Importance of Operating Systems Type in Computer Forensics

Hüseyin ÇAKIR, Mehmet Serkan KILIÇ
IT Institute, Gazi University, Ankara, Turkey
hcakir@gazi.edu.tr, mserkanklc@hotmail.com

Abstract

This article works on determining the effect of operating systems on Computer forensic especially in nowadays that the need for Computer forensic is increasing due to the increase in cybercrimes. Suited to the purpose of the study and methods of interview, 15 people with minimum of 4 years of experience in informatics have been interviewed, in addition, the reports of court experts from cases which are continuing in Ankara administration of Justice and domestic and foreign sources have been analyzed technically. With the outcome of the analysis, it has been observed that the studies and investigations are prepared according to an operating system, software or a certain device because of the commercial concerns or habits, for this reason it appears that it would be helpful to make an academic study in; sessions, workshops, seminars about gathering electronic evidences. Article studies the identification of differences and similarities between the operating systems and its effects on forensic studies with 5 headings and subheadings. According to the study, non-existence of a standard Computer forensic process and the need for different specialties are discovered, for this reason it is assessed that the Computer forensic experts need to specialize in sub-specializations especially related to operating systems.

Index terms: computer forensic, cybercrimes, electronic evidence, evidence collection, operating systems

1. Introduction

Computer forensics is a systematic research with the purpose of documenting the evidence on what is happening on the computer media and who is responsible for it [1]. With the light of this discipline, struggled on crime and criminals and innocent people (without any connection to crime) are protected.

Works related to computer forensics, involves the laboratory studies during the process of introduction of the electronic evidences taken from the crime scene to the court [2]. It is not possible to make a full list of the evidences that can be found in the crime scene. It is likely to encounter different types of evidences related to the suspects' financial status, social status and their interests towards technology. Although it is found that media, used from computers vary in every aspect of life according to place of use and purpose, they all share one major commonality and it is using an operating system. The general idea of the computer forensics studies is; to analyze the operating system and detect deleted data, used programs and executed functions on computer media. This is highlights the importance of the type of operating systems used and its structure.

Hidden in every intelligent device and computer system is the software that controls processing, manages resources and communicates with peripherals such as display, screens, disk, computer networks and printers [3]. Operating systems vary not only based on price, performance and application improvement, they are also different in the means of data keeping, saving and reading.

It has been observed in a literature research about classification and detection of digital data (electronic data) that mostly, the detection and classification are developed for one certain device type (personal computer, mobile phone, PDA etc.), one certain operating system (Windows NT, Windows XP, Unix, Linux etc.) or one certain purpose (data saving, computer forensics, computer network, computer based data analysis, code breaking etc.) [4]. As a result of updating and modifying technology, computer media with different operating systems are involved in crime and they are gathering data via these media. However studies related to the subject show the investigations are only in a single direction towards one device or one operating system.

The study aim is find an answer the question of *"What are the effects of operating system types on the computer forensics investigations?"* Reason to work with this context is to keep the process of computer forensics as a whole and prove the effects of different operating systems on computer forensics investigations.

Base data to the study are these:

- In the national thesis databank of YOK, last 50 theses (M.S.) and dissertations (Ph.D.) related to either computer forensics or cybercrime
- Expert witness reports about 3 court cases located in Administration of Justice in Ankara
- Notes from interview with 15 public and private sector employees who has a minimum of 4 years of experience in computer forensics

Because of the numerous type of computer media exist and place of usage and purpose are different, there is large quantity of operating systems and version is exist. While analyzing the operating systems in accordance with the objective of the study, Windows 7, Windows XP, Mac OS X and Ubuntu 9.0 is selected to analyze. Thus, unmentioned of other PC operating systems, server operating systems and mobile operating systems is the limits of the study.

