Iraqi Journal of Information and Communications Technology(**IJICT**)
**Vol. 3, Issue 3, June 2020**

**ISSN:2222-758X**

# DESIGN OF DIGITAL CHAIN CUSTODY FOR REPUBLIC OF IRAQ

**Shireen M. Abed Zaid** [1], **Bayan M. Sabbar** [2]
[1,2] College of Information Engineering, Al-Nahrain University, Baghdad, Iraq
shireen.elaf@gmail.com [1], bayan.mahdi@coie-nahrain.edu.iq [2]

Received:21/4/2020, Accepted:10/07/2020

***Abstract*- The growth of information technology lead to increasing number of users for various types of electronic equipment that resulted in the rise of cybercrime. Increasing cybercrime lead to increasing volume of digital evidence handled by the investigators; that mean more documentation, complexity of management and complexity to keep its integrity. So that, a significant procedure in handling of evidence and investigation is called as a chain of custody (CoC) , which a concept and process designed to ensure the integrity of evidence including digital evidence (DE) and to document the digital evidence from the time it collected to the time where the evidence actually presented at the court. Without a chain of custody, the evidence is valueless so that it played a vital role in the digital forensic investigation process. The solution offered in this paper is to build a Digital chain of custody application software in order to ensure the integrity and originality of digital evidence also to document these evidences from various types of digital evidence file such as network packet capture files, disk image files, extracted document files, multimedia files and more. The application is constructed through four approaches to keep the integrity of evidence: applying Hash function for each evidence and save the information in XML file, watermarking, extract metadata for each evidence and specify a geolocation for each evidence. Also, there is a privilege for users to access the application, no one can access the application without admin permission. There are two types of the chain of custody information, which are the information entered by the user and information extracted from the metadata of digital evidence file. The output from a chain of custody application is a form in the .pdf document format.**

***keywords:*** **Chain of custody (COC) , Digital integrity, Digital evidence, Metadata, XML and Preservation.**

## I. INTRODUCTION

Chain of custody can define a set of procedures to document files according to its chronological [1] . Giova [2] , states that digital evidence should be accepted as valid in court only if the evidence chain of custody can be founded. Also If the COC stay intact, each witness, from the officer to the custodian of evidence, can certify that all the items presented in the courtroom is indeed the item that was collected at the crime scene and tested by the lab [3] . Work with DE properly during investigation process is very significant step. In cyber-crime the evidence is divided in two type, digital evidence and physical evidence. So that, chain of custody is used to document these evidences. Chain of custody doesn't have any stander or special regulation because each country has their own investigation process. Chain of custody is a significant part in the investigation process to ensure the admissibility of evidence in the courtroom. It will document the case related to where, when, why, who and how the evidence is carried out at each stage of the investigation. Each evidence should be preserved based on integrity and authenticity according to the condition when it discover till then will be presented to the court of law [4] . So that, the COC should include at least (Five W's and 1 H) , The 5 Ws are the When, Who, Where, Why, What and the 1 H is the How [5] , and answer the question [6] which are:

1) Who came into contact, manage, and discovered the digital evidence ?
2) What procedures executed on digital evidence?
3) When the digital evidence is discovered, accessed, examined, or transferred ?
4) Where was digital evidence discovered, collected, managed, saved, and examined ?
5) Why the digital evidence was collected ?

6) How was the digital evidence collected, used, and stored ?

Digital evidence has different form so in order to document it and preserve its integrity is very hard using register book or forms unlike the physical evidence. Although they have different characteristic but they have the same information and concept to be documented in chain of custody [7] , [8] . Therefore, for the importance of chain of custody in investigation process, a Digital chain of custody application has been design using SQL and XML approach. SQL database used for document the information of submitting case while XML are used to store the information of each evidence including hash value. Some advantages of using an XML approach are it's robust, strong, easy to manipulate, data independence and free for anyone, also easy for store , transfer and identify of information [9] . Then extract digital evidence metadata information [10] , [12] to check if the image has been modified using any editor software application like photoshop. Finally allocate geolocation for the collected DE. The aim of the proposed application is to present a solution that improve the integrity and credibility of digital evidence in order to be acceptable and admissible in the court of law. Also capture the attention of government officials in Iraq so as to fully develop and adopt chain of custody applications build for the republic of Iraq.

