A Systematic Literature Review in Cyber Forensics: Current Trends from the Client Perspective

Conference Paper · October 2018

DOI: 10.1109/ETCM.2018.8580266

5 authors, including:

Bryan Daniel Coronel
University of Cuenca
2 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Priscila Cedillo
Universidad de Cuenca
39 PUBLICATIONS **52** CITATIONS
SEE PROFILE

Karina Campos
University of Cuenca
4 PUBLICATIONS **5** CITATIONS
SEE PROFILE

Alexandra Bermeo
University of Cuenca
9 PUBLICATIONS **10** CITATIONS
SEE PROFILE

A Systematic Literature Review in Cyber Forensics: Current Trends from the Client Perspective

Bryan Coronel[1], Priscila Cedillo[1,2], Karina Campos[1], Jessica Camacho[1], Alexandra Bermeo[1]
[1]Faculty of Engineering, University of Cuenca
[2]Computer Science Department, University of Cuenca
Cuenca, Ecuador
{bryan.coronel, priscila.cedillo, karina.campos, jessica.camacho, alexandra.bermeo}@ucuenca.edu.ec

***Abstract*— Nowadays, with the demand of web applications there is also an increase in the number of problems and crimes that demand an investigation that requires digital forensics techniques in order to manage web evidence. Although there are several studies that address cyber forensics, they are mainly oriented to manage evidence at server side, as far as we know, no systematic literature reviews have been reported on how cyber forensics is addressed at clients' side; considering the internationals standards. Thus, this paper presents a literature review about how cyber forensics is addressed at clients' side related to techniques of identification, collection, analysis, preservation and report of digital evidence. Also, a review of how standards are being used in cyber forensics focused on the client side. The aim of this study is to provide a background of relevant activities that are considered by investigators to handle potentially digital evidence from web environments, considering what internationals standards are solving for this purpose. Thus, a total of 37 studies have been selected and analyzed in this study. Moreover, this study provides important insights about the need to create methodologies aligned with formal standards that support the management of the evidence in an appropriate way.**

Keywords*— *digital evidence, cyber forensics, client side, systematic review, standards

I. INTRODUCTION

Currently, web applications have been adopted in the majority of transactional systems of organizations. Also, there are applications deployed on web environments for different purposes (e.g., social networks, email, cloud storage). With the mass use of online applications, there is also an increase in the number of crimes, cyber-attacks, and punishable by law activities [1]. In general, people use web browsers or desktop applications that request pages and resources to a server; therefore, it is important to manage digital evidence left in client's computers by using suitable forensics guidelines [2].

Moreover, with the emergence of new web technologies and cloud computing with their service models (i.e., Infrastructure as a Service, Platform as a Service and Software as a Service) [3] the importance of digital evidence has increased substantially [4]. Also, there are studies that consider the current increase in the number of applications deployed on the cloud, several authors address their studies in a similar way to both web and SaaS (Software as a Service) applications at client's side [5], [6], because in both cases forensics investigators do not have access to the server.

Then, a literature review is a way to identify, evaluate, and interpret all available research relevant to a particular topic area, or phenomenon of interest [7]. There are studies that provide systematic reviews or mappings about cyber forensics and the managing of digital evidence [8]–[10]. For starters, Guo et al., [8] provide concepts, principles, and a process for performing a forensic investigation; however, they do not cover cyber forensics and it specific considerations at client's side. In addition, Hatole y Bawiskar [9] present a literature review about email forensics, which also consider techniques and tools; however, this study addresses a forensics process designed only for emails. Finally, Kaur et al. [10] propose a literature review on cyber forensics and its analysis tools; however, they are focused on general aspects, without taking into account the client perspective and the classification of the evidence that investigators can find.

Consequently, this paper presents a secondary study about cyber forensics with guidelines that support the forensics management from web environments focused on the client's side. Also, it analyses the standards that can be useful for forensics investigations, which are: (i) ISO/IEC 27037, which reviews guidelines for identification, collection, acquisition, and preservation of the digital evidence [11]; (ii) ISO/IEC 27042, provides guidelines for the analysis and interpretation of digital evidence [12]; (iii) ISO/IEC 27041 which provides guidance on assuring suitability and adequacy of incident investigative method [13]; (iv) ISO/IEC 27017, which is a code of practice for information security controls based on ISO/IEC 27002 but can be used specifically for cloud services [14]; and, (v) ISO/IEC 27050 that provides requirements and guidance on activities in electronic discovery [15]. The result of this systematic review is an overview of current research studies related to cyber forensics in order to manage digital evidence from web environments at the client side.