2. Analyzing the operating systems in respect of their usage rate

It is a hard matter to know which operating systems the end users prefer, for this reason instead of making a general study on the subject, data from a statistical service from Roxr Software Ltd. called Clicky Web Analytics was used. Clicky tracks and saves information such as the visitor count (total and individual), browser information, operating system information, Country / State information, the time spent on the website and source code for visiting the website from 443.553 websites daily.

According to the data of Clicky Web Analytics; the rate of Windows operating system usage around the worldwide is %84.4, Macintosh operating system is %14.4 and Linux operating system is %1.2. Relative information is given in Table 1.

Table 1. Operating systems usage rates (%)

Countries	Linux Operating System	Macintosh Operating System	Windows Operating System
U.S.A.	0,9	20,9	78,2
Iran	0,5	1,2	98,3
Japan	1,4	20,8	77,8
Canada	1,0	21,6	77,4
Norway	6,5	20,3	73,2
Russia	1,9	4,8	93,3
Romania	2,8	5,5	91,7
Turkey	0,4	2,4	97,2
World Average	**1,2**	**14,4**	**84,4**

When we analyze the end users' preferences in operating systems we see that; Windows Operating System is the most preferred operating system worldwide. Until June 2011, XP was the most commonly used operating system, after that date it left its place to Windows 7. Today, %52 of the Windows users prefer using Windows 7, %34 prefer Windows 8.x, %15 prefer Windows 10, %8 prefer Windows XP, %2 prefer Windows Vista and %5 prefer other Windows versions (Windows Server 2003, Windows Server 2008, Windows Me…) Windows Vista was marketed throughout the world on 30 January 2007 however couldn't get a full score by end users and extensively criticized, for this reason many Windows users in the world continued to use Windows XP or directly passed to Windows 7, Windows 8 or Windows 10.

From the countries with high GNP rates to the countries that criticize USA, Windows OS is the most preferred operating system and Windows 7 is the most popular version.

In light of the gathered data, experts of computer forensics are encountering mostly Windows 7 and Windows XP, in addition to this, the order of other operating systems encountered is; Windows Vista, Mac OS X and Linux operating systems.

A participant who was interviewed about the frequency of encountering different operating systems said that:

"*The matter that I'm having the most difficulty is, besides the windows analysis, I can't find domestic data. English sources can be quite hard. We needed Mac/Linux analyses in 4 cases and spent much time to prepare the report…*"

It is expected from computer forensics experts to have a good grasp on Windows OS forensics analyses because encounter it frequently. Other operating systems usage is approximately %15.

Since the documents related to computer forensics are largely made of publications from trading items, these publications are prepared specially for a certain security resolution, software brand or an operating system because of the commercial concerns [4]. So, countries must be take into account the usage rate of operating system type and version and prepare necessary documents.

Related to this matter, another participant has a claim that:

"*Besides from Windows, I have never analyzed any other operating systems but I don't believe there would be a huge difference, after all, they all work with the same idea. Anyhow it would be possible to have an analysis and gather evidences…*"

With the special education to be given to computer forensics experts, it should be made that they will be aware of the usage rate of operating systems, frequency of encountering a forensic case and have basic knowledge on the differences between them.

Also, for the computer forensics experts, education and continually updating notes should be prepared regarding the analysis of Windows, Macintosh and Linux in this order.

1.1. Comparison on supported file systems

File system is the base structure that allows the data to be held systematically, it is formed of sectors getting together as a result of shaping the computer media [5]. In the analysis to be made on a hard disk, file system in the computer media is as important as the operating system.

When the 10 widespread file systems are analyzed, it is observed that Linux operating system supports ext2/ext3, FAT16/FAT32/HFS, HFS+, LTFS, Joliet, ISO 9660, NTFS, BRFS and UDF file systems.

When shortly examined, Linux operating system supports 9, Macintosh operating system supports 7 and Windows operating system supports 5 file systems. Related information is given in Table 2.

