Journal of Emerging Computer Technologies
Review Article
Received: *2022-08-05* | ***Reviewing:*** *2022-08-06* & *2023-02-27*| ***Accepted:*** *2023-02-27* | ***Online:*** *2023-02-27* | ***Issue Date:*** *2022-12-31*

A Review about Forensic Informatics and Tools

Çiğdem BAKIR
Kütahya Dumlupınar University
Software Engineering Department
Kütahya, Turkiye
cigdem.bakir@dpu.edu.tr
0000-0001-8482-2412

Mecit YÜZKAT
Yildiz Technical University
Computer Engineering Deparment
İstanbul, Turkiye
myuzkat@yildiz.edu.tr
0000-0003-4808-5181

***Abstract*— Due to the rapid increase in the use of internet and electronic devices in our age, forensic informatics is becoming a very important field. A good understanding of forensic processes is necessary for the protection of states, institutions and personal information. In addition, when a crime is committed, it is a great precaution to make the right decision when making decisions about this crime. In the article study, researches on the importance of forensic science, its areas of use and the tools used in these areas were made. The study consists of three main stages. In the first stage of the study, the general definition of forensics, its precautions, common areas of use and recent studies on forensics were examined in detail. networks are offered. In the second stage, the process of collecting, analyzing and reporting, which is a process of forensic informatics, was made and the types of evidence were mentioned. In the third part of the study, information about legal informatics law is given. In the final stages of the conclusion and suggestion section, suggestions were made about the importance of forensic science, the lack of academic understanding of forensic sciences in our country and how these deficiencies can be eliminated.**

Keywords*— *Forensic computing, hardware tools, software tools, mobile forensic computing, cloud computing

I. INTRODUCTION

In today's world, with the spread of electronic devices, a large number of digital forensics crimes are being faced with every passing day. In order to cope with these crimes, it is necessary to know well the new methods of investigation. Thus, before working in the field of digital forensics, it is also necessary to know the steps of the digital forensics process well and to obtain the evidence used in this field without any problems. When incorrect methods are applied to the evidence, the evidence may be damaged, and irreparable consequences may occur.

In the second part of this study, researches made in recent years about forensics were discussed, in the third part, forensic computing (definition of forensics, its current importance and usage areas) were discussed. In the last part of the study, the conclusion obtained with forensic informatics and discussion in detail.

II. LITERATURE REVIEW

In recent years, there has been an increase in studies related to digital forensics, and the importance of this issue is increasing every day. The information obtained in some previous studies related to the issue of digital forensics is briefly mentioned below. In Table 1, studies related to forensic informatics in the literature are given in detail.

TABLE I. CURRENT STUDIES IN THE LITERATURE

Source	Method
Robbins [1]	Judd Robbins, a digital forensics expert, revealed that digital forensics was based on analysis techniques applicable to investigation and legal evidence [1].
Hand and Lin [2]	Hand, Lin, and their colleagues mentioned Bin-Carver, which was the first system of its kind for automatically recovering deleted or corrupted metadata and executable files. In the study conducted with thousands of binary code files, accurate results were obtained with a recovery rate of 93.1% without files being corrupted [2].
Narayanan and Ashik [3]	In their study, Narayanan and Ashik discussed digital forensics analysis tools and their usage in an application. In this study, basic research concepts and how to use a specific tool were explained for beginners in the field of digital forensics [3].
Pal and Memon [4]	In a study conducted in 2009, Pal and Memon touched on file carving (that is, works such as restoring deleted files or recovering data on a corrupted device). While the study was successful in recovering text and images, the same success could not be achieved for video, audio, executable, and other file formats. Therefore, they talked about the creation of new techniques [4].
Ballenthin [5]	It isconducted a study on commercial open source tools, and mentioned the index structure and the contents of index entries. For example; EnCase, FTK and TSK etc. they have recently released INDXParser.py, an open source tool that parses NTFS index files into Excel and CSV file formats, as well as a search for free fields [5].
Mutawa and Baggili [6]	It is focused on conducting forensic analyses in three social networking applications (Facebook, Twitter, and MySpace) that are commonly used on smartphones. The tests were conducted on three popular smartphones (BlackBerry, iPhone and Android). The tests were carried out in the form of installing social networking applications on each device, conducting common user activities through each application, obtaining a forensically healthy image of each device, and performing manual forensic analysis on each resulting image. The results showed that no traces were found in BlackBerry devices, while a significant amount of data that can be recovered and used by forensic investigators was obtained from iPhone and Android phones [6].
Krishnun [7]	In another study, it was mentioned different approaches for digital forensics investigations of flash drives. Three different data collection methods were discussed for creating complete memory copies of flash memory devices. While doing this, 45 different brands and models of USB flash drives were used. Which steps were needed to convert the extracted data in an understandable form by the common forensic media analysis tools was shown. However, it was emphasized that further research was necessary for flash memory data that could not be converted directly to the file system level [7].
Arthur and Venter [8]	In the study, the common points of digital forensics tools and their main differences were discussed, and what features should be developed in these tools to make them achieve effective results on storage devices was mentioned. In addition, some digital forensics tools were used in this study and the authors focused on the missing features of these tools [8].