The structure of this paper is: Section 2 presents an overview of the state of the research related to web forensics at client's side. Section 3 describes the research method that is used to identify the relevant literature related to this contribution. Section 4 presents the results of the research method and describes the relevant approaches according to the mentioned classification. Section 5 presents a discussion of the results obtained by the followed methodology according to the literature. Finally, the conclusions are presented in Section 6.

II. RELATED WORK

There are some secondary studies related to guidelines to manage digital evidence from web environments [8]–[10], [16]–[18]. Guo et al. [8] present some definitions and principles related to computer forensics and digital evidence; however, the authors study the digital evidence in a general

78-1-5386-6657-9/18/$31.00 ©2018 IEEE

manner, without specifically considering the obtaining of evidence on the client's side. On the other hand, Garfinkel [17] presents a literature review where the author addresses the problems of current forensics processes and challenges in the near future; however, digital evidence from web environments is not covered. Simou et al. [16] address a review of cloud forensics; the authors are focused on available technical solutions presented in primary studies that have applicability on cloud computing, specifically the SaaS service model; and provide general guidelines to be considered about artifacts in that service model. However, this study does not provide details about the management of digital evidence found at client's side. Hatole and Bawiskar [9] propose a literature review of email forensics which is focused on tools available for managing data from emails. But, they do not cover areas for general cases and artifacts from others web services. Kaur et al. [10] propose a literature review related to cyber forensics; here, the authors present general details and summarize information about a variety of tools to manage digital evidence. Nonetheless, they do not cover specific topics about evidence found at client side: locations of evidence, and dependences of platforms. Then, Bhosale et al. [18] propose a review on computer forensics where they define some guidelines to collect digital evidence from web environments, but they do not cover the client's side. Consequently, although there are several secondary studies, they present two main limitations: (i) Most of studies do not mention internationals standards to guide their research. (ii) Most of them do not cover aspects related to cyber topics at client's side.

III. Research Method

A systematic literature review is a means of categorizing and summarizing all available research that is relevant to a particular research question, topic area, or phenomenon of interest [7]. Also, it is used to identify, evaluate and interpret all available studies related to a particular research topic.

In this section, a set of primary studies has been analyzed, which contributes in answering the gaps addressed during the web forensics research when it has been considered the evidence found at clients' side. In order to perform this literature review, the Kitchenham methodology [19] has been applied. This methodology has three main activities: i) planning the review, ii) conducting the review, and iii) reporting the review.

A. Planning the Review

The first step towards accomplish this step is to define the research question, the search strategy, the selection of the primary studies, and finally, define the extraction criteria.

The research question to be answered is: *Which forensics procedures are considered by forensic researchers for the management of digital evidence hosted on the clients' side of a web environment?*

The research sub-questions are: (a) *RQ1: What kind of digital evidence from web environments can be found on clients' computers?* (b) *RQ2: Where could be found the web evidence at client's side?* (c) *RQ3: How is it possible to preserve digital evidence in order to guarantee its integrity?* (d) *RQ4: In which way could the standards be used in the management of digital evidence?*

The period covered starts in 2004, this milestone was chosen because it is the start point of web 2.0. To perform this study, different sources have been chosen (i.e., representative books, important journals, conferences and workshops). For the automatic search, the selected digital libraries are: IEEEXplore, ACM Digital Library, SpringerLink, and SinceDirect. The search string is *"(FORENSIC) AND (WEB OR BROWSER OR CLOUD) AND (DIGITAL) AND (EVIDENCE)"*.

In order to include the primary studies to be analyzed, the following inclusion criteria have been selected:

a) Studies presenting methods to collect and process digital evidence from the use of web applications.
b) Studies presenting methods to safeguard digital evidence.
c) Studies presenting tools, which allow to automate computer forensic processes.

The exclusion criteria are:

d) Introductory papers of special issues, books and workshops.
e) Duplicate reports of the same study in different sources.
f) Short papers with less than five pages.
g) Papers not written in English.

Moreover, the strategy to obtain the data was defined by breaking down each research question into more specific extraction criteria shown in Table 1.

Table 1. Extraction Criteria and accepted items.

