		FTK	Forensic	Encase	X way
Evidence Type	Physical	+	+	+	+
	Logical	+	+	+	+
	Image File	+	-	+	+
	Contents Folder	+	-	-	-
	Fernico Device (multiple CD/DVD)	+	+	+	+
Image Type	Raw	+	+	+	+
	Smart	+	-		-
	E01	+	+	+	+
	AFF	+	+		-
	Others	-	-	-	+
Fragmentation		+	+	+	+
Compression		+	+	+	+
Encryption		+	-	+	+
Image Mounting		+	-	+	+
Decrypt		+	-		+
Verify		+	+	+	-
Capture Memory		+	-	+	+
Hash	MD5	+	+	+	+
	SHA1	+	+	+	+
	SHA256	-	+	-	+
	Others	-	-	-	+

When Table 2 is taken into account, it can be said that the commonly used software FTK Imager is more efficient than other *ST* [22-26]. In the second step of the running the names of the *HT*, image types and source-target connection interface information are compared and presented in Table 5 and Table 6 [20,25-28].

Table 5. Properties of Acquisition *HT*

Duplicate Type	Hardware	Write Protection Interface	Target Interface	Image format	Hash	Compression
Hardware	Tableau TD3 Forensic Imager	USB, SATA, Expansion, Network	USB,SATA, Network	DD E01	MD5 SHA1	+
Hardware	CRU Ditto	IDE, USB, eSATA, Expansion, Network	Network, eSATA	DD E01	MD5 SHA1	+

Table 6. Properties of Hardware-Software Duplicator

Hardware	Write Protection Interface	Target Interface
Tableau SATA/IDE Bridge (T35U)	USB, IDE, SATA	USB 3.0
Digital Intelligence USB 3.0 Forensic Card Reader	xD, SD, MMC, MicroSD, Memory Stick, Compact Flash	USB 3.0
Tableau Forensic USB 3.0 Bridge (T8U)	USB 3.0	USB 3.0
Tableau Forensic SAS Bridge (TK6U)	SAS	USB 3.0
Tableau Forensic Firewire Bridge (TK9)	Fireware,USB 2.0	Fireware 800/400
CRU Wiebetech Forensic RTX	SATA	USB 3.0, SATA
CRU DataDiode	USB 3.0	USB 3.0
CRU USB Write Blocker	USB 3.0	USB 3.0
CRU Forensic UltraDock	SATA,IDE	USB 3.0, eSATA, FW800
CRU Media Write Blocker	Compact Flash, SD, XD	USB 3.0

In the last step of the running, considerations in the joint review according to the findings derived from hardware and software acquisitions are determined and the results are given in Table 7 and Table 8.

Table 7. Findings Derived during Hardware *IA*

Device	Format	Time	Verification Time	Average Transmission Rate	Interface Type
DITTO	E01	01.10.26	01.08.45	n/a	Sata
	DD	01.12.58	01.08.37	n/a	Sata
TABLEAU	E01	01.41.00		66.3 MB/sec	Sata
	DD	01.25.00		78.3 MB/sec	Sata

Table 8. Findings Derived during Software *IA*

Bridge	Program	Format	Image Type	Time	Average Transmission Rate	Size	Disc Interface	PC Interface Type
RTX	FTK Imager	E01	Compression - 0	01.12.12	n/a	186 GB	eSATA	USB 3.0
			Compression - Middle	01.08.57	n/a	186 GB	eSATA	USB 3.0
		DD		01.30.21	n/a	186 GB	eSATA	USB 3.0
	Forensic Imager	E01	Compression - 0	02.14.36	37.080	186 GB	eSATA	USB 3.0
			Compression - Middle	02.15.39	36.130	186 GB	eSATA	USB 3.0
		DD		01.18.48	42.306	186 GB	eSATA	USB 3.0
CRU	FTK Imager	E01	Compression - 0	01.03.20	n/a	186 GB	eSATA	USB 3.0
			Compression - Middle	01.02.14	n/a	186 GB	eSATA	USB 3.0
		DD		01.02.27	n/a	186 GB	eSATA	USB 3.0
	Forensic Imager	E01	Compression - 0	02.09.22	36.972	186 GB	eSATA	USB 3.0
			Compression - Middle	01.31.32	37.217	186 GB	eSATA	USB 3.0
		DD		01.17.04	43.511	186 GB	eSATA	USB 3.0
TABLEAU	FTK Imager	E01	Compression - 0	01.04.32	n/a	186 GB	eSATA	USB 3.0
			Compression - Middle	01.02.09	n/a	186 GB	eSATA	USB 3.0
		DD		01.03.09	n/a	186 GB	eSATA	USB 3.0
	Forensic Imager	E01	Compression - 0	01.30.27	36.858	186 GB	eSATA	USB 3.0
			Compression - Middle	01.30.57	36.655	186 GB	eSATA	USB 3.0
		DD		01.17.34	42.976	186 GB	eSATA	USB 3.0

Copyright © 2018 MECS

The durations measured with FTK Imager and Forensic Imager *ST* and through the devices CRU, TABLEAU and RTX are shown in Figure 2.