Source	Method
Guo, Jin, and Shang [9]	In their studies, it was presented the definition and various models of cloud computing. In addition, they compared classic forensic investigations with forensic investigations in the cloud and analyzed the challenges of forensic investigation in cloud environments. For this reason, the necessity of a broader range of technical knowledge on a wide variety of hardware platforms and operating systems, as well as a deep understanding of a wide variety of technologies, applications, networks, has been mentioned with forensics [9].
Van Houten et al [10]	In a study conducted by Van Houten et al., the difficulty of identifying the video source from low-quality videos was deeply examined [10].
Garfinkel [11]	Garfinkel mentioned the design and use of DFXML. As discussed in this study, digital forensics XML (DFXML) is an XML language that allows the exchange of structured forensic information. In digital forensics, DFXML represents the origin of data. DFXML also documents the specific tools used to produce the results and their processing techniques. The automatic reprocessing of forensic information when tools were developed was also discussed in this study [11].
Tang [12]	In another study, the current state of digital forensics investigations, their future trends, and a typical platform of the software system commonly used in Linux were mentioned. In addition, the problems caused by the fact that many of the current works were based on manual applications were discussed [12].
Milani et.al. [13]	Milani et.al. presented an overview of current video processing techniques. They also mentioned the possibility of identifying all possible terms that could be operated on a single signal and footprints that could reveal important information about its origin and use. They showed that this was possible on the assumption that each processing step does not create an excessive amount of distortion on the signal. It did not give good results as a serious deterioration in signal quality would render it useless [13].
Yin Pan et al [14]	Yin Pan et al. conducted a study on games related to digital forensics. They focused on designing and developing game-based digital forensics work in a real computing environment by using the game-based learning (GBL) approach. In this study, interactive visualization was used to help students understand intangible and inaccessible abstract concepts such as deleted, hidden, over-written, or encrypted digital evidence [14].
Yinghua [15]	Yinghua, Slay, and Beckett focused on the topic of verification and validation of tools used in digital forensics. Thus, they conducted some tests and applied these tests to some real tools such as EnCase and FTK, which are widely used in the market. In addition, they mentioned a quantitative model for evaluating the results of verification and validation. In this study, how to evaluate whether a tool was validated was also discussed [15].
Cho [16]	In the study conducted by Gyu Sang Cho, a digital forensics analysis method for a directory on the NTFS file system was presented. In the study, especially if there are a large number of files in the directory, digital forensics methods were used. From a digital forensics perspective, information was provided about how the directory entries and traces on the directory entry record remain when the files are deleted [16].
[17,18]	In this study, fuzzy logic and genetic algorithms were used for intrusion detection systems on server computers. First of all, abnormal behaviors were detected by examining user behaviors over log records [17, 18].
Kobayashi [19]	In their study, Kobayashi and colleagues aimed to detect suspicious areas in a video recorded from a static scene by using noise characteristics to detect changes made on cameras [19].
[21]	Data recovery technology on a computer is one of the most important technologies in the field of digital forensics. Data can be recovered using professional digital forensics tools such as Encase [20] and Easy recovery [21], even in cases where the data has been completely deleted on a computer and even the disk has been formatted more than once.
[22]	Considering the spread of cybercrimes on portable devices, Joe Grand introduced some software for digital forensics works on portable devices with operating systems [22].
Ronghua Shi et al [25]	Ronghua Shi et al. discussed their studies on the design of a matrix-based visualization system for digital forensics in network traffic. They stated that because users' information on the network could be easily obtained from the interface, this system could provide a comprehensive analysis of network traffic and it had certain advantages for efficiently revealing clues related to digital forensics [23].
[24,25]	Forensic network traffic tools, such as TCPDump [24] and Snort [25], capture network traffic in different formats at different levels and analyze them by matching rules and creating event logs.
Ghafarian [26]	In his research, Ahmad Ghafarian focused on the analysis of cloud storage services in digital forensics and he carried out his study on a copy of Dropbox. He analyzed the traffic log files by using the Wireshark forensic network tool. In this way, much more information such as the suspect's file access history, the identity of the person who accessed the file, and the operations performed on the file, was revealed [26].
Khan et al. [27]	Khan et al. compared the conventional network forensics and SDN (Software-Defined Networking) forensics to highlight the fundamental differences between them. They presented a brief motivation for SDN forensics in order to emphasize its significance. Moreover, they discussed challenges faced in SDN forensics by highlighting potential research areas for academicians, researchers, and investigators [27].
Easwaramoorthy et al [28]	Easwaramoorthy et al. used Microsoft One Drive and Amazon Cloud Drive, which are two popular open cloud service providers, to carry out forensic evidence collection procedures through the browser and service provider on a Windows 7 computer [28].
Quick [29,30]	In their research, Darren Quick and his colleagues focused on the collection of data related to users in multiple cloud storage, which is one of the main difficulties in cloud storage [29]. They obtained various types of evidence data that are located on the end-user machine in cloud storage and are access points of forensic investigators for examining and collecting evidence in the time period [30].

