Intelligence Network & Secure Platform for Evidence Correlation and Transfer

D2.3 Reference Digital Forensics Domain Model

Document Summary Information

Grant Agreement No	833276	**Acronym**	INSPECTr
Full Title	Deliverable D2.3: Reference Digital Forensics Domain Model		
Start Date	18/04/2020	**Duration**	42 months
Project URL	https://inspectr-project.eu		
Deliverable	2.3		
Work Package	2		
Contractual due date	M21 - 31/05/2021	**Actual submission date**	31.05.2021
Nature	Report	**Dissemination Level**	PU
Lead Beneficiary	CNR		
Responsible Author	Fabrizio Turchi		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 833276

Document Version Control:		
Version 0.1	Originated by: CNR (Fabrizio Turchi)	On 18/04/2020
Version 0.2	Modified by: CNR (Fabrizio Turchi)	On 12/10/2020
Version 0.3	Modified by: CNR (Fabrizio Turchi)	On 13/10/2020
Version 0.4	Modified by: CNR (Fabrizio Turchi)	On 14/10/2020
Version 0.5	Modified by: CNR (Fabrizio Turchi)	On 15/10/2020
Version 0.6	Modified by: CNR (Fabrizio Turchi)	On 16/10/2020
Version 0.7	Modified by: CNR (Mattia Epifani)	On 23/10/2020
Version 0.8	Modified by: CNR (Fabrizio Turchi)	On 26/10/2020
Version 0.9	Modified by: CNR (Claudia Meda, Fabrizio Turchi)	On 27/10/2020
Version 1.0	Reviewed by SIREN (Felipe Cora)	On 05/02/2021
Version 1.1	Reviewed by: UNIL (Eoghan Casey)	On 07/02/2021
Version 1.2	Included feedback and modified by CNR (Fabrizio Turchi)	On 09/02/2021
Version 1.3	Modified by CNR (Fabrizio Turchi)	On 15/02/2021
Version 1.4	Reviewed by CNR (Fabrizio Turchi)	On 28/05/2021

Deliverable D2.3: Reference Digital Forensics Domain Model

List of abbreviations

Acronym	Explanation
CASE	The open-source Cyber-investigation Analysis Standard Expression (CASE) is a community-developed ontology designed to serve as a standard for interchange, interoperability, and analysis of investigative information in a broad range of cyber-investigation domains, including digital forensic science, incident response, counter-terrorism, criminal justice, forensic intelligence, and situational awareness.
EXIF	Exchangeable image file format, a standard that specifies the formats for images, sound, and ancillary tags used by digital cameras (including smartphones), scanners and other systems handling image and sound files recorded by digital cameras.

List of Figures

List of Tables

Executive summary

This Deliverable, D2.3 “Reference digital forensics Domain Model” (hereinafter ‘Deliverable D2.3’), illustrates the forensics domain model/data for types of evidence commonly used during an investigation, and demonstrates how this model represents the Forensic Artifacts[1] extracted by the most popular and powerful digital forensic tools, commercial and free ones, currently available to all involved stakeholders.

To accomplish the aforementioned objectives the following activities have been carried out:

- Collected a large dataset of forensic images, which are complete copies of data stored on mobile devices and hard drives. These images are freely available to researchers, forensic experts, forensic tools vendors and the data is fictitious, therefore, there is no issue from the privacy perspective (see Sections 1.2 and 1.3)
- Selected a set of mobile and computer forensic tools to process those forensic images and to extract Cyber items from the dataset (see Section 2)
- Exported a set of XML reports containing the Cyber items extracted by the selected forensic tools, and performed an analysis of these reports, including data and structure. The analysis of the XML reports supported the identification of the most suitable digital forensics model to adopt within the INSPECTr project, for each different type of Cyber item (see Section 3)
- Identified gaps in the CASE standard (see Appendix B) for representing Cyber items and collaborated with the CASE developer community to create change proposals that cover a wider range of evidence, specifically SQLite databases, URL History, and Contacts.
- Presented a brief analysis of other important Cyber items not included in the above study, in order to cover a wider range of evidence that can be encountered during an investigation. This last Section (see Section 4) explains Cyber items such as:
  - Windows “Jump Lists”: quick lists of recent applications or files that a user launched.
  - Windows “Recycle Bin”: items that were moved to the Recycle Bin.
  - Windows "USB Devices": a history of all USB devices that have been connected to the system.
  - Windows “Timeline Activity”: information about application usage, such as application start and end times and duration of usage.
  - Windows "Encryption/Anti-forensics Tools": the encryption or anti-forensics tool(s) that have been found in the searched evidence.
  - Windows "Virtual Machines": Virtual Machine files that have been found on the object being searched.
  - Android "Amazon Alexa Audio Activity": details about audio activity detected by the Amazon Alexa app.
- Dedicated a brief Section (Section 5) to a set of Cyber items that should be considered but that are strictly connected to specific operating system, actually each operating system, both desktop and mobile has peculiar Cyber items.
- Provided a representation of certain types of Cyber items in the standard language CASE (Appendix B) also providing a brief introduction to the CASE ontology.

The list of actions described above is depicted in Figure 1.

[1] Forensics artifacts are objects that have forensic value: any objects that contain data or evidence of something that occurred.

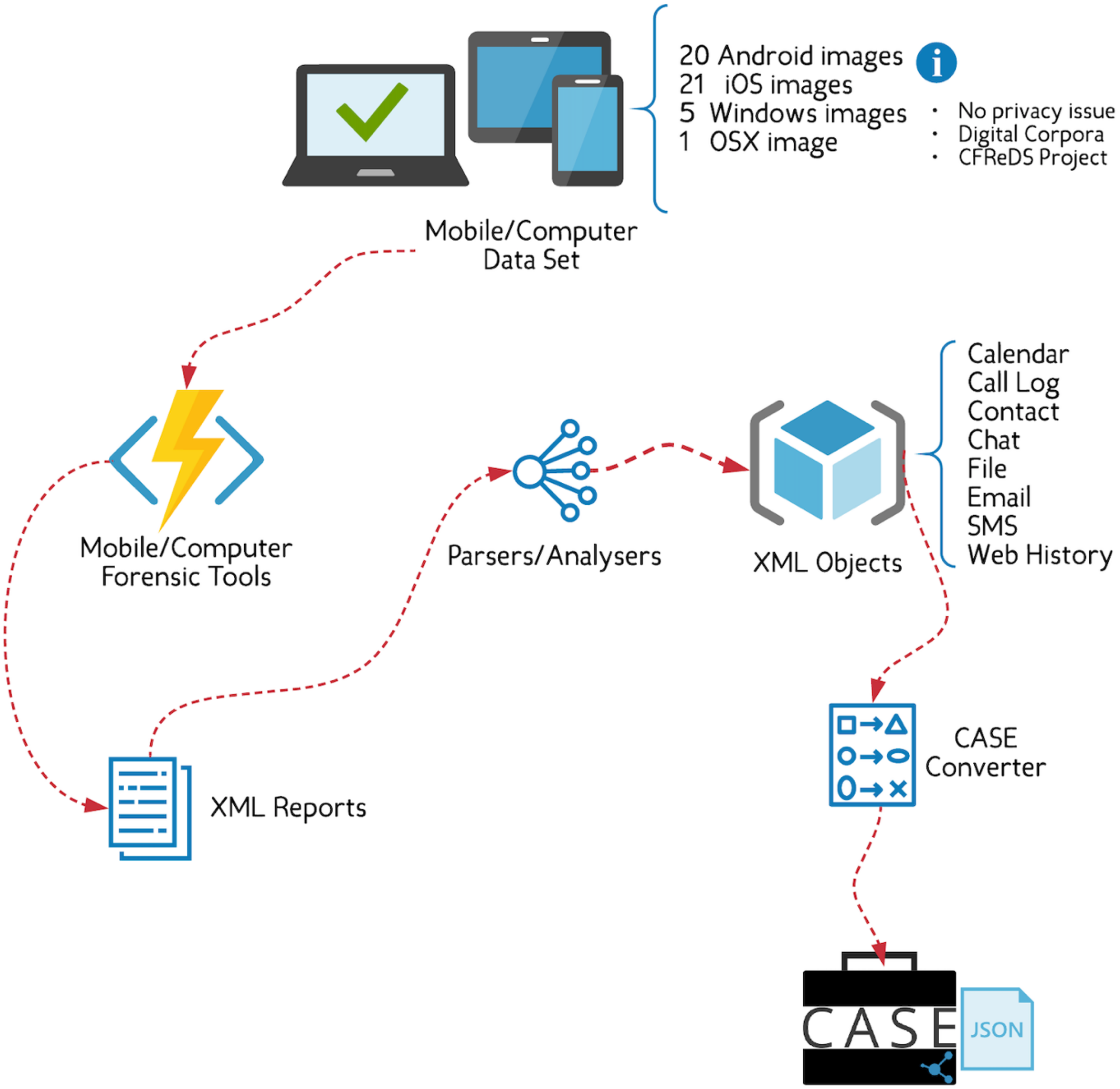

Figure 1: Actions carried out with the aim to determine the forensics domain model (SERE)

Finally, three Appendixes have been included in the present deliverable:

- Appendix A – Data set forensic images that illustrates full details about each image in the tailored data set
- Appendix B – CASE and Cyber items representation that provides a brief introduction to the ontology CASE and its representation of some Cyber items described in this deliverable, using the JSON serialization.
- Appendix C – AXIOM Artifacts Reference Table of Contents that presents the complex list of potentially extractable Artifacts from smartphone (Android, iOS and Windows Phone), Windows, OSX, Cloud and Kindle.

The content of this Deliverable D2.3 includes the following Section:

- Section 1: Data set. It describes the forensic images selected among the ones made available by varied forensic organization with the main aim to provide data for testing tools both in terms of completeness and reliability
- Section 2: Selected forensic tools. It illustrates the commercial tools that have been taken into consideration and the main reasons in support of this choice
- Section 3: Domain Forensic Model. It explains the model to cover the fundamental Cyber items processed during an investigation
- Section 4: Other important Cyber items. This Section describes some Cyber items that are relevant from an investigative point of view, but less fundamental compared with the ones illustrated in Section 3
- Section 5: Cyber items in future perspective. This section is dedicated to a set of Cyber items that should be considered but that are strictly connected to specific operating system.
- Appendix A - Data set forensic images
- Appendix B – Cyber item CASE representation.
- Appendix C -- Axiom Artifacts Reference: Table of Content.

1 Data set

In this section we provide a description of the collected dataset. The dataset is composed of forensic images made available on the following resources:

- Computer Forensic Reference Data Sets project (CFReDS)[2]
- Digital Corpora[3]
- Drone Forensics project[4]

All the provided data is fictitious, imaginary, so there is no issue at all from the privacy point of view, because the National Institute of Standards and Technology (NIST) that provides these datasets aims at offering the data to investigators for examination but they represent sets of simulated digital evidence. The gathered dataset is huge in size, it has about 300 GB.

