Identifying Metadata Elements in Computer Forensics in Malaysia

Alwi Mohd Yunus, Nor Sakila Asnawi, Irwan Kamaruddin Abdul Kadir

Faculty of Information Management,
Universiti Teknologi MARA (UiTM),
Malaysia

Email: alwiyunus@uitm.edu.my, ila93syakila@gmail.com

Received Date: 27 December 2020
Publish Date: 1 April 2021

Abstract. Computer forensics is a scientific investigation and analysis technique toward crimes in computing environment. Different set of skills and methods are needed in conducting computer forensics investigation process. Metadata is one of the requirements in computer forensics investigation. This study attempts to gain greater understanding on the use of metadata elements in computer forensics investigation especially in Malaysia. Metadata elements are required to extract information from the evidence without delaying any important information. Therefore, to give impact on the acceptance of electronic evidence in the court of law. Through qualitative method, face-to-face interview was conducted with two agencies responsible in computer forensics investigation namely; the CyberSecurity Malaysia and the Royal Police Malaysia (RPM). An analysis was done manually after the interviews were conducted. Based on the interviews and analysis, the study found that both agencies agreed on the importance of the right metadata elements needed in computer forensics investigation. This paper is written to give overall view of the study.

Keywords: Computer Forensics, Metadata Elements, Computer Forensics Investigation Process, Acceptance Evidence, CyberSecurity Malaysia & Royal Police Malaysia (RPM).

1 Introduction

The emergence of technology has led to the appearance and significance of computer forensics. History of Information (2017) mentioned that metadata term was coined by Philip Bagley who is an American computer scientist in November 1968, he defines metadata as “data about the containers of data”. From there on,there are quite a number of studies focusing on metadata particularly in the process of extracting important data and information. Computer forensics according to Wiles (2007) is about what happened to the past by abstract and analyse these data onto systems or can also be explained as a scientific investigation that is performed by using the computer (Muhammad Zulkifly, 2018). This was also mentioned by Mohd Sharulazam (2018) by stating computer forensics is related to scientific examination and analysis that have potential in identifying evidence for trial in court. Fundamentally, computer forensics is about respond to the incident (Wan Abdul Malek, 2018) which agreed by Muhammad Zulkifly (2018) that believe computer forensics is a scientific investigation that only respond after incidents happens.

Computer forensics is always related to metadata as it is a basic requirement as in any computer applications. Having proper set of metadata can strengthen the evidence gain from the process of computer forensics. Mohd Sharulazam (2018) explained that metadata function is to lead investigation where through metadata, it helps forensics investigator to gain more insight of the data. Metadata is like a birth certificate for any data or evidence. It is very important and should be the first place to look at in computer forensics investigation. (Muhammad Zulkifly, 2018).

Currently metadata is extremely significant due to the increasing number of cases related to computer crimes. According to one of the leading institution in computer forensics in Malaysia, CyberSecurity Malaysia, there are quite a numbers of cases from online soccer gambling, high profile cases and political cases require their experience and expertise specifically in identifying the metadata from the forensics investigation (Nurainolmardhiah Abdul Halim, 2015). CyberSecurity Malaysia also reported that in Malaysia there are more than 7900 cases require the involvement of computer forensics investigation.

Another enforcement agency which is the Royal Police Malaysia also reported that they are more than 3,000 cases with more than 14,000 exhibits by their forensics lab in the year of 2016 itself (Mohd Zaidi Abu Hassan, 2017). Due to the claimed statistics by the two agencies, it in undeniably the role of computer forensics in dealing with the metadata is crucial.

2 Understanding Metadata in Digital Forensics

It is an abstraction of data, it tells about other data, and it exists in computer system. It is basically a stamp created automatically and attached to a data object in a computer system. In record keeping system, according to Yunus, A. M., & Kadir, I. K. A. (2017), it is critical to verify and authenticate a digital record within the electronic records management environment and system, hence the use and application of record keeping metadata is critical for that purpose. Such process is known as data discovery process through computer forensics to understand the context and history of a digital documents or transactions or digital records, activities within a computer system and its application. It functions as;

1. Resource discovery
    1. Allowing resources to be found by relevant criteria;
    2. Identifying resources;
    3. Bringing similar resources together;
    4. Distinguishing dissimilar resources;

