symmetry

MDPI

Article

An Ontology Based on the Timeline of Log2timeline and Psort Using Abstraction Approach in Digital Forensics

Sandeepak Bhandari * and Vacius Jusas

Software Engineering Department, Kaunas University of Technology, Studentu St. 50, LT-51368 Kaunas, Lithuania; vacius.jusas@ktu.lt
* Correspondence: Sandeepak525@gmail.com

Received: 17 March 2020; Accepted: 7 April 2020; Published: 17 April 2020

Abstract: Digital forensics practitioners encounter numerous new terminologies during time-intensive digital investigation processes because of the explosive growth of the web, an immense amount of data, and rapid changes in technology. In such a scenario, the time needed to find and interpret the cause of the potential digital incident can be affected by the complexity involved in understanding the meaning of newly encountered terminologies. Although various approaches have been designed to assist digital practitioners in understanding the newly encountered terminologies during the investigation of the accident, none of them is capable of supporting investigators to interpret new terminologies. Our work focuses on reconstructing and analyzing the timeline of events and artifacts backed by the abstraction concept to help practitioners in reasoning about the perceived meaning of different digital forensics terminologies that are encountered during the investigation. This paper introduces an ontological approach based on the abstraction concept to reconstruct the timeline provided by command-based digital forensic tools, i.e., Log2timeline and Psort in the L2TCSV format, and assist in resolving the meaning of new encountered concepts. The performed experiments show that the novel methodology is capable of enhancing the timeline and assisting practitioners in determining the significance of encountered terminologies or concepts.

Keywords: digital forensics; ontology; symmetry properties; timeline; abstraction; operating system; events and artifacts

1. Introduction

Digital forensics practitioners face regular challenges in keeping track of continuous innovations in technologies such as Windows, Android, and iPhone operating system based devices. Investigating these digital devices to attain meaningful information is a very time-consuming process because of the enormous amount of data, diversity of data, rapid innovation in technologies, and fast growth of the internet. Moreover, during digital forensics investigations process investigators detect various new terminologies. In such a scenario, the time needed to find and analyze the cause of a digital accident can be influenced by the complexity involved in determining the meaning of newly detected terminologies. The limitation exists in the digital forensics approaches that they cannot assist digital investigators in determining the meaning of distinct digital forensics terminologies or how these terminologies are perceived by individuals primarily when used in their domain of expertise. If digital forensics approaches are designed in such a way that they assist digital investigators in resolving the meaning of newly encountered terminologies during the investigation process, then the time needed to find and analyze the cause of the digital accident can be reduced extensively, and these are the objectives of our paper. To defined new terminologies in any particular domain, ontology is the appropriate approach.

Nowadays the development of an ontology, i.e., explicit formal specifications of the terms in the domain and association between these terms, has been moved from artificial-intelligence laboratories to the desktops of domain experts and become popular on the world-wide web which allows sharing and reusing of domain knowledge. This paper contains a summary of our novel abstraction based approach to reconstruct the timeline and to assist digital practitioners in understanding the timeline and attaining the evidence within the appropriate time. Firstly, the developed approach is implemented on different operating system based devices, namely Windows, Android, and iPhone, to show the capability of abstraction approach and demonstrate that it can be implemented on distinct operating systems. Secondly, during the reconstruction of timeline backed by the abstraction concept of these three operating system based devices, distinct terminologies are detected. For this, a novel ontological approach is developed.

This paper consists of five sections where Section 2 presents a review of literature studies. Section 3 presents the developed approach and novel ontology for this research. Section 4 discusses the implementation and results by implementing a novel methodology and ontology. Lastly, we discuss conclusions in Section 5.

2. Literature Review

The term ontology has its origins in metaphysics and philosophical sciences. Aristotle first defined ontology as a philosophical discipline that examines existence or being [1]. The ontology explains the nature and principle attributes and association among all beings. Ontology is based on facts and, its nature being independent of one's background, shows understanding, perspective, and knowledge of the world [2]. First, artificial intelligence researchers used the ontology approach from philosophy, as shown in Figure 1 [3]. Since then, the concept of ontology has been used by scientists from information and computer fields.

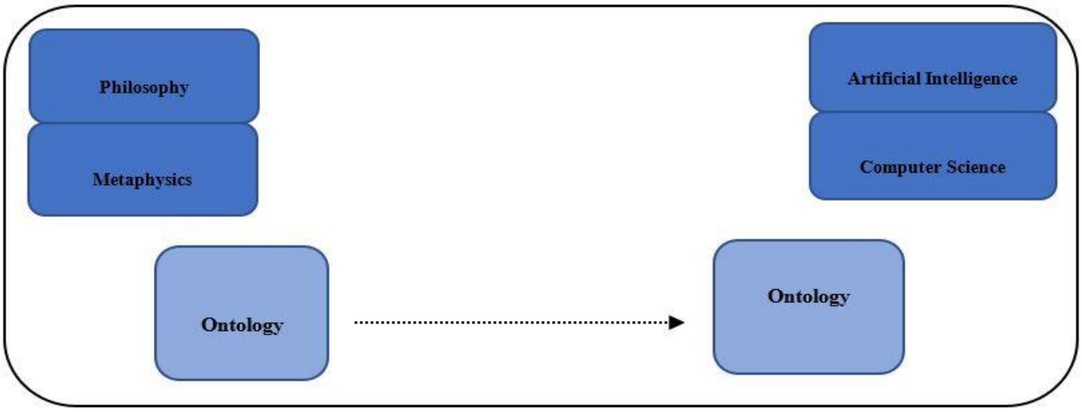


Figure 1. The shift of ontology to the computer science field.

Generally, a group of researchers who want to share information in a particular domain develop an ontology. There are numerous reasons [4] for developing an ontology, including common understanding, reusing, sharing, analyzing of the domain knowledge, separation of domain knowledge from operational knowledge, and making domain assumptions explicitly. A distinct explanation of ontology is available in the computer and information science literature. However, all researchers agree on the importance of ontology in the representation, sharing, and reuse of existing domain knowledge [5]. The most common definition of ontology among researchers is the following [6]: "A body of formally represented knowledge is based on conceptualization. A conceptualization is an abstract, simplified view of the world that we wish to represent for some purpose. Every knowledge base, knowledge-based system, or knowledge-level agent is committed to some conceptualization, explicitly or implicitly. An ontology is an explicit specification of a conceptualization." In the digital forensics domain, it is not viable to develop an ontology that would be sufficiently "large" to contain all the concepts that occur, and which are of interest to people who conduct forensics investigations [7,8]. An ontological representation of the collected data can solve the problem of diversity of data in digital forensics [9,10].

In the paper [9], authors discuss the benefit of the semantic web in digital forensics. They propose a methodology based on the semantic web technologies that supports the digital practitioner to correlate and present information obtained from forensic data. According to the authors, this methodology can enhance the process of a digital investigation because of its automation and data integration properties, but it is only demonstrated theoretically.

Ashley Brinson et al. [11] stated that the area of cyber forensics is still in the outset with a solid requirement for direction and definition. For this purpose, the authors developed the cyber forensics ontology for identifying the exact layers for specialization, certification, and education within the cyber forensics domain. The ontological model split the topic of cyber forensics into two major subtopics, technology and profession. Subtopic technology is divided into hardware and software. The subtopics hardware and software are split further into large scale digital devices, small scale digital devices, computers, storage devices, obscure devices, and analysis tools, operating system, and file system, respectively.

The subtopic profession is split into law, academia, military, and private sector. The law section focuses on law enforcement, courts, and legal aspects of cyber forensics. Academia is split into research and education, while the military category focuses on what cyber forensics duties military personnel perform. The military section can be defensive and offensive. The private sector was divided into consulting and industry. The objective of creating this ontological model was to define the right levels of educations, certifications, and specializations. The limitation of this approach is that it does not consider and analyze the factors that influence the implementation of this ontological approach.

In the paper [12] the authors stated that digital forensics is a relatively new discipline with various technical and non-technical terminologies that can be hard to comprehend. The main problem addressed by the authors is that there is no approach in digital forensics that can help investigators in reasoning concerning the perceived meaning of different digital forensics terminologies encountered during a digital forensics investigation process. To solve this problem, the authors examined the concept of developing ontologies for digital forensics terminologies and proposed an ontological approach to resolve the meaning of different digital forensics terminologies. Moreover, the approach was only discussed theoretically and is a drawback of this paper. In the paper [13], the authors highlight the problems encountered by the digital practitioner during digital investigations to interpret digital evidence, primarily because of misinterpreting or false understanding of various vital concepts. An ontology of digital evidence was developed to figure out this problem. According to the authors, this ontology can be used to share a common understanding of the structure of this domain (digital forensics) between forensics investigators and other personnel that have to deal with digital evidence, among software agents and between forensics investigator and software. This ontology was only explained theoretically which is a limitation of the research.

In the paper [14], the authors stated that digital forensics investigators face a challenge such as the high volume of data, which are becoming continuously vast and diverse because of the growth of new technologies. Therefore, the interpretation of digital evidence and the reconstruction of events is a complicated and time-consuming task for the investigator. Moreover, the authors also identified seven vital factors that a reconstruction tool must have to handle these three challenges, namely volume, heterogeneity, and legal requirements. An approach to SADFC, i.e., Semantic Analysis of Digital Forensics Case, based on three layers of ontology, called ORD2I, is introduced to present any digital events. This ontology is related to a collection of tools for obtaining information from the sources of evidence, instantiating ontology, inferring new knowledge, and interpreting it. However, the performance of the approach still needs to improve. David Christopher Harrill and Richard P. Mislan [15] stated that Small Scale Digital Device Forensics (SSDDF) is a new area of study which needs direction. The devices and their corresponding forensics processes are not transparent. The objective of this paper was to design an ontological approach to provide law enforcement with the appropriate knowledge about the devices found in the SSDD domain. The limitation of this ontological approach is that it is not able to address both old-fashioned as well as the latest digital devices.

Kahvedzic and Kechadi [16] propose DIALOG, i.e., Digital Investigation Ontology, a model to encapsulate the knowledge related to digital investigation cases. DIALOG presents a dictionary of concepts and associations in the form of an ontology to define the semantics of cases. To define the four areas of the case, four sub-ontologies are defined, namely cybercrime type, types of data locations, type of data itself, and tools used to find that data. The purpose of the model is to describe properties and attributes of vital forensics ideas for better understanding by investigators. Authors demonstrated the implementation of DIALOG ontology by modeling the semantics of the knowledge associated with the Windows Registry. The major limitation is that the authors considered only a single-source, i.e., the registry, to annotate evidence and that is not sufficient to demonstrate the capability of the approach.

Heum Park et al. [17] developed Cyber Forensics Ontology for the cyber investigations in cyberspace. The authors classified Cybercrime into two classes—cyberterror and general cybercrime—and how these two classes are related. The analysis of cyberterror needs the latest technology, system environment, and experienced experts, and general cybercrime is related to a general crime by digital evidence. Authors described the concepts and associations between crime types, evidence collection, criminals, and crime case and law. The drawback of this approach is that it is least based on digital evidence and other stages that are essential to collect and interpret digital evidence in the digital investigation process. Only one stage, namely "collection" is mentioned by the authors. In the paper [18], the authors present an ontology-based network forensics knowledge representation approach. This ontology gives a formal description of the concepts defining the network forensics domain and describes the associations. The limitation of this approach is that it is not fully explained, and there is no means to have the source of information of the ontology. In the paper [19], the author highlights the importance of retrieval of evidence in digital forensics. For extraction of the evidence, the author proposed an ontology framework approach. This approach is based on the hierarchy of layers and contains two layers called analysis tools and operating system. The second layer is automatically developed to assist the practitioner in retrieving the evidence.

