Meta Data as a Part of Digital Forensic Investigation

Premal C. Patel[1] Dr. B.K. Sharma[2]
[1]Research Scholar (Ph.D.) [2]HOD
[1]Rai University, Ahmedabad, Gujarat [2]R.B. Institute of Management Studies, Ahmedabad, Gujarat

Abstract— Digital forensic Investigation is a big challenge in current Era. Mostly digital forensic process is associated with their proprietary tools and techniques. All tools collect digital information from system as per their pre-define commands and processes. Finding the evidence from all collected information is a challenge for investigator. This paper describes the role of metadata in digital forensic investigation. The Meta Data can be useful to minimize time and storage in the digital forensic investigation process. Role of Meta Data in investigation is important to identify the suspicious System.

Key words: Metadata, XML, Forensics, Dfxml, Investigation, Evidance.

I. Introduction

In the Growing phase of digitalization of data and file types are increased day by day. Therefore, investigation process takes more time and resources to analyze digital devices. It is also a very tedious task to back up all data of different computer system in order to find suspicious computer. Even more back up storage devices also needed to archive data. This will lead to complex digital investigation for investigators. More resources are needed to solve digital crime. In order to save resources to investigate a digital crime there is a need of different technique that will reduce usage of resources.

II. Metadata

Metadata means data about data.[1] There are so many metadata which performs important role in digital forensic investigation. It should be structured enough to be analyzed. Metadata always appears in textual format. In order analyze and store in structured is also a challenge for digital investigator. Because of heterogeneous environment of digital media. Using XML is a best choice to store digital information in structured format. User defined tags can be made in XML to represent digital information.

III. Importance of Metadata in Digital Forensics

Metadata provides information of file and directory properties which is useful to find suspicious system[2]. It also provides behavior and attributes with value. Digital investigator need data back up to investigate digital crime. Another way to solve digital crime is to fetch only digital forensic information (Metadata) in place of data. Enough Digital forensic information needed to solve digital crime. Thus, Digital forensic investigators need only digital forensic information that can prove suspicious computer. Task is to fetch digital forensic information of data instead of data. Information related to any data whether it is a larger or smaller requires less storage amount compared to data. Properties related to any data would be stored in some specific format XML. So, there is a need to create a structure which has enough capacity to store digital forensic information. There are some tags created using XML which can store digital information and proved to be committed crime or suspicious computer. DFXML is also providing facility to store Metadata in XML Structure Format. DFXML allows the sharing of structured information between independent tools and organizations.[3] In XML Structure all metadata can be stored in particular tag. Each tag should be stored in particular object and every object should be stored in particular file with specific format.

IV. User Defined Tags of XML

File Object to store file Metadata[4]

– <fileInformation>:- Specifies information of particular file
– <fileobject>:- Includes all Objects of file
– <filename>:- Provide File name Object
– <location>:- Provide File Location Object
– <filesize>:- Provide File Size Object
– <Obtype>:- Folder(Directory)/File
– <shared>:- True/False (To identify Whether file/directory is shared)
– <contains>:- Provide contains Whether contains subdirectories or files, If contains then specifies no of subdirectories and files
– <nooffiles>:- Provide Number of files Included in Folder
– <noofdirectory>:- Provide Number of Directory Included in Folder
– <signature>:- Provide File Signature to identify nature of file.
– <created> :- Created date and time to identify when File is created
– <modified> :- Modified date and time to identify when has been modified
– <accessed>:- Accessed date and time to identify when file is accessed
– <attribute>:- Specifies attributes of file to identify mode of file
– <readonly>:- read only attribute identify whether file is in read only mode or not (return true/false)
– <hidden>:- Attribute identify whether file hidden or not
– <encrypted>:- Attribute identify whether file encrypted or not.
– <readytoarchive>:- Attribute identify whether file is ready to archive mode or not
– <revisionno>:- No. of times file has been modified and saved to identify that how many time file has been modified
– <hashdigest type='MD5'>:- Footprint of file using algorithms of md5

