Storage Area Network Architecture to support the Flexibility of Digital Evidence Storage

Moh. Ali Romli
Departmen of Informatics
Universitas Islam Indonesia
Yogyakarta Indonesia

Yudi Prayudi
Department of Informatics
Universitas Islam Indonesia
Yogyakarta Indonesia

Bambang Sugiantoro
Department of Informatics
UIN Sunan Kalijaga
Yogyakarta Indonesia

ABSTRACT
Cybercrime is a criminal activity that utilizes computers and the internet as a media in committing its crimes. In solving the case of cybercrime, it is useful with the help of digital forensics. The critical component in digital forensics is electronic evidence that has a physical form and digital evidence that has form in the binary file. Both types of evidence require handling in the storage process with different treatments. In this case, physical evidence of physical nature will be stored in the evidence room while digital evidence will be stored in evidence storage. The solution that has existed so far is through the mechanism of storing digital evidence stored in evidence storage based on internal storage with limited accessibility to one device. It causes inflexibility and effectiveness to support collaborative efforts between officers and law enforcement in the process of investigating and handling digital evidence. This research is to develop previous research on digital evidence storage and handling systems. This paper presents a solution for centralized and network-based digital evidence storage architecture to address the weaknesses of previously available solutions. Flexibility repositories based on SAN (Storage Area Network) and web-based technology are used as network-based centralized storage architectures. The system is expected to help between law enforcement in terms of chain of custody management for digital evidence.

General Terms
Digital Forensics, Digital Evidence, Chain of Custody, SAN, Evidence Storage

Keywords
Digital Evidence, Storage Area Network, Repository, Flexibility, Web Based

1. INTRODUCTION
Cybercrime is a criminal activity that utilizes computers and the internet as a media in committing its crimes. In solving the case of cybercrime, it is useful with the help of digital forensics. The critical component in digital forensics is electronic evidence that has a physical form and digital evidence that has form in the binary file. Both types of evidence require handling in the storage process with different treatments. In this case, physical evidence of physical nature will be stored in the evidence room while digital evidence will be stored in evidence storage.

One study that provides a solution to the storage of digital evidence is conducted by [1]. In this study, provides solutions in the form of application of chain of custody for digital evidence documentation with an XML approach. Fortunately, this research has limitations in terms of storage based on internal storage and accessibility which only depends on one device. While the desired demand for digital evidence storage solutions is a flexible and effective system, this is needed to support collaborative efforts between law enforcement in the management of digital evidence in the process of investigating cybercrime cases handled.

This paper presents a solution to the limitations of previous research by [1] with a solution in the form of a centralized network-based digital evidence storage and chain of custody approach with the concept of repository flexibility. COC Reflex identified as a system. This concept is supported by SAN (Storage Area Network) technology as a network-based centralized storage architecture, while for accessibility and system interfaces web-based technology is applied, then for external metadata information files from digital evidence stored on the MySQL database. The system is expected to help collaborative efforts between law enforcement in conducting the investigation process in the case of cybercrime that is handled so that it becomes more flexible and useful. Furthermore, this paper will discuss digital evidence, chain of custody, SAN architecture design, simulation and implementation, and analysis.

2. DIGITAL EVIDENCE
Digital evidence is the primary object in the digital forensic activity that contains information used to support the process of investigating a case of cyber crime [2]. Digital evidence can include information about audio files, videos, images, e-mail, encrypted files, steganography files [3]. While the primary purpose of digital forensic activities is to maintain, collect, validate, identify, analyze, interpret, document, and present the results of documented digital evidence analysis in the form of a chain of custody for presentation in court of law [4].

Legally each country has its provisions regarding the type, character, and procedure of digital evidence to be accepted at the trial of law [2]. However, in general, digital evidence can be accepted in court if it fulfills some characteristics, namely, admissible, authentic, complete, reliable, and believable [5]. Through these criteria it can be maintained the integrity of the digital evidence that will be used, the clear linkages with the case being investigated, the completeness of the evidence collected also can be trusted.