In the paper [20], the authors highlight the challenges faced by the digital evidence field such as volume and variety of data. Based on these challenges, they proposed the Digital Evidence Semantic Ontology (DESO). The proposed ontology is based on Gene Ontology and assists digital practitioners to cull evidence from the potential sources and compare them. In the paper [21], the authors stated that the big data produced by web services make the investigation process complicated and time-consuming. For this, the authors proposed an extensible standards-based semantic ontology for the representation of web service log data. The main aim of ontology is to extract hidden information and eventual scenarios of cyber-attacks in weblogs. Digital investigators can specify validation rules and execute them using a logical reasoner over the proposed ontology to get a forensic report. According to the authors, the proposed ontology can support the investigator in analyzing the task and minimize the required time.

In the paper [22], the authors highlight the concept of chain of custody of digital evidence and its importance in the digital forensic field. They also focus on factors that can affect the chain of custody of digital evidence such as who, when, where, why, and how during the various stages of the digital investigation process. The authors also defined taxonomy and used an ontological approach to maintain the chain of custody of digital evidence. The taxonomy was based on a top-down approach, i.e., the most specific concepts were first defined and specialized afterwards. In the paper [23], the authors stated that technology evolves at rapid speed. So, the digital forensic field needs to be continually adapting by developing novel tools and techniques to implement forensic analysis on many different systems such as desktops, portable devices, sensor devices, and many more. The authors mentioned that researchers use the concept of ontology to classify the digital forensic domain in various dimensions. Still, there is no ontology to define the capabilities and relationships among various digital forensic tools. To address this issue, they developed an ontological approach based on Resource Description Framework (RDF) and Web Ontology Language (OWL), which is searchable by using SPARQL and a list of standard digital forensic tools. The main objective of ontology is to assist the digital investigator in selecting the appropriate tools for analysis of digital devices.

In the paper [24], the authors proposed Forensic-Driven Ontologies for Smartphones (F-DOS), a set of ontologies that models the smartphone content for forensic analysis. The F-DOS ontology consists of two main ontologies, namely upper ontology and domain ontology. The domain ontology is further divided into four sub ontologies namely contact ontology, message ontology, investigation case ontology, and other domain ontology. This idea is specified only theoretically. In the paper [25], the authors focus on the benefits of online social networks (OSNs) in digital forensics. Authors stated that no ontology uses OSNs data to support the investigation process. For this, the author proposed an ontology called SC-Ont. The SC-Ont ontology consists of three pillars, namely people, crime, and crime-solving. The main objective of the proposed ontology is to provide an ontological prototype for supporting crime-solving by using data found in OSNs. Moreover, this ontology is not yet fully developed and implemented.

In the literature review section, an overview of ontology, including origin commonly accepted definition and purpose of ontology in the digital forensics domain among researchers, is provided. Based on the literature studies it was found that first, the digital investigators encountered various technical and non-technical terminologies that can be hard to comprehend and face challenges in interpreting digital evidence, primarily due to the misunderstanding of certain vital terms. Various approaches are developed to assist digital practitioners in understanding the newly encountered terminologies, each one with its drawbacks and not able to assist investigators in reasoning about the perceived the meaning of different encountered digital forensics terminologies. It is not viable in the digital forensics domain to design an ontology that would be adequately vast to contain all terminologies that occur due to massive amount of data, diversity of data, rapid changes in technology, and accelerated growth of the internet.

The purpose of this paper is first to examine the concept of building ontologies for digital forensics terminologies and secondly to propose an ontological approach based on a reconstructive timeline of Log2timeline and Psort tools backed by the abstraction concept. The proposed ontological approach will assist practitioners in reasoning with regard to the perceived meaning of different digital forensics terminologies encountered during investigations.

3. Proposed Methodology

In this section, the first methodology for reconstruction of the timeline in digital forensics [26] is discussed. This approach is based on the outcome of the digital forensics command based tools, i.e., Log2timeline and Psort. The Log2timeline tool was used to generate timeline from a disk image file or other sources of data in the .plaso file format, which was sorted out and converted into a familiar format file format such as CSV by Psort in the form of L2TCSV format, i.e., Log2timeline Comma Separated Values. The L2TCSV file contained 17 distinct fields which provided vital and detailed information related to various activities performed by the user on the typical device in the form of a timeline of events and artifacts. So, these fields were defined as data properties in the novel ontology, as shown in Figure 2. The abstraction-based approach used one of the properties of an object-oriented programming language called abstraction, which also follows the definition of symmetry in software. This approach split the timeline into four distinct levels of abstraction, i.e., events: high level, events: low level, artifact location: high level, and artifact location: low level. The concept/objective behind the four levels of abstraction was to follow a specific structure for all sources at each level to compose a uniform and relevant timeline. The specific structure imposed the correctness of the timeline and contained only information that was useful to recognize and interpret actions performed by users by analyzing distinct sources and fields. At the time of timeline reconstruction, numerous new terminologies or concepts were encountered. For this, a novel ontology for digital forensics was developed.

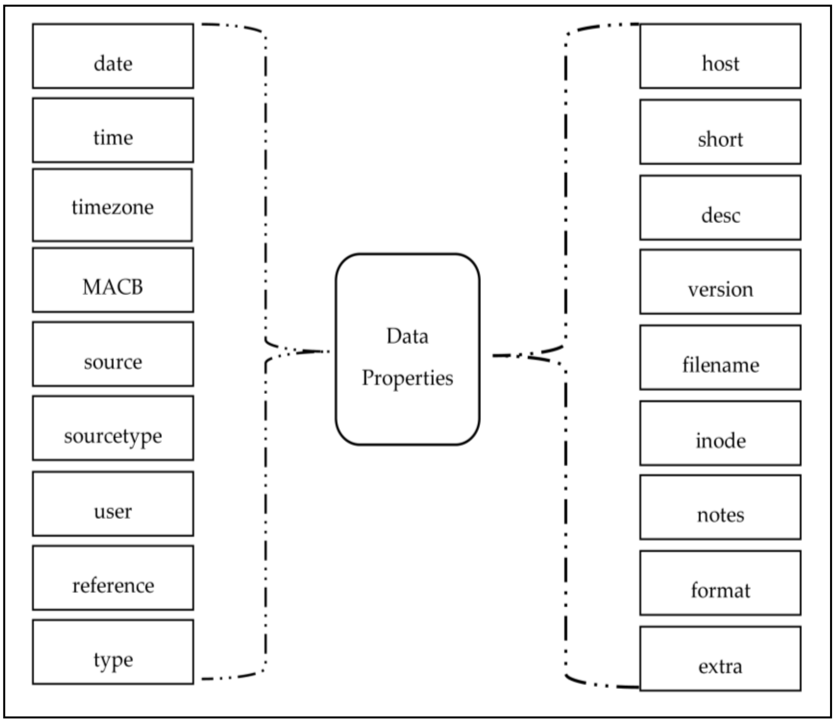


Figure 2. Data properties.

Secondly, we discuss in detail this novel ontology for digital forensics domain. Digital forensic tools generate unstructured timelines from various sources of data. The unstructured timelines are difficult to interpret because of cognitive overload and diversity of semantics. Thus, digital practitioners are not able to understand the newly encountered terminologies and to attain evidence.

To figure out these issues, a promising approach containing correct and reliable representations that allow the user to structure data and to standardize their representation is required. For this, a digital forensic approach backed by a knowledge model called the ontological approach was developed. This approach facilitates correct representation of a digital incident and other actions that are taken during the investigation to get the results. A structured and formal knowledge presentation allows formation of automatic processes more conveniently by composing information in a way that is understandable by the machine and provides an easy way for digital investigators to query, interpret, and visualize the information. An ontology is a prototype the representation of knowledge of domains by structuring this knowledge using classes or entities, relationship, and constraints.

The other features of ontology are first, that it allows automatic reasoning of data by showing the vital relationship among concepts. Secondly, an ontology supports very coherent and easy navigation as that user moves using available concepts in the ontology. Thirdly, ontology can represent any form of data, namely structured and unstructured data. The developed ontology was also supported by our novel abstraction based approach, as shown in Figure 3. All these characteristics of the ontological approach combine to represent correctly the knowledge generated during investigations, assist the practitioner in interpreting the information, attain evidence from the timeline, and identify the causes of digital accidents.

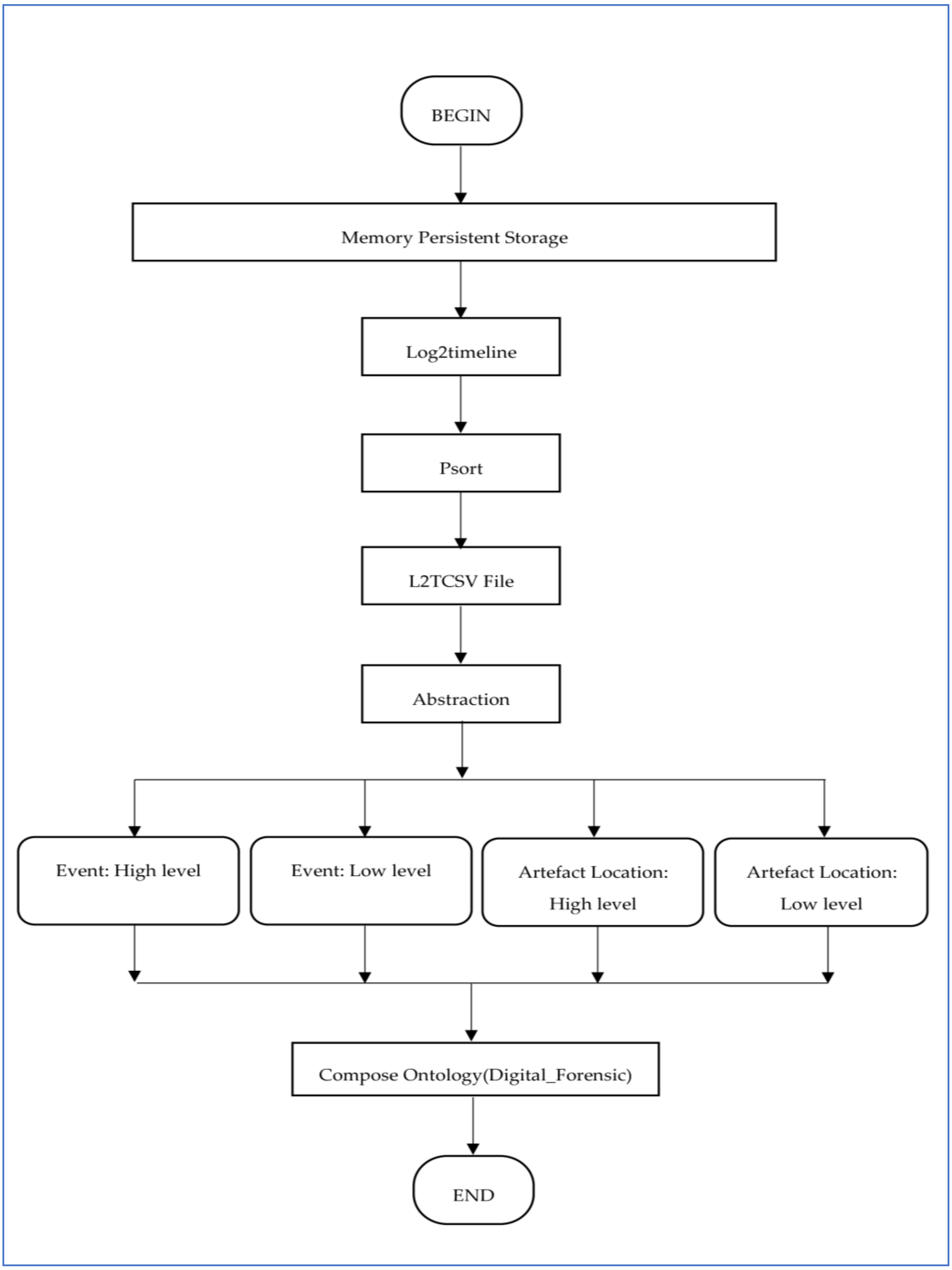

BEGIN
Memory Persistent Storage
Log2timeline
Psort
L2TCSV File
Abstraction
Event: High level
Event: Low level
Artefact Location: High level
Artefact Location: Low level
Compose Ontology(Digital_Forensic)
END

Figure 3. Methodology.