V. Flow of Information Storage Structure

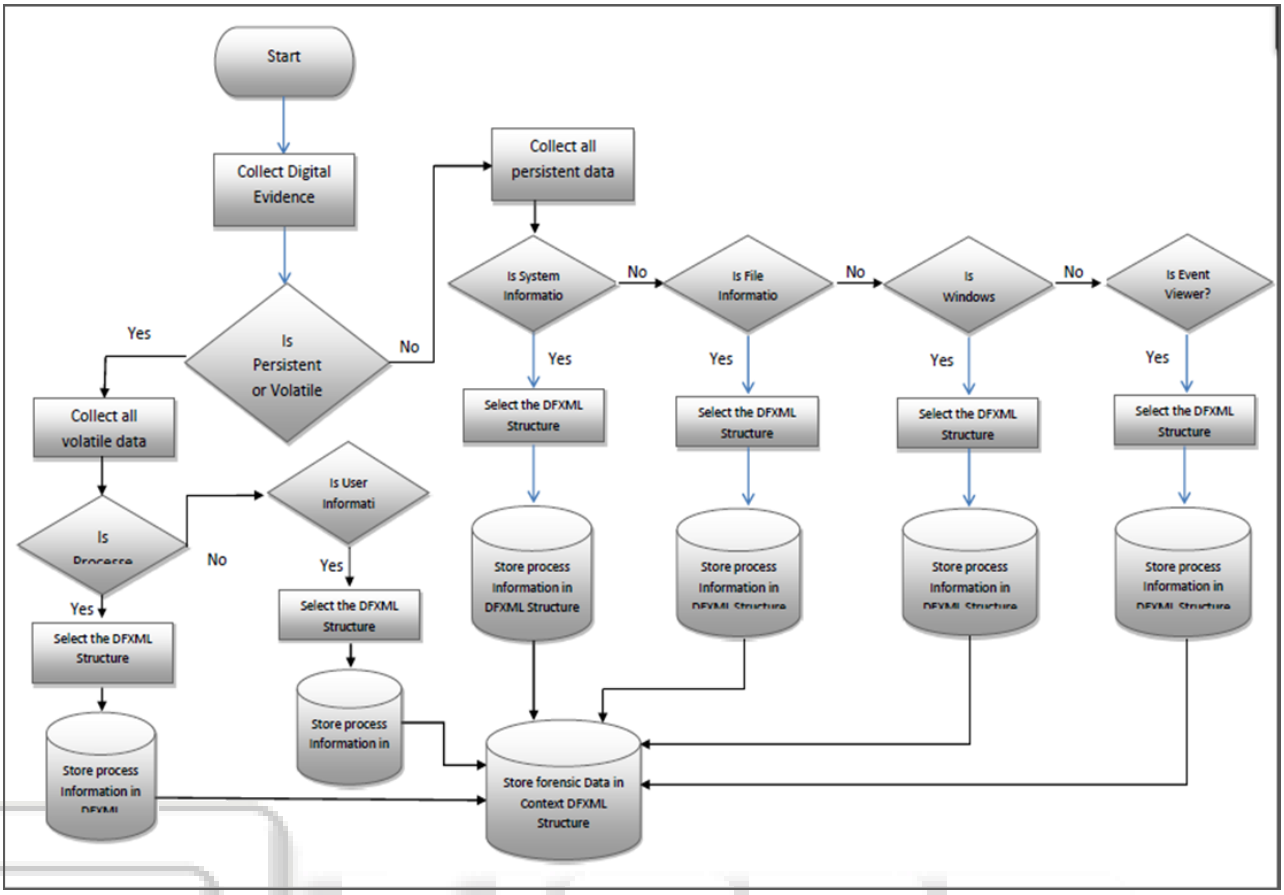

Start
Collect Digital Evidence
Is Persistent or Volatile
Yes
No
Collect all volatile data
Is Process
No
Yes
Select the DFXML Structure
Store process Information in DFXML
Is User Informati
Yes
Select the DFXML Structure
Store process Information in
Collect all persistent data
Is System Informatio
No
Yes
Select the DFXML Structure
Store process Information in DFXML Structure
Is File Informatio
No
Yes
Select the DFXML Structure
Store process Information in DFXML Structure
Is Windows
No
Yes
Select the DFXML Structure
Store process Information in DFXML Structure
Is Event Viewer?
Yes
Select the DFXML Structure
Store process Information in DFXML Structure
Store forensic Data in Context DFXML Structure