Table 2. Supported file systems

File System	Linux OS	Macintosh OS	Windows OS
ext2/ext3	YES	NO	NO

FAT16/FAT32	YES	YES	YES
HFS/HFS+	YES	YES	NO
LTFS	YES	YES	NO
MFS	NO	YES	NO
Joliet (CDFS)	YES	YES	YES
ISO 9660	YES	YES	YES
NTFS	YES	NO	YES
BFS	YES	NO	NO
UDF	YES	YES	YES
TOTAL	**9/10**	**7/10**	**5/10**

Version information related to operating system and the detection of the held file system information are one of the digital evidences needs to be gathered in the process of computer forensics. Additionally, as part of informatics system, discovering the file systems regarding the CD, DVD, hard disk, external disk, floppy disk, external DVD drive, memory stick, memory card which can be used with the purpose of saving the data and/or moving it [4].

Each file system has a different way of keeping the data on the hard disk. When the status of 10 different file systems being supported by the operating system are studied, many file systems are observed to be supported, for this reason, it is considered to require more effort and knowledge to analyze a computer with Linux operating system than Windows and Macintosh operating systems.

Related to the matter, an interviewed participant had expressed this:

"... we most certainly state the name, version and file system of the operating system in our reports. This remains continuous as printed."

Studied court case number 3 shows the court expert's report and it provides this information related to computer media as meta-information:

- .....
- *EnCase Version*
- *System Version*
- *File Sytem*
- *Write Blocked*
- *Compressed*
- *Total Size*
- *Total Sectors*

Computer forensics report is the view of an expert to be given to those associated with the evolution about computer technology. Prepared reports include the operating system and file system types to the court just as it is stated in the computer forensics report analysis of the interviewed people. Furthermore, taking the whole inspected computer media into consideration and in case of detecting incoherence in the file systems, having it present in the report provides great help with the lightening of the case.

Another interviewed participant stated his memory regarding an operating system:

"The most important experience about operating systems in my case is a friend of mine, a very observant police officer to find a USB with ext2 format. The computer it was taken from had Windows XP and he noticed it. Later on, he asked the suspect of the where bounds of his Linux Computer and this led the suspect to be very shocked and eventually admit."

It is highly possible to create the link between the computer media found in the crime scene and the file systems that the operating systems support. For instance, finding a portable memory device with ext2 or ext3 file system near a computer with Windows operating system points the existence of a secondary operating system. Ext2/ext3 file system is not supported by Windows operating system and this indicates the device could not be used with that computer.

1.2. Comparison on Metadata

The importance of the metadata information is most obvious when the need to link evidences reasonably arise, however it is observed the metadata can be dissimilar because every operating system has different file systems.

Of all the 6 categories of analyzed metadata information, only one of them; File Date is recorded on all operating systems. File

ownership and ACL information are not recorded on Windows XP and File creation time are not recorded on Linux operating systems.

Nevertheless, file deletion time is recorded only on Linux and Last Archive time is recorded only on Macintosh operating systems.

According to this, the metadata information was analyzed as 6 categories and 2 of them are recorded on Windows XP, 4 of them are recorded on Linux and Windows 7 and 5 of these categories are recorded on Macintosh operating systems. Related comparison information is given in Table 3.

Table 3. Metadata information types

Metadata Info.	Linux OS	Mac OS X	Win. XP OS	Win. 7 OS
	ext2/ ext3	HFS/ HFS+	FAT16/ FAT32	NTFS
File Author Info	YES	YES	NO	YES
File Creation Time	NO	YES	YES	YES
File Change Time	YES	YES	YES	YES
Last Archive Time	NO	YES	NO	NO
Access Control List	YES	YES	NO	YES
File Del. Time	YES	NO	NO	NO
TOTAL	**4/6**	**5/6**	**2/6**	**4/6**

The next step to take after gathering digital evidences is to combine all the evidences and link them reasonably in the meantime. Until the definite and absolute evidences are gathered which will conclude to a result, linking the evidences and the correlation will continue in loop and more evidences will be gathered in the process [6].