The main ideas behind the development of a novel ontology for digital forensics are first to assist practitioners in understanding the new terminologies and connections among them that are encountered during the investigation. Moreover, it is not possible to develop an ontology that covers all the terminologies, but existing ontologies can be reused to develop new ontologies. A second idea behind ontology development is to share the domain (digital forensics) knowledge among researchers, digital practitioners, and users. We reviewed the timeline and encountered the new terms, their properties, and relationships among them. The abstraction based approach was implemented multiple times on Windows, Android, and iPhone based operating systems devices to identify various new terms. That developed ontology will depict the maximum number of terms and relationships which are identified on a typical Windows, Android, and iPhone operating systems based device.

In the practical terms, developing a particular ontology consists of following major steps:

1. To define the classes.
2. To organize the classes in a taxonomic hierarchy.
3. To describe slots and values.
4. To fill the values into slots.

Lastly, an individual instance of the classes was defined, the value filled into the slot, and restrictions were defined to create a knowledge base. In the developed ontology, the top-down approach was used to define the classes and organize the taxonomy of classes. It begins with the explanation of the most general concepts in the domain, followed by an explanation of specialization concepts. Digital _Forensics is a base class which represents the general concept in the forensics domain for which ontology is being developed to defined common vocabulary, share information, and reuse and analyze domain knowledge. From the base class, three subclasses are defined to represent more specific concepts of the digital forensics domain: Artefact_Investigation, Artefact_Location, and Artefact_Reference. To show the relationship between these classes two object properties are defined such as includesartefact and hasprovenancereference as shown in Figure 4, and to show the relationship between an instance or an individual and a data value, 18 data properties were defined as shown in Figure 2.

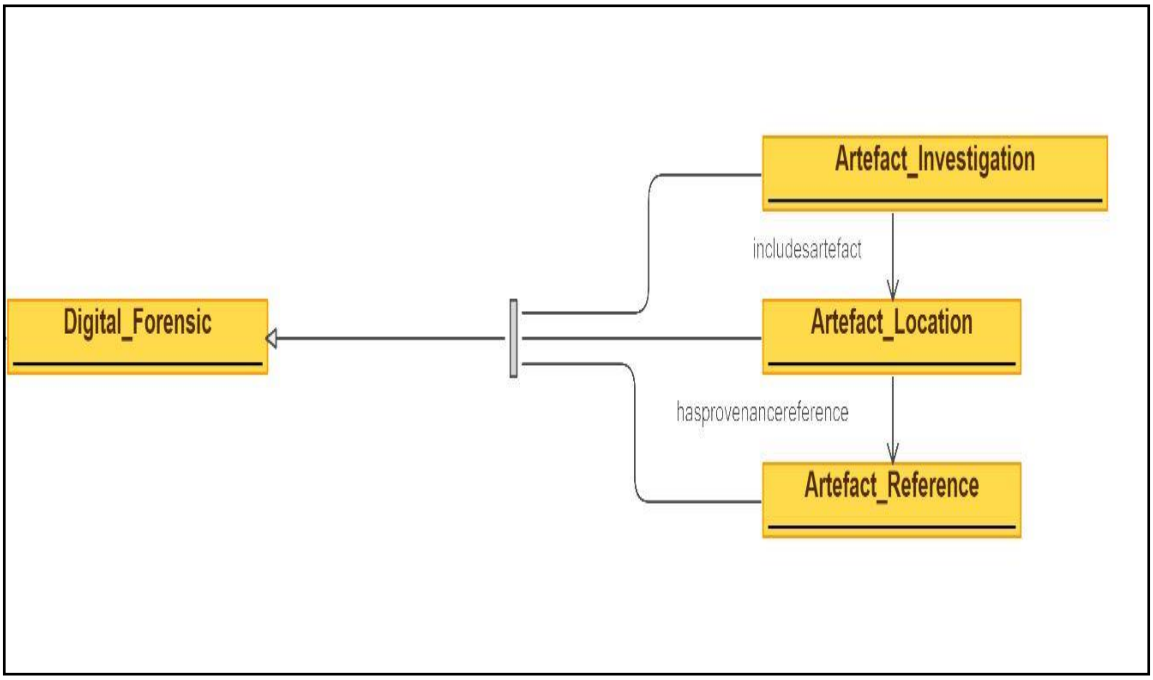


Figure 4. Classes and object properties.

3.1. Artefact_Investigation

The first sub-class Artefact_Investigation defines the basic terms related to the digital forensics process, and different actions are to be taken at various stages by different specialists during the investigation of the case. In ontology, each concept is described by defining a class. To define the sub-terms related to the Artefact_Investigation subclass, new subclasses were defined as shown in Figure 5. A digital attack is committed against an individual or group of individuals (the victim) intentionally with a criminal motive to harm physically or mentally.

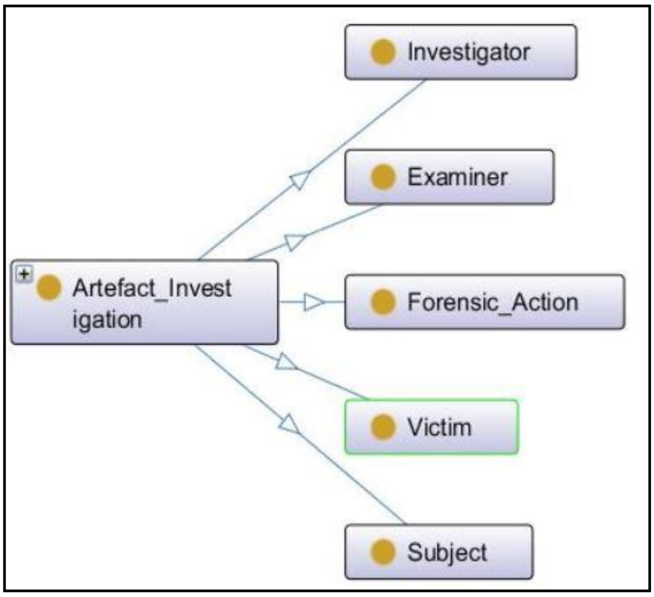


Figure 5. Artefact_Investigation.

The subject provides descriptive information about a specific attack that is committed and forensic processes such as details of the victim, investigator, examiner, digital attack, and many more.

Forensic_Action represents a recognized scientific and forensics process used by digital practitioners in digital forensics investigations to collect the evidence from digital devices. It is a multiphase process beginning from the recognition of digital devices as potential digital evidence to the stage where it is demonstrated as evidence in a court of law. The sequence of the various phases of the digital forensics process is shown in Figure 6 [27]. The forensics investigator is the person who is initially responsible for examining the captured evidence from the scene of the incident. The investigator documents the several types of captured data and provides research on the parameters and technical specifications of the data storage devices, and details of various data components of the evidence as it is presented to him by the data capture specialist. Then the forensics investigator provides his/her report in the form of evidence to the forensics examiner who is independently responsible for analyzing this evidence. The forensic examiner job is to provide logical conclusions about the dataset and what it reveals as to the nature and purpose of the evidence.

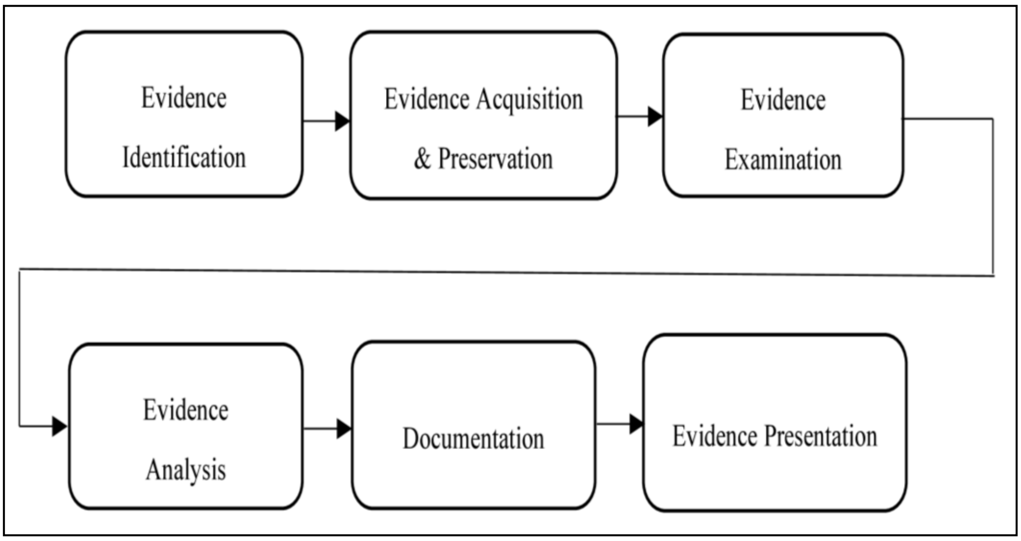


Figure 6. Forensics action.

3.2. Artefact_Location

The Artefact_Location subclass represents our novel abstraction based approach for reconstruction of the timeline. The abstraction based approach consists of four abstraction levels of the timeline as shown in Figure 7 namely events: high level, events: low level, artifact location: high level and artifact location: low level. At each level of abstraction different number of sources and fields are considered to analyses and reconstruct the timeline. The number of sources to be considered at each level can be varied and is dependent upon the maximum number of sources available in the timeline. At events: high level information related to the creation of new files and web surfing activities such as access of web pages and download files is provided with a higher level of abstraction by considering six different fields which compose a unique structure.

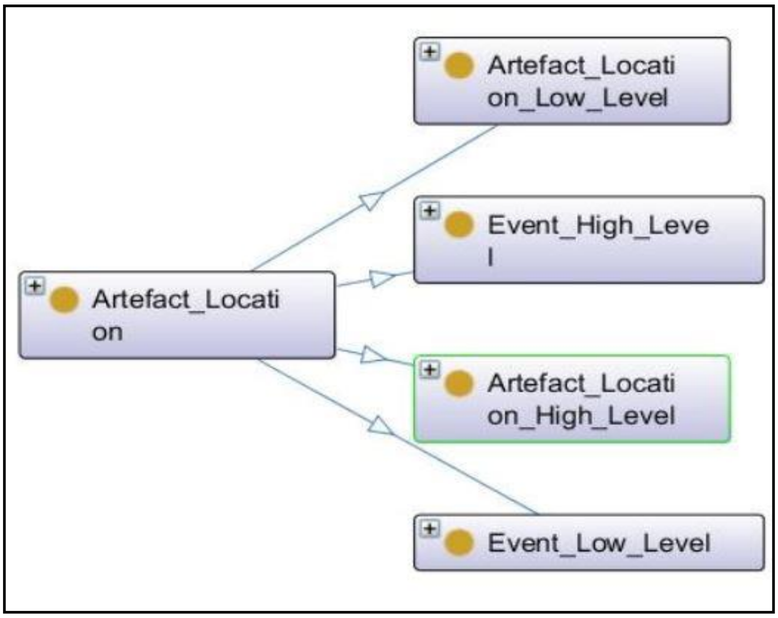


Figure 7. Abstraction Approach.