Fig. 1: Flowchart Digital Information Storage Structure

Figure-1 is defining the Flow for all metadata can be stored in particular category wise on based of its object. In this flowchart we can categorize all information so it can easily examine on base of investigation requirements.

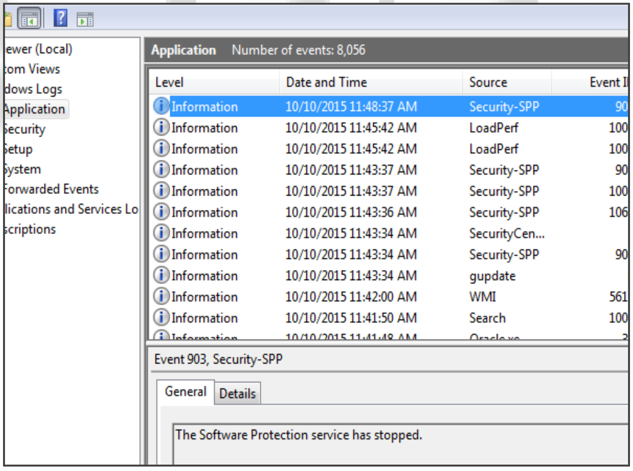
Windows Registry is very important for Digital investigation. First the structure of Windows Registry was analyzed, then elements within the Windows Registry that may be of evidential so it must be store in proper structured manner. XML format is well known for aggregation of the data and Metadata. It helps making the forensic data investigation easy by preserving the integrity of data and also by making it interoperable with other tools and applications.[5]

A. *From Registry we can identify:*

Attached devices from registry path
-HKLM\SYSTEM\ControlSet00x\Enum\USBSTOR
Mounted Devices from
-HKLM\SYSTEM\MountedDevices
URLs which are typed by user in IE from
-HKCU\Software\Microsoft\ Internet Explorer\TypedURLs

It is important for computer forensic experts to understand the complexity of the Windows Registry. The information and potential evidence that reside in the Registry make it a significant forensic resource; uncovering this data can be crucial to any computer related investigation.[6]

Windows provides Event Viewer and Microsoft Management Console to review the events from Windows event logs. It allows for filtering the events based on various fields such as event ID, user ID, and time period.


ewer (Local)
om Views
dows Logs
Application
Security
Setup
System
Forwarded Events
lications and Services Lo
scriptions

Application Number of events: 8,056

Level	Date and Time	Source	Event I
Information	10/10/2015 11:48:37 AM	Security-SPP	90
Information	10/10/2015 11:45:42 AM	LoadPerf	100
Information	10/10/2015 11:45:42 AM	LoadPerf	100
Information	10/10/2015 11:43:37 AM	Security-SPP	90
Information	10/10/2015 11:43:37 AM	Security-SPP	100
Information	10/10/2015 11:43:36 AM	Security-SPP	106
Information	10/10/2015 11:43:34 AM	SecurityCen...	
Information	10/10/2015 11:43:34 AM	Security-SPP	90
Information	10/10/2015 11:43:34 AM	gupdate	
Information	10/10/2015 11:42:00 AM	WMI	561
Information	10/10/2015 11:41:50 AM	Search	100
Information	10/10/2015 11:41:48 AM	Oracle.vs	3

Event 903, Security-SPP

General Details

The Software Protection service has stopped.

Fig. 2: Event Viewer logs

Windows event logs in serving as digital forensics evidence that could be accepted in the court of law[7]

Windows logs contain five separate logs (Application, Security, System, Setup, and ForwardedEvents). Event logs and information also can be stored in the XML format to examine at any platform with its consistent state.