3. CHAIN OF CUSTODY
Chain of custody is a chronology of documentation and an essential part of evidence from the investigation process that will guarantee the evidence as can be received in the trial process [3]. Judging from the method of documentation, the process of a chain of custody carried out without using an application tends to be inefficient, and applicable digital forensic procedures cannot guarantee its integrity. It is because the processes that are manual have not yet implemented authentication and authorization [6]. In this case, the chain of custody documentation can be received in

court if it includes 5W + 1H information (what, when, who, why, where, and how) to any information that occurs in the investigation process carried out [7].

a. What represents what handled cases.

b. When to explain the time of the chain of custody process carried out starting from digital evidence uploaded and changed.

c. Who is used to explain users who interact directly or indirectly, in the system of chain of custody there are two classifications of users involved in the system, namely internal parties and external parties, namely:

1. First Responder is a user who acts as the first person in uploading digital evidence to the DCOC reflex system, as well as filling out the chain of custody form which includes information from uploaded digital evidence such as electronic evidence information, as well as digital evidence information.

2. Investigator is a user whose task is to analyze digital evidence uploaded to the system, and fill in the form chain of custody for the results of the analysis carried out.

3. Officer is the officer who adds the user and gives access rights to the users involved in the DCOC reflex system and tasked with the approval process on the input results from first responders and investigators.

4. External means a user such as prosecutors, judges, lawyers, and other law enforcement parties that involved in handling cases, access rights to the system, including view and download of verified digital evidence reports as a result of investigation and analysis.

d. Why is used to answer the background of events related to digital evidence.

e. Where which is the flow process of the used and stored of digital evidence.

f. How the process of dealing with digital evidence (chain of custody).

4. ARCHITECTURE SAN DESIGN

4.1 Architecture SAN Design

SAN is a segmented area of the network that handles data storage and transfer between computers and storage elements [8]. SAN is a particular network architecture consisting of servers, storage, and hosts designed to handle large amounts of data traffic between servers and storage devices and separate intensive backup traffic from normal traffic. The SAN consists of a communications infrastructure that provides connections, storage, and computer systems, to produce secure data transfers. From the concept of SAN performance, the Reflex COC system will apply the SAN network architecture to the storage management process and digital proof documentation. The following is the design of the SAN architecture on the COC reflex system.

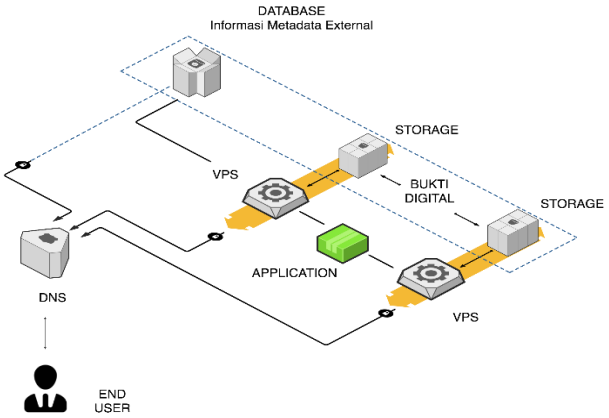

Fig 1: SAN Architecture Design

The design of the SAN architecture is a general description of the system activity for digital evidence processing, as well as the realization of the concept of the proposed COC reflex system. Figure 1 is a SAN architectural design consisting of 4 structures which include:

a. *End user* which is an aspect of the personnel involved in using the COC reflex system and managing digital evidence according to the access rights granted, in the COC reflex system the user divided into two categories, internal and external parties. For internal parties to access the system, they must enter a username and password that has been registered in the system, while external parties simply enter a system token that will be given manually by the internal party in charge of giving access rights, because external parties can only view and download reports analysis results from the digital evidence.

b. DNS is a server that used as a domain gateway with an IP server.

c. VPS as a processing media and runs the COC reflex system application.

d. *Storage* is a storage medium for digital evidence that managed in the COC reflex system, which includes storing digital evidence and information on external metadata stored separately in the database.

4.2 System Design Reflex COC

The SAN architecture described in Figure 1 used as a reference in designing the COC reflex system as needed in terms of digital evidence management. Below is an overview of the design of the COC reflex system.