Metadata information is utilized to create a link between the gathered evidences and to come up with reasonable outcomes related to the matter.

Metadata describes a document and it holds information such as where the file contents are located, size of the file, last writing date (or access date), access control information etc. Example of the data structure of these information can be given as, directory input for FAT file system, MFT input for NTFS file system and inode structures for UFS, Ext2 and Ext3 file systems [7].

Metadata contains various information based on file type. For instance, it shows the information of the username for MS Office file and for the image file; it shows the information regarding the machine which took the photo. Metadata mentioned here however, is the information recorded by the operating system (actually the file system installed on operating system) regardless of any file types.

Finding the contents of all the data located in file system of the operating system and identification (metadata) is one of the necessary digital evidences that needs to be gathered in the computer forensics process [4].

A participant calls attention to a matter related to metadata:

"... Knowing the operating system and its features makes the job of analyzing person easier. For instance, in an analysis of a file which is directly deleted without visiting the recycling bin, file created date is shown as deletion date. This is actually because of the analyzing program. It looks for the deletion time in FAT32 or NTFS but since it cannot find it, it pastes the create date on the column. Windows operating system does not even record the deletion date, so this finding is caused by the lack of information."

Related to the analysis of metadata under 6 categories; file ownership information and ACL information are not kept in Windows XP operating systems, thus it is not possible to make a statement about the ownership of a file or accessibility of users in Windows XP operating system with FAT32 file system.

File Creation Time is recorded by all operating systems except for Linux operating

system. For this reason, in an analysis of a computer with Linux operating system, it is not possible to gather the information related to the date of file created with file system. Only in case the file is saved by the program it belongs to.

When it comes to *File Deletion Time*, the situation is exactly the otherwise. If a file is deleted without being sent to the recycling bin first, it isn't possible to find the information on Windows and Macintosh operating systems. However Linux operating system allows for this information to be gathered.

The last comparison about metadata is Last Archive Time to be kept only on Macintosh operating systems. The time of a file archived can be discovered with a feature of HFS+ file system.

1.3. Comparison on Main Directory Structures

Operating systems execute the file writing, reading according to their own specific systematic. It is understood from the interviews that in the detection of operating system, directory structure was of use.

With the analyses made by computer forensics programs, hidden folders and system files are observed to be listed as a whole under a main directory, moreover the user directory located in the main directory shows different logons and different files belonging to them. Similarly, programs directory features the installed programs on the computer.

Each operating system completes its function by keeping data in their own systematic ways. Difference of main directories would negatively affect the case to be investigated by computer forensics experts but it also provides useful information.

The most obvious disadvantage of dissimilar directory systems is; not knowing what type of data are located in the directory containing the user files and other directories. On the other hand, the computer forensics expert who knows main directory structure of the computer will be able to detect the operating system of the computer image. Furthermore, they will be able to comment on whether the image is damaged or not with the integrity of the data located there.

An interviewed applicant describes his experience about main directory structure:

"... Out of habit, if we find other than the drivers we used to see in the computer image, such as C, D in Windows; we used to type "Linux" in our reports. Later on, we noticed the Macs have similar driver structures (directory structure) to Linux."

In the analyses performed with computer forensics programs, hidden folders and system files are listed under the main directory completely. Each operating system has different main directory structure, for this reason main directory structure can be useful to determine the operating system of the analyzed computer image.

An applicant shares this information about the process of analysis and inspection:

"The first location I check in my analysis is the user folder in computer. Important organizational files are often saved here..."

Defined user identities (accounts) and finding files in defined users' recycling bin, are the digital evidences need to be gathered in process of computer forensics. Located in the main directory, analysis of the user directory allows access to office, picture, music and other files of the user. During the arrest, taking the image and to quickly assess the process of preliminary examination, it is necessary to examine the user directory with high priority.