III. FORENSIC COMPUTING

Digital forensics is also described as the process of examining electronic devices for the purpose of collecting evidence related to a crime on all types of electronic devices by using special examination and analysis techniques [31].

James Barek likens forensic informatics to the process of examining the crime scene or performing an autopsy on a victim. The purpose of digital forensics can be defined as the collection, examination, analysis, and reporting of evidence, respectively [32].

Nowadays, the potential for harm caused by an ever-increasing number of digital forensics crimes due to the widespread use of electronic devices continues to enter and occupy our lives. The Federal Bureau of Investigation (FBI) estimates that the cost of cybercrime in the world is more than 100 billion dollars a year. In order to cope with these crimes, it is necessary to know well the new and previous methods of investigation. Due to improper intervention, evidence can be damaged, destroyed, or changed [33].

Digital forensics investigation techniques help to solve cases related to not only the crimes, such as cyber hacking or child pornography, but also other crimes such as murder, terrorism, organized crime, tax evasion, drug trafficking, and extortion. In the digital age in which we live, it is practically not possible to obtain the types of evidence needed to solve many of the cases brought into the court system. Therefore, nowadays, digital forensic science is an extremely reliable and useful resource that is necessary for many cases.

Modern digital forensics has a wide range of applications. With the rapid development of informatics in the world, digital forensic science is also developing in parallel, and new ones are being added to its application areas every day. Common application areas are given below:

- Storage and recovery of data
- Conversion of data safely
- Transportation of data safely
- Encryption and decryption
- Detecting and preventing abuses
- Search for hidden files
- Control works in financial audits
- Investigation and analysis of all types of commercial disputes
- Reviews related to legal proceedings and trials

In the literature, Digital Forensics is divided into different types with very different names. In fact, although they are divided into different types, the functioning of the processes in each branch of digital forensics is the same. Within the scope of this study, we examine the types of digital forensics as four different sub-branches in general: Computer Forensics, Network Forensics, Mobile Forensics, and Social Network Forensics.

Nowadays, forensic investigations performed on computers and their components are known as the most commonly used digital forensics type. In the field of computer forensic science (computer forensics), it is necessary to ensure the safety and examination of all types of computers and their components, used by the offender or located in the environment where the crime was committed, by the forensic units in accordance with the rules of procedure [34].

One of the issues that should be considered at the first stage for all types of computers and their components found at the crime scene is to take the "Write Blocker" precaution. That is, first of all, it is necessary to take images of computer components that are at the crime scene.