At events: Low level detailed information is provided related to distinct categories of activities that are performed by the user related to file such as modification, access, changes and birth, and web surfing activities. It also includes the address of particular web pages that are accessed by user and download of information from the web. At this level, seven different fields are considered to compose timeline. The first two levels, i.e., events: high level and events: low level, provides information related to only user activities. To have a clear view of timeline and activities additional information is required such as a list of all executable files executed by a user, applications and files that are regularly accessed by user and authors of files. Besides, detailed information is also provided related to distinct activities performed by the user on the web. For example, in the case of web browsing activity, the detailed information will include the name of used web browser and how (LNK—user follows a link, TYPED—user type the URL, RELOAD—user refresh the web page) web page is accessed. Such detailed and relevant information is provided at artifact location: high level and artifact location: low level by analyzing 10 and 17 fields respectively.

3.3. Artefact_Reference

The Artefact_Reference subclass shows different types of sources of data available in the reconstructed timeline. The number of sources varies, depending upon the operating system and its version and quantity of data. However, the source will support the investigator in recognizing the information available in the timeline and different actions performed by the user on a particular device efficiently.

The novel ontology for the digital forensic domain based on the Log2timeline and Psort tools is composed of three major subclasses: Artefact_Investigation, Artefact_Location, and Artefact_Reference. The subclass Artefact_Investigation presents a recognized scientific and forensics process used by different specialists during the investigation of the case to interpret the digital evidence. The second subclass Artefact_Location shows a novel abstraction based approach for reconstruction of the timeline and its symmetry properties such as regularity, structure, and uniformity to support the investigators in understanding the new terms. In the end, the third subclass Artefact_ Reference shows the newly encountered terminologies and their definitions.

4. Experiment and Discussion

This section presents the implementation of the abstraction based approach on Windows, Android, and iPhone operating system based devices to demonstrate the capability of the approach. For implementation, the object-oriented programming language Java was used and to develop the ontology based on the reconstructive timeline provided by abstraction approach, the ontology editor Protégé 5.5.0 Build Beta-9 version was used with visualization plugins, namely OWLViz, OntoGraf, and VOWL, and an ontology visualization tool OWLGred.

This section consists of four subsections, in which first three subsections show the outcome of the abstraction based approach in the form of a reconstructive timeline of the above mention three different operating system based devices and ontologies corresponding to each of them. In the last subsection, the comparison between the timelines of these three operating systems is shown.

4.1. Windows-Based Timeline and Ontology

For Windows-based ontology, the abstraction based approach is implemented on Windows 10, version 1909 having the new technology file system (NTFS) and around 150 gigabytes of hard disk images of data. The abstraction based approach has four levels of timelines with different levels of detailed information provided at each level by considering a distinct number of data properties (fields) and artifact references (sources). In this section, the two case studies of the Windows based timeline are discussed, namely the "WEBHIST" and "LNK" sources. Figure 8 contains four different timelines corresponding to four levels of the abstraction based approach of source "WEBHIST". At each level of the timeline a different number of data properties (fields) 6, 7, 10, and 18 at events: high level, events: low level, artifact location: high level and artifact location: low level respectively are considered to compose a relevant, detailed, understandable, and structured timeline. The first two levels of timelines provide an overview of web activities performed by a user. It includes an only the addresses of web pages browsed by the user. The last two levels provide detailed and vital information such as the complete address of the web pages, the used browser, and how a particular web page is accessed. All these features of the abstraction based approach for reconstruction of timelines support the practitioner to interpret new terminologies. Similarly, for source "LNK", the four levels of abstraction of the timeline are shown in Figure 9 and provide information related to files that are most frequently accessed by a user.

We designed an ontology based on the outcome of the approach to define new terminologies and relationships among them. It included classes, object properties, and data properties where a class described a new concept or term in the domain, object properties defined the relationship among instances or individuals of different classes, and data properties described the relationship among instances and data values. The results showed that there were nine new terminologies encountered in the Windows-based system timeline, which were described as subclasses of the Artefact_Reference subclass in the ontology of the Windows-based system, as shown in Figure 10. Each terminology represents the source of different information related to different actions performed on the Windows-based system. It includes information related to online operations, offline operations, frequently accessed applications and files, deleted files, and many more. A short description of each subclass is defined in Table 1.

Table 1. New terminologies and their description.

Terminologies (Sub-Classes)	Description
WEBHIST	Information related to browsing activities; it includes the address of web pages accessed by the user, mailing addresses of the user, downloaded files, and application (name of web browser) used to access online services.
RECBIN	Information about files that have been deleted by the user from the system and recycle bin.
LOG	Stores the information about events that take place in an operating system or other program runs.
PE	PE stands for Portable Executable. PE formatted files include .exe, .dll, and .sys (driver files).
FILE	Information related to a particular file is provided such as name, type, location, and size.
META	Meta is often describe as "data about data". It includes modification, access, change, and birth (created) information of a particular document or file.
LNK	Shortcut files that are connected to an application or file commonly found on the desktop of a user or throughout a system and end with the .LNK extension. It is very helpful to access files that are no longer available in the system.
REG	Information about used applications and .DAT files that are only meant for support of applications.
OLECF	OLECF stands for Object Linking and Embedding compound file. It contains .msp, .msi, .asd, and .automaticdestination-ms files which provide information about updates of the Windows operating system and other programs.

Events: High Level (Level 1)
Date: 11/14/2017
Time: 11:46:15
Source: WEBHIST
Short: https://mail.google.com
Visit: mail
Reference: 257192

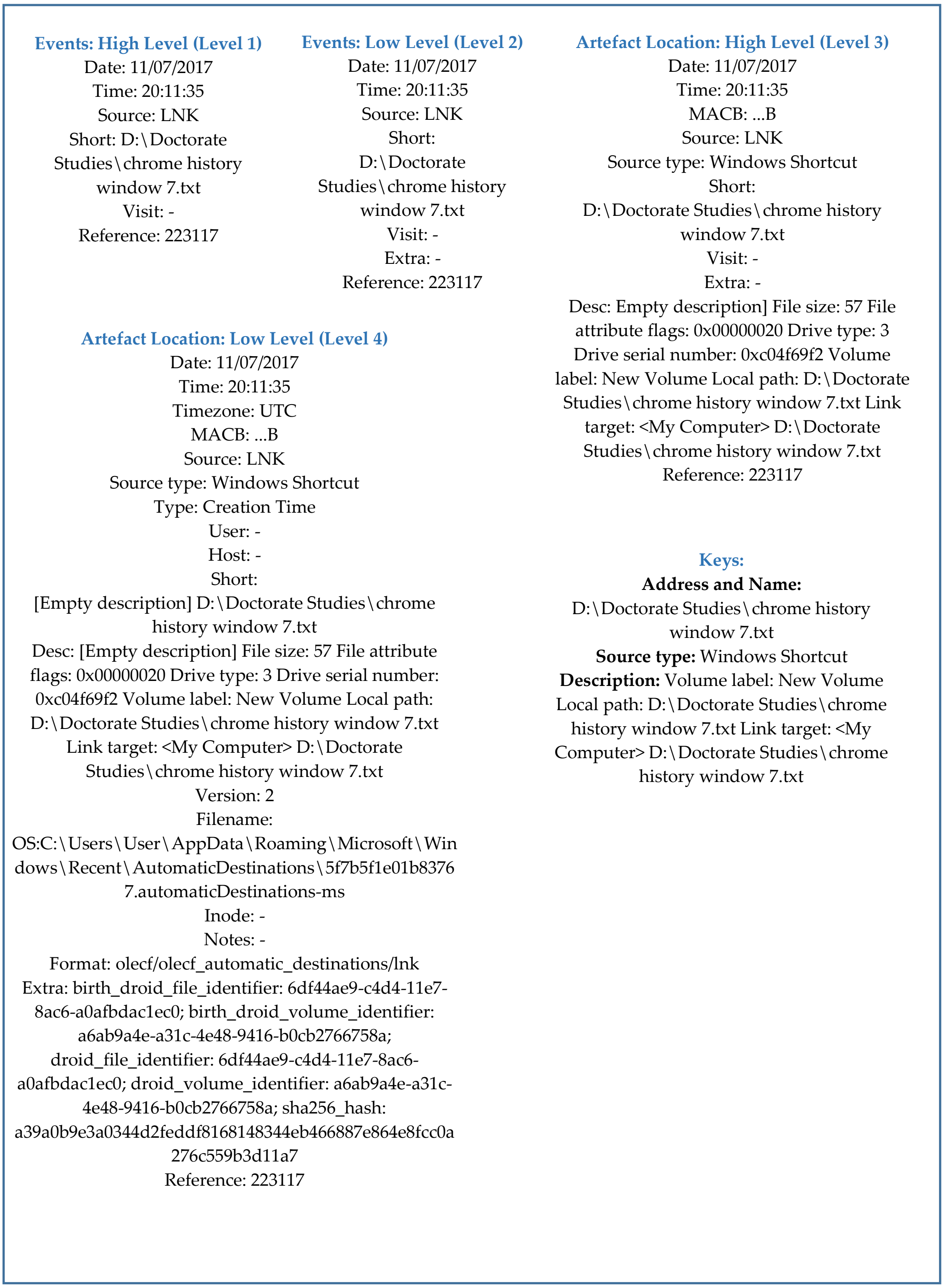
Events: Low Level (Level 2)
Date: 11/14/2017
Time: 11:46:15
Source: WEBHIST
Short:
https://mail.google.com
Visit: mail
Extra:
https://mail.google.com/mail
Reference: 257192

Artefact Location: High Level (Level 3)
Date: 11/14/2017
Time: 11:46:15
MACB: .A..
Source: WEBHIST
Source type: Chrome History
Short:
https://mail.google.com/mail/u/0/#inbox/15fba5850d593d64 (FCI Recruitment 201..
Visit: mail
Extra: https://mail.google.com/mail
Desc: sanxxxxxx525@gmail.com
Reference: 257192

Artefact Location: Low Level (Level 4)
Date: 11/14/2017
Time: 11:46:15
Timezone: UTC
MACB: .A..
Source: WEBHIST
Source type: Chrome History
Type: Last Visited Time
User: -
Host: -
Short:
https://mail.google.com/mail/u/0/#inbox/15fba5850d593d64 (FCI Recruitment 201...
Desc:
https://mail.google.com/mail/u/0/#inbox/15fba5850d593d64 (FCI Recruitment 2017 For 380 Vacancies Apply Now - sanxxxxxx525@gmail.com - Gmail) [count: 0] Host: mail.google.com Type: [LINK - User clicked a link] (URL not typed directly - no typed count)
Version: 2
Filename:
OS:C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\History
Inode: -
Notes: -
Format: sqlite/chrome_history
Extra: schema_match: False; sha256_hash:
582bcc588c7bc39ce0d789951fde1bd8296982a04d8a26eb09a582a901302ae3
Reference: 257192

Keys:
URL:
https://mail.google.com/mail/u/0/#inbox/15fba5850d593d64 (FCI Recruitment 2017 For 380 Vacancies Apply Now - sanxxxxxx525@gmail.com - Gmail)
Search Term: mail
Browser: Google Chrome
Description: LINK - User clicked a link

Figure 8. Windows operating system timeline.