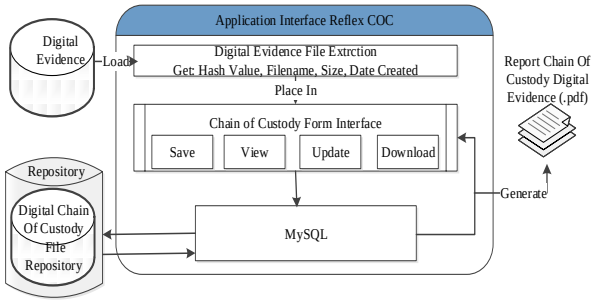

Fig 2: System Design Reflex COC

In the design of the reflex system, COC is a user interface of the repository system that will implement the concept of SAN architecture and web-based technology as a managed digital evidence storage media, and MySQL for external metadata information databases. While for the personnel/users involved in the system are divided into four, including first responders, investigators, officers, and external parties. Each user has different access rights to the COC reflex system as well as managed digital evidence.

4.3 COC System Reflex Flow Path

The COC reflex system activity flow is a functional description of the system workflow in digital evidence processing based on the design concept of the SAN architecture.

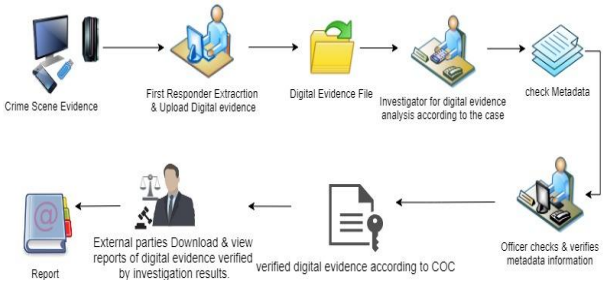

Fig 3: Reflex COC Flow Path

The flow of COC reflex system activities is the processing of evidence to become a report that will use in the law enforcement process. The first step is to collect electronic evidence from the crime scene, and if there is a connection with the handled case, then the electronic evidence is carried out an extraction process to obtain digital evidence to be analyzed. After the extraction process completed, first responders tasked with uploading digital evidence to the COC reflex system, during the upload of digital evidence the first responder officer filled out the form to complete information on the digital evidence that has uploaded.

The next step is for the investigator doing the process of analyzing digital evidence by first downloading the COC reflex system. Next is the process of analyzing the digital evidence, when the analysis process has completed, the investigator officer completes the analysis results from information as external metadata from the digital evidence that is analyzed. The next step is for the officer to re-correct the information form that has been filled in by the investigator if the form is incomplete, the officer will reject the file to be analyzed, then the investigator will be asked to edit and re-upload. If the filling process is complete, the officer will carry out the approval process, and the results of the analysis are downloadable in pdf format. The final result is the final report for the law enforcement process carried out by external parties (prosecutors, judges, lawyers) and officers who have the granted access rights.

5. IMPLEMENTATION

The implementation of the COC reflex system supported by SAN architecture and web-based technology using the PHP programming language. MySQL database for storing external metadata information. The COC reflex system can run in various platforms and can be accessed using public IP.

5.1 User Interface of COC System Reflex

The user interface is a display of the COC reflex system that implemented on a web-based system. Figure 4 below depict the COC reflex system user interface.

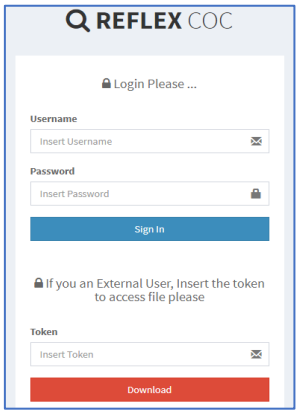

Fig 4: Login User Page

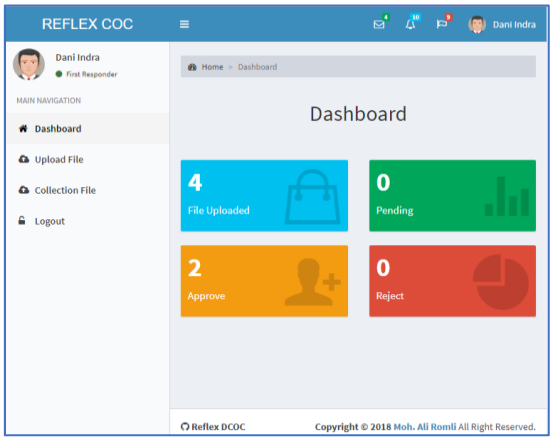

Fig 5: Firts Responder Dashboard Page

Furthermore, Figure 5 shows the first responder dashboard display in which several menus are used to assist in digital evidence processing. Figure 6 is a view for the file upload form used to upload digital evidence on the server. Digital proof files taken from the drive where digital evidence stored. Uploaded digital proof files can support all formats.