	Extraction Criteria	Options	Studies
RQ1: What kind of digital evidence from web environments can be found on clients' computers?			
EC1	Type of Artifacts	Browsing Indicators	[1], [2], [4], [6], [20]–[32].
		Temporary Files (e.g., caches, cookies, others)	[1], [2], [4], [6], [16], [20], [22]–[27], [29], [30], [33]–[36].
RQ2: *Where could be found the web evidence at client's side?*			
EC2	Perspectives	Client Side	[1], [4], [5], [16], [20], [21], [35], [37]–[40]
		Transit	[1], [4], [21], [34], [35], [40], [41].
		Server Side	[1], [16], [20], [34], [35], [37], [39]–[41].
EC3	Local Source	Browser	[1], [2], [6], [20]–[24], [25, p. 8], [26]–[31], [33], [35]–[37], [39].
		Desktop Application	[2], [4]–[6], [16], [20], [24], [25], [27], [28], [30], [31], [35], [41].
		System Logs	[4], [17], [23], [25]–[27], [30], [31], [35].
RQ3: *How is it possible to preserve digital evidence in order to guarantee its integrity?*			
EC4	Preservation of Digital Evidence	Authentication Methods	[4], [17], [27], [35], [37], [39], [42]
		Integrity Methods	[1], [4], [5], [21]–[24], [26], [28], [34], [35], [39], [42], [43]
RQ4: *In which way could the standards be used in the management of digital evidence?*			
EC5	Standards Involved in the Solutions	ISO/IEC 27037	[37], [39], [41], [43]–[48]
		ISO/IEC 27042	[41], [44], [45], [48]
		ISO/IEC 27041	[47], [48]
		ISO/IEC 27050	[47], [48]
		ISO/IEC 27017	[44], [48]

The selected papers related to EC1 can be classified in one or more type of artifacts existing in client computers (i.e., browsing indicators focused on logs or system events, temporary files as cache, cookies, and other files). On the criterion EC2, a paper can be classified in one or more perspectives depending on the storage location of data [4]: (i) data located in the server (e.g., cloud provider, web server); (ii) data in transit (i.e., between client and server) (iii) data at client's side: if data are in the clients' computer, consequently the investigation is performed there. Also, there are automation tools to collect or analyze found artifacts.

Regarding the criterion EC3, a paper can be classified in applications that can leave evidence at clients' computers (e.g., browsers, desktop applications, system logs) [2], [6].

Next, related to the criterion EC4, a paper can be classified in one or more methods to preserve digital evidence: authentication methods, that protect evidence to avoid unauthorized access to data, also it is necessary to register everyone that have access to digital evidence; for those purposes there are several methods employed by experts [43]; it is also important to preserve digital evidence without variations, thus there are methods to validate the integrity of the evidence.

Lastly, with regard to the criterion EC5, a paper can be classified in one or more standards that are used on research about cyber forensics; the standards that are best adapted to the analysis in web environments are the family of the ISO/IEC 27000 especially the 27017, 27037, 27041, 27042, and 27050, because these provide guidelines for the correct handling of digital evidence.

IV. Research Results and Discussion

In this section, it is presented the summary of the findings of the management of digital evidence from web environments as techniques of identification, collection, analysis, preservation, and presentation of digital evidence from web environments, taking into account how standards are being used on investigations and what guidelines are provided by standards. Before applying the extraction and exclusion criteria 1415 papers were obtained, from those only 37 were included in this study. The studies found in digital libraries are distributed as follows: 11% in ACM, 74% in IEEE, 8% in Science Direct and 7% in Springer Link. Moreover, it is presented a summary of the main findings, which are related to each step that involves a forensics research [12]: i) identification, ii) collection, iii) preservation iv) analysis and report of digital evidence, and finally, v) a brief review about how standards are working in current studies. These results are presented in the third column of the Table 1, they present the criteria for analysis, and the papers used in this review that fulfill each criterion in the management of digital evidence from web environments.

A. Identificaction

As the first step of a forensics research, it has been considered the identification phase. Here, the place in which the evidence is located depends on the different web perspectives (i.e., server/cloud provider, client, network).

Related to web perspectives (i.e., cloud provider/server perspective, carrier/network perspective, client perspective), when the evidence is located at the server side, Morioka and Sharbaf [4] suggest to acquire the data directly from the servers. However, it depends on the jurisdiction of each country and its laws for accessing to the information. Then, the study of Howden et al. [37], uses APIs provided by web applications to extract information. Moreover, the authors of [5], [20] analyze the data that is gathered from SaaS applications with the use of APIs and data structures in order to extract logs from SaaS applications (e.g., Google Docs, slides, sheets). Jang and Kwak [1] recommend that the extraction of forensics evidence should be performed from the user's account. When the digital evidence is in transit (carrier perspective), they also recommend to capture the volatile data before their modification. Morioka and Sharbaf [4] presented the importance of searching information from the interaction between user interactions and the web application; which can be recorded by the Internet Service Provider (ISP); however, it is not always possible due to laws and regulations of each country. Those laws are different and can present constraints that promote the data protection in order to preserve the user's privacy. Moreover, Chen et al., [34] suggest that the dependence of providers makes the forensics work difficult. Thus, it is possible that the judge can allow the access to the user accounts in order to request information. Finally, when the evidence is at the client's side, Morioka and Sharbaf [4] state that it is necessary to look into the local files generated by applications and browsers in local machines. With reference to the local evidence, in studies such as [4], [35] the authors state that, when a client interacts with applications deployed on cloud environments, some files are fragmented and web cache is stored in the client machine. Oh et al., [2] propose an advanced evidence analysis on the client's browser, where the history, cookies, cache and bookmarks are analyzed. They also present guidelines to recover deleted information because browsers allow users to erase log information (e.g., cache, cookies, download list). The same authors recommend to do a timeline of the suspect activities, considering the correct time zone; however, there are not specific guidelines to preserve the evidence. Later, Jang and Kwak [1] give a methodology to identify, collect, and analyze evidence; however, it only provides a guide in social networks where the digital evidence is gathered from users profiles, records of conversations.

