UFSM

REGET/UFSM
Revista Eletrônica em Gestão, Educação e Tecnologia Ambiental

ISSN 2236-1170
Acesso aberto

REGET, Santa Maria, v. 25, e5, 2021 • https://doi.org/10.5902/2236117063798
Submitted: 25/09/2020 • Approved: 29/12/2020 • Published: 22/ 03/ 2021

Environmental Technology

Digital forensics and its role in promoting criminal prosecution

Análisis forense digital y su papel en la promoción del enjuiciamiento penal

Seyyed Sajjad Kazemi[I], **Sajjad Heidari**[II]

[I] Assistant Professor, Malayer University, Malayer, Iran
[II] Hamadan Branch, Islamic Azad University

ABSTRACT

Digital forensics is essentially synonymous with computer forensics, but the term "digital forensics" is generally used for the technical review of all devices that have the ability to store data. Today, digital criminology is challenged in cloud computing. The first problem is to understand why and how criminal and social actions are so unique and complex. The second problem is the lack of accurate scientific tools for forensic medicine in cyberspace. So far, no complete tools or explanations for criminology have been provided in the virtual infrastructure, and no training for security researchers has been provided in detail. Therefore, the author of the present descriptive-analytical research is based on library resources and using fish taking tools. To investigate suspicious cases related to cyberspace, criminologists must be well-equipped with technical and legal issues to deal with. In this article, we analyze digital criminology and its role in judicial law. The benefit of computer forensic knowledge is not only an indispensable necessity for security and judicial institutions, but also professional users and owners of computer systems, systems and networks must be fully aware of and properly comply with its legal and technical requirements.

Keywords: Digital Forensics; Criminalization; Judicial Law; Cloud Computing

RESUMEN

El análisis forense digital es esencialmente sinónimo de análisis forense informático, pero el término "análisis forense digital" se utiliza generalmente para la revisión técnica de todos los dispositivos que tienen la capacidad de almacenar datos. Hoy en día, la criminología digital se enfrenta al desafío de la computación en la nube. El primer problema es comprender por qué y cómo las acciones criminales y sociales son tan únicas y complejas. El segundo problema es la falta de herramientas científicas precisas para la medicina forense en el ciberespacio. Hasta ahora, no se han proporcionado herramientas completas o explicaciones para la criminología en la infraestructura virtual, y no se ha proporcionado ninguna formación detallada a los investigadores de seguridad. Por lo tanto, el autor de la presente investigación descriptivo-analítica se basa en los recursos de la biblioteca y en el uso de herramientas de pesca. Para investigar casos sospechosos

relacionados con el ciberespacio, los criminólogos deben estar bien equipados con los problemas técnicos y legales que abordar. En este artículo analizamos la criminología digital y su papel en el derecho judicial. El beneficio del conocimiento forense informático no solo es una necesidad indispensable para las instituciones de seguridad y judiciales, sino que también los usuarios profesionales y propietarios de sistemas, sistemas y redes informáticas deben conocer y cumplir debidamente sus requisitos legales y técnicos.

Palabras clave: Forense digital; Criminalización; Derecho judicial; Computación en la nube

1 INTRODUCTION

Digital forensics experts have a variety of tools to prove or disprove the charges against criminals or citizens. Digital forensics is technically divided into several sub-categories: Computer forensics Network forensics and intrusion detection Forensics malware Forensics analysis Data forensics Mobile forensics (TURKMANI ET AL, 2017).

Cloud computing is still an emerging technology and will inevitably expand in the future. However, defective policy makers as well as ineffective laws have made criminology researchers in cybercrime problematic. Many technical issues need to be carefully considered when investigating cloud computing issues (CONTI et al, 2018). Today, digital criminology is being challenged for cloud computing. The first problem is to understand why and how criminal and social practices in cloud computing are so unique and difficult. The second problem is the lack of accurate scientific tools for forensic cloud computing. To date, no complete tool or explanation has been provided for criminology in the cloud infrastructure, and no training has been provided to security researchers accurately (TAYLOR ET AL, 2014). This article analyzes digital criminology and its role in law judicial review.

2 METHODOLOGY

The methods of this study is descriptive-analytical research is based on library resources and using fish taking tools.

Continue...