User names located in home directory in Linux operating systems are not located in Macintosh operating systems' main directory. In Windows XP operating system, active logins are located in main directory but other user names are located in Documents and Settings directory. In Windows 7 operating system, user names are located in the Users directory. Cognizing main directory structure of the computer and user directories allows the determination of the different logins and files regarding these logins.

3. Analysis of operating systems in respect of their analyzability by computer forensics software

With technology advancing, many computer forensics procedures that are done by the computer forensics programmers are easily processed automatically. For instance, information regarding the last used date of the computer, hard disk information, user information and such basic information can be gathered with EnCase software without the need of any other third party software.

Operating system of the computer, affects the computer forensics software which would be used in analysis. For this reason, information related to the 10 most commonly used computer forensics software and about the operating systems they support are given in Table 4.

Table 4. Computer forensics software analyzability

Computer Forensics Software	Linux OS	Macintosh OS	Windows OS
EnCase	YES	YES	YES
FTK	YES	YES	YES
Mac Marshal	NO	YES	NO
Mac Forensics Lab	YES	YES	YES
OSForensics	NO	NO	YES
ProDiscover Forensics	YES	NO	YES
P2 Commander	YES	YES	YES
Second Look	YES	NO	NO
Autopsy (Sleuth Kit)	YES	NO	YES
X-Ways	YES	YES	YES
TOTAL	**8/10**	**6/10**	**8/10**

When the computer forensics software are studied for comparison, it is observed that they try to support all 3 operating systems. While there are 8 available computer forensics software able to operate on Windows and Linux operating systems, there are 6 software that can operate on Macintosh operating system, nonetheless, Mac Marshal; especially designed for Macintosh operating system and Second Look; designed for Linux are available.

Computer forensics experts have the need of using software that will allow them to speed up their file analysis [1]. Thereby, special programs with functionality have been discovered. Their function is to gather related data related to computer forensics studies and their analysis [8].

An expert's report from the court case 2 indicates this information:

"The analysis on the hard disk have been conducted without harming its integrity by removing the write protection in order the take the image of the hard disk with a digital evidence analysis program called Forensic Toolkit 3.1, accepted as a standard worldwide…"

According to the expert's report from the court case number 3, preliminary information regarding computer media is given:

- ...
- *Acquisition MD5*
- *Verification MD5*
- *GUID*
- *EnCase Version*
- *System Version*
- ...

EnCase, FTK and X-Ways computer forensics software, widely preferred in our country can analyze computers with Linux, Macintosh and Windows operating systems. Thereby, it can be observed that MacForensicsLab and MacMarshal computer forensics software are compatible with Macintosh operating systems and Secondly Look and Autopsy computer forensics software are compatible with Linux operating systems.

Occasionally, during the process of computer forensics analyses, need of using other software for the same computer arises. Computer forensics software do not differ in the means of performance and speed however it is beneficial to gather different data with different software on operating systems

especially Linux and Macintosh to compare the results.

A participant delivers a warning related to computer analysis:

"*One of the first rules of analyzing a computer is to determine the operating system of the analyzed computer. By doing this, analysis can start with the correct software. If the approach focuses on letting the software do the entire job, a lot of data may not be gathered at all."*

Before the study of computer forensics, in order to create an operation plan some matters must be taken as groundwork such as; type of case, computer forensics expert count and qualification, physical attributes of the device to be analyzed and estimated time of analysis [4]. In addition to these, using the correct software on the operating system in analysis must be taken into consideration.

Another participant makes a metaphor related to the subject:

"Analyzing a computer is like buttoning a shirt. Deciding on which software will be used for analysis is the first button and if the first one is buttoned wrong it may lead the entire analysis to a false result…"

With the technology advancing, a lot of procedures are done automatically by the computer forensics software and for this reason computer forensics experts are expected to use all the functions of the software efficiently and know the data type that can be gathered.