Windows event log contain references to messages and other important information that is pulled from .dll files and other sources when the system is running and the event log is viewed.

B. *Event Object to store Event Log Information:*

- <Event>:- describe information of event viewer object start

- <EventID>:- describe event ID
- <Ename>:- describe Event provider name
- <Execution_ProcessID="548" ThreadID="5056" />:- process ID and Thread ID of executing event
- <Channel>:- describe main category of path hierarchy
- <Computer>:- define System name
- <username>:- describe user for correlated event
- <EDate_time>:- describe date and time for that event
- <source>:- describe source user for that event
- <level>:- describe type of event – error, information, warning
- <process_id>:- process id for event
- <key_words>:- status of event -- audit success, audit failure, classic
- <task_category>:- describe type of task -- logon , general, special logon

These are the basic user define tags to store the information of event viewer in xml format. Event is an object of all metadata of event information which store and make separate each logs details.

In the digital forensic investigation volatile information is also very essential as well as persistence information. Task manager is a key resource to acquire volatile information. Information about each running process, such as create times, exit times, open files, executing code, and child process are stored in main memory. This type of evidence is useful if a malicious program is running or another program has been corrupted on a live system. Unlike the non-volatile memory, this evidence cannot be erased from memory as long as malicious code is running.[8]

C. Process Object to store Process Information in XML:

- <process>:- Define Process Object Starts
- <pid>:- Specifies Process ID
- <ppid>:- Specifies parent Process ID
- <pname>:- Specifies name of process
- <description>:- Describes the process details
- <status>:- describe status of process – stop, running, blocked
- <memory-usage>:- Memory usage of specified process

These are the tags which are identified with their role to store volatile information about processes.

All above XML tags from each object are used to collect Metadata from system and to store in particular approach. All objects are collection of their details information and the properties of file or directory.

VI. Conclusion

The Role of Metadata in digital forensic defines their importance which is useful to find suspicious system to commit the crime or malicious activity. By examine the Metadata we can save time and storage in process of Digital forensic Investigation. Another advantage of metadata that it can be examine at any platform. Digital forensic information should be store in specific format so collection of all metadata can be archive in single file for investigation. It can be preserve integrity and consistency by creating hash value of evidence file.

Acknowledgment

I would like to express my heartily thankfulness towards my guide Dr. B.K. Sharma for this guidance on various aspects of this document and his support on the progress of my work. I appreciate the thoughtful contributions that he has made to my efforts. It has been a great privilege to work under him. With his guidance and persistent help this research becomes possible. also be very thankful to my all family members to afford their important times. Lastly I would also like to give a special thanks to my friends, colleagues and Parents for playing an important role in strengthening my approaches in this work.

References

[1] www.en.wikipedia.org/wiki/Metadata

[2] Pritam Dash ,"Fast Processing of Large (Big) Forensics Data" Indian Academy of Sciences Summer Research Fellowship Program - 2014

[3] Simson Garfinkel, "Digital Forensics XML and the DFXML Toolset", Naval Postgraduate School, 900 N. Glebe, Arlington, VA 22203

[4] P.C.Patel, E.P.Panchal, J.R.Patel, "An Approach for Interoperability of Forensic Data between Forensic Tools" 2nd International Conference CSCIT2015 PaperID CSCIT166-2015.

[5] Premal C. Patel, "Design a Structure to Aggregate Windows Registry for Digital Forensics Investigation", E-Journal Nirupan.

[6] Derrick J. Farmer, "A Windows Registry Quick Reference: For the Everyday Examiner"

[7] Nurdeen M. Ibrahim & A. "Sufficiency of Windows Event log as Evidence in Digital Forensics", University of East London School of Computing, IT and Engineering, UK

[8] E.P.Panchal," Extraction of Persistence and Volatile Forensics Evidences from Computer System", (IJCTT) - volume4 Issue5–May 2013