        5. Giving location information.
2. Organizing e-resources
    1. Organizing links to resources based on audience or topic.
    2. Building these pages dynamically from metadata stored in databases.
3. Facilitating interoperability
    1. Using defined metadata schemes, shared transfer protocols, and crosswalks between schemes, resources across the network can be searched more seamlessly.
        1. Cross-system search, e.g., using Z39.50 protocol;
        2. Metadata harvesting, e.g., OAI protocol.
4. Digital identification
    1. Elements for standard numbers, e.g., ISBN
    2. The location of a digital object may also be given using:
        a. a file name
        b. a URL
    3. some persistent identifiers, e.g., PURL (Persistent URL); DOI (Digital Object Identifier)
    4. Combined metadata to act as a set of identifying data, differentiating one object from another for validation purposes.
5. Archiving and preservation
    a. Challenges:
        i. Digital information is fragile and can be corrupted or altered;
        ii. It may become unusable as storage technologies change.
        iii. Metadata is key to ensuring that resources will survive and continue to be accessible into the future. Archiving and preservation require special elements:
            1. to track the lineage of a digital object,
            2. to detail its physical characteristics, and to document its behavior in order to emulate it in future technologies.

3 Metadata Elements

Metadata provides benefits in identifying useful information to the forensics investigator (Purohit, Hemrajani and Dave, 2011). Through the forensics investigation process, metadata can be identified and therefore will enable the original owner of the files to be tracked down. Since metadata itself is embedded in the computer system, its existence is generated by whatever done to the system. It just records everything occurred to the computer system provided that the metadata elements are first set up and embedded earlier in during system development or else withstanding metadata elements are universally available in any system installed in computer systems. Such is a generic metadata elements available in any system.

Metadata could help forensics investigator to find conclusion in investigation in a more efficient and effective way. It works in such a way in the back end processes in any computer system. It records everything as a complete audit trails information. In this case, metadata provides situational information which is who, how and when digital artefacts are created, modified or accessed at any given time by any users who logged into any computer system. This could help in identifying the truth in investigation process. (Raghavan, 2014).

The findings of the study conclude the importance of metadata elements in computer forensics investigation process. Both of the agencies understudy believe that metadata elements are compulsory and needed in all cases. On top of the findings, the study also identified emerging metadata elements analysed from the interviews done with the two agencies. This is shown in Table 1:

Table 1. Emerging Elements of Metadata

Emerging Elements of Metadata	Description
Agency 1: 1. System Version 2. Model & Serial Number 3. Storage	*Description by Informant 1:* To identify OS version used in computer forensics To differentiate model & serial number that used for exhibits. To identify capacity of computer for easier the documentation of investigation
Agency 2: 1. Geo-Location 2. Equipment 3. Software Version	*Description by Informant 2:* To provide coordinate of information To identify model, version, and software used based on type of digital equipment. To provide information related to software used.

The table shows that metadata elements are used widely in verifying information contains in evidence cases. The emerging metadata elements will ensure reliability and admissibility of evidence found in the process of the forensics investigation.

4 How Metadata Works in Computer Forensics Investigation Process?

Duryana, (2014) stated that, process of analysis of the evidence becomes more challenging in producing reliable evidence. There are also cases dismissed from court due to analytical gap between the data and the opinion (Garrie, 2014).

One of the forensic agency in Malaysia explains that there are five (5) stages of investigation that need to be taken throughout any forensics investigation. It started with identification, preservation, collection, analysis and presentation. Every process in each of the stage, metadata will be analysed. Identification stage is when the information is collected and preserved. After the exhibit is identified, all digital goods will go through the process of preservation which is by making identical copy. All materials are analyzed by the help of metadata. Forensics tools like Encase, Axiom Magnet, FTK Imager and others will also be used. The functions of verifying information are to extract the digital evidence and, the presentation will focus on the report made by the experts. All cases may not be presented in court, since it depends in the nature of the cases. However, all information gained from the forensics investigation process still need to be delivered and reported (Mohd Sharulazam, 2018).

Another enforcement agency in Malaysia believes that investigation process started from the acceptance of data or evidence cases. Next all evidence cases that are accepted will be registered. Then, the process of imaging which is cloning the data will be done before the process of analysis which is focusing on the metadata. Some tools are used in analyzing the evidence such as Encase, FTK, IAF. After the process of analysis is conducted the agency will make a report and presented in the court as part of evidence (Muhammad Zulkifly, 2018).