The dataset is made up of 36 forensic acquisitions divided as follow:

- **Mobile devices**
    - 20 Android Images:
        - 14 downloaded from CFReDS Project; some of them contains two types of acquisition, one obtained via a JTAG approach and the other obtained via a Chip Off approach
        - 5 downloaded from Digital Corpora
        - 1 provided by UNIL
    - 8 iOS images:
        - 1 downloaded from Champlain College
        - 1 downloaded from Digital Corpora
        - 1 downloaded from CFReDS
        - 1 downloaded from Magnet Virtual Summit
        - 3 downloaded from Drone Forensics
        - 1 provided by Mattia Epifani
- **Computer device**
    - 5 Windows images
    - 1 OSX image

[2] https://www.cfreds.nist.gov/
[3] https://digitalcorpora.org/
[4] https://www.droneforensics.com/

1.1 Mobile device dataset

Details on Android mobile dataset are shown in *Table 1* below, for the URL where the images have been obtained and the corresponding SHA-256 value, see the *Appendix A.1* for further details:

ID	*Dataset*	*Phone model*	*OS*	*Acquisition mode*
01_HTC_Desire_626_Chip_Off	CFReDS	HTC Desire 626	6.0.1	Chip Off
02_HTC_Desire_S_Chip_Off	CFReDS	HTC Desire S	2.3.5	Chip Off
03_HTC_Desire_S_JTAG	CFReDS	HTC Desire S	2.3.5	JTAG
04_HTC_One_Mini_Chip_Off	CFReDS	HTC One Mini	4.4.2	Chip Off
05_HTC_One_Mini_JTAG	CFReDS	HTC One Mini	4.4.2	JTAG
06_HTC_One_XL_Chip_Off	CFReDS	HTC One XL	4.1.1	Chip Off
07_HTC_One_XL_JTAG	CFReDS	HTC One XL	4.1.1	JTAG
08_LG_K7_Chip_Off	CFReDS	LG K7	5.1.1	Chip Off
09_LG_E510_JTAG	CFReDS	LG Optimus	>= 2.3	JTAG
10_Moto_E_Chip_Off	CFReDS	Moto E	5.1	Chip Off
11_Samsung_S2_Chip_Off	CFReDS	Samsung S2	4.1.2	Chip Off
12_Samsung_S4_Chip_Off	CFReDS	Samsung S4	4.4.4	Chip Off
13_Samsung_S4_JTAG	CFReDS	Samsung S4	4.4.4	JTAG
14_ZTE_Z970_Chip_Off	CFReDS	ZTE Z970	4.4.4	Chip Off

ID	*Dataset*	*Phone model*	*OS*	*Acquisition mode*
15_LG_H790_UFED_NOUGAT	Digital Corpora	LG H790	7.1.2	UFED 4PC
16_LG_H790_UFED_OREO	Digital Corpora	LG H790	8.1	UFED 4PC
17_GOOGLE_G013A_PIE	Digital Corpora	G013A Pixel 3	9.0	UFED 4PC
18_GOOGLE_G013A_10	Digital Corpora	G013A Pixel 3	10	UFED 4PC
19_CROSSOVER	UNIL	Samsung SM-G925F	6.0.1	UFED 4PC
20_UFED_ANDROID_LGE_Nexus5	Digital Corpora	Nexus 5	6.0.1	Magnet Acquire

Table 1: Android mobile acquisition dataset

Details on iOS mobile dataset are shown in *Table 2* below, for the URL where the images have been obtained and the corresponding SHA-256 value, see the Appendix A:

ID	*Dataset*	*Device model*	*OS*	*Acquisition mode*
01_IPAD_IOS_9_3_5	Champlain College	iPad Third Gen	9.3.5	iOS Full File System
02_IPHONE_IOS_13_4_1	Digital Corpora	iPhone SE	13.4.1	iOS Full File System
05_IPHONE_IOS_4_3_1	CFReDS	iPhone 3GS	4.3.1	iOS Physical
06_IPHONE_IOS_12_4	Magnet Virtual Summit	iPhone XS	12.4	iOS Full File System
07_DF072_QYSEAE_FISH_P3	Drone Forensics	iPad Mini 4	11.4	iOS Backup
08_DF079_PARROT_ANAFI	Drone Forensics	iPad Mini 4	11.4	iOS Backup
09_DF082_MAVIC_2_ENTERPRISE	Drone Forensics	iPad Mini 4	11.4	iOS Backup

ID	*Dataset*	*Device model*	*OS*	*Acquisition mode*
10_IOS_IPHONE_7	Mattia Epifani	iPhone 7	10.0.1	unknown

Table 2: iOS mobile acquisition dataset

1.2 Computer device dataset

Details on Computer dataset, Windows and OSX operating systems, are shown in *Table 3* below, for the URL where the images have been obtained and the corresponding SHA-256 value, see the Appendix A:

ID	*Dataset*	*OS*	*Source type*	*Source size*	*Acquisition mode*
01_NARCOS_KOWHAI	Digital Corpora	Windows 10	Virtual Disk	30 GB	FTK Imager
02_NARCOS_ESTEBAN	Digital Corpora	Windows 10	Virtual Disk	30 GB	FTK Imager
03_NARCOS_FREDRICKSEN	Digital Corpora	Windows 10	Virtual Disk	30 GB	FTK Imager
04_OWL	Digital Corpora	Windows 10	Physical Disk	500 GB	Ewfacquire
05_CROSSOVER	UNIL	Windows 10	Physical Disk	128 GB	Tableau TD2u
01_TUCK	Digital Corpora	OS X	unknown	unknown	unknown

Table 3: Computer acquisition dataset, Windows and OSX operating systems

1.3 Pen Drive dataset

Details on Pen Drive dataset are shown in *Table 4* below, for the URL where the images have been obtained and the corresponding SHA-256 value, see the Appendix A:

ID	*Dataset*	*File system*	*Source size*	*Acquisition mode*

FALCON_LOGICUBE_R29_PC_E01_manner	Mattia Epifani	NTFS	56 GB	Falcon Logicube (E01)
FALCON_LOGICUBE_R30_Pendrive_DD_manner	Mattia Epifani	NTFS	56 GB	Falcon Logicube (DD)

2 Selected digital forensic tools

This document focuses on the commercial digital forensic tools, both for mobile devices and computer. The description of the model to cover the Cyber items involved relying on the analysis of the XML reports generated by the chosen forensic tools during the exporting process, a feature provided by each of the selected tools.

2.1 Mobile Forensic Tools

The mobile forensic tools used in this work were selected using the following criteria:

- survey provided within the INSPECTr project (see Appendix D)
- the direct experience of the digital forensic experts on the team responsible for this deliverable
- the availability of a regular license of this kind of tool, generally licenses are rather expensive
- based on a questionnaire, distributed to the potential users in other European projects[5]
- some market analysis[6]

Each acquisition of the forensic images described in Table 1 and Table 2 has been processed with the following four Mobile Forensic tools:

– *UFED Physical Analyzer* (v. 7.24, 7.32, 7.33, 7.37)
– *Oxygen Forensics Detective* (v. 12.0 and 12.4)
– *Magnet Axiom Process* (v. 3.4, 3.8 and 4.01)
– *MSAB XRY* (v. 4.4.0), the license expired at the end of 2019

For each tool, two different reports have been created: a report in XML format and a report in the proprietary format.

2.2 Computer Forensic Tool

The computer forensic tool used in this work was selected using the following criteria:

[5] Evidence project (GA 608185), deliverable D7.1 -Report on Prima Facie Size of the Market (http://www.evidenceproject.eu/the-activities/deliverables.html)

[6] See https://www.marketsandmarkets.com/Market-Reports/digital-forensics-market-230663168.html, https://www.researchandmarkets.com/reports/4480876/europe-digital-forensics-market-analysis-2017, https://www.thebusinesstimes.com/wp-content/uploads/4797-Global_Digital_Forensics_Market_Growth.pdf.

- the direct experience of the digital forensic experts of the team responsible for this deliverable
- the availability of regular license of this kind of tools, generally licenses are rather expensive

Each acquisition of the forensic images described in Table 3 has been processed with the following Computer Forensic tool:

- *Magnet Axiom Process* (v.3.8 and 4.01)

Other tools have been identified for the task, in particular the following ones:

- *EnCase Forensic* by Open Text
- *Forensic Toolkit* (*FTK*) by Access Data

2.3 Forensic Imaging Tool

To provide a wider range of scenarios, a forensic imaging tool named *Logicube by Falcon* has been added to the analysis of the domain model; this kind of tool has been selected due to the availability of a regular license at the disposal of the team responsible for this deliverable.

As in the case of the above digital forensic tools, two different reports have been created: a report in XML format and a report in the proprietary format.

The following sections describe the main data to be included in the domain forensic model, considering the different types of Cyber items, extracted by the aforementioned digital forensic tools.

3 Digital Forensics Domain Model

The model is divided into the most relevant Cyber items that is possible to extract from these kinds of evidence sources: mobile device, hard disks, USB pen drive.

Each field of the data model begins with the prefix **DFDM** that stands for Digital Forensic Domain Model, followed by the name of the **Cyber item**, followed by the name of the **field/data.** Unless otherwise stated, the data/field should be considered mandatory for the representation of the Cyber item.

3.1 Cyber item Calendar Entry

In the Table below the first column indicates the field of the data model related to the Calendar Entry Cyber item, the second column contains the meaning of the field.

Data model	Meaning
DFDM_CALENDAR_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_CALENDAR_status	**Status** of the item, the value indicates if the item has been parsed/extracted or carved.
DFDM_CALENDAR_category	**Category** of the Calendar item (optional).
DFDM_CALENDAR_subject	**Subject** of the Calendar item (optional).
DFDM_CALENDAR_s**tartDate**	The **Start Date** of the Calendar item.
DFDM_CALENDAR_end**Date**	The **End Date** of the Calendar item.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement No 833276

***DFDM_CALENDAR*_repeatUntil**	**Repeat Until Date** of the Calendar item (optional).
***DFDM_CALENDAR*_repeatDay**	**Repeat Day** of the Calendar item (optional).
***DFDM_CALENDAR*_repeatInterval**	The **Repeat Interval** of the Calendar item (optional).

Table 4: Cyber item Calendar, data model field and their meaning

In Figure 1 is represented the hierarchical structure of the Calendar Cyber item, from the XML report generated by AXIOM Process[7] along with some of the data model fields indicated in Table 4.

[7] In this Deliverable the MAGNET AXIOM XML reports have been considered due their clear and well documented structure.

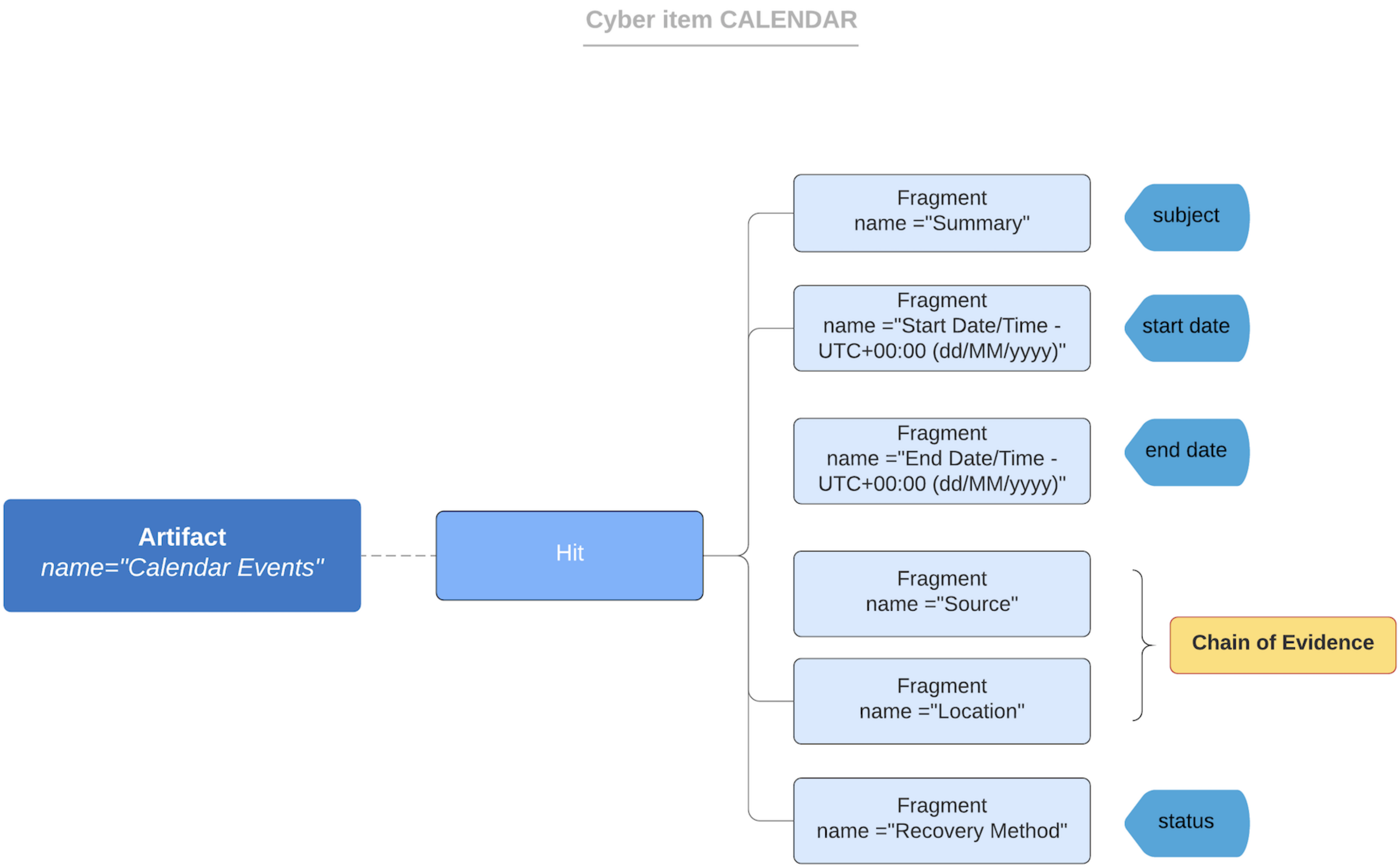

Figure 1: Cyber item Calendar, XML element hierarchical structure and data model

3.2 Cyber item Call

In the Table below the first column indicates the field of the data model related to the Call Cyber item, the second column contains the meaning of the field.