Network Forensics refers to the forensic examination carried out as a result of criminals infiltrating the network systems of any institution or persons and damaging these systems for financial gain or personal entertainment, as well as monitoring carried out by forensic units to prevent or detect such incidents. In such cases, it is necessary to examine the packets outgoing over the network when performing network forensic analysis. The most important evidence that can be analyzed is packet data captured over the network.

Thanks to network forensics, transmitted packets are examined instantaneously or at certain time intervals. The important data obtained as a result of the examinations are used in early warning systems when it is considered necessary.

Network forensics is usually used in two conditions. The first is related to security. This includes monitoring a network for abnormal traffic and identifying interventions. For example, suppose that through a network, the security mechanism has been breached, and after obtaining important information on a computer, all log files have been deleted. In this case, only network-based data and signs can be used as evidence [35]. The second case is more related to law enforcement agencies. This may include tasks such as analyzing network traffic, reassembling transferred files, and ensuring the security of communications.

Mobile Forensics (or mobile device forensics) is the acquisition of criminal devices for all types of crimes committed using different brands of mobile devices, the identification, analysis, and reporting of information that may be a criminal element in such devices by using the necessary software, and transmission of them to the judicial authorities. The term mobile device usually refers to mobile phones; however, it may also refer to any digital device with both internal memory and communication capabilities, including PDA devices, GPS devices, and tablet computers.

Mobile devices can be used to save various personal information, such as photos, calendars, notes, and SMS/MMS messages. Smartphones can also contain video, email, web browsing information, location information, social sharing messages, and contacts.

The important reasons why mobile devices have been used a lot in digital forensics in recent years are as follows [36]:

- The fact that they store personal and corporate information
- Increased use of mobile phones for communication
- The use of mobile phones in online transactions
- The fact that many of the recent crimes have been committed using mobile phone devices

The biggest disadvantage encountered when conducting a digital forensics investigation on mobile devices is that because many different brands and models of smartphones are used today, the investigations to be conducted are model-dependent in some cases.

Social Network Forensics has been accepted as a new type of digital forensics in recent years due to the increasing number of social networking sites in parallel with the spread of the internet and, accordingly, the increasing number of criminal acts [37]. Due to the widespread use of social networking sites, the spread of malware has become easier and some acts such as human trafficking, drugs, prostitution, and fraud have increased. At the stage of detecting these actions and evaluating electronic evidence, social network forensics is used.

Important social networking applications such as Facebook, Twitter, and Linkedin can cause misuses such as copyright infringement, data protection violations, libel,

identity theft, harassment, and the dissemination of confidential information. The means used to prove an incident that has occurred are called evidence [38]. Digital forensic evidence is all types of information or digital objects that can record data and perform all kinds of automated operations on this data and that can be accepted at the stage of clarification of a committed crime.

Based on the above description, it can be said that all digital devices that have the ability to store data during the intervention at the initial stage of the incident are potential evidence and must be examined. Any information and data that can be transmitted or stored by digital devices are called digital evidence.

When digital forensics evidence is compared with classical evidence, it can be said that they are much more sensitive than classical evidence. This is because it is very difficult to notice by looking from the outside when changes are made to digital forensics evidence. However, the changes made to the classical evidence can be noticed very easily [39]. Digital forensics evidence should have all the characteristics such as acceptability, reality, integrity, and reliability that should be present in classical evidence.

Nowadays, due to the rapid development of technology, new types of forensic evidence are emerging every day. Some of the most important types of digital forensics evidence are as follows:

- Computers systems (desktop, laptop, server) and their data files
- Computer system components (HDD, Memory) and their data files
- Memory cards, external hard drives and removable backup tools
- Digital cameras and their data
- Mobile devices and their data
- Network devices and their data
- Printers, scanners, and their data
- Biometric tools and their data
- All types of credit cards and their data
- Electronic watches and their data

Digital forensics investigations usually follow the standard stages of the forensic process. To understand and address the legal framework of digital forensics evidence, the stages of the process model are shown in Fig 1. These stages are evidence acquisition, examination, analysis, and reporting.

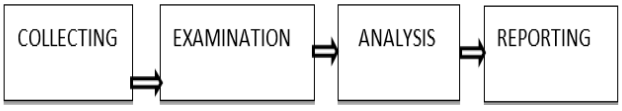

FIG I. FORENSIC COMPUTING PROCESSES

When an accident, crime, or any bad event occurs, the need for an investigation arises. The origins and causes of the incident can be investigated with the help of digital media [40, 41].