Marturana et al., [6] and Mehreen and Aslam, [25] extract information from desktop applications, this is done because the application storages information in the clients' computer. This digital evidence could be found as synchronization logs, recently opened, modified or deleted files that are stored on Dropbox platforms; however, they do not present a general method to collect, preserve, and report forensics results. On the other hand, Baca et al., [22] present some cases of study where they collect artifacts from Facebook, such as images, Facebook status, and URLs; nevertheless, this methodology can only be used with that platform, and it cannot be generalized. In [23], [30], there are guidelines to collect information from web browsers, which present the way to gather evidence from cache, temporary files and hard disks. In those locations, information about mail accounts, images, videos and browsing history could be found. The process presented by Mahaju and Atkison [36] was focused only in the Firefox browser. Here, the evidence from Firefox log files that the investigator considered relevant (e.g., websites visits, cookies, downloads, bookmarks, logins) is collected. Then, Nalawade et al., [29] collect cache memory, history and cookies from different

browsers; while Castiglione et al., [33] are focused on images obtained from Online Social Network (OSN), those images have different sizes, formats, and metadata. Moreover, it is important to consider information such as the file name of each image, which depends on the social network where it was collected. The gathered information is useful to identify the origin of such image. Simou et al., [16] present a review about cloud forensics solutions; here, the authors recommend the design and implementation of an application that logs all potential digital evidence; however, a methodology about the application and the process to perform the gather of the information was not provided. Finally, Nalawade et al., [29] establish the possibility of obtaining evidence from a private session; this is possible because of the extensions that each browser uses, which could disable the private mode. Lastly, Ohana and Sashidhar [23], identify digital evidence (e.g., usernames, images, email accounts, etc) from private and portable sessions.

B. Collection

About collection of digital evidence, in studies such as [23], [26] the authors analyze and collect digital evidence in private sessions; like Ohana and Shashidhar [23] whom collect evidence from a portable browser. On the other hand, the authors in [21], [27] establish that in private browsing only a minimum amount of information is stored in the hard disk of a user's computer. In the studies [27], [30], [31], there are presented recommendations about artifact collection, these studies indicate areas that are frequently addressed by forensic investigators in a computer with Windows OS (e.g., Windows registry, AppData folder, system event logs, deleted data, temporary files). Lee et al., [39] describe general digital evidence collection, and establish specific steps to preserve integrity; however, this study is focused on general digital evidence; therefore, it does not take into account specific considerations for evidence from web environments. Raju and Geethakumari [38] propose a model for cloud forensics investigation; they iteratively consider the collection and preservation stage of artifacts until the identification of an incident; after that, the digital evidence is ready for the investigation; however, they do not present specific characteristics of evidence from web environments (e.g., tools, locations). In [39] authors recommend the gathering of general digital evidence in order to prioritize volatility in the following way i)registers cache, ii) routing table, iii) arp cache, iv) process table, v) memory, vi) temporary files, vii) disk, viii) remote logging, and ix) monitoring data that is relevant to the system in question, physical configuration, configuration, network topology, archival media. The authors use the Integration Forensic tool EnCase to make an image of the disk, mount the image, create a hash, and do a checksum. Also, Baca et al., [22] propose a case study, where the general phase create a disk image and mount it on a virtual machine. Then, in [23], [25] authors use FTK tool to collect data without altering the original evidence. Chen et al., [34] analyze some tools for cloud and social network (e.g., EnCase Servlet, P2P). Also, the authors of that paper propose tools such as Internet Evidence Finder, which allows the recovering of artifacts deployed on cloud and social network, including private sessions. Tools to collect data from computers are presented in [30] such as WinHex to recover files that have been deleted or WinSpy to find Internet activities. Chow [28] describes a file system integrity which enables users to examine the files based on hash values to collect data.