3 RESULTS

3.1 Digital forensics

One consequence of the expanding space of information and communication exchange is the many challenges that trade secrets have created as valuable and confidential information, such as the widespread response of governments to the use of coercive tools that have strong deterrent effects has been with Terry (KARAMPIDIS et al., 2018). But the unique features of cyberspace, along with a variety of ways of exploiting it, minimize the possibility of identifying infringers and give rise to the idea that current criminal policy has the potential to be effective in protecting trade secrets does not have. Therefore, business secrets are forced to use the most dynamic security tools available to protect their vital information, in addition to the fact that the legislature has borne some of the cost of crime prevention (CHANG et al, 2019).

Entering the age of information and communication technology has created a new era of human life, which is referred to as the information society. Cyber space, as the most iconic product of this community, has given people immense opportunities to search for or store massive amounts of information. This has not only brightened the face of information, especially scientific and economic findings, but also led to the rise of targeted cyber-attacks aimed at unauthorized access to such valuable information. In the meantime, the idea of protecting trade secrets has gained double importance as information of independent economic or competitive value (LIEBLER et al, 2019).

Article 65 of the E-Commerce Act covers trade secrets including a wide range of confidential data such as formulas and templates, software, tools and methods, unpublished authorship, methods of doing business, techniques, techniques, Maps, metrics, financial information, customer lists and business plans know that the information holder has made reasonable efforts to protect and protect them. The Uniform Commercial Secrets Act also defines trade secrets: "Information including a formula, pattern, composition, program, device, method, technique, or process whose first, economic, actual or potential value This results from the fact that no one is generally known and is not readily available to other

persons who can gain economic benefit by disclosing or using it. Secondly, conventional efforts have been made to keep it secret (LOSAVIO, 2018).

With the advances in technology and the increasing use of human technology, we are witnessing the advent of computers in all social, economic, political and legal activities. This progress is so much seen in different realms of life, that it can be claimed that computers have become inseparable components of people's lives in the present age. And it has brought a new branch to the forensic scientists to identify and respond to abuses of technology and cyberspace (CARLTON, & KESSLER, 2018). And there were specialized laws and organizations specialized in this regard, such as the International Computer Forensics Organization and the International Organization for Digital Evidence. Computer forensics was formed to gather evidence from computer equipment and storage devices and to provide them to the judicial authorities in a meaningful and coherent format. Due to the increasing progress of science and technology, computer science and digital devices, the field of computer criminology has now been upgraded to digital criminology.

In today's modern world, with the advent of technology, crime is on the rise. Therefore, identifying and gathering sufficient reasons to substantiate the crime and to identify who it was and by what means and how it happened is essential. Digital forensics seeks to gather, analyze, and analyze information available on computer systems that collect evidence that investigates the offender and the circumstances of the crime and discovers credible evidence to be presented to the court and legal authorities (POPESCU & FARID, 2004).

Digital forensics involves monitoring network traffic and determining whether or not there is anomalies in traffic and proving whether the attack is present or not! If an attack is detected then the nature of the attack is also identified. Network crime-detection techniques enable researchers to track attackers. The ultimate goal of digital forensics is to provide sufficient evidence to allow the defendant to be prosecuted (GARFINKEL et al, 2009). The ultimate goal is to provide sufficient evidence to authorize the prosecution of the accused. This process first requires identifying and gathering information about the attack and its accuracy. Then by combining the correct information using the a priori algorithm, one can analyze the attack and the output of the algorithm is evaluated by decision-based

integration. This helps improve situational awareness. The outputs of this issue include a detailed understanding of the vulnerabilities and vulnerabilities that make the attack possible. This information helps security administrators configure systems to prevent similar events from happening in the future (CHANG et al, 2019).

2. Tools used in digital scaling:

• Data Recovery Software: This tool can recover deleted or manipulated files by criminals.

• Memory Copy Software: Because it removes part of the memory as soon as the computer is turned off and makes it difficult to access hard data, the software is used to copy the memory.

• Data Comparison Tools: In order to prove that the data presented to the court is the data that was left out of the crime, we need to compare them together to provide valid evidence.

• Meta Data Accessibility Tools: When stored on a computer or used on a computer, that file sends a series of details about itself to the operating system that can be used as evidence.

• Data and passwords decryption tools: Sometimes more advanced criminals encrypt files for different files and parts, making it difficult and time consuming for the forensic examiner to decode. At this time, decoders can solve the problem (CONTI et al, 2018).