If the computer forensics expert knows what to look for and uses searching programs (Search function of the computer forensics software) it proves useful for the analysis-time cost [9].

A good computer forensics software must compose a file and directory catalogue for all the computer media as well as supporting FAT12, FAT 16, FAT32, exFAT, TFAT, NTFS, Ext2, Ext3, Ext4, CDFS/ISO9660/Joliet, HFS, HFS+/HFSJ/HFSX, ReiserFS, Reiser4, UDF file systems [10].

4. Assessment of operating systems type in respect of computer forensics experts

In terms of criminal procedure, expert is the person who reveals the traces and tracks for evidences related to the case or it is the person who analyzes the collected information [11]. Computer forensics experts however, know many methods to discover, reveal, repair the damaged data and save the protected data located in the computer systems [12]. Electronic data are easily modified or changed because of their structure, thus it is necessary to have certain processes and procedures with standards in the analyses of the evidences [13].

Today, the computer media are increasing in diversity, communication methods via internet are changing, and informatics systems are becoming widespread, thus a superior level of information is obligatory especially for an active struggle against cybercrimes.

An interviewed applicant expresses his memory about lack of information:

"*In one of the analyses we did, we couldn't gather any data from a laptop with Linux operating system. We wrote the image was either broken or coded on the report, but that analysis just didn't feel right…"*

Expert report from court case number 3:

"*The hard disk image with serial code was taken as 2 images, Raw image (dd) and smart image (e01) however, since the operating system was Linux no analysis were conducted but information related to operating system was gathered and screen was simultaneously shared…*"

Not conducting any research or analysis because of the operating system indicates the results of not having sufficient information, in this respect, lack of enough computer forensics experts brings another matter in hand; capability of current experts.

The experts obtain their certificates only through theoretical tests and that creates question marks about qualification. Similarly,

a computer engineer working on computer software is obviously not qualified as an expert on crimes committed on computer network or internet which requires experience and expertise in system administration [11].

A certificate should not be considered enough to assign a person as expert. Certain number of requirements must be made and an objective regulation regarding this matter is needed [14].

In USA, certain people are given accreditation in order to use special programs about computer informatics. In consequence, not only having the license to use the program, but also the training personnel who will use that program is necessary [15].

Some criminals, especially forensics criminals (cybercriminals) are over certain cultural and IQ levels, they are also called "white-collar crime" and when this is taken into consideration, the known methods shortly become obsolete. This proves the necessity of the technical personnel to constantly renew and update their training [16].

In order to have the Computer forensics expert or court expert title, expertise regarding the process of trial is required as well as computer forensics and as for choosing the experts, standards and sub-specializations must be set. These must be made in an environment where the court (judge, advocate and prosecutor), enforcements officers, chambers, organizations and manufacturer company attorneys can assemble. Training programs with the designated standards should determine the sub-specializations and computer forensics experts. In this context, areas of expertise for the computer forensics experts can be specified like this:

- Expertise in The Analysis of Windows Operating System;
- Expertise in The Analysis of Linux Operating System;
- Expertise in The Analysis of Macintosh Operating System;
- Expertise in Mobile Device Analysis;
- Expertise in Server Analysis;
- Expertise in Analysis of Wireless and Cable Network;
- Encoding and Decoding Expertise;
- Expertise in Identification of Malicious Software.

Governments should make investigations in selection of computer forensics expertise, training and inspection just as it makes investigations by following the developments in technology and speeding up the trials.

During the process of gathering the evidences and their analyses, not following the principles and procedures causes the evidence to be shadowed and rejected by the court authorities [17]. For this reason, Computer forensics studies must be done by units equipped with high technology and these units must consist of trained and expert personnel with advanced skill and knowledge [18].

Result of study shows the need for variant technical knowledge on different operating systems and many computer forensics experts' lack of knowledge especially on Linux operating systems.