C. Preservation

The authors of [6][18] recommend that evidence should be collected taking into account the volatility. Moreover, in [1][21], it is recommended the use of forensic images of the digital evidence before performing the analysis. Moreover, Jang and Kwak [1] recommend the recording of video for gathering evidence in order to guarantee the integrity of the process; also, the authors state that is not advisable that just one person collects the evidence. Sivaprasad and Jangale [30] recommend techniques to preserve digital evidence by reviewing the disk image and checking the integrity of it by using hash codes. On the other hand, the studies [6] and [20] propose a process to guarantee the integrity of the evidence, which has 3 steps: i) an schema that posts hash and check sum values to public digital evidence, ii) a system that manages digital evidence in order to create a MAC value (Message Authentication Code) and record it to the chain of custody document, and iii) an online authentication system using digital evidence collector's digital signature. Lastly, authors recommend analyzing each of those three procedures. Mehreen and Aslam recommend to preserve the integrity by checking hash values of the original volume and the image. Moreover, in [42], researchers present guidelines to evaluate a method of digital evidence security, the evaluation criteria used as follows: selection of security properties (integrity, confidentially, non-repudiation), identification, and authentication, accuracy, binding of functionality, strength of mechanisms, attacks and vulnerability assessment, easy to use, computational efficiency. Finally, in [4] authors recommend that it is necessary to ensure the integrity of the tools; therefore, the used technics should be reported and stored by investigators.

D. Analysis and report

Related to the analysis, the authors of [36] take into account only the tools for Firefox. They perform a comparison about the forensics tools which are independent for operating systems (i.e., NetAnalysis V2, FoxAnalysis V1.6.0, PasswordFox, Browser History Examiner, Mz History Viewer) in order to analyze the performance, portability, simplicity, speed, classification of user activities, memory, and CPU consumption. Then, Nalawade et al., [29] analyze tools used for web browser analysis on a Windows platform, such as Internet Explorer (IE), Safari, Chrome, and Opera. Chow et al., [28], which describes the Digital Evidence Search Kit (DESK), which is a system used by Hong Kong police to illustrate features of an effective evidence collection tool. In [2] the authors present tools for analyzing different artifacts from diverse browsers; for example, it is presented Pasco Web Historian 1.3, which is portable for Internet Explorer, Firefox, Safari and Opera. Also, Chrome Analysis 1.0 that can be used in Chrome browser to analyze cookies, history, download list, history, cookies, bookmarks and list search. Finally, there are presented tests performed by the authors, were live forensics tools were used, to analyze cache, cookies, history, process for Windows OS, and also with Internet Evidence Finder v4.0. [6]. After analysis, Oh et al., [2] state that the investigator should generate a report based on relevant information and its confirmation. As it has been found, the most of studies are proved by means of case studies or proofs of concept [6], [22], [23], [49], where the feasibility of the solutions is shown in practice. And, the trend is Forensics as a Service (FaaS) such a new service model [40].

E. Standards review

The selected papers do not follow common guidelines in their approach; they are strongly coupled to certain tools or have their own methodologies. However, ISO standards can generate a better approach such as in reducing the research time, implementing tools, improving the investigative process and even obtaining clear and precise results, and generalize the existing methods towards a feasible forensics process. Next, an analysis of how the regulations could be included for correct management of digital clues in cloud environments is presented. Here, the information should be protected by the systems that process it, which is one of the main objectives for the investigative process. In order to manage all the information, and for it to be used for a judicial process, it is necessary to have a method in which everything is documented, with security bases and risk assessment. To comply with all the requirements, there are standards for the management of the information security, identification of risk and implementation of security controls [44].

The ISO/IEC 27000 is a set of standards that include the best practices in the field of information security. Then, the standards that articulate forensic computing practices, related to the activities of the forensics process are ISO/IEC 27017 [14], 27037 [11], 27041 [13], 27042 [12] and 27050 [15].The ISO/IEC 27041 standard helps during the selection of the methodology for the analysis of the evidence, this selected methodology can be used for any similar activity [45]. Whereas, ISO/IEC 27037 [11] and 27042 [12] describe 7 main activities in forensic investigation that are: i) plan, ii) prepare, iii) respond, iv) identify, collect, acquire, preserve, v) understand, vi) report, and vii) close. [41]. The standard ISO/IEC 27037 [11], does not promote the use of particular tools, it presents tasks to the seven activities and the trained personnel (first responders) involved in the investigation.