## II. Related Work

Chain of custody is very important in digital forensic filed for keeping the integrity of an evidence as well as to document the evidence. But, there are few solutions provided by other researchers the keep the integrity and document the digital evidence such as proposed framework for handling digital chain of custody with the digital cabinet concept [13] , creating the business model of digital evidence handling and cybercrime investigation [7] , build a framework of the to improve a chain of custody of digital evidence investigation [14] , the ontology approach using in managing the information needed in chain of custody [15] , [16] , using an XML document type for digital evidence documentation like the concept of plastic bag of evidence [17] and imply XML approach to document a digital evidence in chain of custody application [18]. According to the above research, there is no application can keep the integrity of digital evidence in different techniques as well as document these evidences. The proposed chain of custody application for digital evidence comes as one of the proposed solutions to enrich the existing solution of the digital chain of custody.

## III. Design Architecture System

The Digital Chain of Custody application is an implementation prototype using the SQL database to save the information of the case and digital evidence hash value using the XML approach. Then store the information of evidence and compare their results with the information in the chain of custody tab. Some advantages of using an XML approach are it's strong, durable, easy to manipulate, data independence, interoperability and free for anyone. XML -based is also easy to identity, store, and transfer of information. This proposed application architecture is basically designed to support various types of digital evidence files such as extracted document files, multimedia files, disk image files, network packet capture files and more. The type of files comes from various electronic evidence sources such as a computer, mobile phone, USB drive, laptop, and others. It provides a potential ground for inadmissibility of such evidence in court and Providing documentation of the control, transfer, and analyses of evidence helps to ensure that the evidence presented before that court has not been contaminated. The main functions accommodated by the application extract the Metadata information of digital evidence files, create documentation files, modify documentation information and save the documentation information on the application. Those functions can be shown in the Digital Chain of Custody application architecture in Fig. 1.

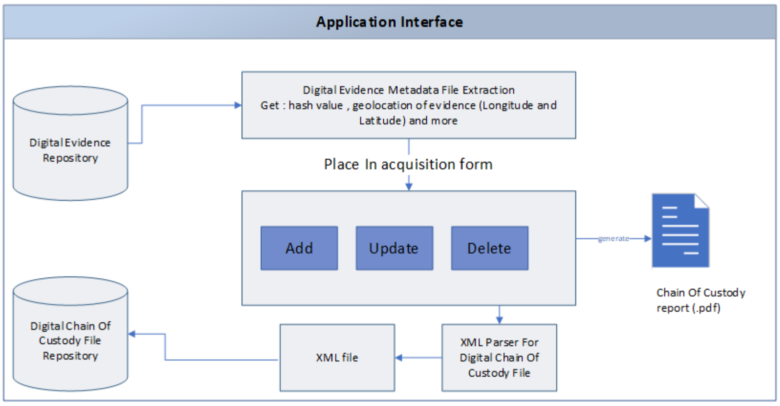

Application Interface
Digital Evidence Repository
Digital Evidence Metadata File Extraction
Get : hash value , geolocation of evidence (Longitude and Latitude) and more
Place In acquisition form
Add
Update
Delete
generate
Chain Of Custody report (.pdf)
Digital Chain Of Custody File Repository
XML file
XML Parser For Digital Chain Of Custody File

Figure 1: Digital chain of custody application architecture

The requirement needed in designing a software are: Visual studio, NET framework 4.5 with C$^\sharp$ software and Sql server 2016 express. Also, the configurations of the software are very easy and can work any operating system or platform. So that, minimum hardware requirements are (processor core i3/ 3rd generation,4 GB RAM and 40GB HDD) . It is recommended not to install the application on (C) drive because of the administrative privileges. User can install database in two ways:

1) Either on individual systems.
2) Or, centrally on server and from the server each computer can be connected.

## IV. Flow of Recording

Recording activity of chain of custody information performs application interface. The recording of the chain of custody information starts from collection info, subsect info electronic evidence, acquisition analysis, digital evidence, a chain of custody and report. The application has two users with different permissions in carrying out the chain of custody information activities, officer (admin) and investigator (user) , An officer is a person responsible for the chain of custody information and, test the digital evidence (in/ out) from the storage Media. Before doing any activity inside this application. User as an officer has full control of information and application. Therefore, every activity performed by the investigator must obtain approval from the officer. The recording functions accommodated within the application are load the digital evidence file into the application, extract the file Metadata information, entry and save the information and generate a report from the chain of custody information presented in a form with a .pdf document. To carry out the action of making the Chain of Custody documentation file in the Digital Chain of Custody (COC) application. Fig. 2 can explain the flowchart of the application design.