3.2 The digital forensic process

The process of digital forensics involves:

1. Seizure of digital devices.

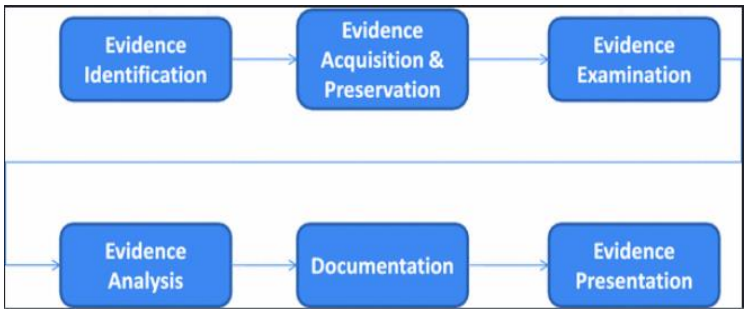
2. Take over all the data carriers (both internal and external) that are called image capture.

3. Analyze and analyze all the content in the generated images.

4. Full report of all the evidence obtained from Step 1 (Documentation)

Continue...

Figure 1- The Digital Forensics Process



Source: Authors (2020)

Based on Figure 1, the scoring algorithm is as follows:

- Identify various crime-related information, components, and entities.
- - Protecting the crime scene and its evidence without any damage or alteration
- -Data collection
- Analyze the data and information collected and evaluated by the tools
- - Provide documentation and final report classified as above
- Types of digital criminology

Divided into two levels:

Low level: small enterprise networks - personal site - personal system (mobile, system, laptop and ...

High Level: National Level - Ministries - Governmental Organizations - Institutions and Organizations After infiltrating the victim system, we do not collect and extract data from computer equipment and report to law enforcement unless it causes high losses. Enter the person (CHANG et al, 2019).

For example, a bank account was hacked by a person's personal site - stealing people's information, including photos, videos, etc. from a high-level personal information system to alert the government to malware, viruses, and the like It does (CARLTON & KESSLER, 2018).

Continue...

3.3 Types of digital forensics

Digital forensics or digital forensics means the science of obtaining evidence, and digital forensics is the process of discovering and interpreting electronic data. The purpose of this process is to preserve and provide evidence in its original form. This is very important in the field of criminology and crime proof in the legal and judicial authorities (POPESCU & FARID, 2004).

It means science is the pursuit of evidence, and digital forensics is the process of discovering and interpreting electronic data. The purpose of this process is to preserve and provide evidence in its original form. This is very important in the field of criminology and crime proof in the legal and judicial authorities (CHANG et al, 2019).

Types of Digital Forensics:

Computer forensics: Discovering, preserving, collecting, analyzing, and reporting documents that exist on computers and laptops for use in judicial authorities.

5. Forensic Mobile: Recovers electronic evidence from mobile phones, smartphones, tablets and SIM cards.

2- Network Forensics: View, record, and store activities and events that occur on the network. This can detect network problems, viruses, malware, network intrusion, and abnormal network traffic.

Forensic Digital Imaging: Digital extraction and analysis of photographic images to verify the authenticity of a photograph by reference to its history.

Digital Forensics Videos and Podcasts: Analyze video and audio to verify it and check whether it has been tampered with or whether it has been accidental or intentional.

Forensic Memory: Recovering Documents from Computer and Laptop RAM.

The Impact of Digital Crimes on Judicial Law

In recent years, along with the development of computer-based technologies in various fields, including information technology, we have witnessed a significant increase in crime at the community level, especially in the Internet. Increasing concerns about the security of computer information systems and networks have led to scientific methods and solutions being combined with criminal and civil laws and regulations, in the hope of

alleviating the material and moral damages of these crimes. It may be argued that the emergence and development of knowledge, known as "computer forensics", was due to the fears and hopes of human society in recent years.

Most people are more or less familiar with crime scenes and work on crime scenes and idioms such as fingerprinting, the discovery of a killer or victim's DNA, as well as forensics and centers such as forensics, but are less likely to use computer forensics. Their ears are not very familiar with it as one of the world's top sciences.

Forensic knowledge has been used for many years (in its general sense) in various countries' lawsuits and criminal cases to provide and submit court-produced evidence to judicial authorities. In this article, we have tried to provide a brief description of this knowledge in the field of computing to the general public as well as those interested in such topics.

Forensic science generally involves the collection, preservation and evaluation of evidence, the analysis and analysis of found and hidden data scientifically and in accordance with legal standards in order to be submitted to the competent authorities. This science comprises several main branches. The following are among the most important (KARAMPIDIS et al, 2018).

• Forensic Physiological Sciences, which is subdivided into Forensic Chemistry, Biology, Dentistry and the like.