Events: High Level (Level 1)
Date: 11/07/2017
Time: 20:11:35
Source: LNK
Short: D:\Doctorate Studies\chrome history window 7.txt
Visit: -
Reference: 223117

Events: Low Level (Level 2)
Date: 11/07/2017
Time: 20:11:35
Source: LNK
Short:
D:\Doctorate Studies\chrome history window 7.txt
Visit: -
Extra: -
Reference: 223117

Artefact Location: High Level (Level 3)
Date: 11/07/2017
Time: 20:11:35
MACB: ...B
Source: LNK
Source type: Windows Shortcut
Short:
D:\Doctorate Studies\chrome history window 7.txt
Visit: -
Extra: -
Desc: Empty description] File size: 57 File attribute flags: 0x00000020 Drive type: 3 Drive serial number: 0xc04f69f2 Volume label: New Volume Local path: D:\Doctorate Studies\chrome history window 7.txt Link target: <My Computer> D:\Doctorate Studies\chrome history window 7.txt
Reference: 223117

Artefact Location: Low Level (Level 4)
Date: 11/07/2017
Time: 20:11:35
Timezone: UTC
MACB: ...B
Source: LNK
Source type: Windows Shortcut
Type: Creation Time
User: -
Host: -
Short:
[Empty description] D:\Doctorate Studies\chrome history window 7.txt
Desc: [Empty description] File size: 57 File attribute flags: 0x00000020 Drive type: 3 Drive serial number: 0xc04f69f2 Volume label: New Volume Local path: D:\Doctorate Studies\chrome history window 7.txt Link target: <My Computer> D:\Doctorate Studies\chrome history window 7.txt
Version: 2
Filename:
OS:C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\5f7b5f1e01b83767.automaticDestinations-ms
Inode: -
Notes: -
Format: olecf/olecf_automatic_destinations/lnk
Extra: birth_droid_file_identifier: 6df44ae9-c4d4-11e7-8ac6-a0afbdac1ec0; birth_droid_volume_identifier: a6ab9a4e-a31c-4e48-9416-b0cb2766758a; droid_file_identifier: 6df44ae9-c4d4-11e7-8ac6-a0afbdac1ec0; droid_volume_identifier: a6ab9a4e-a31c-4e48-9416-b0cb2766758a; sha256_hash: a39a0b9e3a0344d2feddf8168148344eb466887e864e8fcc0a276c559b3d11a7
Reference: 223117

Keys:
Address and Name:
D:\Doctorate Studies\chrome history window 7.txt
Source type: Windows Shortcut
Description: Volume label: New Volume Local path: D:\Doctorate Studies\chrome history window 7.txt Link target: <My Computer> D:\Doctorate Studies\chrome history window 7.txt

Figure 9. Windows operating system timeline.

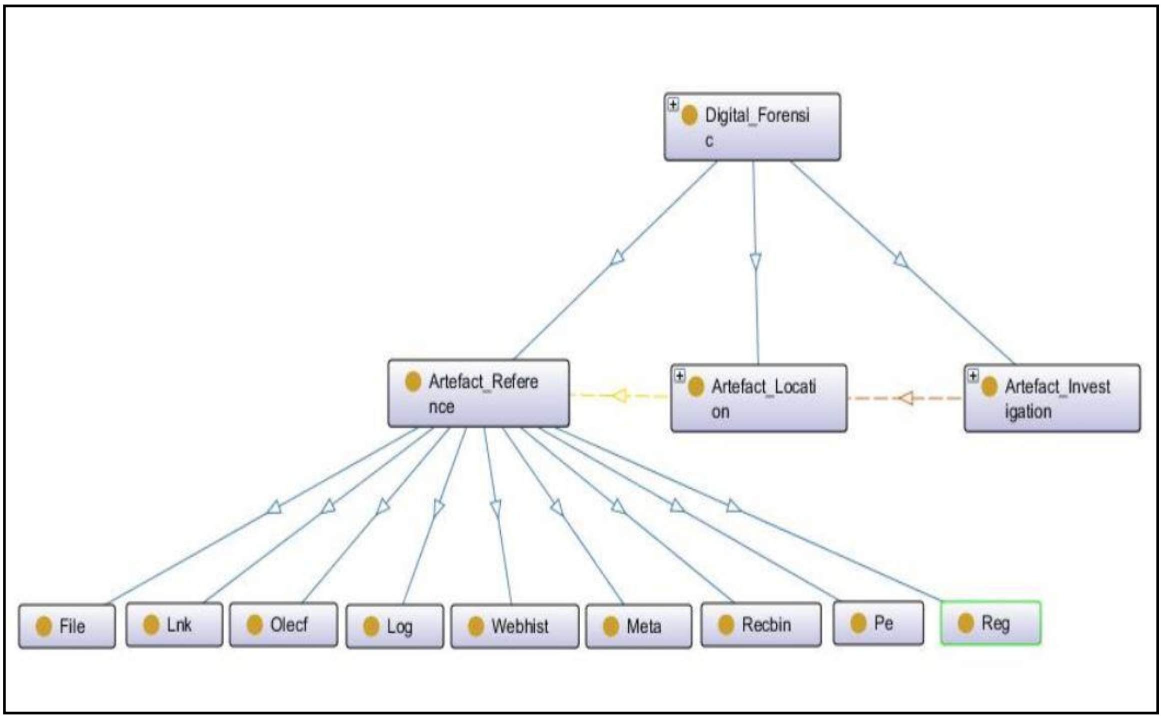
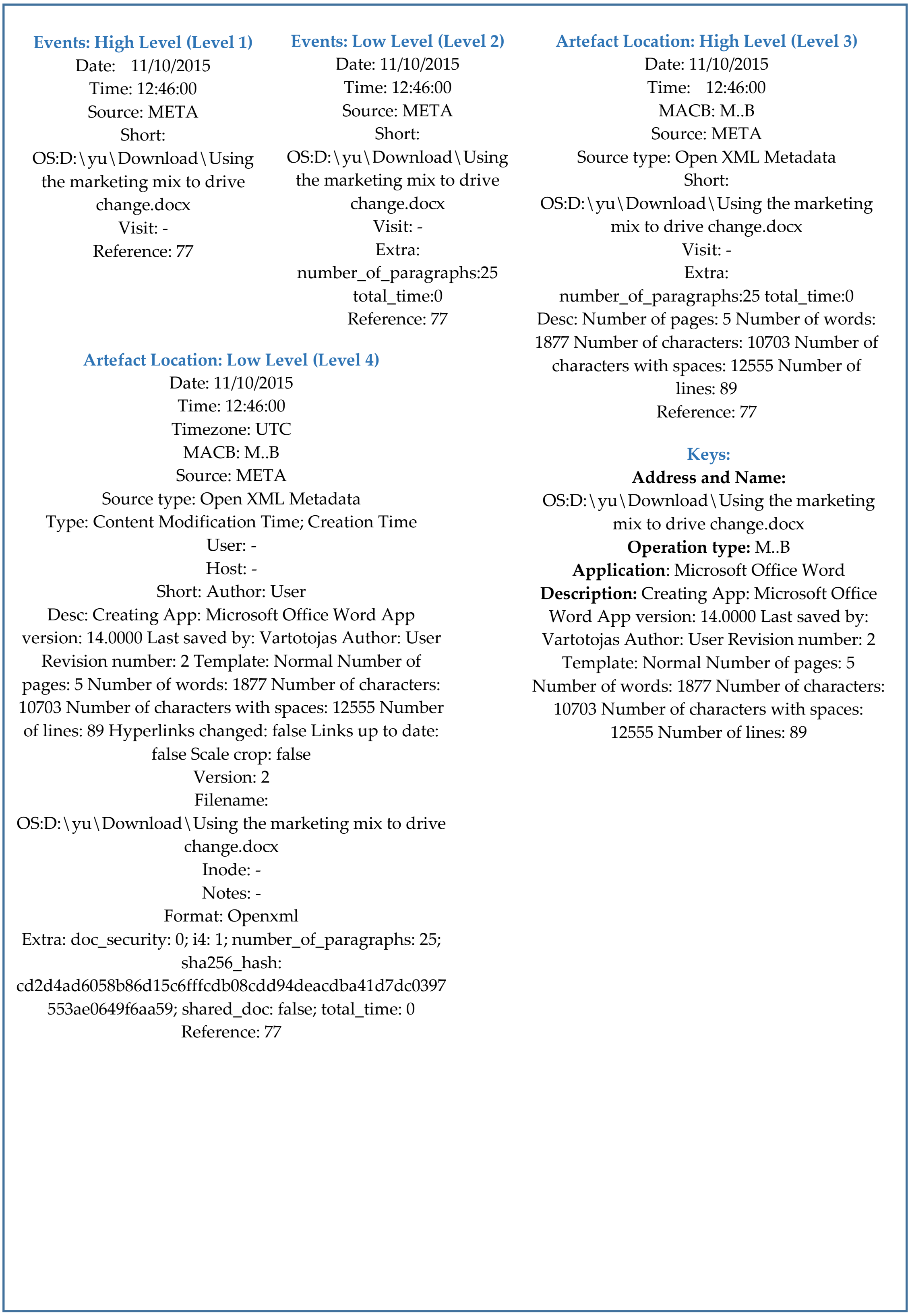


Figure 10. Windows operating system ontology.

4.2. Android-Based Timeline and Ontology

For Android-based ontology, the abstraction based approach was implemented on two different Android-based mobile phones with Android operating system versions L5.1.1 and 9 PKQ1.180904.001 with 12 gigabytes and 20 gigabytes of data respectively.

In this section, two case studies of the Android timeline are discussed, namely data about data, i.e., the "META" source and "FILE" source. As with the Windows operating system, the Android operating system also considered the same number of data properties (fields) at each level of the abstraction based approach to compose a structured timeline. Figure 11 presents the four levels of abstraction of the timeline of the "META" source. The first level, i.e., event: high level, provides brief information such as name, type, and storage location of a particular file. The event: low level and artifact location: high level provide additional information related to contents of a file such as number of words, number of characters, and much more. Artifact location: low level provides vital and useful information related to a particular file such as author name and name of the application used to access, change, or modify the file. In Figure 12, the four levels of abstraction of timelines of the source "FILE" are presented. In this study case, information about a particular file was provided at a different level of the timeline with a distinct level of abstraction of detail. It included name (Tum_Ho_Mera_Pyar-K_K(DesiTape.Com).mp3), type (audio), and size (about 2.16 MB) of the file and much more.



Events: High Level (Level 1)
Date: 11/10/2015
Time: 12:46:00
Source: META
Short:
OS:D:\yu\Download\Using the marketing mix to drive change.docx
Visit: -
Reference: 77

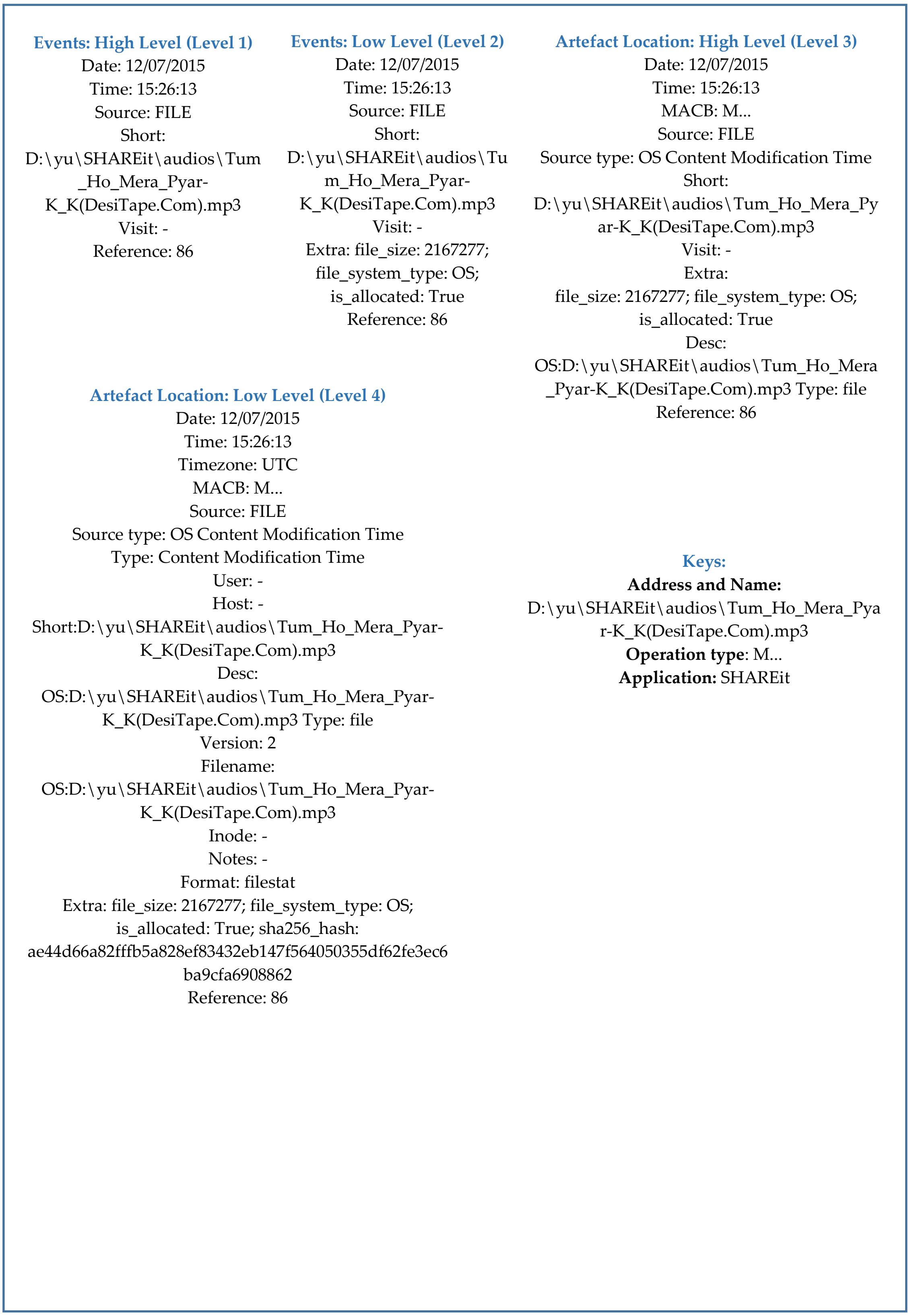
Events: Low Level (Level 2)
Date: 11/10/2015
Time: 12:46:00
Source: META
Short:
OS:D:\yu\Download\Using the marketing mix to drive change.docx
Visit: -
Extra:
number_of_paragraphs:25
total_time:0
Reference: 77