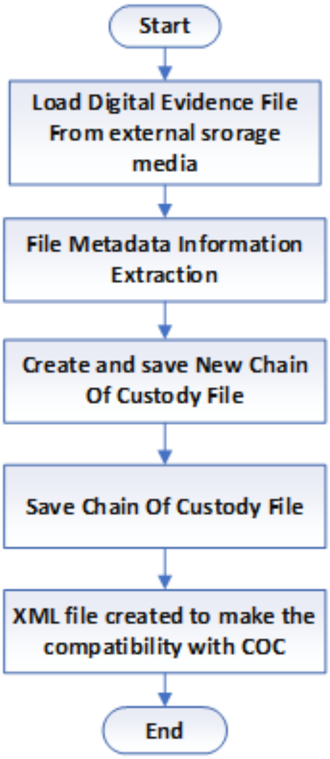
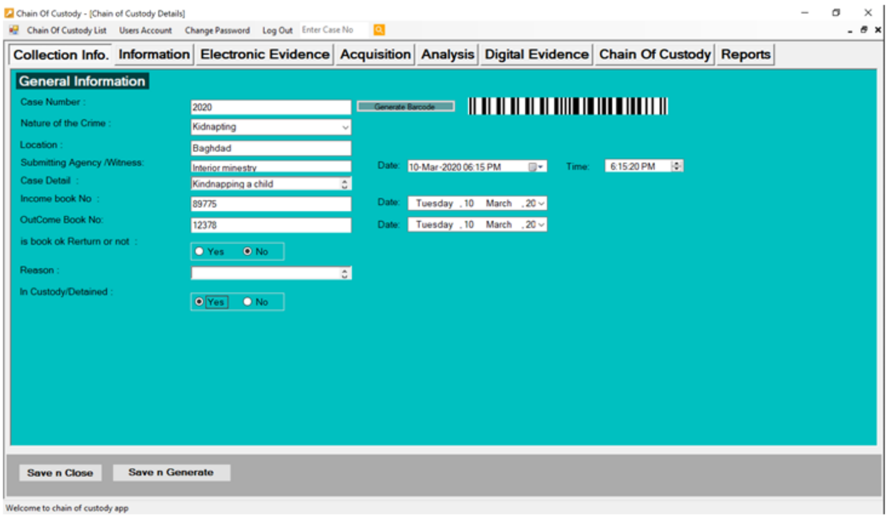

Start
Load Digital Evidence File From external srorage media
File Metadata Information Extraction
Create and save New Chain Of Custody File
Save Chain Of Custody File
XML file created to make the compatibility with COC
End