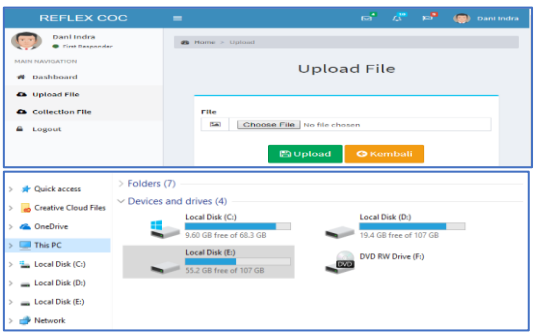

Fig 6: Upload Data Digital Evidence Page

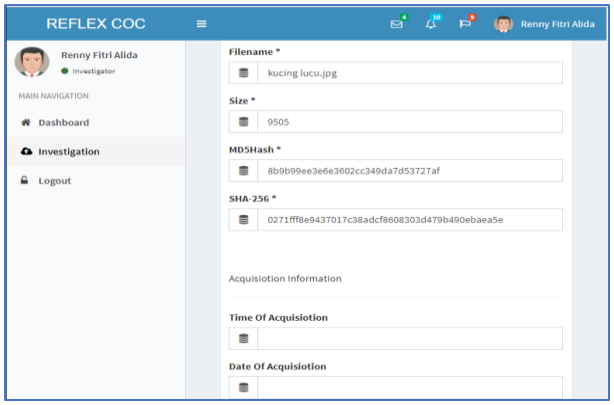

Fig 7: Form COC Investigator

Figure 7 is a display of Form chain of custody which is a form used to add external metadata information from digital evidence from an investigator's analysis, the information data of the metadata is stored in the database.

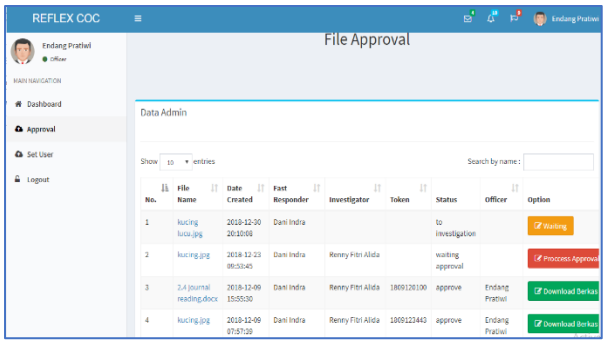

Fig 8: Officer Approval Page

Figure 8 is the approval page, which is the page used in checking the upload of external digital data metadata data information that has been inputted by the investigator, if the information entered is complete in terms of data filling, the approval process will be carried out by the officer.

5.2 Simulation & Test Scenario

The simulation and scenario phase are functional testing stages of the system based on the concept of SAN architecture that is implemented on the COC reflex system. Testing is done by accessing a system that has been implemented in the cloud, with the formation according to the access rights given as follows:

a. First responder is the first person in charge of uploading digital proof files according to the case handled.

b. Investigator is tasked with investigating the digital evidence uploaded according to the case.

c. Officer is an officer who gives access rights and approval to digital evidence.

d. External is the party that gets the access rights to view and downloads in the form of a report on the results of the investigation of digital evidence according to the cases handled, such as judges, public prosecutors and lawyers.

From the above formation, a simulation scenario carried out as shown in the following table:

Table 1. Scenario Simulation Table

Scenario	First Responder	Investigator	Officer	External
1	1	1	1	n
2	2	1	1	n
3	2	2	1	n
4	2	2	2	n

In the Table 1, the test scenario of the concept of SAN architecture that implemented on the COC reflex system, it is done by validating the system. The used criteria are the fulfillment of flexibility needs by utilizing the cloud as a digital evidence storage media to support the chain of custody documentation process.

For more details of the test scenario, it can be seen on the flowchart as follows:

a. Figure 9 is Testing Scenario 1. This test is carried out with the formation of one first responder, one investigator, and one officer. The uploaded digital evidence is handled by each user until it becomes a report.

