ICIC Express Letters
Volume **13**, Number **8**, August **2019**

ICIC International ©2019 ISSN 1881-803X
pp. **663–672**

FRAMEWORK FOR ESTABLISHING CONFIDENCE LEVEL OF DIGITAL EVIDENCE ADMISSIBILITY

Zulfany Erlisa Rasjid[1], Benfano Soewito[2], Gunawan Witjaksono[2] and Edi Abdurahman[3]

[1]Doctor of Computer Science, School of Computer Science
[2]BINUS Graduate Program
[3]BINUS Graduate Program, School of Statistics
Bina Nusantara University
Jl. K. H. Syahdan No. 9, Kemanggisan, Palmerah, Jakarta 11480, Indonesia
zulfany@binus.ac.id; { bsoewito; gwitjaksono; edia }@binus.edu

Received December 2018; accepted February 2019

Abstract. *Digital evidence refers to data obtained from digital storage and used as supporting evidence in court. The admissibility of digital evidence depends on several factors, including improper handling, virus infection, deliberate tampering, or faulty hardware that might compromise its integrity. The integrity of digital evidence is highly dependent on use of a cryptographic hash function to provide a seal on the evidence. In this paper, we analyze the causes of evidence inadmissibility to the courts, specifically during a chain of custody in which the evidence is passed from one investigator to another, and therefore is at risk of compromise. We introduce a confidence level of admissibility to identify the percentage of trust accorded to evidence. When the level of integrity is intact, then the confidence level of admissibility is 100%. For evidence under investigation, the confidence level is reduced as the changes have been made to the documents. We propose a framework for establishing the confidence level of evidence admissibility. Based on this framework, we construct a model that enables the calculation of the confidence level of admissibility, from which we can produce a history log for document traceability.*
Keywords: Admissibility of digital evidence, Integrity, Framework, Confidence level

1. **Introduction.** The number of crimes and cybercrimes is increasing with growth in technology. In the current technology era, a large amount of information can be stored in storage media. Information can also be hidden in any storage media. Digital evidence refers to information that is obtained from digital storage and used as supporting evidence in court. Digital evidence may originate from a range of sources, including laptops, smart phones, hard drives, the Internet and computer system peripherals [1]. The data also grow in terms of their sizes; therefore, it is also necessary to consider the security of Big Data; for example, the data coming from large organization need additional and extra analysis in order to justify the data integrity [2]. It may also come from suspects as well as victims. The challenge of obtaining digital information as evidence has become more complex with time, and investigators must ensure the integrity of digital evidence so that it may be used in court. The admissibility of digital evidence can be threatened in several ways, including improper handling, virus infection, deliberate tampering, or even by faulty hardware that compromises its integrity. The preservation of digital evidence involves three main factors: i) maintaining the reliability of the data, ii) ensuring the uses of the evidence, and iii) maintaining the security of the evidence [3]. Care must be taken to ensure that the digital evidence is consistent with the data collected from a crime scene and during investigations. How the digital evidence is extracted, which extraction tools are used, and which hashing algorithm is used all play an important role in determining the

DOI: 10.24507/icicel.13.08.663

data's integrity [3]. Several digital extraction tools are in use today, with most tools using the message digest (MD5) hashing function and a few using the secured hash algorithm (SHA) hashing function. However, a weakness has been identified in both the MD5 and SHA, whereby two different files can experience hash collisions [4]. As a result, several researchers have been working to develop other methods to locate collisions on the MD5 and SHA series to obtain improved performances [5-13]. Hash collisions can cause evidence to become inadmissible in court, as they compromise the authenticity and integrity of the evidence. The evidence found at a crime scene must not be used for direct investigation, because its integrity and authenticity must be preserved. Therefore, a clone is created on which investigators may work. The evidence and its duplicates must be preserved for at least 18 to 24 months (or until the case is completed) [3]. Analyzing a hard drive usually provides more information than does analyzing a computer's main memory, as the main memory storage space is volatile [14]. Analysis from hard drives may be used to reconstruct an event using bits of low-level information that is scattered around in hard drives [14]. The current procedure for handling digital evidence is to sort them with respect to two locations: the crime scene and the forensic laboratory. Figure 1 shows a flowchart of the procedure for handling evidence at a crime scene [15]. The first step is preparation, in which it is necessary to prepare for all types of evidence, as different types of evidence require different equipment. For example, in the case of a computer/laptop with the status 'ON', volatile data must be handled immediately to avoid sudden a shut down due to low battery power. The evidence obtained must then be preserved and ensured that it remains intact. In the data-collection phase, all available information is collected and then finally confirmed. Evidence is identified by its digital seal provided by means of a digital hash function.