Figure 2: Flowchart of create chain of custody file

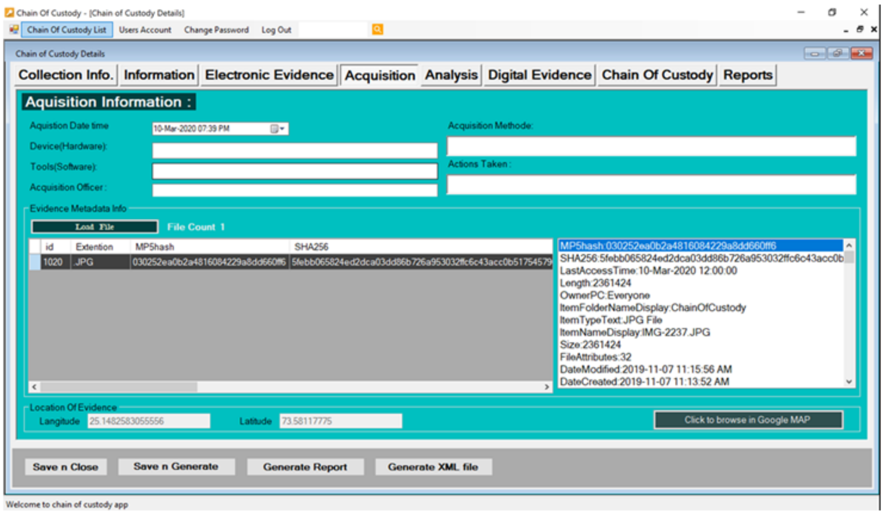
## V. Implementation & Results

Requirements for gathering and analyzing are the first phase of creating and develop a chain of custody application software. In the phase the focus on some important issues to achieved what needs from design the Application. The information and the digital evidence of the case should not change or altered only when an interaction with the digital evidence from and to the storage media. Most of the information fields for the chain of custody are obtained from Iraqi cyber- crimes directorate[1] and the other information is from models downloaded from the internet[2,3] . The form used in identification and extraction is a form of evidence chain of custody for all types of crimes cases. There are 8 tabs named Collection information tab, Information tab, Electronic tab, Acquisition tab, Analysis tab, Digital Evidence tab, Chain of Custody tab and Report tab, So that there are 66 fields for the COC application are needed to document all case details (digital and physical evidence) and to ensure their integrity. All these fields are important to file for any case that should be documented. After gathering requirements, some analytical studies are conducted to find the system's requirements in order to be designed and implemented later. Briefly, it is very important to build a friendly user interface that the investigators and officer find it easy to use have all records to documents the case details. Fig. 3, shows that the application can create a barcode for each input case depending on the case number. Fig. 4, is a form that shows metadata information that will appear after saving the DE in the application. Metadata information such as file name, file size, create time, modified program, date modified geolocation of image (Longitude and Latitude) and others. Metadata is very important in the digital forensic field because this information helps the investigator to know if the image is forged or not and which software is used. Also, the place that this image was collected by display the result on Google Maps. The application can also save an image with watermarks by embedded the logo of ministry of interior for each image. Also, the application can create hash value (MD5 and SHA256) for each digital evidence file, very quickly regardless of image size.



Case Number : 2020
Nature of the Crime : Kidnapting
Location : Baghdad
Submitting Agency /Witness: Interior minestry
Date: 10-Mar-2020 06:15 PM
Time: 6:15:20 PM
Case Detail : Kindnapping a child
Income book No : 89775
Date: Tuesday , 10 March , 20
OutCome Book No: 12378
Date: Tuesday , 10 March , 20
is book ok Rerturn or not : ○ Yes ● No
Reason :
In Custody/Detained : ● Yes ○ No

Figure 3: Interface of collection information tab



Aquistion Date time: 10-Mar-2020 07:39 PM
Acquisition Methode:
Device(Hardware):
Tools(Software):
Actions Taken :
Acquisition Officer :

File Count 1

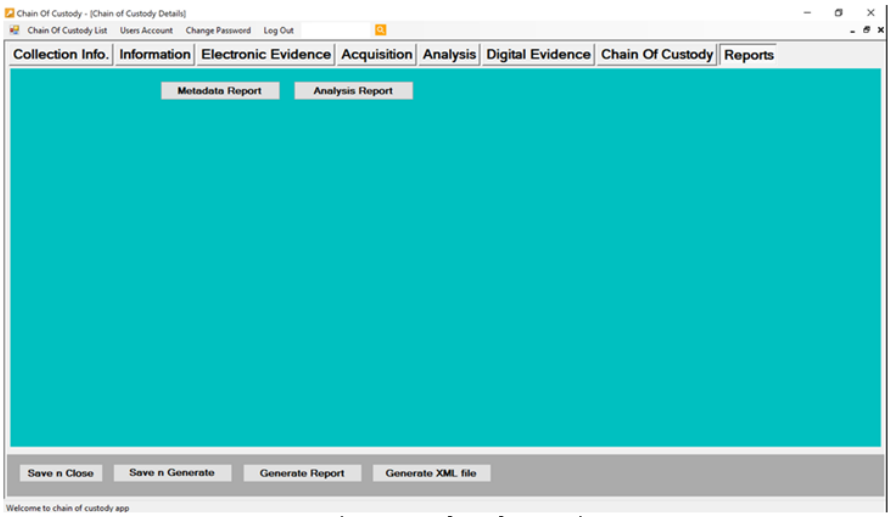
| id | Extention | MP5hash | SHA256 |
|---|---|---|---|
| 1020 | .JPG | 030252ea0b2a4816084229a8dd660ff6 | 5febb065824ed2dca03dd86b726a953032ffc6c43acc0b51754579 |

MP5hash:030252ea0b2a4816084229a8dd660ff6
SHA256:5febb065824ed2dca03dd86b726a953032ffc6c43acc0b
LastAccessTime:10-Mar-2020 12:00:00
Length:2361424
OwnerPC:Everyone
ItemFolderNameDisplay:ChainOfCustody
ItemTypeText:JPG File
ItemNameDisplay:IMG-2237.JPG
Size:2361424
FileAttributes:32
DateModified:2019-11-07 11:15:56 AM
DateCreated:2019-11-07 11:13:52 AM

Langitude 25.1482583055556 Latitude 73.58117775

Figure 4: Interface of acquisition tab

After all information are input, the application produces a function that create general report in pdf format. Also, these is another report for analysis and metadata reports are found in report tab as shown in Fig. 5.