Artefact Location: High Level (Level 3)
Date: 11/10/2015
Time: 12:46:00
MACB: M..B
Source: META
Source type: Open XML Metadata
Short:
OS:D:\yu\Download\Using the marketing mix to drive change.docx
Visit: -
Extra:
number_of_paragraphs:25 total_time:0
Desc: Number of pages: 5 Number of words: 1877 Number of characters: 10703 Number of characters with spaces: 12555 Number of lines: 89
Reference: 77

Artefact Location: Low Level (Level 4)
Date: 11/10/2015
Time: 12:46:00
Timezone: UTC
MACB: M..B
Source: META
Source type: Open XML Metadata
Type: Content Modification Time; Creation Time
User: -
Host: -
Short: Author: User
Desc: Creating App: Microsoft Office Word App version: 14.0000 Last saved by: Vartotojas Author: User Revision number: 2 Template: Normal Number of pages: 5 Number of words: 1877 Number of characters: 10703 Number of characters with spaces: 12555 Number of lines: 89 Hyperlinks changed: false Links up to date: false Scale crop: false
Version: 2
Filename:
OS:D:\yu\Download\Using the marketing mix to drive change.docx
Inode: -
Notes: -
Format: Openxml
Extra: doc_security: 0; i4: 1; number_of_paragraphs: 25; sha256_hash: cd2d4ad6058b86d15c6fffcdb08cdd94deacdba41d7dc0397553ae0649f6aa59; shared_doc: false; total_time: 0
Reference: 77

Keys:
Address and Name:
OS:D:\yu\Download\Using the marketing mix to drive change.docx
Operation type: M..B
Application: Microsoft Office Word
Description: Creating App: Microsoft Office Word App version: 14.0000 Last saved by: Vartotojas Author: User Revision number: 2 Template: Normal Number of pages: 5 Number of words: 1877 Number of characters: 10703 Number of characters with spaces: 12555 Number of lines: 89

Figure 11. Android operating system timeline.



Events: High Level (Level 1)
Date: 12/07/2015
Time: 15:26:13
Source: FILE
Short:
D:\yu\SHAREit\audios\Tum_Ho_Mera_Pyar-K_K(DesiTape.Com).mp3
Visit: -
Reference: 86

Events: Low Level (Level 2)
Date: 12/07/2015
Time: 15:26:13
Source: FILE
Short:
D:\yu\SHAREit\audios\Tum_Ho_Mera_Pyar-K_K(DesiTape.Com).mp3
Visit: -
Extra: file_size: 2167277;
file_system_type: OS;
is_allocated: True
Reference: 86

Artefact Location: High Level (Level 3)
Date: 12/07/2015
Time: 15:26:13
MACB: M...
Source: FILE
Source type: OS Content Modification Time
Short:
D:\yu\SHAREit\audios\Tum_Ho_Mera_Pyar-K_K(DesiTape.Com).mp3
Visit: -
Extra:
file_size: 2167277; file_system_type: OS;
is_allocated: True
Desc:
OS:D:\yu\SHAREit\audios\Tum_Ho_Mera_Pyar-K_K(DesiTape.Com).mp3 Type: file
Reference: 86

Artefact Location: Low Level (Level 4)
Date: 12/07/2015
Time: 15:26:13
Timezone: UTC
MACB: M...
Source: FILE
Source type: OS Content Modification Time
Type: Content Modification Time
User: -
Host: -
Short:D:\yu\SHAREit\audios\Tum_Ho_Mera_Pyar-K_K(DesiTape.Com).mp3
Desc:
OS:D:\yu\SHAREit\audios\Tum_Ho_Mera_Pyar-K_K(DesiTape.Com).mp3 Type: file
Version: 2
Filename:
OS:D:\yu\SHAREit\audios\Tum_Ho_Mera_Pyar-K_K(DesiTape.Com).mp3
Inode: -
Notes: -
Format: filestat
Extra: file_size: 2167277; file_system_type: OS;
is_allocated: True; sha256_hash:
ae44d66a82fffb5a828ef83432eb147f564050355df62fe3ec6ba9cfa6908862
Reference: 86

Keys:
Address and Name:
D:\yu\SHAREit\audios\Tum_Ho_Mera_Pyar-K_K(DesiTape.Com).mp3
Operation type: M...
Application: SHAREit

Figure 12. Android operating system timeline.

The results showed that there were four terminologies encountered in the Android-based system timeline, which were described as subclasses of the Artefact_Reference subclass in the ontology of the Android-based system, as shown in Figure 13. The three subclasses “OLECF”, “META”, and “PE”, excluding subclass "FILE", provided the same information which was described above (see Table 1). The two new subclasses "Application" and "Browsing_History" of the subclass "FILE" were explicitly defined to show the information about user browsing activities as there was no information implicitly available in the timeline for browsing activities.

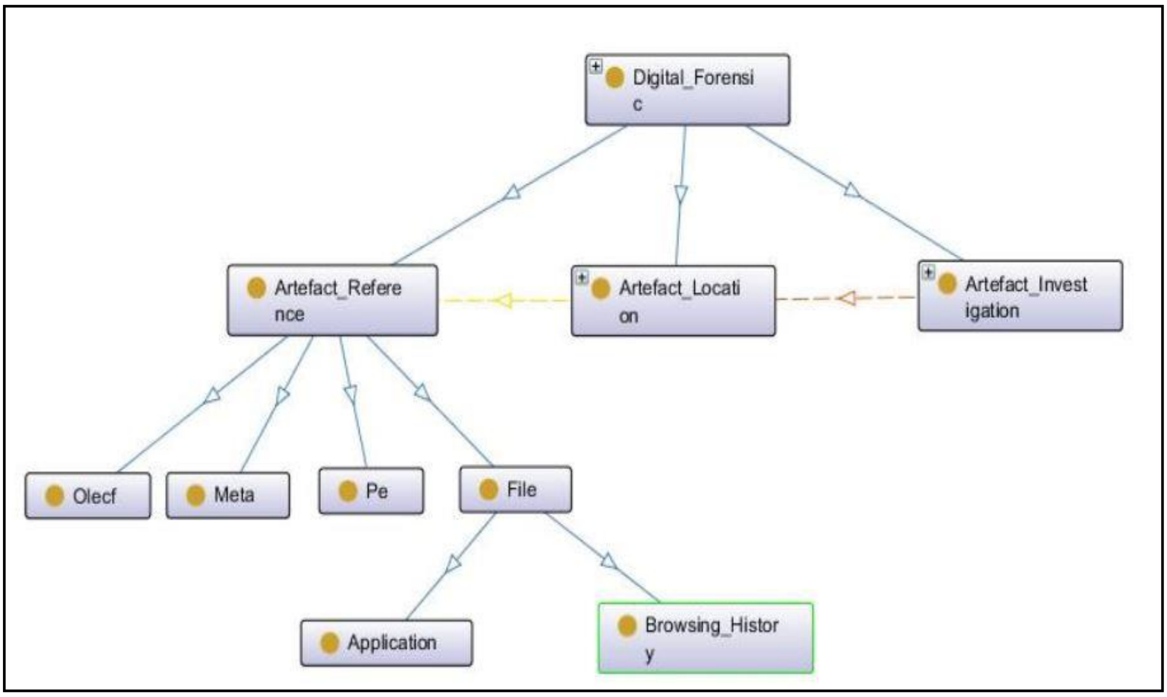


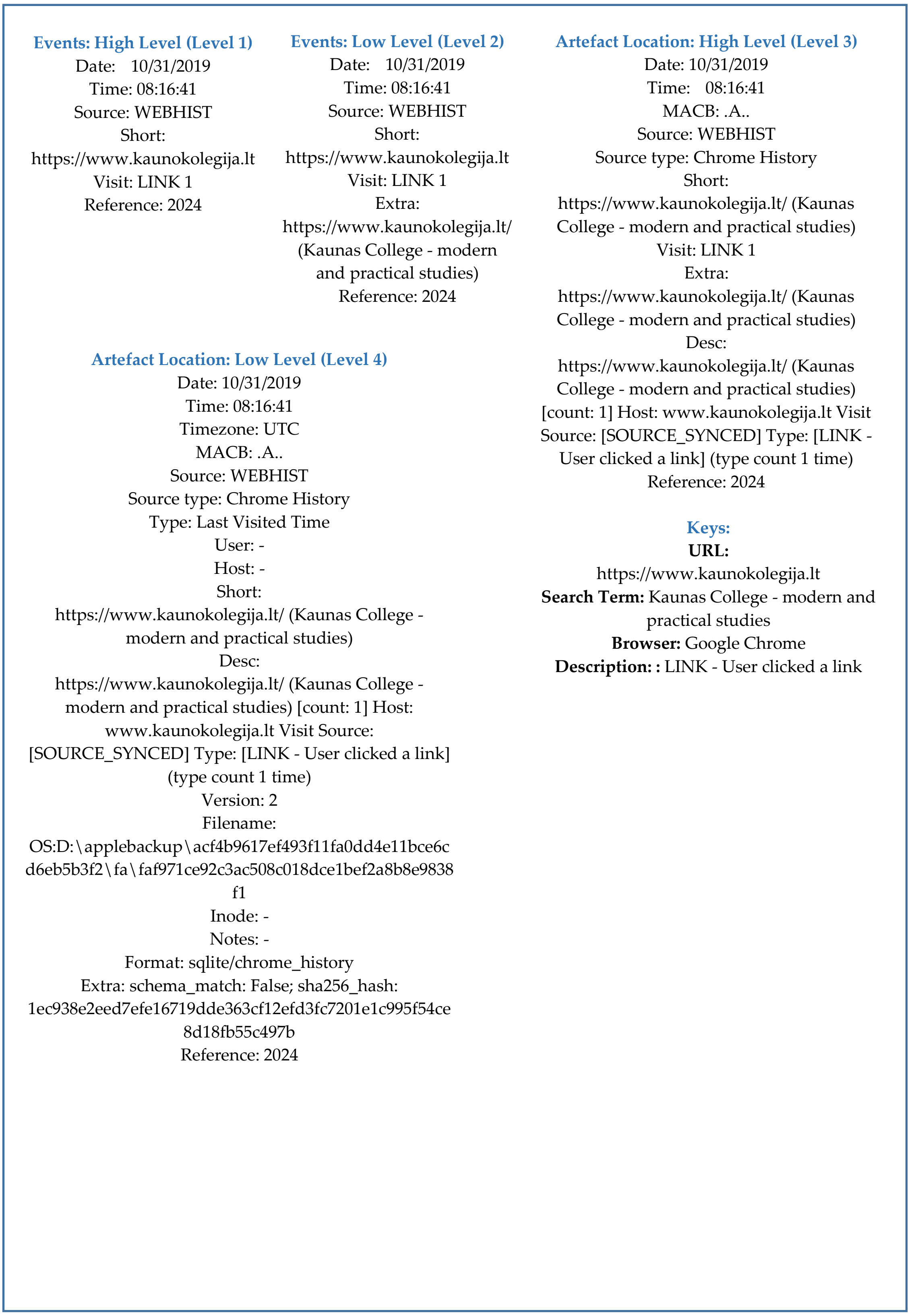
Figure 13. Android operating system ontology.