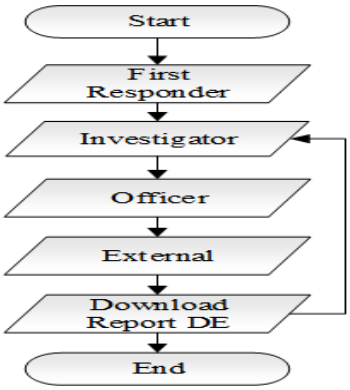

Fig 9: Experiment Scenario 1

b. Figure 10 is a test in scenario 2. In this scenario, there are two first responders, one investigator, and one officer, in this test the investigator will choose one case from the first respondent to be processed by the officer.

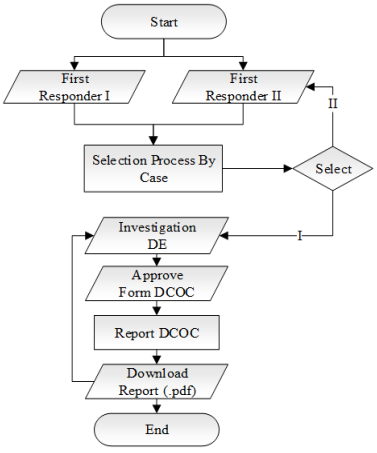

Fig 10: Experiment Scenario 2

c. Figure 11 is a test in the third scenario. In this scenario, there are two first responders, and two investigators, in this test each investigator will choose one of the digital evidence from the first respondent, then the officer will proceed by selecting one of the results investigations of two investigators.

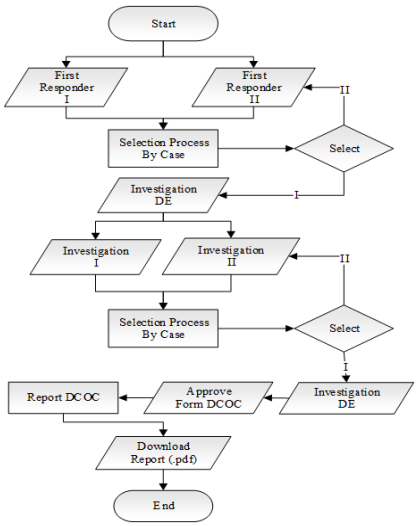

Fig 11: Experiment Scenario 3

d. In Figure 12 is testing the 4th scenario. In this scenario, there are two first responders, two investigators, and two officers, in this test each officer will choose one of the results of the investigation for approval.

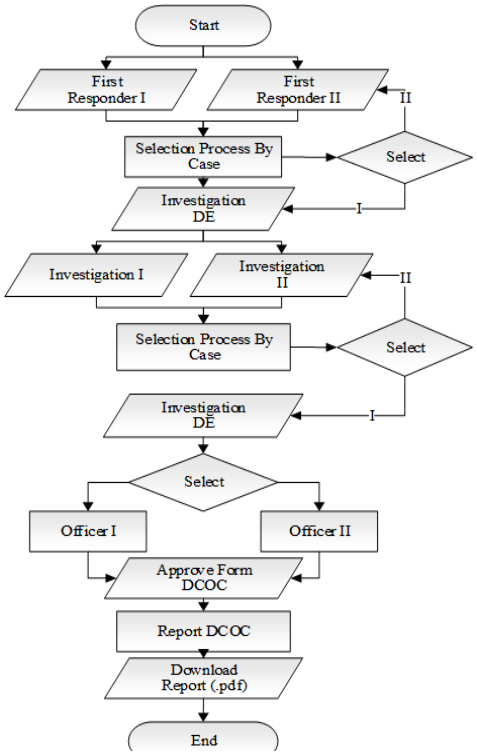

Fig 12: Experiment Scenario 4

5.3 Analysis of Scenario Simulation

Scenario simulation analysis is the result obtained after performing a series of functional accessibility tests on the Reflex COC system, the results of each scenario tabeled in the following table:

Table 2. Scenario Result

Scenario Testing	1	2	3	4
Number of first responder	1	2	2	2
Number of Investigator	1	1	2	2
Number of Officer	1	1	1	2
Number of External	~	~	~	~
File upload testing	Succeded	Succeded	Succeded	Succeded
Investigation testing	Succeded	Succeded	Succeded	Succeded
Approval Testing	Succeded	Succeded	Succeded	Succeded
Download Report Testing	Succeded	Succeded	Succeded	Succeded
Function of Reflex COC System	According to flow	According to flow	According to flow	According to flow
Overall test results	Function	Function	Function	Function

The Reflex COC system is a web-based system that utilizes cloud storage. In the process of storing files, the COC reflex system uses the file transfer protocol (FTP) method. FTP or File Transfer Protocol is an internet protocol that used for sending data in computer networks such as uploading and downloading files carried out by FTP clients and FTP servers. When we upload large files using FTP, it takes time to transfer according to the file size. Then to use the COC reflex system is by using the browser. The browser version affects user experience. A particular browser such as Google Chrome is required to get optimal performance.