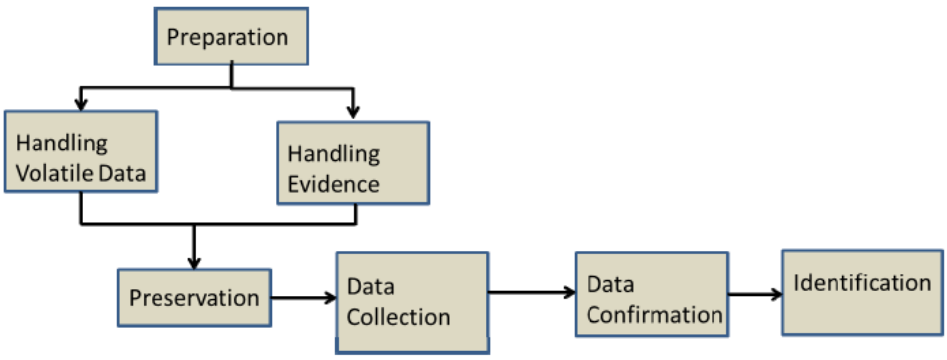

FIGURE 1. Handling digital evidence at crime scene [15]

In the forensic laboratory, after receiving evidence, it is hashed again to ensure that its integrity is intact. A clone is then created and hashed to make sure that the cloning process has created an exact copy. Once the clone is completed, analysis is performed on the clone. All information that is found is recorded. There may be more than one forensic analyst involved in the investigation. After the investigation is completed, all findings must be reported in the form of a technical report based on the investigation and analysis of the evidence. Finally, the results must be presented, which means collecting all the reports of different forensic analysts. Once collected, these reports are presented as one case. The minutes of a meeting are used as a request to the court to allow evidence to be admitted [16]. Considering the overall handling procedure from the crime scene to the forensic laboratory, security breaches can occur in four locations, as illustrated in Figure 2. Points 1 through 4 show the possibilities of security breaches where the evidence is under investigation. Therefore, the probability of evidence tampering increases as more

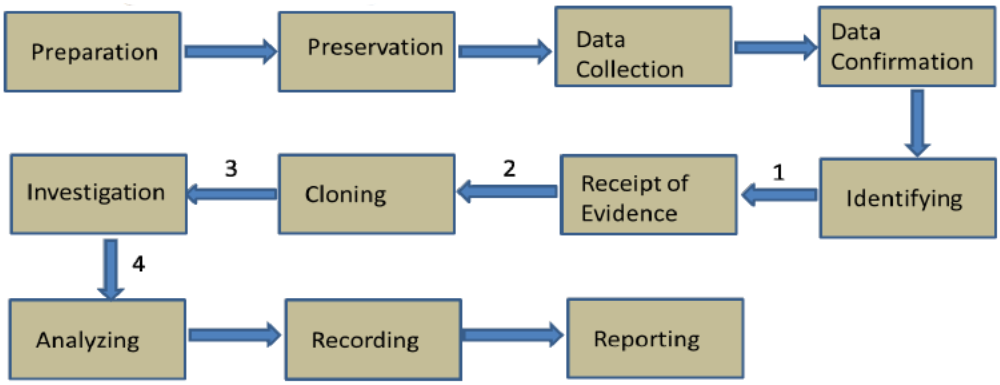

FIGURE 2. Security breach during digital evidence handling

investigators work on the same evidence. A security breach can occur for several reasons, including deliberate tampering and hardware failures.

To date, no model has been developed that covers all the requirements for the admissibility of evidence (see Table 1) [3]. In the table, a value of 1 indicates that the guidelines are fully considered, a value of 2 indicates that they are somewhat considered, and a value of 3 indicates that they are not considered at all in the model. We can see that there are still several guidelines with respect to digital evidence admissibility that have not been considered by existing frameworks. A harmonized model of digital assessment was introduced by Antwi-Boasiako and Venter [17], where the assessment model is divided into three phases: the Evidence Assessment Phase, Evidence Consideration Phase and Evidence Determination Phase. We are interested in the Evidence Consideration Phase, whereby the core requirements involve the Chain of Custody Requirement and Assessment. During the Chain of Custody the integrity of the digital evidence must be maintained.

From Table 1, some points have been considered; however, transmission (point 14) and traceability (point 15) were not considered in the existing framework [3]. Prayudi and Priyambodo proposed a secure and trusted environmental strategy that takes five components into consideration, one of which is the human factor. To ensure authenticity and integrity with respect to the human factor, the authors require that the handling must be executed by a professional and competent individual [18].