Following the activities given by the standard, the first and second steps are used by researchers and professionals. The third step is to determine the scope of the incident, in case of the cloud the first step will be checking if there are any law related to the jurisdiction. The fourth step collects the information, configuration of the network and the related systems. If there are problems in the analysis, the researchers must use the cloud providers and work together, remember that the approaches to data security are described in the ISO/IEC 27000 series. To complement the ISO/IEC 27037 [11], it uses the cloud computing services as described in the ISO/IEC 27017 [14], where advises customers to verify that the suppliers comply with standard [44]. In the same step, data collection is maximized, but the cloud infrastructure is large and is always changing, therefore it generates conflicts when the professional wants to extract information, so it must define the appropriate information and use live tools and techniques. In order to complete this step, the ISO/IEC 27050 is applied, this standard describes the process of discovering information on mobile devices such as computers, this is useful for researchers as non-technical people [15]. The fifth step is focused on ensuring the complete extraction of evidence throughout the acquisition procedure. Now, one of the problems is the capacity of storage in the cloud, this can reach up to terabytes [41]; in these cases, data mining techniques are applied and extraction of the data according to their importance. Finally, the preservation of the evidence must not be contaminated, the investigators must guarantee that the evidence is not altered. The professional must make a copy since the original evidence must not be treated. As cloud storage has advanced, providers offer encryption for their customers, so, the ISO/IEC 27017 proposes that cloud service customers should limit the data in a way that if an employee of the provider obtains access, they will not be able to use it. In case of not having access, providers help to access the required data. The sixth step is a report of the whole process and the findings, in this case the ISO/IEC 27042 and 27043 explain, not only the analysis of the evidence, but also the interpretation of the results, the report, and the presentation of the analysis results [45], [48]. Also, Veber and Smutny in [46] explain that the ISO/IEC 27037 standard is not entirely practical but, using it together with the other mentioned standards, this would be a good guide for forensics investigation, as well as the improvement of the methods and tools. Another point to be addressed is that standards not only help researchers but also serve as basis for judicial experts. The standard helps experts to understand the various issues presented in the final report.

Consequently, answering each research question; RQ1 has been replied in identification section, it has been found web artifacts in clients´ host (eg., caches, cookies, or temporary files) to prove user actions. Also, RQ2 has been replied in identification section, where it was found that applications leave web artifacts in directories of local systems (e.g., AppData folder, from Windows OS, storages web artifacts as Google Chrome cache). On the other hand, RQ3 has been responded in preservation section. There, it has been identified methods (e.g., digital signature, hash values), which are employed by experts to preserve digital evidence (including evidence from web environments). Finally, RQ4 has been answered in standard review section; such section was focused on the ISO/IEC standard family 27000, which provides guidelines for information security.

V. Conclusions and Further Work

This paper presents a systematic literature review on cyber forensics analysis focused on client side. This review addresses the objectives of the research about digital evidence gathered from web environments and its manage along with an analysis about how standards could improve or guide the current studies. For this research, 37 papers were selected, it was identified different options to answer the raised research questions. It was found that there are few studies that mention or use standards, also the majority of researches and second studies focused on server side and the possible attacks. Moreover, the ISO/IEC 27000 family that affects digital evidence analysis was presented. Each document has an impact in the area of investigation, and helps to the standardization for the method development. The guidelines provide a way to ensure the results of the investigation, the investigators should adapt them to the changes and new standards in order to warranty the development of the analysis method. Researchers must adapt to changes and new rules to ensure the proper development of the method of analysis.

It is important to emphasize that the standards provide guidelines for the correct handling of digital evidence; however, there are only few studies that use them for solving the forensics cases. The processes associated with the standards (identification, collection, acquisition and preservation) are used for research process. They maintain the integrity of the evidence, provide an acceptable methodology, manage systematically and preserve their

integrity.

As further work, it is planned to study the field of mobile devices (e.g., cellphones, tablets, smartwatches) and its specific needs; identifying current methods, tools, guidelines to manage digital evidence. It will help investigators to understand new challenges, restrictions, and solutions for the next years.

REFERENCES

[1] Y.-J. Jang and J. Kwak, "Digital forensics investigation methodology applicable for social network services," *Multimed. Tools Appl.*, vol. 74, no. 14, pp. 5029–5040, Jul. 2015.

[2] J. Oh, S. Lee, and S. Lee, "Advanced evidence collection and analysis of web browser activity," *Digit. Investig.*, vol. 8, pp. S62–S70, Aug. 2011.

[3] P. M. Mell and T. Grance, "The NIST Definition of Cloud Computing," *Spec. Publ. NIST SP - 800-145*, Sep. 2011.