The problem in previous research is the use of systems that require installation and processing of data carried out on internal hard drives. This method makes the system not flexible. Users must use the same computer when there is a need for data processing. This condition makes the evidence and the system operated cannot be done remotely. Furthermore, it required a system that has the same function but has a usage method approach that can be accessed remotely. The Reflex COC system resolves the problems of previous researchers by changing the method to be explained in the following table:

Table 3. Feature Comparison

No	System Feature	Old	New
1	System Installation	Install on Pc Client	Install on Server
2	System Access	PC client centered	Multiplatform
3	File Storage	PC client centered	Cloud
4	Remote Access	No	Through Internet
5	Flexibility	Can not access remotely	Using browser and Internet

Other systems in the literature using the default internal or hard disk storage media from the PC. The system developed on a desktop that requires local installation. The system can operate without having to be connected to the internet so that it can operated by offline. While the COC reflex system is a cloud-based system in file storage by using a website platform so that it can be accessed from various devices with media browser access. In its use, the COC reflex system requires internet access to be able to connect with the server. The COC reflex system does not require installation. So that the COC reflex system provides solutions that can be accessed remotely and flexible.

6. CONCLUSION & FUTURE WORKS

According to the repository system that related to SAN as a network-based centralized storage architecture concept and web-based technology, it concluded that the Reflex COC system has been able to answer previous problems. Regarding digital evidence storage based on internal storage and access systems that depend on one device. With the SAN architecture approach and web-based to build repository flexibility, it makes it easy in the implementation process in storing and accessing digital evidence flexibly and effectively. Also, the COC reflex concept supports collaborative efforts between officers in handling managed digital evidence, because digital evidence is managed stored in cloud-based external storage.

This research has not focused on the concept of uploading digital proof files. So further research needs to develop a repository system for digital evidence with the SaaS concept in the use of each user access and digital evidence management process using the cloud, and the addition of Virtual Private access features Network (VPN) to manage access rights.

7. ACKNOWLEDGMENTS

Our thanks to the experts who have contributed towards development of the template.

8. REFERENCES

[1] D. Ratnasari, Y. Prayudi and B. Sugiantoro, "XML Approach for the Solution of Chain of Custody of Digital Evidence," International Journal of Computer Applications, vol. 179, no. 23, p. 0975 – 8887, 2018.

[2] Y. Prayudi, "PROBLEMA DAN SOLUSI DIGITAL CHAIN OF CUSTODY DALAM PROSES INVESTIGASI CYBERCRIME," in Seminar Nasional Sains dan Teknologi Informasi, Makasar, 2014.

[3] Y. Prayudi and A. Sn, "Digital Chain of Custody: State of The Art," International Journal of Computer Applications, vol. CXIV, no. 5, pp. 1-9, 2015.

[4] E. Morioka and M. S. Sharbaf, "Digital Forensics Research on Cloud Computing: An investigation of Cloud Forensics Solutions," IEEE Symposium on Technologies for Homeland Security (HST), vol. X, no. 16, pp. 1-6, 2016.

[5] J. Richter, N. Kuntze and C. Rudolph, "Securing Digital Evidence," IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, vol. VI, no. 15, pp. 1-10, 2010.

[6] K. Widatama and Y. Prayudi, "Konsep Lemari Penyimpanan Bukti Digital Menggunakan Struktur Bahasa XML," in Seminar Nasional Informatika dan Aplikasinya, Cimahi, 2017.

[7] J. Cosic, "Formal Acceptability of Digital Evidence," Springer International Publishing, vol. CXV, no. -, pp. 327-348, 2017.

[8] M. Davis, G. Manes and S. Shenoi, "A Network-Based Architecture for Storing Digital Evidence," The International Federation for Information Processing, vol. CXCIV, no. -, pp. 33-42, 2005.