The purpose of this research was to provide framework for estimating the security confidence level, which can then be presented in court, along with the traceability of the evidence to convey its degree of admissibility. The significance of this research is to provide information on how much trust is put in the digital evidence by providing a confidence level percentage, as a guide to the judges before giving the final verdict.

The rest of this paper is organized as follows. The problem statement and preliminaries describing the problem and related works are presented in Section 2. The result is presented in Section 3. Section 4 contains the analysis and discussion of the results and finally the conclusion is presented in Section 5.

2. **Problem Statement and Preliminaries.**

The admissibility of digital evidence in court depends on several parameters, one of which is the control of physical evidence where integrity is the main issue, its traceability and the risks involved in the case of the evidence being transferred from one investigator to another.

We propose the concept of the confidence level of admissibility to identify the percentage of trust given to evidence. When the integrity of evidence remains intact, then its confidence level of admissibility is 100%. In the case of evidence under investigation, the confidence level is reduced once the documents have been passed through the four points of possible security breach, as changes might be applied to the documents at these points.

TABLE 1. Digital preservation models vs. digital evidence admissibility policy compliance [3]

No.	Guidelines	Existing framework				Notes
		PREMIS	OAIS ISO 14721 :2003	DAMM	NDSA	
1	Legality of evidence. The evidence that meets the legal provision for the preservation	3	3	3	3	
2	Respect for fundamental rights	1	1	3	3	
3	The reliability of the evidence	2	1	1	1	In PREMIS, only the metadata preservation is considered.
4	Effectiveness of evidence	1	1	1	3	
5	Respect the rules of data protection	1	1	3	3	
6	The respect for the privacy of communications	1	1	3	3	
7	Respect for the right to freedom of expression	1	1	3	3	
8	Confidentiality	3	3	3	3	
9	Authenticity	1	1	1	1	
10	Integrity	1	1	2	2	In DAMM, tracking is not included and in NDSA only handles file types.
11	Roles of responsibility	2	1	1	1	In PREMIS, no roles are assigned to direct responsibility.
12	Preservation management roles	3	3	1	3	
13	Control of physical evidence	3	3	3	3	
14	Transmission	3	3	3	3	
15	Traceability and continuity of preservation	3	3	3	3	

Note that the investigations might be performed by more than one investigator, thereby also causing a reduction in the confidence level of admissibility. The variable version ID is used to represent a transfer of the original clone and the variable version number represents when a clone is transferred. At the end of the investigation, these variables are used to calculate the confidence level of admissibility.

3. **Main Results.** The framework we propose here covers the core requirement described in the harmonized model of digital evidence assessment [17] and the guidelines of the digital model admissibility [3] as well as the security and integrity of the digital evidence [19,20] by ensuring the integrity of the digital evidence and determining its confidence level. In addition, in several cases, investigators must use different types of forensics tools

to perform their investigations [21], and in most cases, investigators have different degrees of expertise with respect to the available tools. Hence, one piece of evidence might require handling by more than one investigator. Therefore, the design of the framework must take consideration of all the requirements previously specified. The proposed framework must also consider all the possibilities that might occur during investigation. These possibilities include the fact that 1) more than one investigator may handle the evidence; 2) during investigation, the investigator might transfer the evidence to another investigator when particular expertise is required; 3) the transferred evidence may be a copy of the original evidence or a clone of the copy, or both; and 4) the evidence may be of different types and sensitivities.

We derived a single model based on all of the above requirements and assumptions. This framework uses the timestamp injected hash function [20] to reduce the possibility of hash collisions.

We then used a scenario involving all possible handling scenarios to test the framework and generated output to provide a history and provide evidence traceability. Figure 3 shows the proposed framework.