• Forensic Behavioral Sciences, which is a forensic psychology subsystem.

• Digital forensics, which includes computer, audio and video forensics, cell phones, databases, and more.

• And more

Digital Forensics As defined by the National Center for Forensic Sciences based at the University of Central Florida, the US is: [Identification, collection, preservation, review and analysis of digital evidence]. According to the center, any valuable cached information stored or moved binary is included in digital documentation. Not only does it include computers in their common sense (PCs and servers) but also audio and video. Graphics and digital movies are also included (CARLTON & KESSLER, 2018).

Computer forensics in particular involves a systematic process of collecting and analyzing data from systems, networks, wireless exchanges, and computer storage devices that combine forensic and computer science elements to file forensic evidence. In fact, the main purpose of the use of computer forensic knowledge is to ensure the accuracy and reliability of the evidence presented to the investigating authorities.

There has been no comprehensive definition of cybercrime so far, but it is generally referred to as crimes in which the computer was either intended for crime or used as a crime tool.

For decades, countries such as the United States, the United Kingdom, and Russia and other IT nations have been thinking about designing and organizing the security of their information systems and computer networks to reduce crime. Therefore, it seems that the technical and scientific tools and techniques of the developed countries in the field of computer forensic science can be used with the least concern and their experience in this field (KARAMPIDIS et al, 2018).

However, since the legal system governing the judiciary and law enforcement authorities in different countries varies, computer forensics practitioners at all levels and situations must act in accordance with their country's rules and regulations to have their documents available to judicial authorities. . Therefore, full awareness of these laws and regulations is essential for all institutions and organizations active and connected to computer systems and networks. In the following, we will look at these two key aspects of computer forensics and provide some tangible examples to clarify this (CHANG et al, 2019).

The legal aspect of computer forensics

One of the most important legal issues in computer forensics is the principle of privacy. In accordance with the standards of most legal systems, all organizations, organizations and computer systems are required to observe this principle by safeguarding and safeguarding the data and information of persons located in a variety of ways. Observing such legal considerations, while helping to raise the level of trust in these organizations and organizations, will help alleviate their legal liability for potential damages in the event of an accident (LIEBLER et al., 2019).

Although the principle of privacy (both real and legal) is one of the most important principles embodied in the legal systems of today's world, it seems to be fully enjoying this fundamental right with the modern world equipped with advanced computer tools and expanding cyberspace, with serious problems Encountered. At least in computerized virtual spaces and networks, it seems like a dream come true. No matter where you are today, the more sophisticated and easy-to-use computer technologies there are the more unfortunate your privacy is (KARAMPIDIS et al., 2018).

Among the important issues in computer security and computer forensics are the level of accessibility of people working in the deployment of computer information systems and systems, and the special attention of the relevant agencies on this issue seems to be urgently needed. Public opinion and legal and technical experts point out, is a low-level security officer's access to this wide range of American people's information consistent with the principles and rules governing that country? According to Edvard Snowden himself, as a regular contractor, he not only had complete access to personal information, but was able to store all of them on a number of laptops without any restriction and to bring them out with the broad security organization. . These include questions that must wait until the end of the scandal to reach an answer, but what is certain is that most of these questions can be answered accurately through computer forensics, so that there is no doubt Don't stay (LIEBLER et al., 2019).

Bitter events have recently taken place in our own country, demonstrating the importance and necessity of utilizing forensic knowledge in its computer domain. Perhaps if computer forensics and security were better adhered to, malicious virus would not easily penetrate the heart of our atomic centers and would not cause such material or moral damage or become more rapidly and accurately probable after the event. More effective follow-up provided this assault in international law communities (POPESCU, AND FARID, 2004).

Other questions related to computer forensic knowledge and privacy that may be on the minds of many are whether the content of emails and messages exchanged in cyberspace by someone on their security or any other charges, Can it be cited as legal

evidence against or against the accused in judicial authorities? The answer that comes to mind is two basic conditions: if those documents are produced in accordance with the scientific and technical requirements of forensic science and at the same time the text of those messages conforms to the criminal content provisions stipulated in the Code of Cybercrime (CARLTON AND KESSLER, 2018).

Another area of concern in computer forensic law is the theft of information in commercial and industrial activities, with increasing material and intellectual damages resulting from it. In any organization there are a limited number of people who have access to critical information stored in computer systems. Computer forensic knowledge is able to provide the necessary evidence in the event that a person within the organization is betrayed in a way that is legally traceable (CONTI et al., 2018).