[4] E. Morioka and M. S. Sharbaf, "Digital forensics research on cloud computing: An investigation of cloud forensics solutions," *IEEE Symp. on Tech. for Homeland Security (HST)*, 2016, pp. 1–6.

[5] V. Roussev and S. McCulley, "Forensic analysis of cloud-native artifacts," *Digit. Investig.*, vol. 16, pp. S104–S113, Mar. 2016.

[6] F. Marturana, G. Me, and S. Tacconi, "A Case Study on Digital Forensics in the Cloud," in *2012 Int. Conf. on Cyber-Enabled Dis tributed Computing and Knowledge Discovery*, 2012, pp. 111–116.

[7] B. Kitchenham, "Procedures for Performing Systematic Reviews," *Keele UK Keele Univ*, vol. 33, Aug. 2004.

[8] H. Guo, B. Jin, and D. Huang, "Research and Review on Computer Forensics," *Forensics in Telecom., Inf., and Multimedia*, 2010.

[9] P. P. Hatole and D. S. K. Bawiskar, "Literature Review of Email Forensics," *Imp. J. Interdiscip. Res.*, vol. 3, no. 4, Apr. 2017.

[10] M. Kaur, N. Kaur, and S. Khurana, "A literature review on cyber forensic and its analysis tools," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 5, no. 1, pp. 23–28, 2016.

[11] "ISO/IEC 27037:2012 - Information technology- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence.", https://www.iso.org/ standard/44381.html.

[12] "ISO/IEC 27042:2015- Information technology -- Security techniques -- Guidelines for the analysis and interpretation of digital evidence." [Online]. Available: https://www.iso.org/ standard/44406.html.

[13] "ISO/IEC 27041:2015, Inf. techn., Security techniques, Guidance on assuring suitability and adequacy of incident investigative method."

[14]"ISO/IEC 27017:2015 - Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services."

[15]"ISO/IEC 27050-3:2017 - Information technology -- Security techniques -- Electronic discovery -- Part 3: Code of practice for electronic discovery." https://www.iso.org/standard/ 66231.html.

[16]S. Simou, C. Kalloniatis, E. Kavakli, and S. Gritzalis, "Cloud Forensics Solutions: A Review," in *Advanced Information Systems Engineering Workshops*, 2014, pp. 299–309.

[17] S. L. Garfinkel, "Digital forensics research: The next 10 years," *Digit. Investig.*, vol. 7, pp. S64–S73, Aug. 2010.

[18] D. V. Bhosale, P. K. Mitkal, R. N. Pawar, and R. S. Paranjape, "Review on Computer Forensic," *Training*, vol. 2, no. 01, 2016.

[19] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering – A systematic literature review," *Inf. Softw. Technol.*, vol. 51, no. 1, pp. 7–15, Jan. 2009.

[20] S. Matsumoto and K. Sakurai, "Acquisition of Evidence of Web Storage in HTML5 Web Browsers from Memory Image," in *2014 Ninth Asia Joint Conf. on Information Security*, 2014, pp. 148–155.

[21] A. S. V. Nair and B. A. S. Ajeena, "A Log Based Strategy for Fingerprinting and Forensic Investigation of Online Cyber Crimes," in *Proceedings of the 2014 International Conference on Interdisciplinary Advances in Applied Computing*, New York, NY, USA, 2014, pp. 7:1–7:5.

[22] M. Baca, J. Cosic, and Z. Cosic, "Forensic analysis of social networks (case study)," in *ITI 2013 35th Int. Conf. on Information Tech. Interfaces*, 2013, pp. 219–223.

[23] D. J. Ohana and N. Shashidhar, "Do Private and Portable Web Browsers Leave Incriminating Evidence? A Forensic Analysis of Residual Artifacts from Private and Portable Web Browsing Sessions," *IEEE Security and Privacy Workshops*, Washington, USA, 2013,

[24] A. Majeed, H. Zia, R. Imran, and S. Saleem, "Forensic analysis of three social media apps in windows 10," in *2015 12th International Conference on High-capacity Optical Networks and Enabling/Emerging Technologies (HONET)*, 2015, pp. 1–5.

[25] S. Mehreen and B. Aslam, "Windows 8 cloud storage analysis: Dropbox forensics," in *2015 12th International Bhurban Conf. on Applied Sciences and Tech. (IBCAST)*, 2015, pp. 312–317.

[26] H. Said, N. A. Mutawa, I. A. Awadhi, and M. Guimaraes, "Forensic analysis of private browsing artifacts," in *2011 Int. Conference on Innovations in Information Technology*, 2011, pp. 197–202.