Data model	Meaning
DFDM_CALL_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_CALL_status	**Status** of the item, the value indicates if the item has been parsed/extracted or carved.
DFDM_CALL_source	**Source** of the Cyber item, it represents the application used to make the call. It may assume the value "Native" if it represents a regular Call, made with the system application.
DFDM_CALL_direction	**Direction** indicates if the Call has been Incoming or Outgoing.
DFDM_CALL_time	**Time** of the Call item
DFDM_CALL_duration	**Duration** of the Call item (optional).
DFDM_CALL_outcome	**Outcome** of the Call item, possible values are: Established, Missed, NotEstablished, UnknowReason, etc (optional)
DFDM_CALL_name	**Name** of the person involved in the Call (optional)
DFDM_CALL_identifier	**Identifier** of the person involved in the Call. A phone number or an application account.

Table 5: Cyber item Call, data model field and their meaning

In Figure 2 is represented the hierarchical structure of the Call Cyber item, from the XML report generated by AXIOM Process along with some of the data model fields indicated in Table 5.

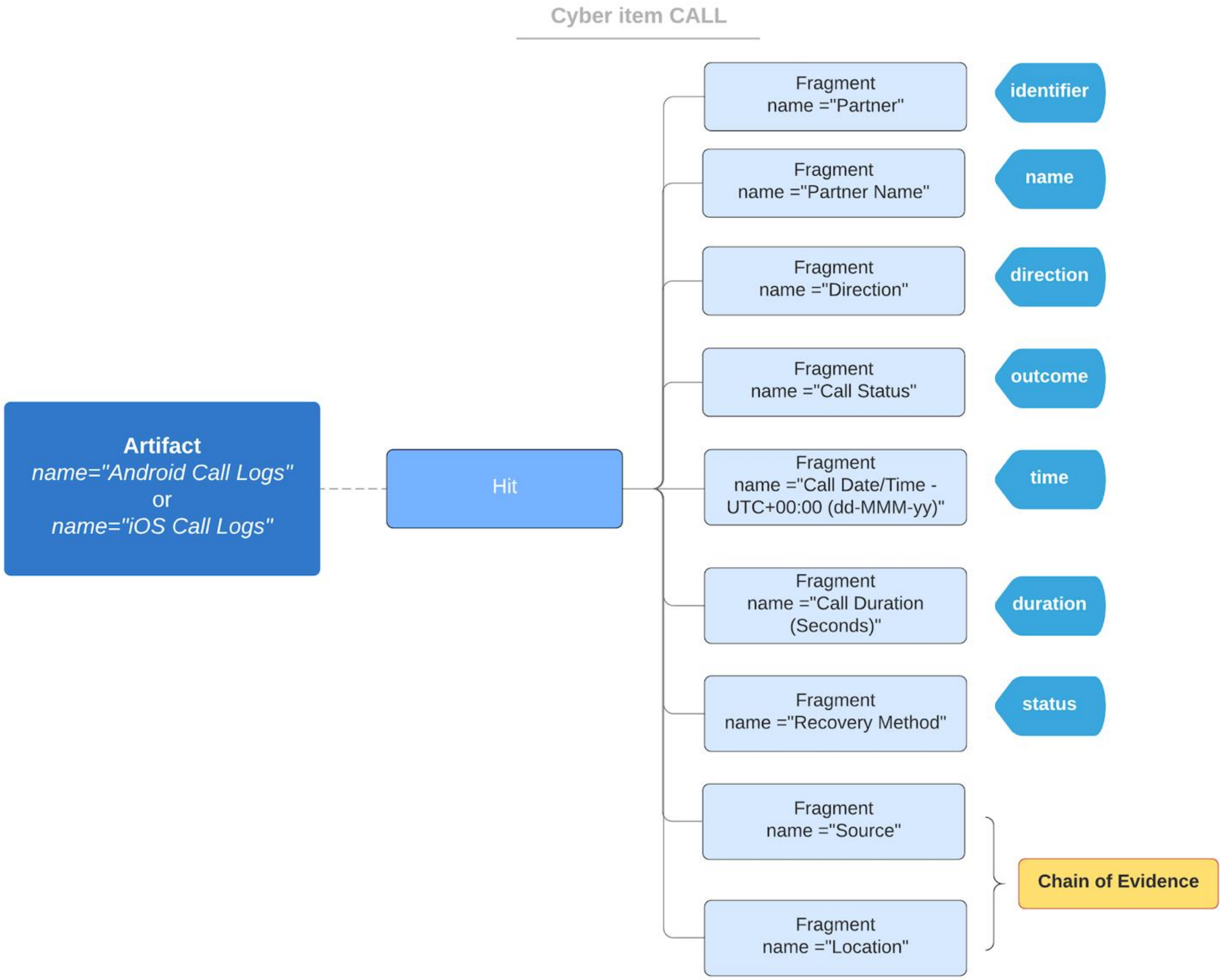

Figure 2: Cyber item Call, XML element hierarchical structure and data model

In Appendix B.2 a representation in CASE-JSON of the Cyber item Call is provided.

3.3 Cyber item Chat

In the Table below the first column indicates the field of the data model related to the Chat Cyber item, the second column contains the meaning of the field.

Data model	Meaning
DFDM_CHAT_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_CHAT_status	**Status** of the item, the value indicates if the item has been parsed/extracted or carved.
DFDM_CHAT_source	**Source** of the Cyber item, it represents the application used to make the call.
DFDM_CHAT_identifierFrom	**Participant Identifier FROM** side, within a single message of the Chat entry.
DFDM_CHAT_nameFrom	**Participant Name FROM** side, within a single message of the Chat item (optional).
DFDM_CHAT_identifierTo	**Participant Identifier TO** side, within a single message of the Chat item.
DFDM_CHAT_nameTo	**Participant Name TO** side, within a single message of the Chat item (optional).
DFDM_CHAT_timeReceived	The **Time** of the item Message received
DFDM_CHAT_timeSent	**Time** of the item Message sent

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 833276

DFDM_CHAT_body	**Body** of the Message item.
DFDM_CHAT_attachment	**Attachment** of the Message (optional).
DFDM_CHAT_attachmentUrl	**URL** of attachment (optional).
DFDM_CHAT_outcome	**Outcome** of the Message item (optional).

Table 6: Cyber item Chat, data model field and their meaning

In Figure 3 is represented the hierarchical structure of the Chat Cyber item, from the XML report generated by AXIOM Process along with some of the data model fields indicated in Table 6.

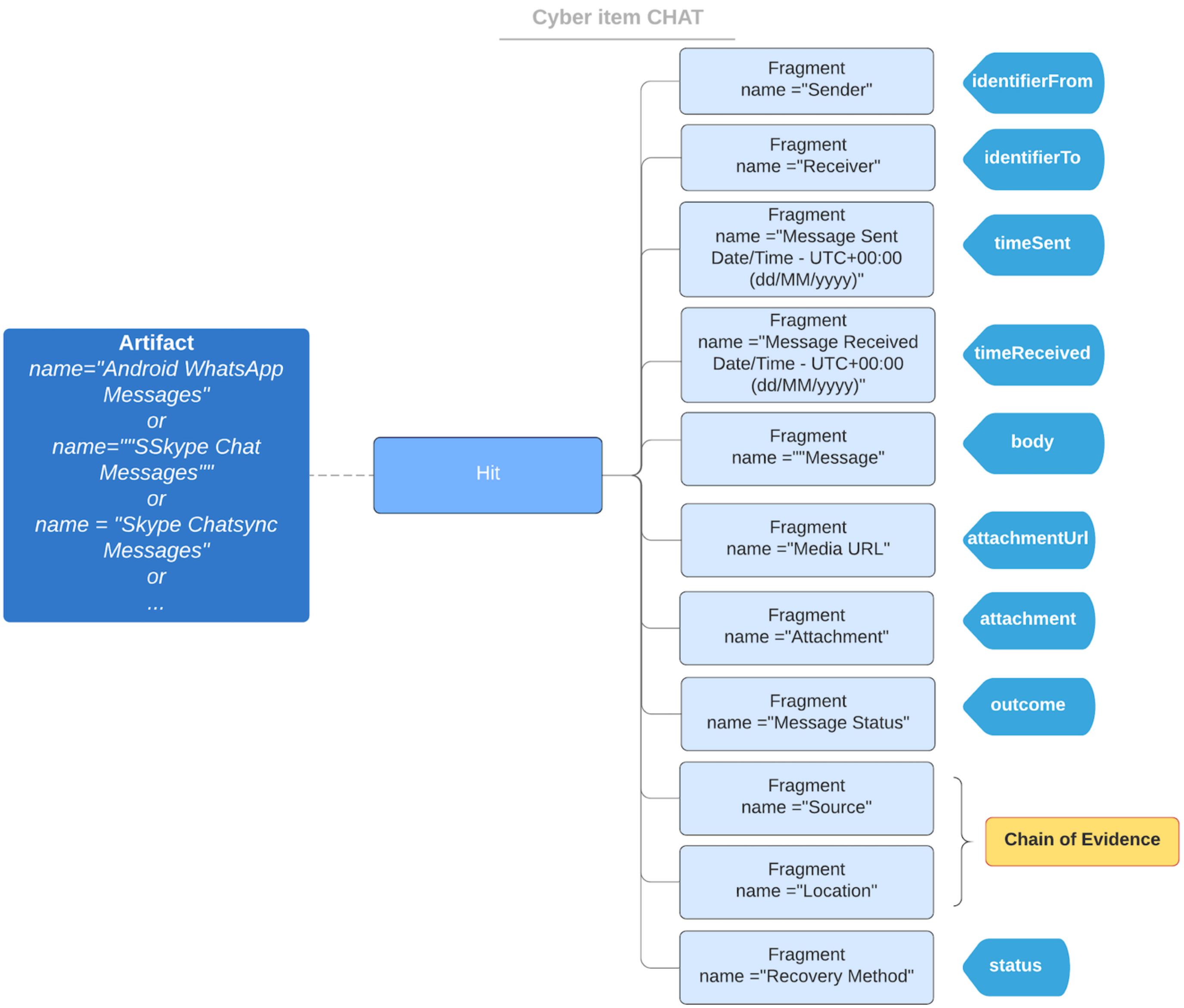
Cyber item CHAT
Artifact
name="Android WhatsApp Messages"
or
name=""SSkype Chat Messages""
or
name = "Skype Chatsync Messages"
or
...
Hit
Fragment name ="Sender"
identifierFrom
Fragment name ="Receiver"
identifierTo
Fragment name ="Message Sent Date/Time - UTC+00:00 (dd/MM/yyyy)"
timeSent
Fragment name ="Message Received Date/Time - UTC+00:00 (dd/MM/yyyy)"
timeReceived
Fragment name =""Message"
body
Fragment name ="Media URL"
attachmentUrl
Fragment name ="Attachment"
attachment
Fragment name ="Message Status"
outcome
Fragment name ="Source"
Fragment name ="Location"
Chain of Evidence
Fragment name ="Recovery Method"
status

Figure 3: Cyber item Chat, XML element hierarchical structure and data model

In Appendix B.3 a representation in CASE-JSON of the Cyber item Chat is provided.