It is clear that digital media is useful in investigating the roots and causes of a crime. As already mentioned, most of the crimes have digital links in some way. The digital forensics investigation is a difficult process; evidence may be lost due to reasons such as incorrect shutdown of the system, manipulation or modification of digital evidence, and access to evidence several times [42]. Therefore, finding digital evidence to combat a crime is a reliable, popular, and effective measure. Since digital evidence helps to explain the sequence of the crime [43, 44], it also helps to catch the criminal.

When conducting a digital forensics investigation, many options and techniques can be used to obtain evidence from the environment in which the crime has been committed. Digital forensics investigation teams have certain authorities to collect evidence from the criminal environment [45, 46]. Digital evidence can be obtained from various sources such as mobile phones, digital cameras, pen drives, hard drives, and memory devices. Special attention should be paid to digital evidence since they are vulnerable to interference or can be destroyed.

In addition, log files containing very important information such as remote access, date, time, who is connected to the computer, and who is using it when the connection is lost can also be a great source of evidence. Collecting evidence and catching a criminal who has committed a crime on flash memory or the internet are equally difficult. This is due to the fact that the tools that can be used to collect evidence are either of poor quality or are not sufficient in terms of revealing the identity of the criminal [47].

After the evidence acquisition stage, the obtained data is processed. Each part of the evidence is matched to form the whole event sequence and to reshape the crime scene [48, 49]. Before proceeding to the examination process, investigation methods related to the committed crime should be determined and an examination plan should be put forward. The purpose of the examination plan is to find out what types of data related to crime should be investigated. At this stage, relevant information is identified and extracted from the collected data using appropriate tools and techniques by experts. In the world, software such as EnCase, FTK, and X-Wasy, which are digital evidence examination software accepted by international standards, are often used by digital forensics authorities [50].

The analysis, which is the third stage in the digital forensics process, is the stage where the necessary technical analyzes are performed on the evidence. When the data obtained at this stage were compared with the original data, there should be integrity and content verification between the evidence. The purpose of the analysis is to put forth the correct data revealing the crime as evidence and to make it ready for the reporting stage in a good way.

In the reporting, which is the final stage of digital forensics, the evidence obtained and analyzed must be reported in an explanatory and understandable language for use by the judicial authorities. In relation to the report to be prepared, the following issues should be considered.

- The report must be being completed.
- The report should also be understandable for people without technical knowledge.
- There should be concrete information in the report.
- The digital forensics methods used in the report should be explained in detail.
- In the report, it should be proved that the integrity of the evidence is not destroyed.
- The report should help to uncover the crime and catch the criminal.

IV. Conclusion And Discussion

Due to the widespread use of information technologies in our country, as in the whole world, it also brings security problems. It is not enough to fight cyber crimes committed through information technologies only with law enforcement. In the fight against cyber crimes, both forensic laboratories and expert personnel are needed.

The principle of protection of personal data and the right to privacy, which are important issues to be considered during the collection of electronic evidence in international law, have also been regulated and secured. The United Nations (UN) Universal Declaration of Human Rights, especially article 12, and article 17 of the UN International Covenant on Civil and Political Rights, in the UN's policy decisions on the protection of personal data issued on various dates, the OECD at different times. The privacy of private life and the protection of personal data are guaranteed in its decisions and many other international texts [51].

Forensic software generally includes many functions, but some tools come to the fore for certain functions [52, 53]. These functions can be grouped as e-mail review, message review, internet history review, data acquisition and location information acquisition. We can group forensic tools according to certain characteristics. As we can group hardware-based and software-based, it can be grouped in various ways according to whether it is open source or not, and finally, according to its functions. In this study, we divided the forensic tools into two as hardware and software tools.

Before doing research, a forensic expert should have a good knowledge of the internal and external structure of the system and the settings of the hard disks. Today, there are many forensic hardware tools such as FRED, Image MASSter Solo, Tableau from the field of forensics. Each hardware tool has different functions according to the research scenario. In addition, these tools include necessary write blockers to prevent tampering with evidence [54].