[27] D. Gupta and B. M. Mehtre, "Recent Trends in Collection of Software Forensics Artifacts: Issues and Challenges," in *Security in Computing and Communications*, 2013, pp. 303–312.

[28] K. P. Chow *et al.*, "Digital evidence search kit," in *First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05)*, 2005, pp. 187–194.

[29] A. Nalawade, S. Bharne, and V. Mane, "Forensic analysis and evidence collection for web browser activity," *Int. Conf. on Automatic Control and Dynamic Optimization Techniques*, 2016, pp. 518–522.

[30] A. Sivaprasad and S. Jangale, "A complete study on tools amp; techniques for digital forensic analysis," in *2012 Int. Conf. on Computing, Electronics and Electrical Technologies (ICCEET)*, 2012, pp. 881–886.

[31] F. Mirza, "Looking for digital evidence in Windows," in *2008 Int. Symp. on Biometrics and Security Technologies*, 2008, pp. 1–7.

[32] A. Levinson, B. Stackpole, and D. Johnson, "Third Party Application Forensics on Apple Mobile Devices," in *2011 44th Hawaii International Conf. on System Sciences*, 2011, pp. 1–9.

[33] A. Castiglione, G. Cattaneo, and A. D. Santis, "A Forensic Analysis of Images on Online Social Networks," in *2011 3rd. Intl Conf. on Intelligent Networking and Collaborative Systems*, 2011, pp. 679–684.

[34] L. Chen, L. Xu, X. Yuan, and N. Shashidhar, "Digital forensics in social networks and the cloud: Process, approaches, methods, tools, and challenges," in *2015 International Conference on Computing, Networking and Communications (ICNC)*, 2015, pp. 1132–1136.

[35] J. Farina, M. Scanlon, N. A. Le-Khac, and M. T. Kechadi, "Overview of the Forensic Investigation of Cloud Services," in *2015 10th Int. Conf, on Availability, Reliability and Security*, 2015, pp. 556–565.

[36] S. Mahaju and T. Atkison, "Evaluation of Firefox Browser Forensics Tools," *SouthEast Conference*, New York, NY, USA, 2017, pp. 5–12.

[37] C. Howden, L. Liu, Z. Ding, Y. Zhan, and K. P. Lam, "Moments in Time: A Forensic View of Twitter," in *2013 IEEE Int. Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*, 2013, pp. 899–908.

[38] B. K. S. P. K. Raju and G. Geethakumari, "An advanced forensic readiness model for the cloud environment," in *2016 International Conference on Computing, Communication and Automation (ICCCA)*, 2016, pp. 765–771.

[39] S. Lee, S. Lee, J. Lim, and H. Kim, "Digital evidence collection process in integrity and memory information gathering," in *First International Workshop on Systematic Approaches to Digital Forensic Eng*, Los Alamitos, CA, USA, 2005, pp. 236–247.

[40] K. K. R. Choo, C. Esposito, and A. Castiglione, "Evidence and Forensics in the Cloud: Challenges and Future Research Directions," *IEEE Cloud Comput.*, vol. 4, no. 3, pp. 14–19, 2017.

[41] E. Miranda Lopez, S. Moon, and J. Park, "Scenario-Based Digital Forensics Challenges in Cloud Computing," *Symmetry*, vol. 8, no. 10, p. 107, Oct. 2016.

[42]S. Saleem, O. Popov, and R. Dahman, "Evaluation of security methods for ensuring the integrity of digital evidence," in *2011 Int. Conf. on Innovations in Information Technology*, 2011, pp. 220–225.

[43]Y. Wang, "Study on Supervision of Integrity of Chain of Custody in Computer Forensics," in *Forensics in Telecom.,Information, and Multimedia*, 2010, pp. 200–206.

[44] C. S. C. Council, *Cloud security standards: what to expect & what to negotiate*. October, 2013.

[45] J. Veber and T. Klíma, "Influence of Standards ISO 27000 Family on Digital Evidence Analysis," *Proc. 22nd Interdiscip. Inf. Manag. Talks*, pp. 103–114, 2014

[46] J. Veber and Z. Smutny, "Standard ISO 27037:2012 and Collection of Digital Evidence: Experience in the Czech Republic," p. 7.

[47] E. Hibbard, "Electronic discovery standardization," vol. 12, p. 19.

[48] J. Veber and T. Klima, *Mapping of ISO 27000 Digital evidence to processes of digital forensics lab*. 2015.

[49] J. Oh, S. Lee, and S. Lee, "Advanced evidence collection and analysis of web browser activity," *Digit. Investig.*, vol. 8, pp. S62–S70,2011.