3.4 Cyber item Contact

In the Table below the first column indicates the field of the data model related to the Contact Cyber item, the second column contains the meaning of the field.

Data model	Meaning
DFDM_CONTACT_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_ CONTACT _status	**Status** of the item, the value indicates if the item has been parsed/extracted or carved.
DFDM_ CONTACT _source	**Source** of the Cyber item, it represents the application used to make the call.
DFDM_ CONTACT _name	**Name** of the Contact Entry represents the name of the Contact.
DFDM_ CONTACT _phoneNumber	**Phone Number** of the Contact. The entry may contain more than one phone number.
DFDM_ CONTACT _timeContacted	**Time Contacted** represents the Time when the Contact entry has been called/contacted (optional).
DFDM_ CONTACT _timeCreated	**Time Create** represents the Time when the Contact entry has been created (optional).
DFDM_ CONTACT _email	**Email** of the Contact entry (optional).
DFDM_ CONTACT _address	**Address** of the Contact entry (optional).

Table 7: Cyber item Contact, data model field and their meaning

In Figure 4 is represented the hierarchical structure of the Contact Cyber item, from the XML report generated by AXIOM Process along with some of the data model fields indicated in Table 7.

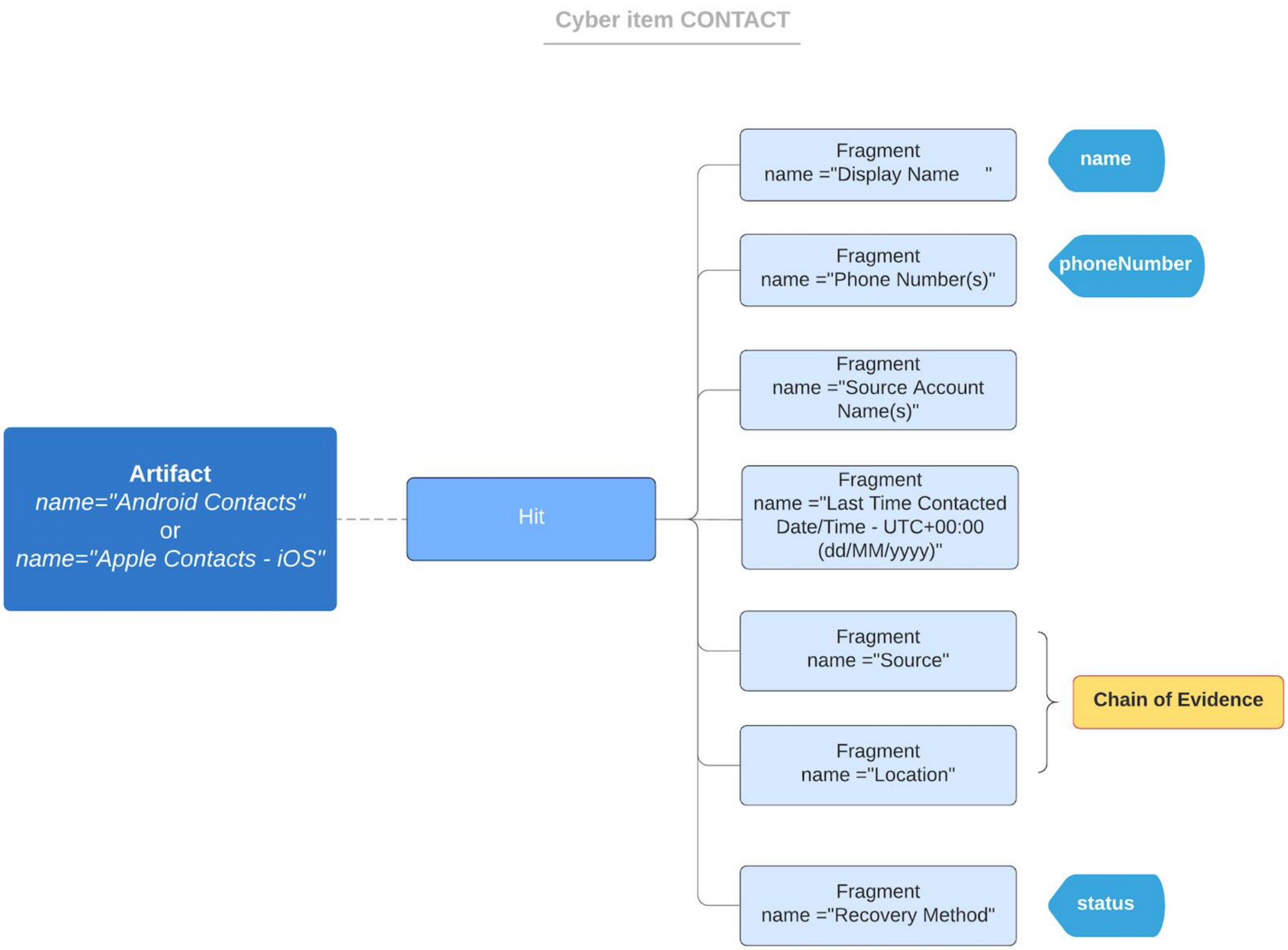

Figure 4: Cyber item Contact, XML elements hierarchical structure and data model

In Appendix B.4 a representation in CASE-JSON of the Cyber item Contact is provided.

3.5 Cyber item Email

In the Table below the first column indicates the field of the data model related to the Email Cyber item, the second column contains the meaning of the field.

Data model	Meaning
DFDM_EMAIL_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_EMAIL _status	**Status** of the item, the value indicates if the item has been parsed/extracted or carved.
DFDM_EMAIL _source	**Source** of the Cyber item, it represents the application used to make the call.
DFDM_EMAIL _addressFrom	**Address From** of the Cyber item represents the Sender of the message.
DFDM_EMAIL _addressTo	**Address To** of the Cyber item represents the Recipient(s) of the messages. It may contain a list of addresses.
DFDM_EMAIL _addressCc	**Address Cc** of the Cyber item represents additional Recipient(s) of the messages. It may contain a list of addresses
DFDM_EMAIL _addressBcc	**Address Bcc** of the Cyber item represents additional Recipient(s) of the messages, kept hidden. It may contain a list of addresses.
DFDM_EMAIL _subject	**Subject** of the Cyber item represents the Subject of the message.
DFDM_EMAIL _body	**Body** of the Cyber item represents the Subject of the message.

DFDM_EMAIL _time	**TimeStamp** of the Cyber item represents the Date and Time of the email message.
DFDM_EMAIL _attachment	**Attachment** of the Cyber item represents the Attachment file (optional).
DFDM_EMAIL _ attachmentMD5	The **MD5** of the attached file (optional).

Table 8: Cyber item Email, data model field and their meaning

In Figure 5 is represented the hierarchical structure of the Email Cyber item, from the XML report generated by AXIOM Process along with some of the data model fields indicated in Table 8.

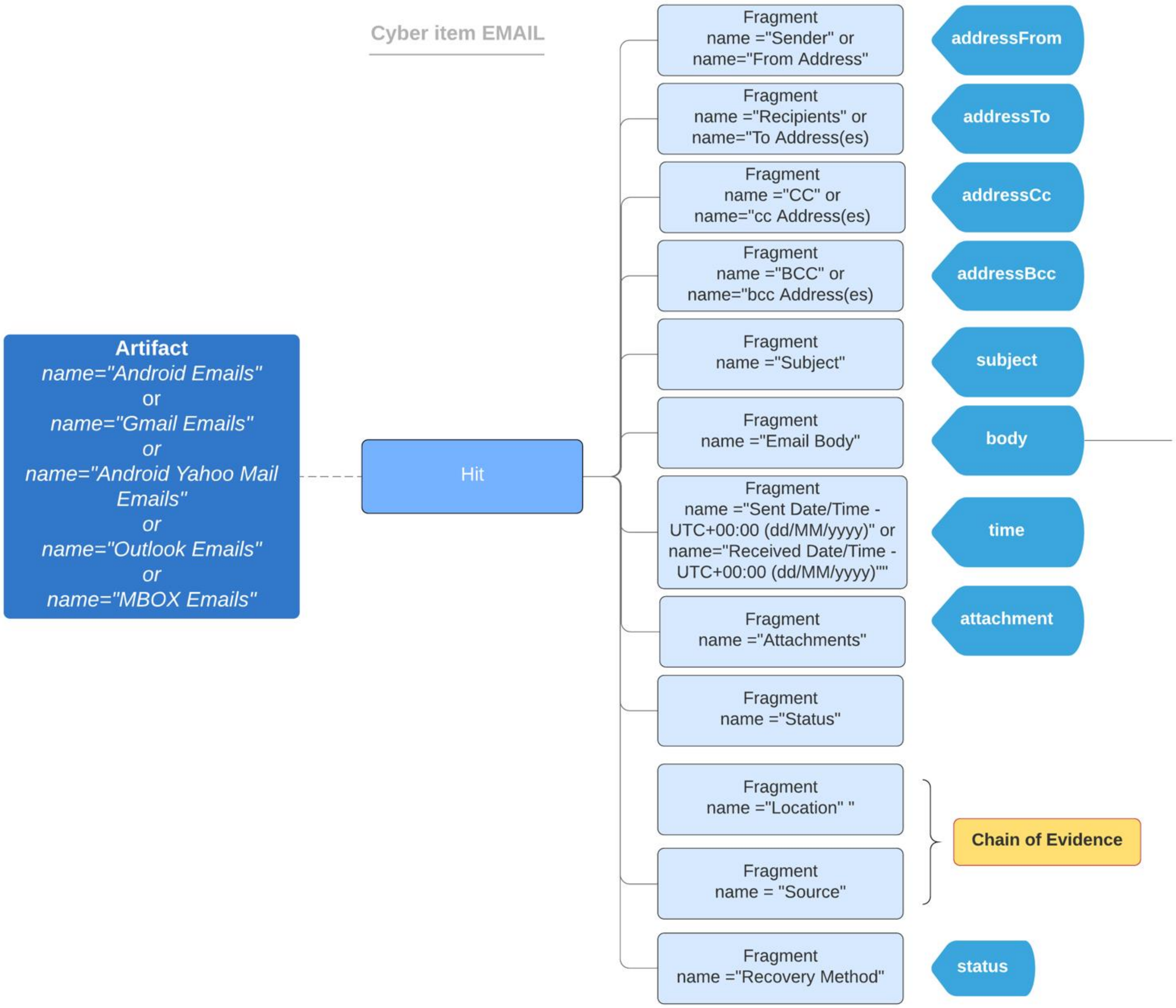

Figure 5: Cyber item Email, XML elements hierarchical structure and data model

In Appendix B.5 a representation in CASE-JSON of the Cyber item Email is provided.

3.6 Cyber item File

In the Table below the first column indicates the field of the data model related to the File Cyber item, the second column contains the meaning of the field. There is a special kind of file, images equipped with the Exchangeable image file format (EXIF, according to JEIDA/JEITA/CIPA specifications)[8] to which a separated section has been dedicated

Data model	Meaning
DFDM_FILE_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_ FILE _status	**Status** of the item, the value indicates if the item has been parsed/extracted or carved.
DFDM_ FILE _name	**File name** of the File item. It contains the whole path to the file in the original source of evidence (device).
DFDM_ FILE _size	**Size** of the File item.
DFDM_ FILE _localPath	**Local path** of File item. It represents the local folder created by the tool during the export in an open format (XML, CSV, etc.).
DFDM_ FILE _kind	**Kind** of file, possible values: Application, Archives, Audio, Configuration, Database, Image, Text, Video (optional).
DFDM_ FILE _sha1	**SHA-1** of the File item, not always present (optional).
DFDM_ FILE _sha2	**SHA-2** of the File item, not always present (optional).