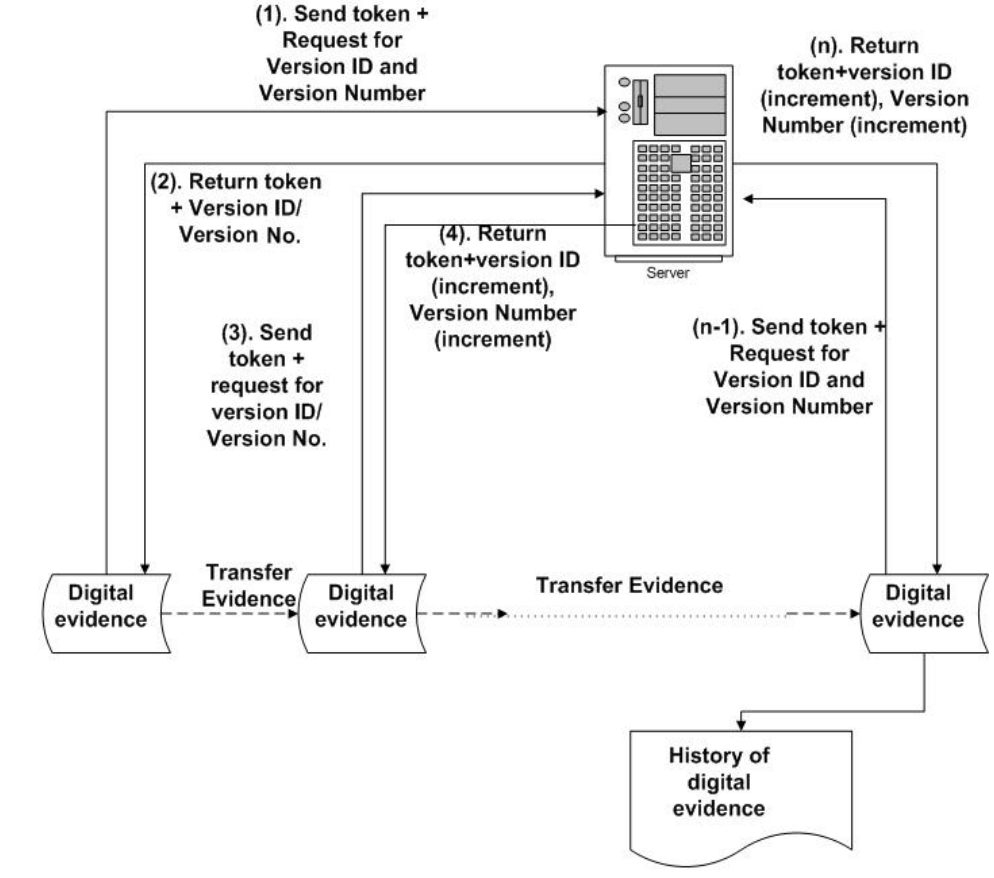

FIGURE 3. Proposed framework for ensuring admissibility of digital evidence

The proposed model uses a server for authentication. All investigators must be registered in this server. The first investigator to review the evidence at a crime scene registers the evidence, which is thereafter identified by its case identification (ID) and evidence ID. Information regarding the evidence is stored as a token, and this token is transferred from one investigator to another. Figure 3 also shows the basic content of the token, the details of which are described in Table 2.

Table 2. Contents of the tokens used in the framework

Token	Description
Case ID	The case of which the evidence belongs to
User ID	The user who handles the evidence
MD5(org)	MD5 original, to make sure the evidence can be traced back until the first copy
MAC ID	MAC (Media Access Control) address of the computer
Version ID	The version of the evidence
Version number	The number of times the clone is copied
TIMD5	Timestamp injected hash function to reduce the possibility of hash collision
Date and time	Current date and time

The security of transferring tokens is ensured by applying a centralized security protocol when sending the token. This protocol is described below.

1. $U_1 \rightarrow S:\ CASE_{ID},\ ID_{U_1},\ CODE_{DE},\ E(K_{U_1,n_1}),\ [T, verID, verNum]_{K_{U_1},S}$

U_1 sends the CASE ID, User ID and the digital evidence code ($CODE_{DE}$) to server S. An encryption key $E(K_{U_1,n_1})$ is shared by U_1, and n_1 is a nonce to ensure freshness. The token T consists of Case ID, User ID, MD5 original, TIMD5, MACID of sender, date and time (current). For Case registration, the initial value of *verID* and *verNum* is set to 0.

2. $S \rightarrow U_1:\ E(K_{U_1,n_1,n_S}),\ [T, verID + x, verNum + y]_{K_{U_1},S}$

The server S acknowledges the shared key and returned with a nonce to ensure freshness. The *verID* and *verNum* are added by x and y respectively. The value of x is 1 when original clone is used and $y = 1$.

3. $U_2 \rightarrow S:\ CASE_{ID},\ ID_{U_2},\ CODE_{DE},\ E(K_{U_2,n_2}),\ [T, verID, verNum]_{K_{U_2},S}$

U_2 sends the CASE ID, USER ID and digital evidence code (assuming the original clone is transferred). The server checks the CASE ID and DE code. The server will respond depending on the condition whether the original clone is sent (step 4) or the clone is copied and sent to another user (step 5).