Today, new forensic software is constantly being developed. The software tools used in this field often vary according to the type of investigation being performed. Forensic software tools can be characterized by data recovery tools, partition tools, disk colonization tools, recovery tools, test tools, RAM test utility, system speed test, hard disk tools, system information tools, DOS tools, and other tools.

Encase, ftk, X-ways are the most used software in the field of forensic informatics. We cannot reach definite conclusions about which of these softwares are better because each software is better in a certain area. For example, while indexing and search methods are more advanced in ftk software, this feature may not be available in all versions of other software. In addition, while the scripts used in Encase software are frequently used by users, this is not the case in other software. Apart from these, it is more logical for a forensic software user to choose which software is more comfortable to use [55].

Digital forensics science is a discipline that is changing and developing every day. Individuals, institutions, or states engaged in scientific studies in this field should adapt to innovations in a short time. Today, with using digital devices by many people, cybercrime is also increasing day by day; in parallel, the analysis of digital evidence is becoming an important element at many crime scenes. The principle of personal data protection and ensuring the confidentiality of private life take place among the important issues to be considered during the collection of evidence in digital forensics investigations. To be able to cope with these crimes, the new and previous methods of investigation should be known well. Due to improper intervention, evidence can be damaged, destroyed, or changed. Digital forensics investigations techniques help not only to solve cybercrime, such as hacking or child pornography, but also to solve other crimes, such as murder, terrorism, organized crime, tax evasion, drug trafficking, and extortion. In the digital age in which we live today, it is practically impossible to obtain the types of evidence needed to solve many of the cases brought into the court system. Although digital forensics has been an exciting popular profession that pays attention to the human element in recent years, it also contains various difficulties due to the need to uncover digital evidence in an ever-changing environment. Due to technological advances and situations where anti-forensics methods can easily come into play, experts working in this field need to comply with current standards and constantly review standard stages of work.

Within the scope of this study, national and international books, theses, articles, papers published in recent years related to digital forensics and internet sites that are good in this field were examined in detail. In the first part of this research, the literature studies conducted in recent years related to digital forensics were included generally. In the literature review, digital forensics tools and methods used to automatically recover deleted or corrupted metadata and files by using different methods were mentioned, and a comparison of these methods was made. In the second part of the research, the general definitions used in the digital forensics literature were mentioned, and taking into account the fact that in today's world the cost of cybercrime is more than 100 billion dollars a year, the importance of digital forensics was discussed. In addition, the application areas of digital forensics were briefly mentioned. In terms of the types of digital forensics, computer, network, mobile, and social network forensics sciences were touched upon in general terms. While studying the digital forensics processes, the standard stages of the forensic process and the evidence acquisition, examination, analysis, and reporting stages were discussed in detail, and the

legislation of digital forensics was touched on shortly. In addition, the general characteristics of hardware and software tools used in digital forensics investigations were mentioned in detail. A comparison of the most popular of these tools was made. This research was prepared as a preliminary study on what kind of path should be followed when conducting a study on digital forensics. Although there are studies related to digital forensics conducted by private companies in our country, any study at the doctoral dissertation level has not been conducted in this field in academic terms. In this context, it is believed that both the provision of high-quality undergraduate education related to digital forensics and the organization of good certificate programs related to this issue will make a positive contribution to this field in our country.

REFERENCES

[1] Walker, C. (2006). Computer forensics: bringing the evidence to court. Retrieved August, 23, 2008.

[2] Hand, Scott, et al. "Bin-Carver: Automatic recovery of binary executable files." Digital Investigation 9 (2012): S108-S117.

[3] Narayanan, A. Sankara, and M. Mohamed Ashik. "Computer Forensic First Responder Tools." Advances in Mobile Network, Communication and its Applications (MNCAPPS), 2012 International Conference on. IEEE, 2012.

[4] Pal, Anandabrata, and Nasir Memon. "The evolution of file carving." IEEE Signal Processing Magazine 26.2 (2009): 59-71.

[5] William Ballenthin, "NTFS INDX Attribute Parsing", http://www.williballenthin.com/forensics/indx/index.html. [Accessed: 10-May-2021]

[6] Al Mutawa, Noora, Ibrahim Baggili, and Andrew Marrington. "Forensic analysis of social networking applications on mobile devices." Digital Investigation 9 (2012): S24-S33.

[7] A forensics overview and analysis of USB flash memory devices, Krishnun Sansurooah. Proceedings of the 7th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia,2009.