[8] EXIF stands for "Exchangeable Image File Format", the definition first given by Japan Camera Industry Association (JCIA) in 1985. The standard is managed by Japan Electronics and Information Technology Industries Association (JEITA) as of today. EXIF is a standard for the specifications of image and sound formats mainly used by digital cameras and scanners. It contains data such as: Manufacture, Time zone, Model, Camera Serial Number, GPS Longitude, GPS Latitude.

DFDM_ FILE _md5	**MD5** of the File item, not always present (optional).
DFDM_ FILE _inodeNum	**Inode number** of the File item (optional).
DFDM_ FILE _inodeModify	**Inode modify time** of the File item (optional).
DFDM_ FILE _gid	**Owner GID** time of the File item (optional).
DFDM_ FILE _uid	**Owner UID** time of the File item (optional).
DFDM_ FILE _timeCreation	**Creation** time of the File item.
DFDM_ FILE _timeModification	**Modification** time of the File item.
DFDM_ FILE _timeAccess	**Access** time of the File item.

Table 9: Cyber item File, data model field and their meaning

In Figure 6 is represented the hierarchical structure of the Email Cyber item, from the XML report generated by AXIOM Process along with some of the data model fields indicated in Table 9.

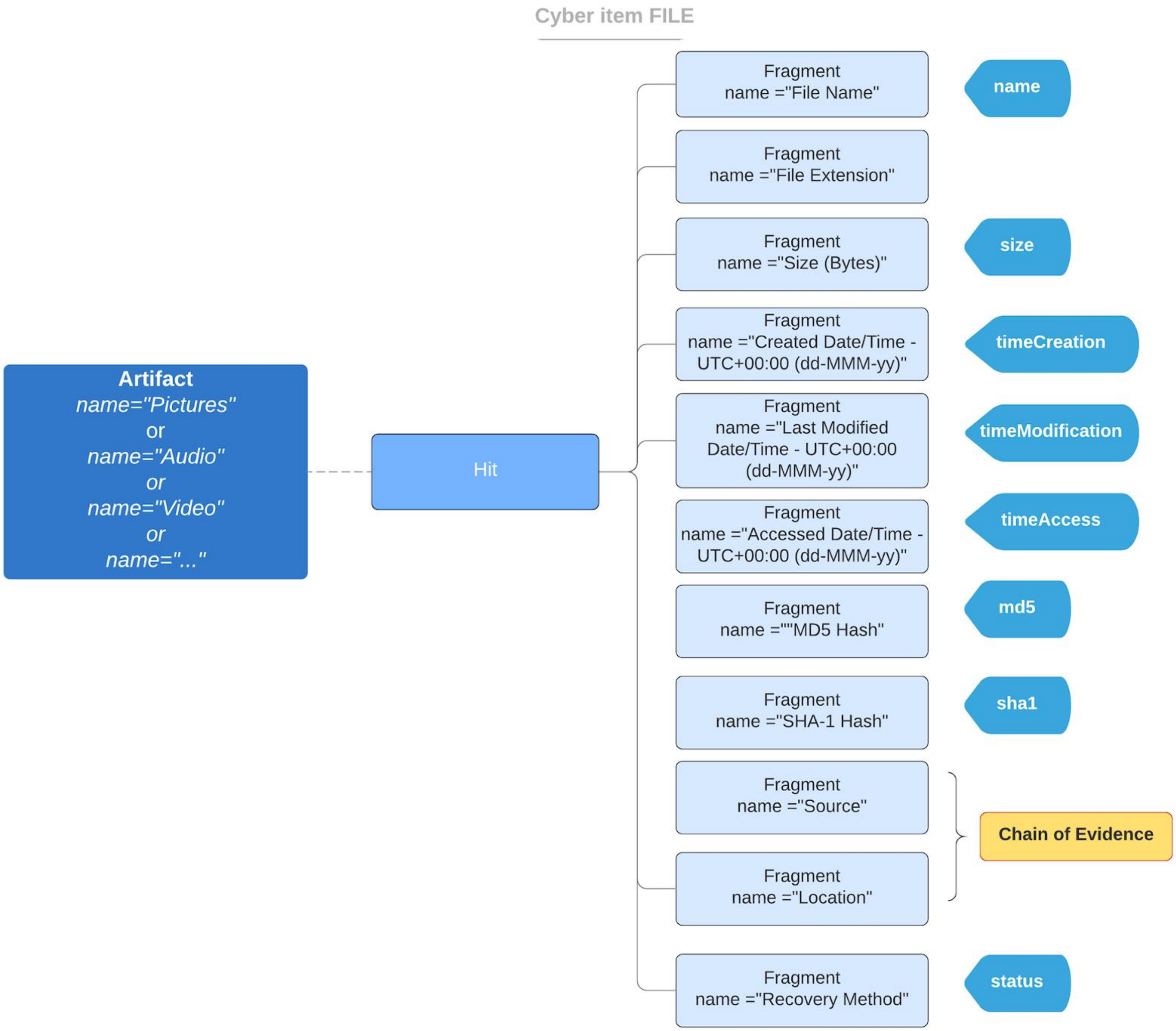

Figure 6: Cyber item File, XML element hierarchical structure and data model

In Appendix B.6 a representation in CASE-JSON of the Cyber item File is provided.

3.7 Cyber item Geolocation position

This represents the last known locations of an Android device, as tracked by the GPS receiver and recovered using *dumpsys*[9]. In the Table below the first column indicates the field of the data model related to the Geolocation Cyber item, the second column contains the meaning of the field.

Data model	Meaning
DFDM_Geolocation_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_Geolocation_status	**Status** of the item, the value indicates if the item has been parsed/extracted or carved.
DFDM_Geolocation_latitude	**Latitude** of the location.
DFDM_Geolocation_longitude	**Longitude** of the location.
DFDM_Geolocation_timestamp	**Date and time** of the stored GPS position.

Table 10: Cyber item GPS Position, data model field and their meaning

[9] dumpsys is a tool that runs on Android devices and provides information about system services. It is possible to run dumpsys from the command line using the Android Debug Bridge (ADB) to get diagnostic output for all system services running on a connected device.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 833276

3.8 Cyber item Picture/Video

In the Table below the first column indicates the field of the data model related to the Picture or Video cyber item, the second column contains the meaning of the field.

Data model	Meaning
DFDM_FILE_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_ FILE _status	**Status** of the item, the value indicates if the item has been parsed/extracted or carved.
DFDM_ FILE _source	**Source** of the Cyber item, it represents the application used to make the call.
DFDM_ FILE _name	**File name** of the File item. It contains the whole path to the file in the original source of evidence (device).
DFDM_ FILE _size	**Size** of the File item**.**
DFDM_ FILE _localPath	**Local path** of File item. It represents the local folder created by the tool during the export in an open format (XML, CSV, etc.).
DFDM_ FILE _kind	**Kind** of file, possible values: Application, Archives, Audio, Configuration, Database, Image, Text, Video (optional.
DFDM_ FILE _sha1	**SHA-1** of the File item, not always present (optional.
DFDM_ FILE _sha2	**SHA-2** of the File item, not always present (optional.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 833276

DFDM_ FILE _md5	**MD5** of the File item, not always present (optional.
DFDM_ FILE _inodeNum	**Inode number** of the File item (optional.
DFDM_ FILE _inodeModify	**Inode modify time** of the File item (optional.
DFDM_ FILE _gid	**Owner GID** time of the File item (optional.
DFDM_ FILE _uid	**Owner UID** time of the File item (optional.
DFDM_ FILE _timeCreation	**Creation** time of the File item.
DFDM_ FILE _timeModification	**Modification** time of the File item.
DFDM_ FILE _timeAccess	**Access** time of the File item.
DFDM_ FILE _exifTimeCreation	**Date** and **time** when the picture has been first taken (from EXIF data).
DFDM_ FILE _exifTimeModification	**Date** and **time** when the picture has been modified.
DFDM_ FILE _exifTimezone	**Timezone** setting on the camera at the time when the picture has been taken.
DFDM_ FILE _exifManufacturer	**Manufacturer** of the camera used to take the picture.
DFDM_ FILE _exifModel	**Model** of the camera used to take the picture.

DFDM_ FILE _exifGpsLongitude	**GPS Longitude** coordinates of where the picture has been taken.
DFDM_ FILE _exifGpsLatitude	**GPS Latitude** coordinates of where the picture has been taken.

Table 10: Cyber item Picture/Video, data model field and their meaning

In Figure 7 is represented the hierarchical structure of the Picture/Video cyber item, from the XML report generated by AXIOM Process along with some of the data model fields indicated in Table 10. Only the EXIF data are shown in the figure, the others have been already illustrated in Figure 6.

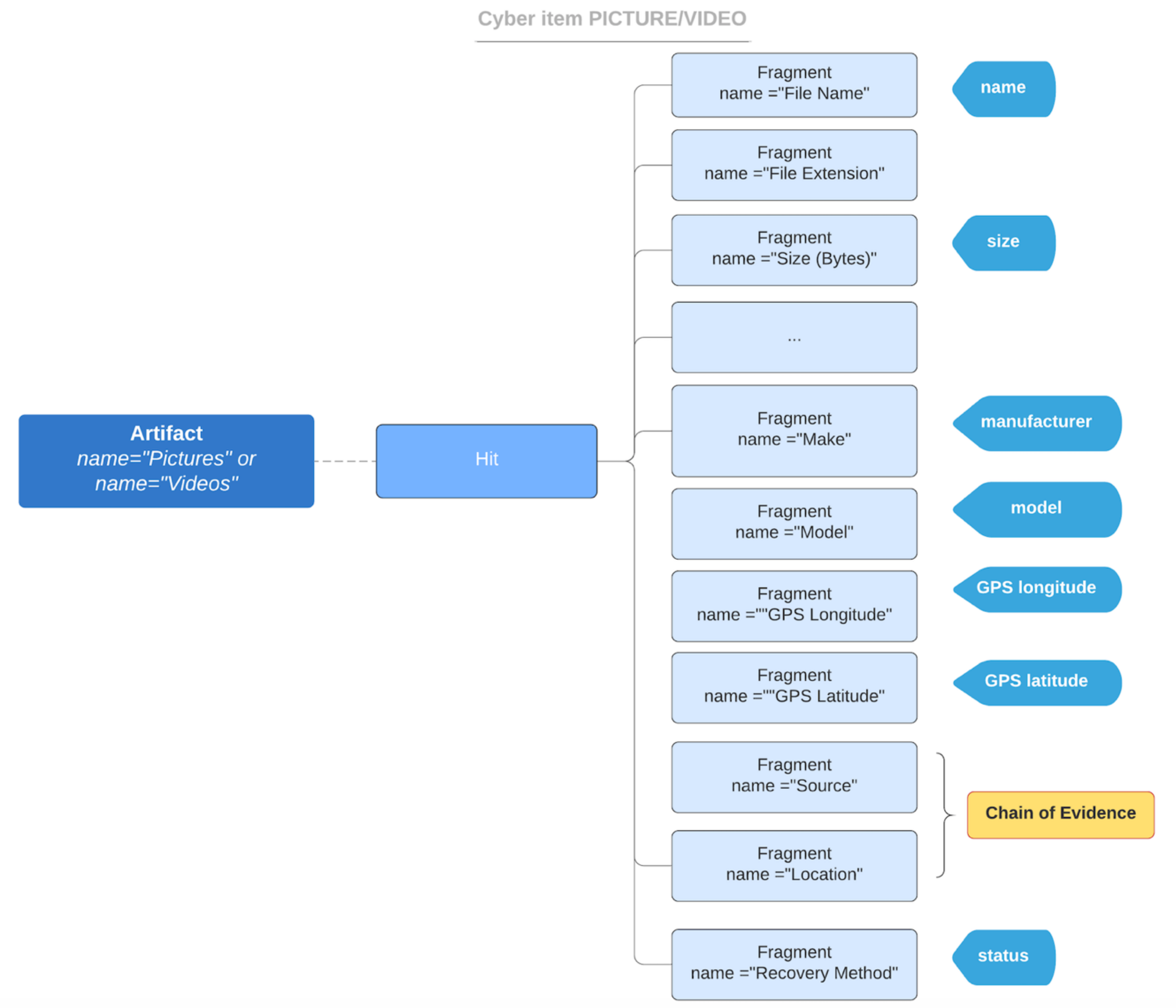

Figure 7: Cyber item Picture/Video, some XML element hierarchical structure and data model

In Appendix B.7 a representation in CASE-JSON of the cyber item File (Picture EXIF) is provided.