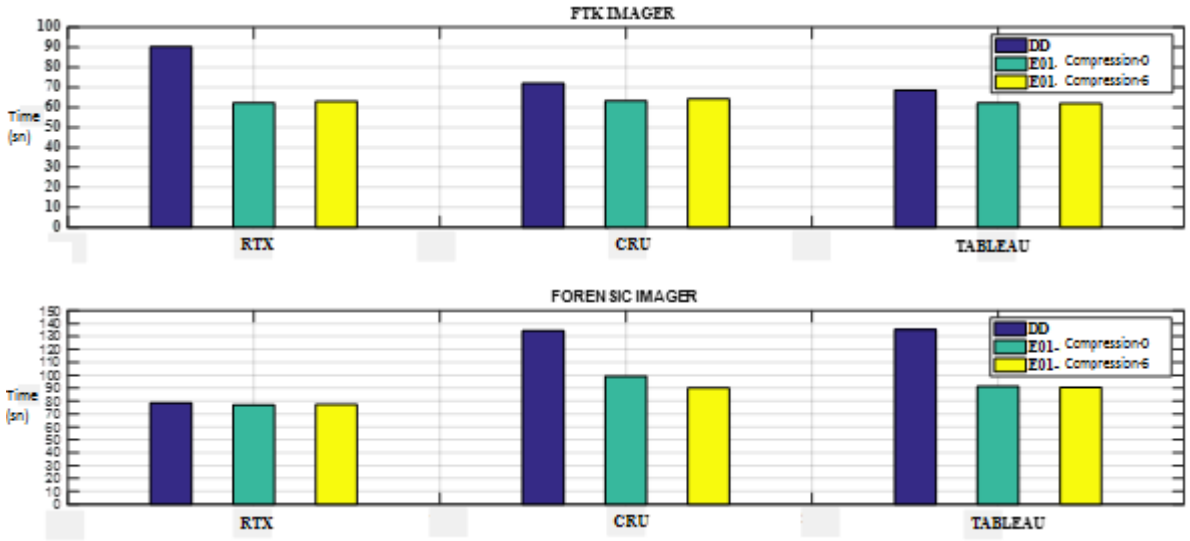

Fig.2. The Durations Measured with FTK Imager and Forensic Imager from the Devices CRU-TABLEAU-RTX

After evaluating the results derived from Table 5 and Table 6, it can be seen that;

- *IA* process take a shorter time through FTK Imager, comparing it with Forensic Imager.
- Hardware IA lasts shorter with Tableau than it does with CRU Ditto.
- FTK Imager is faster when using bridge.
- CRU Ultradock, CRU RTX, Tableau Bridge take images in close durations.

Findings show that, if the stated devices are available it becomes more of an issue for an investigator to use them properly in order to save time.

V. Conclusions

In digital forensics, live analysis without damaging the originality of evidences or *IA* process underpin the investigation. In judicial cases, for digital forensics specialists to analyze the electronic evidences definitely either *W-P* interfaces must be used or live analysis has to be done. Thus, the evidence can be examined without being falsified during the judicial process. In this study, the judicial process through acquisition *W-P* hardware and software images is examined. Findings on hand show that Tableau TD3 is faster than Ditto CRU at hardware *IA*. As for hardware and software *IA* via bridges, it is observed that FTK Imager, completes the process faster than Forensic Imager, yet they take images in close durations. These findings will lead the way for using the acquisition period effectively. If the stated tools are available and the factors which are complicating the digital forensics investigators acquisition process are known, the whole process can be much more productive through proper planning.

Following this study; performances of disk type, connection type of the disk and *IA* software during *IA* process will be evaluated.

References

[1] A. Lazzez, T. Slimani,"Forensics Investigation of Web Application Security Attacks", *International Journal of Computer Network and Information Security*, vol.7, no.3, pp.10-17, 2015.DOI: 10.5815/ijcnis.2015.03.02.

[2] Y. Prayudi, A. Ashari, T. K. Priyambodo, "A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia". *International Journal of Computer Network and Information Security*, vol. 7 no. 11, 1, 2015.

[3] J. Sharma, M. Singh, "CUDA based Rabin-Karp Pattern Matching for Deep Packet Inspection on a Multicore GPU", *International Journal of Computer Network and Information Security*, vol.7, no.10, pp. 70-77, 2015.DOI: 10.5815/ijcnis.2015.10.08.

[4] S. Jaiswal, S. Dhavale, "Video Forensics in Temporal Domain using Machine Learning Techniques". *International Journal of Computer Network and Information Security*, vol. 5 no. 9, 58, 2013.

[5] Y. Vural, Ş. Sağıroğlu, "A Review on Enterprise Information Security and Standards". Journal of the Faculty of Engineering and Architecture of Gazi University, vol. 23 no. 2, 2008.

[6] M. Geddes, P. B. Zadeh, "Forensic analysis of private browsing. In Cyber Security and Protection of Digital Services (Cyber Security)", *2016 International Conference On*, pp. 1-2. IEEE, 2016.