[8] Arthur, Kweku K., and Hein S. Venter. "An Investigation Into Computer Forensic Tools." ISSA. 2004.

[9] Guo, Hong, Bo Jin, and Ting Shang. "Forensic investigations in cloud environments." Computer Science and Information Processing (CSIP), 2012 International Conference on. IEEE, 2012.

[10] Wiger van Houten, Zeno J. M. H. Geradts, Katrin Franke, and Cor J. Veenman, "Verification of video source camera competition (camcom 2010)," in ICPR Contests, 2010.

[11] Garfinkel, Simson. "Digital forensics XML and the DFXML toolset." Digital Investigation 8.3 (2012): 161-174.

[12] Ling, Tang. "The study of computer forensics on linux." Computational and Information Sciences (ICCIS), 2013 Fifth International Conference on. IEEE, 2013.

[13] Bestagini, Paolo, et al. "An overview on video forensics." Signal Processing Conference (EUSIPCO), 2012 Proceedings of the 20th European. IEEE, 2012.

[14] Pan, Yin, et al. "Game-based forensics course for first year students." Proceedings of the 13th annual conference on Information technology education. ACM, 2012.

[15] Guo, Yinghua, Jill Slay, and Jason Beckett. "Validation and verification of computer forensic software tools—Searching Function." digital investigation 6 (2009): S12-S22.

[16] Cho, Gyu-Sang. "NTFS Directory Index Analysis for Computer Forensics." Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2015 9th International Conference on. IEEE, 2015.

[17] Kaur, Harjinder, and Nivit Gill. "Host based anomaly detection using fuzzy genetic approach (FGA)." International Journal of Computer Applications 74.20 (2013).

[18] Deepak Scholar, Hitesh Gupta, "Digital Crime Investigation using various Logs and Fuzzy rules: A Review", IJARCCE, Vol 2, Issue 4, April, 2013.

[19] Michihiro Kobayashi, Takahiro Okabe, and Yoichi Sato, "Detecting forgery from static-scene video based on in-consistency in noise level functions," IEEE Transactions on Information Forensics and Security, vol. 5, pp. 883– 892, 2010.

[20] Li Weiwei. Computer Forensics Analysis based on EnCase System. Jilin Normal University Journal. 2011. Vol 32.

[21] Kroll Ontrack. Ontrack EasyRecovery. http://www.krollontrack.co.uk/data-recovery/data-recovery-software/. [Accessed: 6-May-2021]

[22] [Joe Grand. pdd: Memory Imaging and Forensic Analysis of Palm OS Devices. Proceedings of the 14th Annual first Conference on Computer Security Incident Handling and Response. 2002.

[23] [Shi, Ronghua, et al. "A Matrix-Based Visualization System for Network Traffic Forensics." IEEE Systems Journal 10.4 (2016): 1350-1360.

[24] [Shorey, R., Kamra, A., Kapila, S., Khurana, V., & Yadav, V. (2006). U.S. Patent No. 7,065,482. Washington, DC: U.S. Patent and Trademark Office.

[25] [Snort. [Online]. Available: http://www.snort.org [Accessed: 4-May-2021]

[26] Ghafarian, Ahmad. "Foreniscs analysis of cloud computing services." Science and Information Conference (SAI), 2015. IEEE, 2015.

[27] [Khan, Suleman, et al. "Software-Defined Network Forensics: Motivation, Potential Locations, Requirements, and Challenges." IEEE Network 30.6 (2016): 6-13.

[28] Easwaramoorthy, Sathishkumar, et al. "Digital forensic evidence collection of cloud storage data for investigation." Recent Trends in Information Technology (ICRTIT), 2016 International Conference on. IEEE, 2016.

[29] Quick, D., & Choo, K. K. R. (2013). Dropbox analysis: Data remnants on user machines. Digital Investigation, 10(1), 3-18.

[30] Quick, D., & Choo, K. K. R. (2013). Digital droplets: Microsoft SkyDrive forensic data remnants. Future Generation Computer Systems, 29(6), 1378-1394.

[31] Adli bilişim, http://www.leylakeser.org/2008/07/adli-biliim-cmk-md-134-ve-dndrdkleri.html [Accessed: 2-May-2021].