4. $S \rightarrow U_2:\ E(K_{U_2,n_2,n_S}),\ [T, verID + x, verNum + y]_{K_{U_2},S}$

The version ID and version number are reset to zero.

5. $S \rightarrow U_2:\ E(K_{U_2,n_2,n_S}),\ [T, verID, verNum + y]_{K_{U_2},S}$

The version number is incremented by 1. Note that steps 4 and 5 can be repeated depending on the requirements.

The notation used and its corresponding meanings are described in Table 3.

Table 3. Security protocol notation

Notation	Description
$U \rightarrow S$	User U sends a message to server S
ID_{U_1}	The ID of U_1
$E(K_{U_1}, n_{U_1})$	Encryption key shared by a sender to another user with a nonce to ensure freshness
$[T, verID, verNum]_{K_{U_1},S}$	Content of token is within the squared bracket, encrypted using shared K between U_1 and S

The procedure for handling the evidence is as follows.

1) First, the evidence is registered in the system. At this point, hash value is assigned to the evidence and the rest of the information is saved in the history file.

2) When the evidence is given to another investigator, a token is sent to the server. The server will check the original MD5 hash value of the file and TIMD5 hash value of

the file. The server will also check these files against the history file. The server then responds by providing a new version ID with a version number starting with 1. A new history file is created for each case.

3) When the original clone is transferred, the number of the version ID increases by 1. When the clone is first copied and then transferred, the version ID remains the same and the version number increases by 1.

4. **Results and Discussions.** Previous work has shown that the condition of digital evidence is complex and there are currently no systems that address all factors when handling the security of digital evidence [14]. The human factor, in particular, is difficult to quantify. In this paper, we assume that a professional and competent individual can cause a change in a document and thereby reduce the integrity of digital evidence. The proposed framework, therefore, includes a mechanism for estimating the confidence levels of different types of evidence, ranging from 99% to 90%. For example, a picture or video is stored in pixel form. A change in one pixel would have a very small effect on the whole picture or video, so its similarity with the original would still be high. In this case, a 99% confidence level is ascribed to this digital evidence. For other file types, in general, the confidence level ranges from 98% to 95%. If the file is sent to another investigator, its confidence level with the second person would be $(99\%)^2$ following a binomial distribution. Therefore, the resulting graph is $y = (99\%)^n$, where n is the number of persons to whom the clone has been exposed. In a case in which the clone of the original evidence is transferred, then the version ID and version number restart from 1. In some cases, the clone is copied and then given to other investigators. For this case, the version ID remains the same and the version number increases by 1. In the worst situation, a small change in a document may have a large effect, so the confidence level could be estimated to be at most 90%. To obtain a detailed and focused confidence level, it is necessary to calculate the exact number of times a piece of evidence has been cloned and the number of time the clone has been cloned during the investigation. In this situation, the dependent variable depends on two other variables, the version ID and version number. The confidence level is dependent on all these variables. For this purpose, we can draw a 3D graph using several methods, such as quadratic and polynomial curve fitting. Using different scenarios, we obtained results that were essentially the same with only very small differences. To facilitate the calculation of the percentage confidence level, we used polynomial curve fitting, a graph of which is shown in Figure 4. In this study, we tested several scenarios, all of which yielded similar results. Table 4 shows an example of one scenario, which involves five different investigators. At one point, the original evidence is cloned and given to another investigator. For this situation, the variable version ID is increased by 1. At another point, the clone is itself cloned and given to another investigator. In this case, the version ID remains the same and the version number is increased by 1. We specifically designed this scenario to incorporate all evidence transfer combinations. The two factors that affect the confidence level are the number of times evidence is transferred and the sensitivity of the document.

The polynomial equation is as follows (from Figure 4):

$$\begin{aligned} f(x,y) = {} & 1.429 - 0.2867y - 0.8045x + 0.4633x^2 + 0.589xy - 0.07297y^2 \\ & - 0.1059x^3 - 0.3557x^2y + 0.02145xy^2 + 0.2069y^3 + 0.008406x^4 \\ & + 0.08148x^3y + 0.00437x^2y^2 - 0.01083xy^3 - 0.0001982y^4 \\ & - 0.006413x^4y - 0.0009869x^3y^2 + 0.001117x^2y^3 \\ & + 0.0001334xy^4 - 0.000003783y^5 \end{aligned} \tag{1}$$

where $f(x, y)$ is the confidence level, x is the version number and y is the version ID. This equation can be used to calculate the confidence level of digital evidence admissibility based on any scenario using the final value of version ID and version number obtained