3.9 Cyber item SMS

In the Table below the first column indicates the field of the data model related to the SMS cyber item, the second column contains the meaning of the field.

Data model	Meaning
DFDM_SMS_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_ SMS _status	**Status** of the item, the value indicates if the item has been parsed/extracted or carved.
DFDM_ SMS _source	**Source** of the Cyber item, it represents the application used to send the SMS.
DFDM_ SMS _time	**Time** of the SMS entry represents the Date/Time when the SMS has been sent/received.
DFDM_ SMS _outcome	**Outcome** of the SMS entry, possible values [Read, Unread, Sent, Unsent].
DFDM_ SMS _role	**Role** of the SMS entry, see **{SMS_FOLDER}** field
DFDM_ SMS _sender	**Sender** of the SMS entry.
DFDM_ SMS _recipient	**Recipient** of the SMS entry.
DFDM_ SMS _name	**Name** of the SMS item, may contain a name or a phone number.

DFDM_ SMS _direction	**Direction** of the SMS entry indicates if the SMS has been sent or received, possible values: Incoming, Outgoing, Queued, etc.
DFDM_ SMS _body	**Body** of the SMS entry indicates the body of the SMS.

Table 10: Cyber item SMS, data model field and their meaning

In Figure 7 is represented the hierarchical structure of the Email cyber item, from the XML report generated by AXIOM Process along with some of the data model fields indicated in Table 10.

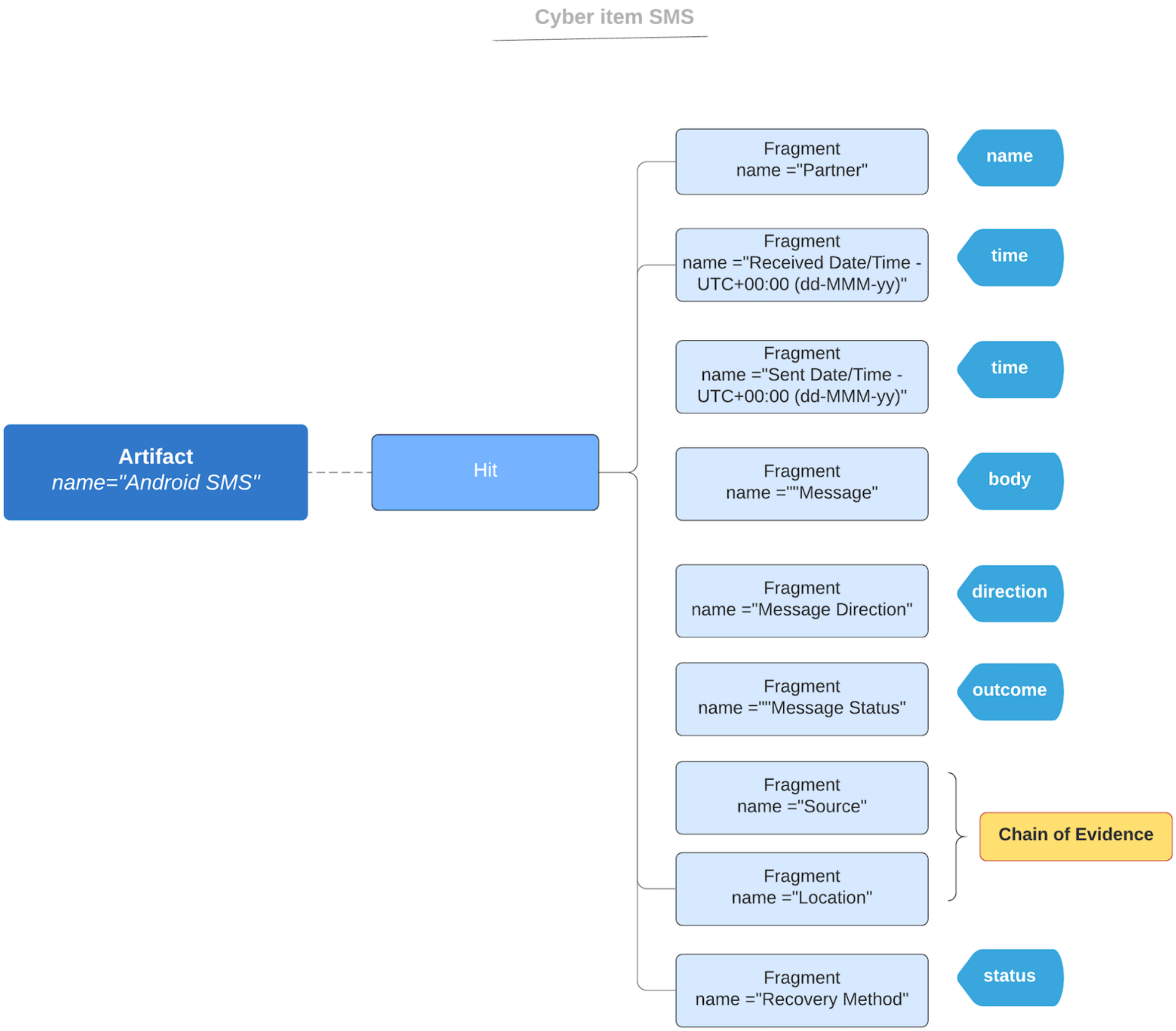

Figure 7: Cyber item SMS, XML elements hierarchical structure and data model

In Appendix B.8 a representation in CASE-JSON of the cyber item SMS is provided.

3.10 Cyber item URL History

In the Table below the first column indicates the field of the data model related to the URL History Cyber item, the second column contains the meaning of the field.

Data model	Meaning
DFDM_WEB_HISTORY_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_ WEB_HISTORY_status	**Status** of the item, the value indicates if the item has been parsed/extracted or carved.
DFDM_ WEB_HISTORY_source	**Source** of the Cyber item, it represents the web browser used to reach the URL address.
DFDM_ WEB_HISTORY_url	**Url** of the Web Page item represents the web address visited with the browser.
DFDM_ WEB_HISTORY_title	**Title** of the Web Page item represents the web address visited with the browser.
DFDM_ WEB_HISTORY_visitCount	**Visit Count** of the Web Page item represents the number of visit to the Url.
DFDM_ WEB_HISTORY_lastVisited	**Last Visited** of the Web Page item represents the last Time Stamp when the Url has been visited.

Table 11: Cyber item Web History, data model field and their meaning

In Figure 8 is represented the hierarchical structure of the URL History Cyber item, from the XML report generated by AXIOM Process along with some of the data model fields indicated in Table 11.

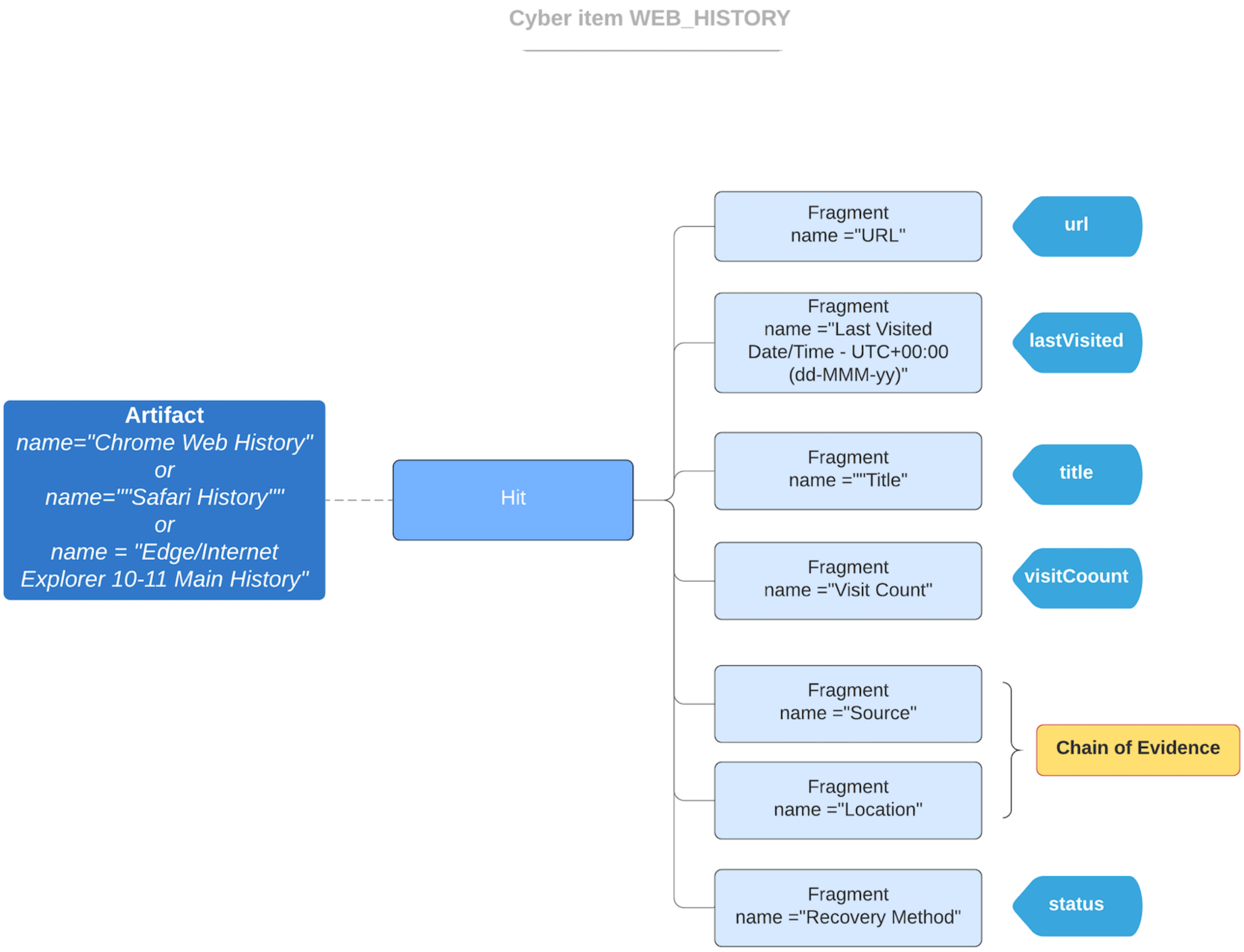

Figure 8: Cyber item Web History, XML element hierarchical structure and data model

In Appendix B.9 a representation in CASE-JSON of the cyber item URL History is provided.

3.11 Cyber item Web Visit

In the Table below the first column indicates the field of the data model related to the Web Visit cyber item, the second column contains the meaning of the field.

Data model	Meaning
DFDM_WEB_VISIT_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_WEB_VISIT_status	**Status** of the item, the value indicates if the item has been parsed/extracted or carved.
DFDM_WEB_VISIT_source	**Source** of the Cyber item, it represents the application used to reach the URL.
DFDM_WEB_VISIT_url	**Url** of the Web Page item represents the web address visited with the browser.
DFDM_WEB_VISIT_title	**Title** of the Web Page item represents the web address visited with the browser.
DFDM_WEB_VISIT_lastVisited	**Last visited** date and time the webpage was last visited.
DFDM_WEB_VISIT_count	**Count** number of times the website was accessed by the user typing the URL.
DFDM_WEB_VISIT_transitionType	**Transition type** describes how the browser navigated to this URL. For instance if the page was visited by clicking a link on another page, the transition type is 'link'.
DFDM_WEB_VISIT_fromUrl	**From Url** in case the transition type is ‘link’, it represents the webpage from which the user comes from.