Welcome to chain of custody app

Figure 5: Interface of report tab

[1] The information is provided from Iraq directorate database\ planning department.
[2] https://floridadep.gov/waste/petroleum-restoration/forms/equipment-chain-custody-form.
[3] https://alphalab.com/index.php/support-services/chain-of-custody-forms.

## VI. Digital Evidence Integrity and Authenticity Techniques

In chain of custody application there are four Methods or techniques are used to keep the integrity of evidence:

1) **Watermarking:** There are many techniques that can be used to protect image copyrighted content and prevent people from make any modification on it. One of them is watermarking. So, in this paper Iraqi interior logo will be embedded for each evidence (image) In COC application using C$^\sharp$ as shown in block diagram, Fig. 6.
2) **Extract Metadata:** The second way using evidence metadata, in metadata. It has (Title and description, Tags and categories, who created and when, who last modified and when, who can access or update) . Then the evidence is checked whether it modified of not and which program has been used as shown in Fig. 7. The input image was modified using a photoshop program, so after extracting metadata info, it shows the name program and date of modification.
3) **Extensible Markup Language (XML) :** The third method to keep the integrity of evidence is using Extensible Markup Language (XML) . So that XML is used for saving each evidence information with hash value in order to find if the file has tampered or deleted. XML file in COC application will be created after save case as shown in Fig. 7. Each file has ID number in both XML file and chain of custody tab, so that the admin can know by any modification or changes occur by comparing the two results as shown in Fig. 8. After deleting any evidence from

the Application, XML file will remove the ID number (1010) from XML file, thus the admin knows that the digital evidence was removed from the application, as shown in Fig. 9.

4) **Barcode:** Applying a barcode for each case using case No. and show it on the extracted report.

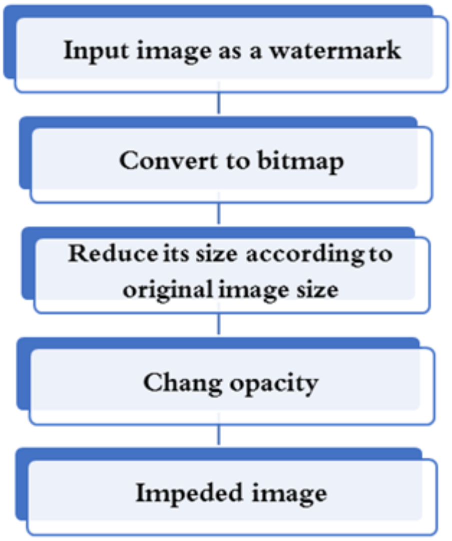
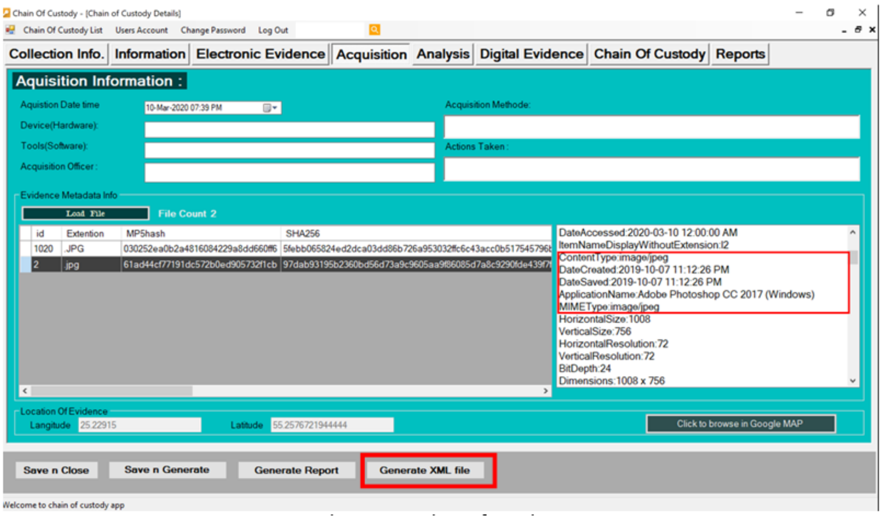