4.3. *iPhone Based Timeline and Ontology*

For the iPhone operating system based ontology, the abstraction based approach was implemented on the iPhone operating system based mobile phone with version IOS 13.3 and about 20 gigabytes of data. Like the Windows and Android operating systems, the same structured was also followed for the iPhone operating system by considering the same number of data properties (fields) at each level.

In this section, the two case studies of the iPhone timeline are discussed, such as web browsing activity (WEBHSIT) and local operation (iMessage) performed by a user. In the first study case, i.e., web browsing activity, each level of the approach provided information related to specific web activity with different levels of abstraction of detail. It included the web address, the browser used to access a particular web page and how, i.e., either user typed the address in the address bar or clicked a link, as shown in Figure 14 The second study case, i.e., timeline of local operation, provided information related to an activity which was performed locally on the device without the usage of internet, as shown in Figure 15. It included vital information such as contact number, mailing address, and much more.

The results show that there were six terminologies encountered in the iPhone operating system based timeline, which were described as subclasses of the Artefact_Reference subclass in the ontology of the iPhone operating system as shown in Figure 16. The four subclasses except for the two subclasses "IMESSAGE" and "PLIST" provided the same information which was described above (see Table 1). The "IMESSAGE" subclass provided information related to all received and sent messages using the Apple iMessage application on the particular iPhone operating system based device. It showed very crucial information such as the contact number used to send and receive messages. The "PLIST" stands for Property List and is a format for storing application data. It was originally developed by Apple for iPhone operating system based devices.



Events: High Level (Level 1)
Date: 10/31/2019
Time: 08:16:41
Source: WEBHIST
Short:
https://www.kaunokolegija.lt
Visit: LINK 1
Reference: 2024

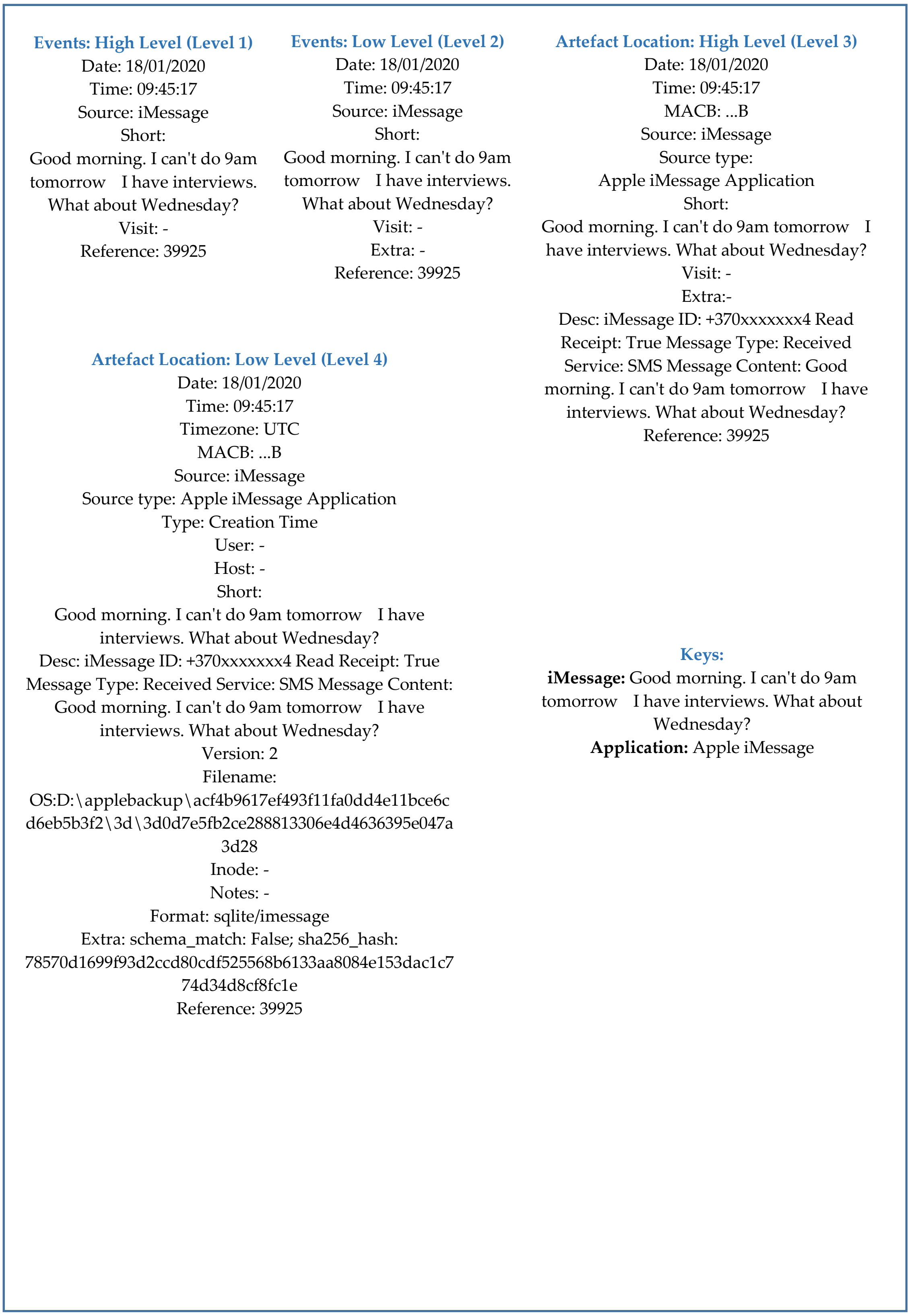
Events: Low Level (Level 2)
Date: 10/31/2019
Time: 08:16:41
Source: WEBHIST
Short:
https://www.kaunokolegija.lt
Visit: LINK 1
Extra:
https://www.kaunokolegija.lt/
(Kaunas College - modern
and practical studies)
Reference: 2024

Artefact Location: Low Level (Level 4)
Date: 10/31/2019
Time: 08:16:41
Timezone: UTC
MACB: .A..
Source: WEBHIST
Source type: Chrome History
Type: Last Visited Time
User: -
Host: -
Short:
https://www.kaunokolegija.lt/ (Kaunas College -
modern and practical studies)
Desc:
https://www.kaunokolegija.lt/ (Kaunas College -
modern and practical studies) [count: 1] Host:
www.kaunokolegija.lt Visit Source:
[SOURCE_SYNCED] Type: [LINK - User clicked a link]
(type count 1 time)
Version: 2
Filename:
OS:D:\applebackup\acf4b9617ef493f11fa0dd4e11bce6c
d6eb5b3f2\fa\faf971ce92c3ac508c018dce1bef2a8b8e9838
f1
Inode: -
Notes: -
Format: sqlite/chrome_history
Extra: schema_match: False; sha256_hash:
1ec938e2eed7efe16719dde363cf12efd3fc7201e1c995f54ce
8d18fb55c497b
Reference: 2024

Artefact Location: High Level (Level 3)
Date: 10/31/2019
Time: 08:16:41
MACB: .A..
Source: WEBHIST
Source type: Chrome History
Short:
https://www.kaunokolegija.lt/ (Kaunas
College - modern and practical studies)
Visit: LINK 1
Extra:
https://www.kaunokolegija.lt/ (Kaunas
College - modern and practical studies)
Desc:
https://www.kaunokolegija.lt/ (Kaunas
College - modern and practical studies)
[count: 1] Host: www.kaunokolegija.lt Visit
Source: [SOURCE_SYNCED] Type: [LINK -
User clicked a link] (type count 1 time)
Reference: 2024

Keys:
URL:
https://www.kaunokolegija.lt
Search Term: Kaunas College - modern and
practical studies
Browser: Google Chrome
Description: : LINK - User clicked a link

Figure 14. iPhone operating system timeline.



Events: High Level (Level 1)
Date: 18/01/2020
Time: 09:45:17
Source: iMessage
Short:
Good morning. I can't do 9am tomorrow I have interviews. What about Wednesday?
Visit: -
Reference: 39925

Events: Low Level (Level 2)
Date: 18/01/2020
Time: 09:45:17
Source: iMessage
Short:
Good morning. I can't do 9am tomorrow I have interviews. What about Wednesday?
Visit: -
Extra: -
Reference: 39925

Artefact Location: High Level (Level 3)
Date: 18/01/2020
Time: 09:45:17
MACB: ...B
Source: iMessage
Source type:
Apple iMessage Application
Short:
Good morning. I can't do 9am tomorrow I have interviews. What about Wednesday?
Visit: -
Extra:-
Desc: iMessage ID: +370xxxxxxx4 Read Receipt: True Message Type: Received Service: SMS Message Content: Good morning. I can't do 9am tomorrow I have interviews. What about Wednesday?
Reference: 39925

Artefact Location: Low Level (Level 4)
Date: 18/01/2020
Time: 09:45:17
Timezone: UTC
MACB: ...B
Source: iMessage
Source type: Apple iMessage Application
Type: Creation Time
User: -
Host: -
Short:
Good morning. I can't do 9am tomorrow I have interviews. What about Wednesday?
Desc: iMessage ID: +370xxxxxxx4 Read Receipt: True Message Type: Received Service: SMS Message Content: Good morning. I can't do 9am tomorrow I have interviews. What about Wednesday?
Version: 2
Filename:
OS:D:\applebackup\acf4b9617ef493f11fa0dd4e11bce6cd6eb5b3f2\3d\3d0d7e5fb2ce288813306e4d4636395e047a3d28
Inode: -
Notes: -
Format: sqlite/imessage
Extra: schema_match: False; sha256_hash: 78570d1699f93d2ccd80cdf525568b6133aa8084e153dac1c774d34d8cf8fc1e
Reference: 39925

Keys:
iMessage: Good morning. I can't do 9am tomorrow I have interviews. What about Wednesday?
Application: Apple iMessage

Figure 15. iPhone operating system timeline.