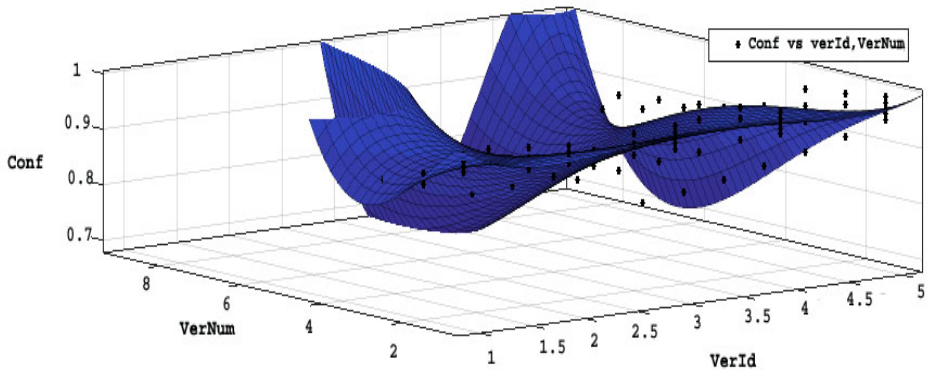

FIGURE 4. 3D graph of confidence level

TABLE 4. Scenario and contents of token during investigation

Step	Scenario	Process in the system	Variable contents	Contents of token
1	The evidence is taken at crime scene.	Evidence(E) is registered.	MD5(E), TIMD5(E), $CASE_{ID} = 1$, $verID = 1$, $verNum = 1$	Registration:CASE01:ZER:[MD5original Hash]:[TIMD5 hash value]:1:1:12112018100000
2	The evidence is cloned and given to investigator 1.	Check MD5(E), TIMD5(E), should be equal to previous one.	$verID = 1$, $verNum = 1$	Receiver:CASE01:ZER:[MD5original Hash]:[TIMD5 hash value]:1:1:15112018100000
3	The same (original) clone is given to investigator 2.	Check MD5(E), TIMD5(E), should be equal to previous one.	Add 1 to $verID$ ($verID = 2$), $verNum = 1$	Sender:CASE01:ZER:[MD5original Hash]:[TIMD5 hash value]:2:1:17112018100000 Receiver:CASE01:HLN:[MD5original Hash]:[TIMD5 hash value]:2:1:17112018100000
4	Investigator 1 forwards his clone to investigator 3.	Check MD5(E), TIMD5(E), should be equal to previous one.	$verID = 1$, Add 1 to $verNum$ ($verNum = 2$)	Sender:CASE01:ZER:[MD5original Hash]:[TIMD5 hash value]:1:2:20112018100000 Receiver:CASE01:ERL:[MD5original Hash]:[TIMD5 hash value]:1:2:20112018100000
5	Investigator 2 forwards his clone to investigator 4.	Check MD5(E), TIMD5(E), should be equal to previous one.	$verID = 2$, Add 1 to $verNum$ ($verNum = 2$)	Sender:CASE01:HLN:[MD5original Hash]:[TIMD5 hash value]:2:2:35112018100000 Receiver:CASE01:NTL:[MD5original Hash]:[TIMD5 hash value]:2:2:35112018100000
6	Investigator 3 forwards the clone to investigator 5.	Check MD5(E), TIMD5(E), should be equal to previous one.	$verID = 1$, Add 1 to $verNum$ ($verNum = 3$)	Sender:CASE01:ERL:[MD5original Hash]:[TIMD5 hash value]:1:3:28112018100000 Receiver:CASE01:RSD:[MD5original Hash]:[TIMD5 hash value]:1:3:28112018100000

from the log files. The log file containing the history of a piece of evidence is very important and represents one of the biggest challenges in digital evidence management [22].

The security of this log file must be maintained. In this proposed framework, a history of the token contents is logged at each step, including the hash values before and after digital evidence is transferred to another investigator. From the history file, each piece of evidence can be traced to check the integrity of the file. Figure 5 shows the contents of the history file up to step 3 of the scenario. In the history file, two hash values are logged, the original MD5 hash and the timestamp injected MD5 (TIMD5) hash. The function of the TIMD5 is to reduce the number of file collisions, and that of the original hash MD5 is to trace the evidence back to the original evidence.

In this framework, the obligation of the forensic investigators is taken into account both to provide a proof of a claim or a disclaimer, as well as to prove the authenticity and integrity of digital evidence [23]. With the inclusion of the human factor in the process, this framework can provide a probability of the level of trust that can accord to evidence by providing its confidence level. The final judgement of reaching a verdict is always then conclusively decided by the judges.