Input image as a watermark
Convert to bitmap
Reduce its size according to original image size
Chang opacity
Impeded image

Figure 6: Flowchart of digital watermark



Aquistion Date time: 10-Mar-2020 07:39 PM
Device(Hardware):
Tools(Software):
Acquisition Officer :
Acquisition Methode:
Actions Taken :

Evidence Metadata Info

File Count 2

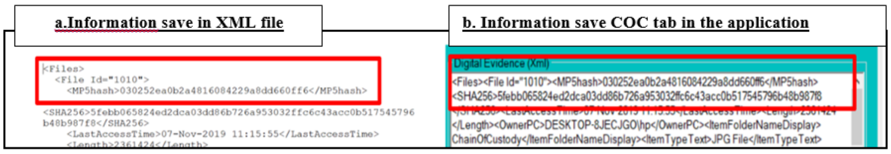
| id | Extention | MP5hash | SHA256 |
|---|---|---|---|
| 1020 | .JPG | 030252ea0b2a4816084229a8dd660ff6 | 5febb065824ed2dca03dd86b726a953032ffc6c43acc0b517545796b |
| 2 | .jpg | 61ad44cf77191dc572b0ed905732f1cb | 97dab93195b2360bd56d73a9c9605aa9f86085d7a8c9290fde439f7 |

DateAccessed:2020-03-10 12:00:00 AM
ItemNameDisplayWithoutExtension:I2
ContentType:image/jpeg
DateCreated:2019-10-07 11:12:26 PM
DateSaved:2019-10-07 11:12:26 PM
ApplicationName:Adobe Photoshop CC 2017 (Windows)
MIMEType:image/jpeg
HorizontalSize:1008
VerticalSize:756
HorizontalResolution:72
VerticalResolution:72
BitDepth:24
Dimensions:1008 x 756

Location Of Evidence
Langitude 25.22915
Latitude 55.2576721944444

Welcome to chain of custody app

Figure 7: Metadata information



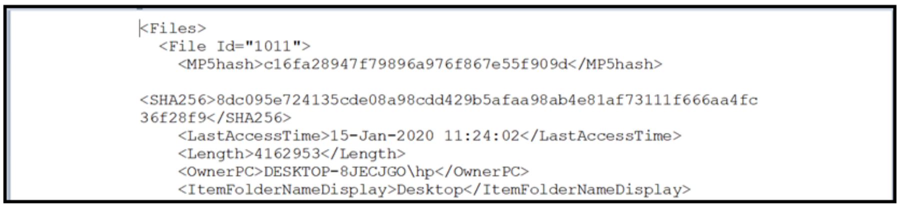
**a.Information save in XML file**

```
<Files>
  <File Id="1010">
    <MP5hash>030252ea0b2a4816084229a8dd660ff6</MP5hash>
<SHA256>5febb065824ed2dca03dd86b726a953032ffc6c43acc0b517545796
b48b987f8</SHA256>
    <LastAccessTime>07-Nov-2019 11:15:55</LastAccessTime>
    <Length>2361424</Length>
```

**b. Information save COC tab in the application**

```
<Files><File Id="1010"><MP5hash>030252ea0b2a4816084229a8dd660ff6</MP5hash>
<SHA256>5febb065824ed2dca03dd86b726a953032ffc6c43acc0b517545796b48b987f8
</SHA256><LastAccessTime>07-Nov-2019 11:15:55</LastAccessTime><Length>2361424
</Length><OwnerPC>DESKTOP-8JECJGO\hp</OwnerPC><ItemFolderNameDisplay>
ChainOfCustody</ItemFolderNameDisplay><ItemTypeText>JPG File</ItemTypeText>
```

Figure 8: a- XML file information, b- COC tab information



```
<Files>
  <File Id="1011">
    <MP5hash>c16fa28947f79896a976f867e55f909d</MP5hash>

<SHA256>8dc095e724135cde08a98cdd429b5afaa98ab4e81af73111f666aa4fc
36f28f9</SHA256>
    <LastAccessTime>15-Jan-2020 11:24:02</LastAccessTime>
    <Length>4162953</Length>
    <OwnerPC>DESKTOP-8JECJGO\hp</OwnerPC>
    <ItemFolderNameDisplay>Desktop</ItemFolderNameDisplay>
```