4 Other important Cyber items

This Section describes some Cyber items that are relevant from an investigative viewpoint, but less fundamental compared with the ones illustrated in Section 3. The INSPECTr team is in collaboration with the CASE community to ensure these Cyber items are fully covered.

4.1 Windows Jump Lists

Jump lists are lists of recent applications or files that a user launched, in the Table below the first column indicates the field of the data model related to the Jump List Cyber item, the second column contains the meaning of the field.

Data model	Meaning
DFDM_JUMP_LIST_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_JUMP_LIST_status	**Status** of the item, the value indicates if the item has been parsed/extracted or carved.
DFDM_JUMP_LIST _appID	**AppID** unique application identifier generated by Windows during the installation procedure.
DFDM_JUMP_LIST_appName	**ApplName** application name.
DFDM_JUMP_LIST_path	**Path** to the target file.
DFDM_JUMP_LIST_arguments	**Arguments** parameters passed to the target file.
DFDM_JUMP_LIST_volumeName	**Volume Name** where the shortcut resides.
DFDM_JUMP_LIST_timeCreated	**Date and Time** the shortcut target file was created.

DFDM_JUMP_LIST_timeModified	**Date and Time** the shortcut target file was modified.
DFDM_JUMP_LIST_timeAccessed	**Date and Time** the shortcut target file was accessed.

4.2 Windows LNK file[10]

In the Table below the first column indicates the field of the data model related to the Link files cyber item, the second column contains the meaning of the field.

Data model	Meaning
DFDM_LNK_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_LNK_status	**Status** of the item, the value indicates if the item has been parsed/extracted or carved.
DFDM_LNK_path	**Path** to the target file.
DFDM_LNK_arguments	**Arguments a**ny parameters passed to the target file.
DFDM_LNK_timeCreated	**Date and time t**he shortcut target file has been created.
DFDM_LNK_timeModified	**Date and time t**he shortcut target file has been modified.
DFDM_LNK_timeAccessed	**Date and time t**he shortcut target file has been accessed.

[10] LNK files are Windows shortcut files to other files on the system.

DFDM_LNK_showCommand	**showCommand** the manner the shortcut should show the target when opened (SW_ SHOWNORMAL, ... etc.).

Table 11: Cyber item LNK Filen, data model field and their meaning

In Figure 7 is represented the hierarchical structure of the Link Cyber item, from the XML report generated by AXIOM Process along with some of the data model fields indicated in Table 9.

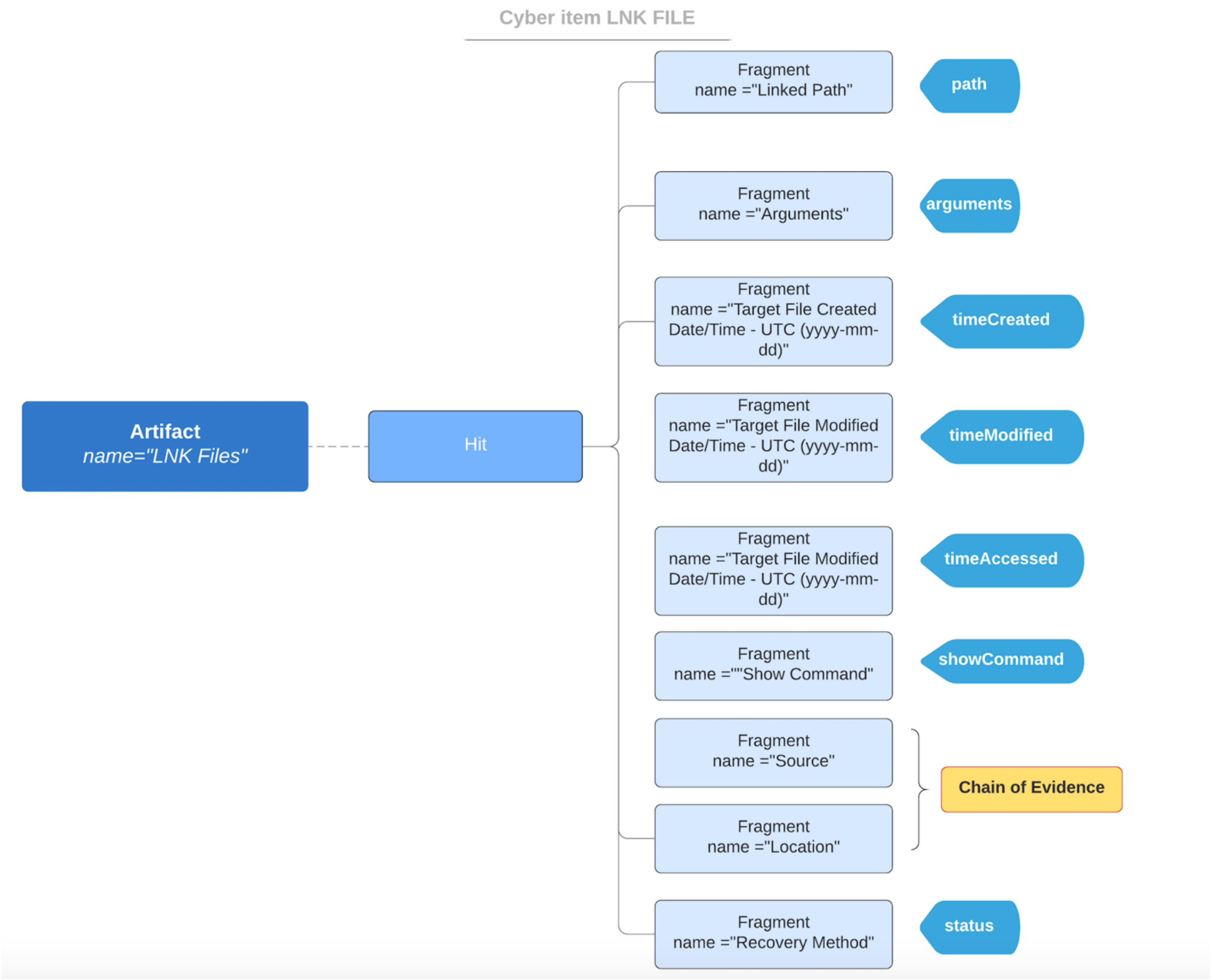

Figure 7: Cyber item LNK File, XML element hierarchical structure and data model

4.3 Windows Recycle Bin

Recycle Bins contains all items that have been moved to the Recycle Bin, in the Table below the first column indicates the field of the data model related to the Recycle Bin cyber item, the second column contains the meaning of the field.

Data model	Meaning
DFDM_RECYCLE_BIN_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_RECYCLE_BIN_status	**Status** of the item, the value indicates if the item has been parsed/extracted or carved.
DFDM_RECYCLE_BIN_fileName	**Filename** or folder that has been deleted.
DFDM_RECYCLE_BIN_deletedDate	**Date and time** the folder/file has been deleted.
DFDM_RECYCLE_BIN_originalPath	**Original Path** of the file/folder before removal.
DFDM_RECYCLE_BIN_type	**Type** indicates if the removed item is a file or a folder.

4.4 Windows USB Devices

USB Devices represents a history of all USB devices that have been connected to the system, in the Table below the first column indicates the field of the data model related to the USB Device Cyber item, the second column contains the meaning of the field.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement No 833276

Data model	Meaning
DFDM_USB_DEVICE_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_ USB_DEVICE_status	**Status** of the item, the value indicates if the item has been parsed/extracted or carved.
DFDM_ USB_DEVICE_serialNumber	**Serial Number** of the USB device.
DFDM_ USB_DEVICE_lastConnected	**Last Connected** date and time the device has been last connected to the computer.
DFDM_ USB_DEVICE_description	Description of the device.
DFDM_ USB_DEVICE_manufacturer	Manufacturer of the device.

4.5 Windows Encryption/Anti-forensics Tools

Encryption/Anti-forensics Tools includes the encryption or anti-forensics tools that have been found in the source of evidence, in the Table below the first column indicates the field of the data model related to the Anti-forensics Tool Cyber item, the second column contains the meaning of the field.

Data model	Meaning
DFDM_ANTI_FORENSIC_TOOLS_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_ANTI_FORENSIC_TOOLS_status	**Status** of the item, the value indicates if the item has been parsed/extracted or carved.

DFDM_ANTI_FORENSIC_TOOLS_fileName	**Filename** of the executable for the encryption or anti-forensics tool.
DFDM_ANTI_FORENSIC_TOOLS_timeCreated	**Date and Time** the encryption or anti-forensics tool has been created on the filesystem.
DFDM_ANTI_FORENSIC_TOOLS_timeModified	**Date and Time** the encryption or anti-forensics tool has been modified on the filesystem.
DFDM_ANTI_FORENSIC_TOOLS_timeAccessed	**Date and Time** the encryption or anti-forensics tool has been accessed on the filesystem.

4.6 Windows Virtual Machines

Virtual Machines contains the Virtual Machine files that have been found the source of evidence, in the Table below the first column indicates the field of the data model related to the Virtual Machine Cyber item, the second column contains the meaning of the field.

Data model	Meaning
DFDM_VM_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_VM_status	**Status** of the item, the value indicates if the item has been parsed/extracted or carved.
DFDM_VM_fileName	**Filename** of the virtual machine.
DFDM_VM_software	**Software** associated with the virtual machine.
DFDM_VM_timeCreated	**Date and Time** the virtual machine has been created on the filesystem.

DFDM_VM_timeModified	**Date and Time** the virtual machine has been modified on the filesystem.
DFDM_VM_timeAccessed	**Date and Time** the virtual machine has been accessed on the filesystem.

4.7 Windows Timeline Activity

Windows Timeline Activity describes information about application usage, in the Table below the first column indicates the field of the data model related to the Timeline Cyber item, the second column contains the meaning of the field.

Data model	Meaning
DFDM_TIMELINE_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_TIMELINE_status	**Status** of the item, the value indicates if the item has been parsed/extracted or carved.
DFDM_TIMELINE_appName	**Appname** name of the executable reporting the timeline data.
DFDM_TIMELINE_appContent	**Content** the executable was displaying.
DFDM_TIMELINE_appTimeStart	**Date** and **Time** the activity started.
DFDM_TIMELINE_appTimeEnd	**Date** and **Time** the activity ended.
DFDM_TIMELINE_timeCreated	**Date** and **Time** the entry has been created.

DFDM_TIMELINE_timeModified	**Date** and **Time** the entry has been modified.
DFDM_TIMELINE_timeAccessed	**Date** and **Time** the entry has been accessed.

4.8 Android Amazon Alexa Audio Activity

Amazon Alexa Audio Activity contains details about audio activity detected by the Amazon Alexa app, in the Table below the first column indicates the field of the data model related to the Alexa Cyber item, the second column contains the meaning of the field.

Data model	Meaning
DFDM_ALEXA_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_ALEXA_status	**Status** of the item, the value indicates if the item has been parsed/extracted or carved.
DFDM_ALEXA_text	**Text** spoken audio as interpreted by the Alexa app.
DFDM_ALEXA_timeCreated	**Date** and **Time** the audio has been recorded.
DFDM_ALEXA_url	**Url** *for the audio file.*

4.9 Memory

The extraction of Cyber items from Memory relies on Volatility[11], an open-source memory forensics framework for incident response and malware analysis. In this deliverable it will be considered the following Cyber items:

- Cmdscan
- Connscan
- Handles
- Netscan
- Plist
- Sockets

4.9.1 Command History (cmdscan)

The Cyber item Command History is related to the history of commands that are run in the Command Prompt and it is based on the utility *cmdscan*[12]. in the Table below the first column indicates the field of the data model related to the Command History cyber item, the second column contains the meaning of the field

Data model	Meaning
DFDM_CMD_HISTORY_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_CMD_HISTORY_processID	**Process ID**, or PID.
DFDM_CMD_HISTORY_processName	**Process Name**.
DFDM_CMD_HISTORY_location	**Location** in memory where the command is located.