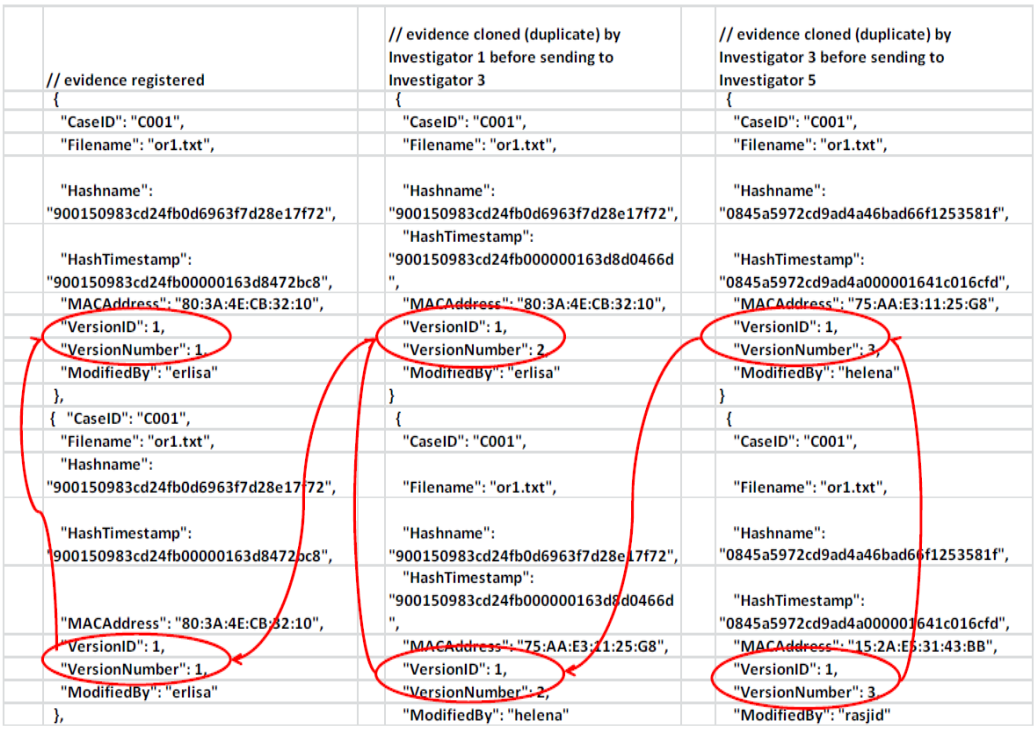

FIGURE 5. Historical file of the digital evidence

5. **Conclusions.** Of the 15 categories found in the policy relating to the digital preservation model vs. digital evidence admissibility listed in Table 1, the framework proposed in this paper addresses reliability (point 3), authenticity (point 9), integrity (point 10), transmission (point 14) and traceability (point 15). In previous models, transmission and traceability have not been highly considered. In this proposed framework, evidence can be traced in the history/log files, and its authenticity and integrity remain strong by the use of two hash functions. The files transferred from one investigator to another using security protocol provide the security in the transmission. The proposed framework provides the court with a confidence level regarding the degree to which the evidence remains intact by reducing the percentage of confidentiality every time the evidence is transferred. The use of security protocol guarantees the integrity of file during evidence transfer among investigators. It also makes it possible to trace evidence to the time at which it was seized, which supports the ability of the judges to issue an appropriate verdict, by combining the forensic reports with the evidence confidence level.

We applied several scenarios in testing the proposed framework. As an example, using the equation for the confidence level, with a final result of version ID = 2 and version number = 3, the confidence level would be 92.84%, and with a final version ID = 3 and version number = 3, the confidence level would be 89%. Note that the confidence level is reduced slightly as evidence is exposed to more investigators. By reporting this information to the court, judges are better equipped to provide a quality judgment toward the verdict.

Acknowledgment. The authors gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] N. M. Karie, V. R. Kebande and H. S. Venter, Taxonomy for digital forensic evidence, *Pan-African Conference on Science Computing and Telecommunications*, 2017.