Figure 9: XML file with new ID number

## VII. Conclusions and Future Work

Chain of custody for the republic of Iraq is one of the proposed solutions for document and keep the integrity and authenticity of digital evidence. Different techniques are used to keep the integrity of digital evidence while SQL and XML approach is used as a tool for store all case information and Hash value of the save files. The application automatically extracts the Metadata for each digital file. Experiments are made for some of the digital evidence files using real case scenarios. According to the results get from the application, the chain of custody application can be used to document the chain of custody information of DE file quite well. In addition, this application displays the geolocation of digital evidence and applies a watermark for store images. Finally, in order to ensure its printed report not forged, the application generates a barcode for each case. For future work adding the Arabic language and develop the application to be a mobile application on both (android and OS) . And add more features that help the investigator in cyber- crime directorate.

## References

[1] Prayudi, Y. and A. Sn, "Digital Chain of Custody: State of the Art" , International Journal of Computer Applications, 2015, 114(5) .

[2] Giova, G, "Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems" , International Journal of Computer Science and Network Security, 2011, 11(1) : pp. 1- 9.

[3] Rubsamen, T, T. Pulls, and C. Reich, "Secure Evidence Collection and Storage for Cloud Accountability Audits" , in CLOSER, 2015.

[4] Varol, A. and Y. U. Sonmez, "Review of Evidence Collection and Protection Phases in Digital Forensics Process" , International Journal of Information Security Science, 2017, 6(4): pp. 39- 46.

[5] Cosic, J, "Formal Acceptability of Digital Evidence" , in Multimedia Forensics and Security, 2017, Springer, pp. 327- 348.

[6] Abbas, T. M. J, "Adoption of Chain of Custody Improves Digital Forensic Investigation Process" , Iraqi Journal of Information and communication technology, 2018, 1(2) : pp. 12- 21.

[7] Prayudi, Y, A. Ashari, and T. K. Priyambodo, "A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia" , International Journal of Computer Network and Information Security, 2015, 7(11) : pp. 1.

[8] Sample, R. B. and E. Quilter, "Chain of Custody Forms and Methods" , 2019, Google Patents.

[9] Salminen, A. and F. Tompa, "Why Use XML ?" , in Communicating with XML, 2011, Springer, pp. 69- 91.

[10] Wahyudi, E, I. Riadi, and Y. Prayudi, "Virtual Machine Forensic Analysis And Recovery Method For Recovery And Analysis Digital Evidence" , International Journal of Computer Science and Information Security, 2018.

[11] Du, X. and M. Scanlon, "Methodology for the Automated Metadata- Based Classification of Incriminating Digital Forensic Artefacts" , in Proceedings of the 14th International Conference on Availability, Reliability and Security, 2019.

[12] Lone, A. H and R. N Mir, "Forensic- Chain: Blockchain Based Digital Forensics Chain of Custody with Poc in Hyperledger Composer" , Digital Investigation, 2019, 28: pp. 44- 55.

[13] Prayudi, Y, A. Ashari, and T. K. Priyambodo, "Digital Evidence Cabinets: A Proposed Framework for Handling Digital Chain of Custody" , International Journal of Computer Applications, 2014, 107( 9) .

[14] Cosic, J. and M. Baca, "A Framework to (Im) Prove Chain of Custody in Digital Investigation Process" , in Central European Conference on Information and Intelligent Systems, 2010, Faculty of Organization and Informatics Varazdin.

[15] Cosic, J, Z. Cosic, and M. Baca, "An Ontological Approach to Study and Manage Digital Chain of Custody of Digital Evidence" , Journal of Information and Organizational Sciences, 2011, 35(1) : pp. 1- 13.

[16] Y. Prayudi, A. L, A. Munasir, R. Pratama, and K. Kunci, "An Ontological Approach for Representing Body of Knowledge of Digital Chain of Custody ( In Indonesian Language) ", Cybermatika, 2014, 2: pp. 36- 43.

[17] Hosmer, C, "Digital Evidence Bag" , Communications of the ACM, 2006, 49(2) : pp. 69- 70.

[18] Ratnasari, D, Y. Prayudi, and B. Sugiantoro, "XML Approach for the Solution of Chain of Custody of Digital Evidence" , International Journal of Computer Applications, 2018, 179(23) : pp. 0975- 8887.