[32] Kim, Y., Kim, K.J.,"A Forensic Model on Deleted-File Verification for Securing Digital Evidence", 978—1-4244-5493-8710 IEEE, 2010;

[33] Ademu, I. O., Imafidon, C. O., & Preston, D. S. (2011). A new approach of digital forensic model for digital forensic investigation. Int. J. Adv. Comput. Sci. Appl, 2(12), 175-178.

[34] Peisert, S., Bishop, M., & Marzullo, K. (2008, May). Computer forensics in forensis. In Systematic Approaches to Digital Forensic Engineering, 2008. SADFE'08. Third International Workshop on (pp. 102-122). IEEE.

[35] Erik Hjelmvik, Passive Network Security Analysis with NetworkMiner http://www.forensicfocus.com/passive-network-security-analysis-networkminer. [Accessed: 5-May-2021]

[36] [Ahmed, R., & Dharaskar, R. V. (2009, March). Mobile forensics: an introduction from Indian law enforcement perspective. In International Conference on Information Systems, Technology and Management (pp. 173-184). Springer, Berlin, Heidelberg.

[37] Özocak, Gürkan, "Sosyal Medyada İşlenen Suç Tipleri ve Suçluların Tespiti", Yenimedya Çalışmaları II. Ulusal Kongresi – Kongre Kitabı, Kocaeli, 2013, s. 465.

[38] Uğur BAHADIR – Devletler Özel Hukukunda İspata Uygulanacak Hukuk http://www.turkhukuksitesi.com/makale_131.htm. [Accessed: 5-May-2021]

[39] Özbek, M. (2013). Adli bilişimde delillerin toplanması ve incelenmesi (Doctoral dissertation, İstanbul Bilgi Üniversitesi).

[40] Bahadur, P., & Yadav, D. S. (2015, November). Computer forensics-digitized science. In SAI Intelligent Systems Conference (IntelliSys), 2015 (pp. 1025-1031). IEEE.

[41] Dunbar, B (January 2001). "A detailed look at Steganographic Techniques and their use in an Open-Systems Environment".

[42] Digital forensics and the legal system: A dilemma of our times James Tetteh Ami-Narh,Patricia A.H. Williams, Proceedings of the 6th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia,December, 2008.

[43] Baryamureeba, V., & Tushabe, F. (2004, August). The enhanced digital investigation process model. In Proceedings of the Fourth Digital Forensic Research Workshop (pp. 1-9).

[44] Conference on Digital Forensics, Security and Law, 2006 http://www.digitalforensics-conference.org/CFFTPM/CDFSL-

proceedings2006-CFFTPM.pdf Marcus K. Rogers ,James Goldman, Rick Mislan,et. al.

[45] Various (2009). Eoghan Casey, ed. Handbook of Digital Forensics and Investigation. Academic Press. p. 567. ISBN 0-12-374267-6. Retrieved 27 August 2010.

[46] Geiger, M. (2005, August). Evaluating Commercial Counter-Forensic Tools. In DFRWS.

[47] Remote Access Forensics for VNC and RDP on Windows Platform. Paresh Kerai, Proceedings of the 8th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, November,2010.

[48] Noblett, M. G., Pollitt, M. M., & Presley, L. A. (2000). Recovering and examining computer forensic evidence. Forensic Science Communications, 2(4), 1-13..

[49] Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. International Journal of Digital Evidence, 1(3), 1-12.

[50] Altschaffel, R., Kiltz, S., Dittmann, J., "From the Computer Incident Taxonomy to a Computer Forensic Examination Taxonomy", 2009 Fifth International Conference on IT Security Incident Management and IT Forensics, 2009.

[51] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,OECD,http://www.oecd.org/document [Accessed: 10-May-2021]

[52] Özen, M., & Özocak, G. (2015). Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134). Ankara Barosu Dergileri, 73(1).

[53] Adli bilişim, http://www.telepati.com.tr/agustos12/konu8.htm.[Accessed: 5-May-2021].

[54] Bill Nelson, Amelia Phillips, Frank Enfinger, Chris Steuart, Computer Forensics and Investigation, Cengage Learning, 2010 ISBN: 1435498836,9781435498839.

[55] Forensic, httpwww.dijitaldeliller.comyazilimlar.htm. [Accessed: 10-May-2021].