[2] G. Kapil, A. Agrawal and R. A. Khan, Security challenges and precautionary measures: Big data perspective, *ICIC Express Letters*, vol.12, no.9, pp.947-954, 2018.
[3] F. M. Granja and G. D. R. Rafael, The preservation of digital evidence and its admissibility in the court, *Int. J. Electron. Secur. Digit. Forensics*, vol.9, no.1, pp.1-18, 2017.
[4] X. Wang, X. Lai, D. Feng, H. Chen and X. Yu, Cryptanalysis of the hash functions MD4 and RIPEMD, in *Advances in Cryptology – EUROCRYPT 2005*, R. Cramer (ed.), vol.3494, Berlin, Heidelberg, Springer, 2005.
[5] N. Kashyap, A meaningful MD5 hash collision attack, *Writing Project*, 2006.
[6] Y. Sasaki and Y. Naito, Improved collision attack on MD5, *IACR Cryptol.*, pp.1-11, 2005.
[7] J. Liang and X. Lai, Improved collision attack on hash function MD5, *J. Comput. Sci. Technol.*, vol.22, no.1, pp.79-87, 2007.
[8] K. Aoki and Y. Sasaki, Preimage attacks on one-block MD4, 63-step MD5 and more, in *Selected Areas in Cryptography SAC 2008*, R. M. Avanzi, L. Keliher and F. Sica (eds.), vol.5381, 2009.
[9] M. Stevens, New collision attacks on SHA-1 based on optimal joint local-collision analysis, in *Advances in Cryptology – EUROCRYPT 2013*, T. Johansson and P. Q. Nguyen (eds.), vol.7881, Berlin, Heidelberg, Springer, 2013.
[10] M. Stevens, Single-block collision attack on MD5, *Cryptology Eprint Archive Report*, 2012.
[11] M. Stevens, A. Lenstra and B. De Weger, Chosen-prefix collisions for MD5 and colliding X.509 certificates for different identities, in *Advances in Cryptology – EUROCRYPT 2007*, M. Naor (ed.), vol.4515, Berlin, Heidelberg, Springer, 2007.
[12] P. Karpman, T. Peyrin and M. Stevens, Practical free-start collision attacks on 76-step SHA-1, in *Advances in Cryptology – CRYPTO 2015*, R. Gennaro and M. Robshaw (eds.), vol.9215, Berlin, Heidelberg, Springer, 2015.
[13] V. Chiriaco, A. Franzen, R. Thayil and X. Zhang, Finding partial hash collisions by brute force parallel programming, *2017 IEEE Long Isl. Syst. Appl. Technol. Conf.*, vol.5, pp.1-6, 2017.
[14] S. Soltani and S. A. H. Seyo, A survey on digital evidence collection and analysis, *International Conference on Computer and Knowledge Engineering*, pp.247-253, 2017.
[15] Y. Prayudi and A. Sn, Digital chain of custody: State of the art, *Int. J. Comput. Appl.*, vol.114, no.5, pp.1-9, 2015.
[16] S. Zawoad and R. Hasan, Digital forensics in the age of big data: Challenges, approaches, and opportunities, *2015 IEEE 17th Int. Conf. High Perform. Comput. Commun., 2015 IEEE 7th Int. Symp. Cybersp. Saf. Secur., and 2015 IEEE 12th Int. Conf. Embed. Softw. Syst.*, pp.1320-1325, 2015.
[17] A. Antwi-Boasiako and H. Venter, A model for digital evidence admissibility assessment, in *Advances in Digital Forensics XIII*, G. Peterson and S. Shenoi (eds.), vol.511, 2017.
[18] Y. Prayudi and T. K. Priyambodo, Secure and trusted environment as a strategy to maintain the integrity and authenticity of digital evidence, *Int. J. Secur. Its Appl.*, vol.9, no.6, pp.299-314, 2015.
[19] S. R. Selamat, S. Shahrin, N. Hafeizah, R. Yusof and M. F. Abdollah, A forensic traceability index in digital forensic investigation, *J. Inf. Secur.*, vol.4, no.1, pp.19-32, 2013.
[20] Z. Rasjid, E. Abdurahman, B. Soewito and G. Witjaksono, Timestamp injected hash function to reduce hash collision, *Pertanika J. Sci. Technol.*, vol.26(T), 2018.
[21] D. Billard, Weighted forensics evidence using blockchain, *Proc. of the 2018 International Conference on Computing and Data Engineering*, pp.57-61, 2018.
[22] G. Narayana Samy, B. Shanmugam, N. Maarop, P. Magalingam, S. Perumal and S. H. Albakri, Digital forensic challenges in the cloud computing environment, in *Recent Trends in Information and Communication Technology*, F. Saeed, N. Gazem, S. Patnaik, A. Saed Balaid and F. Mohammed (eds.), Springer, 2017.
[23] E. Casey, Clearly conveying digital forensic results, *Digit. Investig.*, vol.24, pp.1-3, 2018.