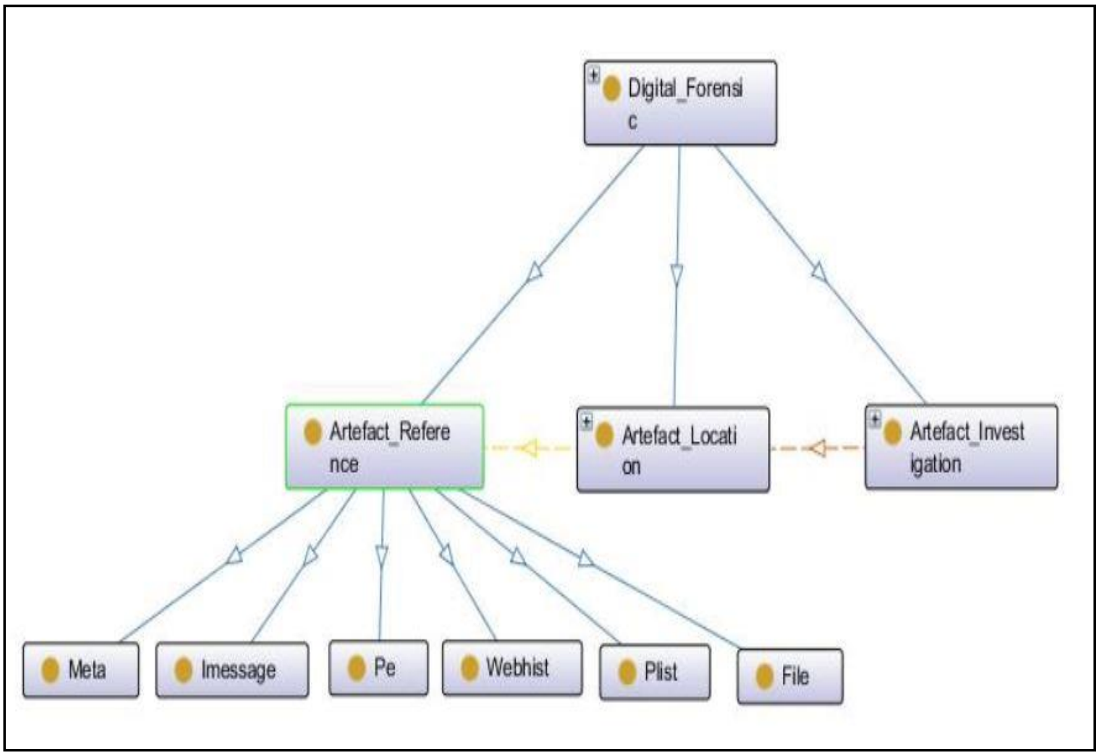


Figure 16. iPhone operating system ontology.

4.4. Comparisons

In this section, two comparisons between Windows, Android, and iPhone operating systems are discussed. First, the comparison shows the maximum number of new terminologies which present the sources of information available for each operating system, and the number of fields (data properties) and the number of sources (artifact references) are considered at different levels of approach to reconstruct the timeline.

From the results (see Table 2), it was found that 9, 4, and 6 were the maximum number of sources (artifact references) available for Windows, Android, and iPhone operating systems respectively. For all operating systems, 6, 7, 10, and 18 fields (data properties) for the event: high level, event: low level, artifact location: low level and artifact location: high level respectively are considered in the timeline. It showed that a unique structure was followed at each level of the abstraction based approach for all operating systems to reconstruct the suitable timeline which followed the definition of symmetry.

Table 2. Comparison between Windows, Android, and iPhone operating systems.

Operating System	**Artefact_Location**	**Number of Fields (Data Properties)**	**Number of Artefact_Reference**
Windows operating system	Event: High level	6	6
	Event: Low level	7	9
	Artifact Location: High level	10	9
	Artifact Location: Low level	18	9
Android operating system	Event: High level	6	3
	Event: Low level	7	4
	Artifact Location: High level	10	4
	Artifact Location: Low level	18	4

Table 2. *Cont.*

Operating System	Artefact_Location	Number of Fields (Data Properties)	Number of Artefact_Reference
iPhone operating system	Event: High level	6	3
	Event: Low level	7	4
	Artifact Location: High level	10	6
	Artifact Location: Low level	18	6

The second comparison showed the availability of different types of information available in the timelines of these three operating systems. From the results (see Table 3) it was observed that the timeline of the Window-based system provided the maximum information regarding all types of operations executed by the user. It included online and offline, most frequently used applications, and deleted files as compared to the Android and iPhone operating systems.

Table 3. Comparison between Windows, Android, and iPhone operating systems.

Parameters	Windows Operating System	Android Operating System	iPhone Operating System
Online Operation Information	Available	Partially Available	Available
Offline Operation Information	Available	Not Available	Available
Mailing Addresses	Available	Not Available	Available
Frequently Used Applications	Available	Not Available	Not Available
MAC Address	Available	Not Available	Not Available
Deleted Files	Available	Not Available	Not Available

From the results, it was found that our novel ontology based on the abstraction approach for three different operating systems, namely Windows, Android, and iPhone operating systems, defined all the terms that were encountered during the investigation. Moreover, a unique structure was also stipulated for all the sources at each level of the timeline, which assisted in understanding the new encountered terminology.

5. Conclusions

The reconstruction of a timeline and understanding of new encountered terminologies or concepts during a investigation of security incident are very crucial to finding and interpreting the cause of incidents so incidents can be avoided in the future. From the literature review, it was found that numerous techniques have been designed to solve this issue, but none of them are suitable.

A novel ontological approach based on a reconstructed timeline of Log2timeline and Psort tools backed by the abstraction concept is presented. The abstraction concept was used to split the timeline into four distinct levels of abstraction of the timeline. It included events: high level (new entries and web surfing), events: low level (web surfing, actions of modifying), artifact location: high level (include all .exe files), and artifact location: low level. The idea behind the split timeline was to follow symmetry properties in software such as regularity, structure, and uniformity, which compose a compact and recognizable timeline. Moreover, other important features of the ontology approach, such as automatic reasoning of data, coherent and easy navigation, and representation of any form of data, will assist digital practitioners in understanding the newly encountered terminologies and in finding the cause of digital attacks. The novel ontological approach was implemented numerous times on Windows, Android, and iPhone operating system based devices to show the capability and flexibility of the approach. The outcome showed that the developed approach is capable of providing understanding of encountered terminologies or concepts by reconstructing the timeline. In the future, this approach can be used as a base to automatically analyze the timeline and, by adding new rules using the SPARQL query language, compose more visualized ontology. It will consider more new artifacts to define more encountered terminologies in digital forensics tools.

Author Contributions: Conceptualization, methodology, S.B.; Formal analysis, V.J.; writing—original draft preparation, S.B.; writing—review and editing, S.B.; supervision, V.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Corazzon, R. Ontology. A Resource Guide for Philosophers. Available online: http://www.formalontology.it (accessed on 20 January 2020).
2. Hadzic, M.; Wongthongtham, P.; Dillon, T.; Chang, E. Introduction to Ontology. In *Ontology-Based Multi-Agent Systems. Studies in Computational Intelligence*; Springer: Berlin/Heidelberg, Germany, 2009; Volume 219.
3. Russell, S.J.; Norvig, P. *Artificial Intelligence: A Modern Approach*; Prentice Hall: Upper Saddle River, NJ, USA, 2016.
4. Gruber, T. Towards Principles for the Design of Ontologies Used for Knowledge Sharing? *Int. J. Hum. Comput. Stud.* **1995**, *43*, 907–928. [CrossRef]
5. Gómez-Pérez, A. Knowledge sharing and reuse. In *Handbook of Applied Expert Systems*; CRC Press: Boca Raton, FL, USA, 1998; Volume 10, pp. 1–36.
6. Gruber, T.R. A Translation Approach to Portable Ontology Specifications. *Knowl. Acquis.* **1993**, *5*, 199–220. [CrossRef]
7. Huang, J.; Yasinsac, A.; Hayes, P.J. Knowledge Sharing and Reuse in Digital Forensics. In Proceedings of the 2010 Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, Oakland, CA, USA, 20 May 2010; pp. 1–6.
8. Noy, N.F.; McGuinness, D.L. Ontology Development 101: A Guide to Creating Your First Ontology. Available online: https://protege.stanford.edu/publications/ontology_development/ontology101.pdf (accessed on 25 January 2020).
9. Amato, F.; Cozzolino, G.; Mazzeo, A.; Mazzocca, N. Correlation of Digital evidences in forensic investigation through semantic technologies. In Proceedings of the 31st International Conference on Advanced Information Networking and Applications Workshops, Taipei, Taiwan, 27–29 March 2017.
10. Alzaabi, M.; Jones, A.; Martin, T.A. An Ontology-Based Forensic Analysis Tool. In Proceedings of the Annual ADFSL Conference on Digital Forensics, Security and Law, Richmond, Virginia, 10–12 June 2013.
11. Brinson, A.; Robinson, A.; Roger, M. A Cyber Forensics Ontology: Creating a New Approach to Studying Cyber Forensics. *Digit. Investig.* **2006**, *3*, 37–43. [CrossRef]
12. Karie, N.M.; Kebande, V.R. Building Ontologies for Digital Forensic Terminologies. *Int. J. Cyber-Secur. Digit. Forensics* **2016**, *5*, 75–82. [CrossRef]
13. Ćosić, J.; Ćosić, Z. The Necessity of Developing a Digital Evidence Ontology. In Proceedings of the 23rd Central European Conference on Information and Intelligent Systems, Varazdin, Croatia, 1 September 2012.
14. Chabot, Y.; Bertaux, A.; Nicolle, C.; Kechadi, T. An ontology-based approach for the reconstruction and analysis of digital incidents timelines. *Digit. Investig.* **2015**, *15*, 83–100. [CrossRef]
15. Harrill, D.C.; Mislan, R.P. A Small Scale Digital Device Forensics ontology. *Small Scale Digit. Device Forensics J.* **2007**, *1*, 1–7.
16. Kahvedžic, D.; Kechadi, T. DIALOG A framework for modeling, analysis and reuse of digital forensic knowledge. *Digit. Investig.* **2009**, *6*, S23–S33. [CrossRef]
17. Park, H.; Cho, S.; Kwon, H.C. Cyber Forensics Ontology for Cyber Criminal Investigation. In Proceedings of the International Conference on Forensics in Telecommunications, Information, and Multimedia, Adelaide, Australia, 19–21 January 2009; pp. 160–165.

18. Saad, S.; Traore, I. Method ontology for intelligent network forensics analysis. In Proceedings of the 8th International Conference on Privacy, Security and Trust, Ottawa, ON, Canada, 1 August 2010.
19. Luthfi, A. The Use of Ontology Framework for Automation Digital Forensics Investigation, International Journal of Computer, Electrical, Automation. *Control Inf. Eng.* **2014**, *8*, 454–456.
20. Brady, O.; Overill, R.; Keppens, J. Addressing the increasing volume and variety of digital evidence using an ontology. In Proceedings of the 2014 IEEE Joint Intelligence and Security Informatics Conference, Hague, The Netherlands, 24–26 September 2014; pp. 176–183.
21. Akremi, A.; Sriti, M.F.; Sallay, H.; Rouached, M. Ontology-Based Smart Sound Digital Forensics Analysis for Web Services. *J. Web Serv. Res.* **2019**, *16*, 70–92. [CrossRef]
22. Ćosić, J.; Ćosić, Z.; Bača, M. An Ontological Approach to Study and Manage Digital Chain of Custody of Digital Evidence. *J. Inf. Organ. Sci.* **2011**, *35*, 1–13.
23. Wimmer, H.; Chen, L.; Narock, T. Ontologies and the Semantic Web for Digital Investigation Tool Selection. *J. Digit. Forensics Secur. Law* **2018**, *13*, 6. [CrossRef]
24. Alzaabi, M.; Martin, T.A.; Taha, K.; Jones, A. The Use of Ontologies in Forensic Analysis of Smartphone Content. *J. Digit. Forensics Secur. Law* **2015**, *10*, 9. [CrossRef]
25. Kalemi, E.; Yayilgan, S.Y. Ontologies for Social Media Digital Evidence. *Int. J. Comput. Inf. Eng.* **2016**, *10*, 335–340.
26. Bhandari, S.; Jusas, V. An abstraction based approach for reconstruction of timeline in digital forensics. *Symmetry* **2020**, *12*, 104. [CrossRef]
27. Bhandari, S.; Jusas, V. An audit: Digital forensic research. *Int. J. Adv. Electron. Comput. Sci.* **2019**, *8*, 71–75.