5. Conclusion

Judge needs evidence to solve a controversy whether it is law or criminal procedure. Judgment of the evidence is a matter of procedural law just as gathering the evidence is of technical.

This technical matter of discovering the electronic evidences is in the field of computer forensics. In addition to this, computer forensics studies need to be undertaken as the process of systematic analyses on computer media, not as gathering absolute evidence and presenting it.

Computer forensics studies is a field which requires extensive technical knowledge, expertise and cautious works as this field is needed in almost all cases of cybercrimes committed in different ways and methods.

Although the judges and prosecutors show great importance and care in the evaluation of electronic evidences, the duty of the computer forensics experts (especially law-enforcement officers) who discover, lay the first hand and report the evidences are equally important.

Computer informatics is not a field fully completed both in our country and the others. This field which serves the justice to be served and it renews itself according to technical developments and looks for the solutions to varying needs.

With the increasing cybercrimes and need of computer forensics works, this study approaches the computer forensics process as a whole and attempts to evaluate the effects of dissimilar operating systems on the process. This matter was studied in accordance of both technical and global standards and not rated juristically.

When the doctorate and master degree theses in YÖK national databank and studies made of computer forensics and/or cybercrimes evaluated; the judicial part is taken into consideration predominantly. Technical works however, are prepared according to a certain device, software or operating system because of commercial concerns and habits.

The effects of operating systems on the computer forensics studies have been analyzed in light of 50 national theses analyzed in this context, interview with 15 people with a minimum of 4 years of experience in computer forensics field and court expert reports from 3 ongoing cases in Ankara administration of Justice.

The publications (books, articles, training notes…) which computer forensics experts have great grasp are largely based on Windows operating system and this can be explained with the %97.2 usage rate in Turkey. It is observed that the experts and publications regarding the Macintosh operating system are insufficient and the rate of usage of Macintosh operating system in our country is %2.4.

As a result of the study, it is discovered that knowing the importance of which operating systems support dissimilar file systems especially on portable storages provides assistance to the speed of the computer forensics process. Another result shows the gatherable metadata will not be standard in case it is copied to another operating system.

When we take a look at the 10 most commonly used computer forensics software worldwide, 7 of them are compatible for use on Windows operating system. Using Windows operating system on the computers that will be used for computer forensics process will prove to be advantageous. Another result is that the most preferred computer forensics software in our country; EnCase, FTK and X-Ways are only compatible with Windows operating system.

One of the very important issues in computer forensics studies is the similar data found in computer media with different operating systems and it isn't possible to gather the data with standard computer forensics software. For this reason, using third party programs will prove useful especially for the analyses of logs and records.

When we study the most commonly used 10 computer forensics software worldwide, we observe they are trying to support all 3 operating systems. Primarily, EnCase and FTK and 3 more other software are capable of analyzing all 3 operating systems. In accordance, it has been discovered that they are especially designed for Linux and Macintosh operating systems.

In order to provide evidences of the crimes committed, and protect the innocent people with no relation to crime whatsoever, it is important for computer forensics experts to be well equipped and informed. For this reason, sub-specialization fields must be designated and experts must intervene to the computer media with their own expertise on the matter.

Certification programs with practice and master and graduate level trainings must be provided to satisfy the need of the computer

forensics experts regarding the matters of system networks, operating systems, decoding and electronic communication of Macintosh and Linux operating systems; especially of the mobile devices.

In addition, certification programs must be made by establishing sub-specializations for computer forensics experts and qualified personnel must be trained with the result of these certification programs. In accordance with this, Experts must take an exam consecutively with certain intervals (like every 2 years) and their knowledge must be tested with the new developments.

References:

[1]. D.S. Jadhav and S.K. Patil, *The Study Of Computer Investigation Methods: Computer Forensics*, The International Journal Of Advanced Research In Technology, Vol. 2, Issue.1, pp. 9-17, 2012.