Another issue that computer forensic science can play a major role in is copyright. Concerns about copyright infringement have become more widespread with the proliferation of digital products such as application software, audio-visual information, books, scientific articles, and the like in computer systems and cyberspace. Undoubtedly one of the effective ways to prevent such occurrences and to help them prosecute if they occur is to use computer forensic knowledge (LIEBLER et al., 2019).

Computer forensics encompasses a very broad field and its application is not limited to legal and controversial issues such as those mentioned in the adventures. There are some reasons why Forensic entered the case to clarify a lawsuit in a case. For example, an organization employee suspected of sending inappropriate content or being accused of conducting an activity in violation of its organization's internal regulations and security policy through its workplace computer systems. Here, forensic science can verify the veracity of the allegations and, if proven, the offender is usually only responsible for the internal rules and regulations of his organization and does not need to refer those lawsuits to the judicial authorities (CONTI et al., 2018).

Continue...

3.4 Technical aspects of computer forensics

The technical aspect of computer forensics is as important as its legal aspect, and in fact its complement. The foremost issue in the forensic sector concerns how data security and data protection practices are implemented and the interoperability of systems, systems and computer networks as well as data retrieval if needed. There is a great deal of connection between computer forensics and computer security, but it should be borne in mind that the two are completely separate in the field of computer science. Generally, the purpose of computer security knowledge is to keep computer systems in the same safe condition as they are intended for, but forensic computer knowledge is to describe how a computer system is being attacked from a legal perspective. While both of these sciences use similar data sources in their mechanisms, some may be at odds with one another. For example, encryption or the use of data cleaners that are essential to computer security can complicate or delay the process of computer forensics implementation.

The first issue in computer forensics is the technical and scientific conditions of people related to forensics, especially its implementers. These individuals must be scientifically, technically and instrumentally capable of assuring the parties of a legal dispute of the accuracy of the evidence they provide. Cybercrime encompasses a wide range of criminal activities, from theft of personal information to the destruction of intellectual property. Therefore, forensic executives must be fully aware of the nature of the evidence they are seeking. Choosing the right tool is another issue that anchors should consider. Computer files may be damaged or encrypted or even deleted. A forensic practitioner must be familiar with various software and methods to prevent further damage to the recovery process.

In the process of running computer forensics, two types of data are collected. Permanent or permanent data stored in drives that remain on the computer after shutdown, and temporary data, called data stored in the computer's cache or data in transit, disappears when the computer is shut down. Temporary data is stored in the registry, computer cache or RAM. Because temporary data are unmanageable, it is essential that forensic executives have a thorough understanding of their recovery methods. Computer system administrators

and security personnel are among those who must have a good understanding of the impact of their management activities on the computer forensics process (KARAMPIDIS et al., 2018).

CONCLUSION

The widespread material and intellectual damages of cybercrime in recent years have had a clear message to the relevant institutions and organizations that they must have a scientific, well-established and continuous plan to mitigate these damages. Particularly in the last two decades, the discovery and investigation of cybercrime has become one of the main tasks of security and judicial institutions in information technology beneficiary countries. One of the most noteworthy cases of cybercrime is undoubtedly the process of discovering and gathering legal and court evidence. The benefit of computer forensic knowledge is not only an indispensable necessity for security and judicial institutions, but also professional users and owners of computer systems, systems and networks must be fully aware of and properly comply with its legal and technical requirements. Without these institutions and organizations working together, it would be impossible to address these crimes. Since forensic issues are a key component of security infrastructure, attention to the formation and management of centers such as CSIRT can play a significant role in enhancing the level of computer forensic knowledge and thus protecting the privacy and security of individuals.

REFERENCES

CARLTON, G. H., & KESSLER, G. C. Disconnects of Specialized Mobile Digital Forensics within the Generalized Field of Digital Forensic Science. International Journal of Interdisciplinary Telecommunications and Networking (IJITN), 10(3), 62-65, 2018.

CHANG, D., GHOSH, M., SANADHYA, S. K., SINGH, M., & WHITE, D. R. FbHash: A New Similarity Hashing Scheme for Digital Forensics. Digital Investigation, 29, S113-S123, 2019.

CONTI, M., DEHGHANTANHA, A., FRANKE, K., & WATSON, S. Internet of Things security and forensics, International Challenges and opportunities, 18, pp, 78-90, 2018.

EOGHAN, C., SEAN, B. advancing coordinated cyber-investigations and tool interoperability using a community developed specification language, telecom law course, 8, pp, 148-160, 2017.