Even though both of the agencies have different way of investigation, the purpose is still the same which is to conduct and respond to the incident in a proper way of investigation. Metadata will give a significant impact on the success of investigation.

Preserving the metadata derived from the process of investigation is compulsory because of its delicate and complex nature. Both agencies emphasise that preservation is important in computer forensics investigation process and, the study also found that both agencies used similar process of preservation which is called as “imaging” process or clone. This is to avoid any issues in future (Muhammad Zulkifly, 2018). Moreover, both agencies follow ASCLD or currently known as American Society Lab Laboratory Directory (ANAB). According to Mohd Sharulazam, (2018), ASCLD is an expert in forensics laboratory and is an institution that is also responsible in auditing the forensics investigation process. Even though there are guideline that they need to adhere to, the forensics investigator is required to be creative in handling cases. This is to allow productive results in computer forensics investigation process (Muhammad Zulkifly, 2018).

5 Conclusion

Metadata elements are undeniably critical and important in computer forensics investigation. Both of the agencies were chosen in the study due to their qualification and the number of experts and certifications in computer forensics investigation. It can be concluded that, without the right metadata elements, it is really difficult, challenging for teams of investigators in finding and verifying evidence in such an investigation process and really a tedious tasks and great challenge in computer crimes environment, particularly in the digital age. Having a metadata as critical aspect in digital crime investigation, helps a lot to team investigators as it facilitates the process systematically and efficiently. A such, the investigation process could be done thoroughly according to specific legal requirement within a stipulated laws and Acts. It will also ensure the evidences produced is acceptable, verifiable, in the court of law. It is hopeful that in the future there will be more research on metadata and computer forensics.

References

Duryana Mohamed & Zulfakar Ramlee. (2014). Cases of electronic evidence in Malaysian courts: The civil and syariah perspective. *ICSSR e-Journal of Social Science Research, 1* (2), pp. 1-10.

History of Information (2017). *Philip Bagley Coins the Term "Metadata".* Retrieved on 22 Oct, 2017, from http://www.historyofinformation.com/expanded.php?id=4241 Interna tional Records Management Trust. (2016). Managing metadata to protect the *integrity of records .pp 1-100.*

Kadir, I. K. A., & Yunus, A. M. (2017). Development of a Generic Model for the Preservatio of Primary Research Data Based Digital Resources Life Cycle. *International Journal of Aca demic Research in Business and Social Sciences*, *7*(11), 39-62.

(Mohd Zaidi Abu Hassan, personal communication, November 29, 2017).

NISO. (2004). *Understanding Metadata*. Bethesda, MD: NISO Press, pp.1-2.

Nurainolmardhiah Abdul Halim, Ginsim, S., & Siti Khadijah Baharuddin (2015*). Case studies: Admissibility of digital records as legal evidence in Malaysia.* National Archives of Malaysia. pp 1-12. Retrieve on 19 Oct, 2017, from http://www.sarbica.org.my/images/stories/doc/SeminarOnElectronicRecords-KL2015/papercase%20studies%20admissibility%20of%20digital%20records %20as %20legal%20evidence%20in%20malaysia.pdf\

Purohit, A. K., Hemrajani,. N., & Dave, R. (2011). Role of metadata in cyber forensic and sta tus of Indian cyber law. *Comp. Tech. Appl, 2*(5), pp. 1582-1588.

Raghavan, S. (2014). *A framework for identifying associations in digital evidence using metadata* (Doctoral dissertation).School of Electrical Engineering and Computer Science, Science & Engineering Faculty, Queensland University of Technology, Brisbane.

Wiles, J. (2007). *Techno security's guide to e-discovery and digital forensics.* pp 1-405. Bur lington, MA: Syngress Publishing.

(Wan Abdul Malek Wan Abdullah, Senior Lecturer, *Computer Forensics,* 2018).

Yunus, A. M., & Kadir, I. K. A. (2017). Managing the Preservation of Records for Digital Primary Data: A Case of Malaysia Institution. *International Journal of Academic Research in Business and Social Sciences*, *7*(11), 102-126.

Gartner, Richard. 2016. *Metadata: Shaping Knowledge from Antiquity to the Semantic Web*. Springer. ISBN 9783319408910.