[2]. A. Ho and S. Li, *Forensic Authentication of Digital Audio and Video Files"in Handbook of Digital Forensics of Multimedia Data and Devices*, Chichester, UK: John Wiley IEEE Press, 2015, pp.133-184.

[3]. D. Comer, "Introduction and Overview" in *Operating System Design: The Xinu Approach*, 2th ed. NW: CRC Press, 2015, pp. 3-15.

[4]. M.İ. Öztürk, *Bilişim Cihazlarındaki Sayısal Delillerin Tespiti ve Değerlendirilmesinde İş Akış Modelleri* (*Models Of Flowchart For Detecting And Evaluating Digital Evidences in IT Equipments*), M.S. thesis, Health Sci. Inst., Ankara Univ., Ankara, Turkey, 2007.

[5]. B. Carrier, *File System Forensic Analysis*, 5th ed. NJ: Pearson Education Inc, 2007.

[6]. Y. Uzunay, "Bilgisayar Ağlarına Yönelik Adli Bilişim" (Computer Forensics Intended for Computer Network) in *Computer Forensics Workshop*, İzmir Institute of Technology, İzmir, Turkey, 2005.

[7]. AccessData, *Windows OS Forensics Training Notes*, unpublished.

[8]. W.G. Kruse and J.G. Heiser, *Computer Forensics – Incident Response Essentials*, 14th ed. IN: Pearson Education Inc, 2010.

[9]. M.K. Rogers, J. Goldman, R. Mislan, T. Wedge and S. Debrota Steve, *Computer Forensics Field Triage Process Model*, Journal of Digital Forensics, Security and Law, Vol.1 No.2, pp.9-38, 2006.

[10]. T. Henkoğlu, Adli Bilişim, *Dijital Delillerin Elde Edilmesi ve Analizi*, 1st ed. Ankara: Pusula Yayıncılık, Turkey, 2011.

[11]. M.B. Eryılmaz, *Ceza Muhakemesi Hukuku Dersleri*, 1st ed. Ankara: Polis Akademisi Yayınları, Turkey, 2012.

[12]. D.S. Thomas and K.A. Forcht, *Legal Methods of Using Computer forensics Techniques For Computer Crime Analysis and Investigation*, Issues in Information Systems Journal, Vol.5 No:2, pp.692-698, 2004.

[13]. B. Nelson, A. Phillips and C. Steuar, "Expert Testimony in Digital Investigations" in *Guide to Computer Forensics and Investigations*, 5th ed. USA: Cengage Learning, 2015, pp. 535-567.

[14]. Adalet Bakanlığı, "Çalıştay Raporu", *Yargılamada Bilirkişilik Müessesesi Çalıştayı*, (*Workshop Of Expert Witnesses at Trial*), Hakimevi, Ankara, Turkey, 2010.

[15]. Y. Çiçek, "Bilirkişi Raporlarının Hazırlanması", *Kamulaştırma Bilirkişiliği Eğitimi Programı (Expert Witnesses at Expropriation Training Program),* TMMOB Harita ve Kadastro Mühendisleri Odası, Ankara, Turkey, 2008.

[16]. A. Karagülmez, *Bilişim Suçlarında Delil Toplamayı Etkileyen Başlıca Konular*, 2. Polis Bilişim Sempozyumu (2nd Police IT Symposium), Sheraton Hotel, Ankara, Turkey, 2005.

[17]. H. Çakır and E. Sert, "Bilişim Suçları ve Delillendirme Süreci", *Örgütlü Suçlar ve Yeni Trendler. Uluslararası Terörizm ve Sınıraşan Suçlar Sempozyumu (International Terrorism and Transnational Crime Symposium)*, Antalya, Turkey, 2010.

[18]. V. Bıçak, *Suç Muhakemesi Hukuku*, 1st ed. Ankara: Seçkin Yayınevi, Turkey, 2011.