GARFINKEL, S., FARRELL, P., ROUSSEV, V., & DINOLT, G. Bringing science to digital forensics with standardized forensic corpora. Digital investigation, 6, S2-S11, 2009.

GRAEME HORSMAN, A. Policing and Crime Act 2017: Changes to pre-charge bail and the impact on digital forensic analysis, digital perspective, 21, pp, 56-78, 2017.

GRAEME, H., KEVIN, G., PAUL, C. Identifying offenders on Twitter: A law enforcement practitioner guide, 2018.

JAHANGIRPOUR, A., MAHMOUD, M. Factors Affecting the Increase of Effectiveness of Detectives' Measures in the Crime of Kidnapping, Law Enforcement Studies, https://www.noormags.ir/view/en/articlepage/1609370, 2020.

KARAMPIDIS, K., KAVALLIERATOU, E., & PAPADOURAKIS, G. A review of image steganalysis techniques for digital forensics. Journal of information security and applications, 40, pp, 217-235, 2018.

KHALFI, A. Prevention of cybercrime with a focus on crime detection, Detective, https://www.noormags.ir/view/en/articlepage/1115784, 2016.

LIEBLER, L., SCHMITT, P., BAIER, H., & BREITINGER, F. On efficiency of artifact lookup strategies in digital forensics. Digital Investigation, 28, S116-S125, 2019.

LOSAVIO, M. M., CHOW, K. P., KOLTAY, A., & JAMES, J. The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security. Security and Privacy, 1(3), e23, 2018.

MAJIDI, A., NAZARI MANZAM, M., HINDI, A., WAFADAR, H. Investigating the Factors Affecting the Criminalization of Fraud in Cyberspace, Law Enforcement Studies, https://www.noormags.ir/view/en/articlepage/1609359, 2019.

MESUT OZEL, H., IBRAHIM BULBUL, H., GUCLU YAVUZCAN, OMER FARUK. An analytical analysis of Turkish digital forensics, Digital focus, 9(4), 89-110, 2018.

PARVANEH, A. Challenge of Security Threats in Cloud Computing Resources, National Vision 1420 Conference and Technological Advances in Electrical Engineering, Computer and Information Technology, Shiraz, Iran New Education Development Center (Metana), https: //www.civilica .com / Paper-ECITCONF01-ECITCONF01_039.html, 2017.

POPESCU, A. C., & FARID, H. Statistical tools for digital forensics. In international workshop on information hiding. Springer, Berlin, Heidelberg, pp. 128-1472004.

RICHARD III, G. G., & ROUSSEV, V. Next-generation digital forensics. Communications of the ACM, 49(2), 76-80, 2006.

TAYLOR, R. W., FRITSCH, E. J., & LIEDERBACH, J. Digital crime and digital terrorism. Prentice Hall Press, 2014.

TIMOTHY BOLLE, EOGHAN CASEY. Using computed similarity of distinctive digital traces to evaluate non-obvious links and repetitions in cyber-investigations, digital conference Kent, 2018.

TURKMANI, M. A., AND KEYVAN, R. A Study of Forensic Challenges in May Computing and Its Comparison with Forensic Challenges in Cloud Computing, 3rd National Conference on Innovation and Research in Electrical Engineering and Computer and Mechanical Engineering, Iran, Tehran, Mehr Arvand Higher Education Institute and Center for Strategies for Achieving Sustainable Development, https://www.civilica.com/Paper-ICCONF03-ICCONF03_037.html, 2017.

AUTHORSHIP CONTRIBUTION

1- Seyyed Sajjad Kazemi

Assistant Professor

https://orcid.org/0000-0002-9943-3150 | E-mail: S.skazemi92@Malayeru.ac.ir

Contribuition: Supervision, Project administration, Writing – review & editing, Investigation, Visualization, Methodology, Software

2- Sajjad Heidari

Department of Law

https://orcid.org/0000-0002-2643-9930 | E-mail: sajjad.heidari@gmail.com

Contribuition: Validation, Data curation, Formal Writing – original draft, Analysis, Funding acquisition, Resources, Conceptualization

HOW TO QUOTE THIS ARTICLE

Kazemi, S. S; Heidari, S. Digital forensics and its role in promoting criminal prosecution. Revista de gestão, educação e tecnologia ambiental, v.25, e5, 2021. Available from: https://doi.org/10.5902/2236117063798. Accessed: Month Abbreviated. Day, year.