[7] K. Conlan, L. Baggili, F. Breitinger, "Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy". *Digital Investigation*, vol. 18, pp. 66-75, 2016.

[8] B. Carrier, "File system forensic analysis". Addison-Wesley Professional, 2005.

[9] U. Akalın, Ç. Uluyol, "Mobile Devices, Mobile Forensic Informatics and Proposed Process Model", *XVIII. Akademik Bilişim Konferansı*, 2016.

Copyright © 2018 MECS

[10] A. Agarwal, M. Gupta, S. Gupta, C. S. Gupta, "Systematic Digital Forensic Investigation Model". *International Journal of Computer Science and Security (IJCSS)*, vol. 5, no. 1, pp.118, 2011.
[11] K. K. Sindhu, B. B. Meshram, "Digital Forensic Investigation Tools and Procedures". *International Journal of Computer Network and Information Security*, vol. 4 no. 4, 39, 2012.
[12] R. Ceylan, A. S. Şirikçi, "Information Technologies Review - Data Reviews", *Forensic Science*, 2, Editor: Cihangiroğlu, B., Gendarmerie Criminal Department Publications, Ankara, pp. 152-174, 2011.
[13] D. Garza, "Data Acquisition and Duplication", *Computer Forensics Investigating Data & Image Files*, Editor: Garza, D., EC-Council, NY, pp. 65-94, 2010.
[14] J. Wiles, A. Reyes, The Best Damn Cybercrime and Digital Forensics Book Period. Syngress.
[15] R. Lutui, "A multidisciplinary digital forensic investigation process model", *Business Horizons*, vol. 59 no. 6, pp. 593-604, 2011.
[16] B. J. Nikkel, "Forensic acquisition and analysis of magnetic tapes". *Digital investigation*, vol. 2 no. 1, 8-18, 2005.
[17] M. Hirwani, Y. Pan, B. Stackpole, D. Johnson, "Forensic acquisition and analysis of vmware virtual hard disks". *In Proceedings of the International Conference on Security and Management (SAM) (The Steering Committee of the World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp)*, 1, 2012.
[18] E. Casey, "Digital evidence and computer crime: Forensic science, computers, and the internet". *Academic press*, 2011.
[19] B. Nelson, A. Phillips, C. Steuart, Guide to computer forensics and investigations. Cengage Learning, 2014.
[20] N. Beebe, "Digital forensic research: The good, the bad and the unaddressed". *In IFIP International Conference on Digital Forensics*. Springer Berlin Heidelberg, pp. 17-36, 2009.
[21] P. H. Yen, C. H. Yang, T. N. Ahn, "Design and implementation of a live-analysis digital forensic system". *In Proceedings of the 2009 international Conference on Hybrid Information Technology*, pp. 239-243. ACM, 2009.
[22] A. Brinson, A. Robinson, M. Rogers, "A cyber forensics ontology: Creating a new approach to studying cyber forensics". *Digital Investigation*, vol. 3, pp. 37-43, 2006.
[23] D. Manson, A. Carlin, S. Ramos, A. Gyger, M. Kaufman, J. Treichelt, "Is the open way a better way? Digital forensics using open source tools". *In System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*, pp. 266b-266b. IEEE, 2007.
[24] T. Vidas, B. Kaplan, M. Geiger, "OpenLV: Empowering investigators and first-responders in the digital forensics process". *Digital Investigation*, vol. 11, pp. S45-S53, 2014.
[25] F. Carbone, Computer forensics with FTK. Packt Publishing Ltd, 2014.
[26] D. Manson, A. Carlin, S. Ramos, A. Gyger, M. Kaufman, J. Treichelt, "Is the open way a better way? Digital forensics using open source tools". *In System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*, pp. 266b-266b. IEEE, 2007.
[27] V. R. Ambhire, B. B. Meshram, "Digital forensic tools". *IOSR Journal of Engineering*, vol. 2, no. 3, pp. 392-398, 2012.
[28] M. K. Rogers, K. Seigfried, "The future of computer forensics: a needs analysis survey". *Computers & Security*, vol. 23, no. 1, pp. 12-16, 2004.

Authors' Profiles

Erhan AKBAL is currently working as an assistant professor at Digital Forensics Engineering Department of Firat University, He received his Ph.D. degree in electrical and electronics engineering in 2012, the M.S. degree in computer engineering in 2007, from Firat University, Turkey. His research interests include computer network security, wireless sensor network, intrusion detection and digital forensics.

Sengul DOGAN received her Ph.D degree in Electrical and Electronic Engineering from the University of Firat, Elazig, Turkey, in 2011. She is currently an Assistant Professor in the Digital Forensics Engineering Department of Firat University. Her research interests cover Data Hiding, Information Security, Digital Forensics, Image Processing and Optimization Techniques.

How to cite this paper: Erhan Akbal, Sengul Dogan,"Forensics Image Acquisition Process of Digital Evidence", International Journal of Computer Network and Information Security(IJCNIS), Vol.10, No.5, pp.1-8, 2018.DOI: 10.5815/ijcnis.2018.05.01