[11] https://www.volatilityfoundation.org/#!25/c1f29.

[12] See https:// github.com/volatilityfoundation/volatility/wiki/Command-Reference#cmdscan for details.

DFDM_CMD_HISTORY_total	**Total** number of commands that are recovered.
DFDM_CMD_HISTORY_command	**Command** the string containing the command that was run.

4.9.2 Connection Scan (connscan)

The Cyber item Connection Scan contains information about network connections, both active and terminated, it is based on the utility *connscan*[13]. In the Table below the first column indicates the field of the data model related to the Connection Scan cyber item, the second column contains the meaning of the field

Data model	Meaning
DFDM_CONN_SCAN_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_CONN_SCAN_localAddress	**Local Address** local IP address (included the connection port)
DFDM_CONN_SCAN_remoteAddress	**Remote Address** local IP address (included the connection port).
DFDM_CMD_SCAN_processID	**Process ID**, or PID.

4.9.3 Handles (handles)

The Cyber item Handles shows the active handles in a process and it is based on the utility *handles*[14]. In the Table below the first column indicates the field of the data model related to the Handle cyber item, the second column contains the meaning of the field.

[13] For more information, see https:// github.com/volatilityfoundation/volatility/wiki/Command-Reference#connscan.

[14] For more information see https:// github.com/volatilityfoundation/volatility/wiki/Command-Reference#handles.

Data model	Meaning
DFDM_HANDLE_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_HANDLE_processID	**Process ID**, or PID.
DFDM_HANDLE_offset	**Offset** in memory.
DFDM_HANDLE_identifier	**Identifier** for the handle.
DFDM_HANDLE_type	**Type** of handle.
DFDM_HANDLE_details	**Details** additional info about the handle

4.9.4 Network info (netscan)

The Cyber item Network info allows to recover network details from memory, such as TCP or UDP listeners and endpoints and it is based on the utility *netscan*[15]. In the Table below the first column indicates the field of the data model related to the Network info cyber item, the second column contains the meaning of the field.

Data model	Meaning
DFDM_NET_INFO_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.

[15] For more information see https:// github.com/volatilityfoundation/volatility/wiki/Command-Reference#netscan.

DFDM_NET_INFO_localAddress	**Local Address** local IP address (included the connection port).
DFDM_NET_INFO_remoteAddress	**Remote Address** local IP address (included the connection port).
DFDM_NET_INFO_state	**State** of the connection.
DFDM_NET_INFO_creationTime	**Creation** date and time the connection was established.

4.9.5 Process (plist)

The Cyber item Process describes the processes that are loaded into memory and it is based on the utility *plist*[16]. In the Table below the first column indicates the field of the data model related to the Process info cyber item, the second column contains the meaning of the field.

Data model	Meaning
DFDM_PROCESS_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_PROCESS_processID	**Process ID**, or PID.
DFDM_PROCESS_processName	**Process Name**.
DFDM_PROCESS_processParent	**Process ID**, of the parent, or PPID.
DFDM_PROCESS_nThreads	**N Threads**, number of threads that the process contains.

[16] For more information see https:// github.com/volatilityfoundation/volatility/wiki/Command-Reference#pslist.

DFDM_PROCESS_startTime	**Start date and time**, date and time the process started.
DFDM_PROCESS_endTime	**End date and time**, date and time the process exited.

4.9.6 Sockets (sockets)

The Cyber item Sockets describes the info on the active and it is based on the utility *sockets*[17]. In the Table below the first column indicates the field of the data model related to the Sockets info cyber item, the second column contains the meaning of the field.

Data model	Meaning
DFDM_SOCKET_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_SOCKET_processID	**Process ID**, or PID.
DFDM_SOCKET_port	**Port** that was opened by the socket.
DFDM_SOCKET_protocol	**Protocol** that the socket is listening for.
DFDM_SOCKET_ip_address	**IP address** associated with the socket.
DFDM_SOCKET_creationTime	**Creation** date and time the socket was created.

[17] For more information see https:// github.com/volatilityfoundation/volatility/wiki/Command-Reference#sockets.

4.10 Windows/OSX iOS Backup

In this deliverable only iOS backup, potentially present on both Windows and OSX, are considered because the iOS backup presents a coherent structure, compared with the Android, where the kind of information may vary in a significant manner depending on the version and the model of smartphone. Therefore, it is easier to indicate the relevant Cyber item data. The kind of mobile backup considered are the following:

- iOS Address Book Backup
- iOS Calendar Events
- iOS Call Logs Backup
- iOS iMessage/SMS/MMS Backup
- iOS Notes
- iOS WhatsApp Messages

It's important to bear in mind that the CASE (see Appendix B) representation of the Cyber items will be the same as Section 3, and they will have a Relationship to show they are "Contained_Within" the iOS Backup.

4.10.1 iOS Address Book Backup

The Cyber item iOS Address Book Backup corresponds to the native iOS application for managing contacts. In the Table below the first column indicates the field of the data model related to the iOS Address Book Backup cyber item, the second column contains the meaning of the field.

Data model	Meaning
DFDM_IOS_BACKUP_ADDRESS_BOOK_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_IOS_BACKUP_ADDRESS_BOOK_status	**Status** of the item, the value indicates if the item has been parsed/extracted or carved.
DFDM_IOS_BACKUP_ADDRESS_BOOK_contactName	**Contact name**.

DFDM_IOS_BACKUP_ADDRESS_BOOK_creationTime	**Creation** date and time of the contact.
DFDM_IOS_BACKUP_ADDRESS_BOOK_modificationTime	**Modification** date and time of the contact.

4.10.2 iOS Calendar Events Backup

The Cyber iOS Calendar Events Backup corresponds to the native iOS application for managing meetings and appointments. In the Table below the first column indicates the field of the data model related to the iOS Calendar Events Backup cyber item, the second column contains the meaning of the field.

Data model	Meaning
DFDM_IOS_BACKUP_CALENDAR_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_IOS_BACKUP_CALENDAR_status	**Status** of the item, the value indicates if the item has been parsed/extracted or carved.
DFDM_IOS_BACKUP_CALENDAR_description	**Description** of the calendar appointment.
DFDM_IOS_BACKUP_CALENDAR_startDate	**Start date and time** of the calendar appointment.
DFDM_IOS_BACKUP_CALENDAR_endDate	**End date and time** of the calendar appointment.
DFDM_IOS_BACKUP_CALENDAR_location	**Location** of the calendar appointment.

4.10.3 iOS Call Logs Backup

The Cyber iOS Call Logs Backup corresponds to the native iOS application for keeping track of phone call data. In the Table below the first column indicates the field of the data model related to the iOS Call Logs Backup cyber item, the second column contains the meaning of the field.

Data model	Meaning
DFDM_IOS_BACKUP_CALL_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_IOS_BACKUP_CALL_status	**Status** of the item, the value indicates if the item has been parsed/extracted or carved.
DFDM_IOS_BACKUP_CALL_phoneNum	**Phone number** that was called.
DFDM_IOS_BACKUP_CALL_name	**Name** that was called.
DFDM_IOS_BACKUP_CALL_duration	**Duration** of the call.
DFDM_IOS_BACKUP_CALL_coutryCode	**Country Code** of the call.

4.10.4 iOS iMessage/SMS/MMS Backup

The Cyber iOS iMessage/SMS/MMS Backup corresponds to the native iOS application for communicating with other users through SMS and MMS messages. In the Table below the first column indicates the field of the data model related to the iOS iMessage/SMS/MMS Backup cyber item, the second column contains the meaning of the field.

Data model	Meaning
DFDM_IOS_BACKUP_SMS_MMS_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_IOS_BACKUP_SMS_MMS_status	**Status** of the item, the value indicates if the item has been parsed/extracted or carved.
DFDM_IOS_BACKUP_SMS_MMS_recipient	**Recipient** of the message.
DFDM_IOS_BACKUP_SMS_MMS_sender	**Sender** of the message.
DFDM_IOS_BACKUP_SMS_MMS_message	**Body** of the message.
DFDM_IOS_BACKUP_SMS_MMS_time	**Date time** of the sent/received message.
DFDM_IOS_BACKUP_SMS_MMS_attachment	**Attachment** of the message.

4.10.5 iOS Notes Backup

The Cyber iOS Notes Backup contains the notes from the iOS. In the Table below the first column indicates the field of the data model related to the iOS Notes Backup cyber item, the second column contains the meaning of the field.

Data model	Meaning
DFDM_IOS_BACKUP_NOTES_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_IOS_BACKUP_NOTES_status	**Status** of the item, the value indicates if the item has been parsed/extracted or carved.

DFDM_IOS_BACKUP_NOTES_title	**Title** of the note.
DFDM_IOS_BACKUP_NOTES_body	**Body** of the note.

4.10.6 iOS WhatsApp Messages Backup

The Cyber iOS WhatsApp Messages Backup contains the messages for communicating with other users through *Whatsapp* application. In the Table below the first column indicates the field of the data model related to the iOS WhatsApp Messages Backup cyber item, the second column contains the meaning of the field.

Data model	Meaning
DFDM_IOS_BACKUP_WHATSAPP_id	**ID** of the item. It is a unique identifier to build up the Chain of Evidence, that is the Relationship with the file which the item comes from.
DFDM_IOS_BACKUP_WHATSAPP_status	**Status** of the item, the value indicates if the item has been parsed/extracted or carved.
DFDM_IOS_BACKUP_WHATSAPP_recipient	**Recipient** of the message.
DFDM_IOS_BACKUP_WHATSAPP_sender	**Sender** of the message.
DFDM_IOS_BACKUP_WHATSAPP_message	**Body** of the message.
DFDM_IOS_BACKUP_WHATSAPP_time	**Date time** of the sent/received message.

5 Cyber items in a future perspective

This section is dedicated to a set of Cyber items that should be considered but that are peculiar features of specific operating system. Each operating system, both desktop and mobile have a set of different Cyber items. These particular Cyber items may be based on common structures such as SQLite or Extensible Storage Engine (ESE)[18] databases, but they must be probed to identify relevant investigative leads.

A few popular examples are shown in the following list:

- For Windows systems:
  - the System Resource Usage Monitor (SRUM). SRUM is a feature in modern Windows systems which collect statistics on execution of binaries.;
  - the information is stored in an Extensible Storage Engine (ESE) database.
- For OSX systems:
  - the Spotlight indexing system;
  - the database KnowledgeC;
  - the database PowerLog;
  - the database InteractionC.
- For Android systems
  - the Usagestats files that contain usage statistics for an app package for a specific time range.

Most of these Cyber items are still under scrutiny by the digital forensic community. For instance, the representation in CASE (see Appendix B) of the data from the KnowledgeC database within the OSX and iOS operating systems is currently under study.

6 Conclusion

This deliverable has presented the main Cyber items to consider for defining the digital forensics domain model relying on the most relevant items commonly extracted from the source of evidence: any digital device capable of creating information that may have a probative value in courts.

Considering the Appendix C (AXIOM Artifact Reference) the number of possible/significant Cyber items is very huge and the domain model, delineated in this deliverable, could not cover each possible potential evidence extractable by a device, hard disk or other kind of digital device but only provides a relevant set of items comprising a rather wide and significant scenario.

[18] ESE is Microsoft’s proprietary single file database format, acting similarly to SQLite, as a default storage engine for many applications.

Appendix A – Data set forensic images

The data set contains images related to mobile devices and computer (hard disk and pen drive).

Appendix A.1 Android mobile data set

ID image	01_HTC_Desire_626_Chip_Off
Dataset	CFReDS
Phone model	HTC Desire 626
Url	https://s3.amazonaws.com/cftt.cfreds.nist.gov/cfreds/mobile/CHIPOFF/HTC+Desire+626/N115018+CHIP+OFF.001
OS version	6.0.1
Acquisition Method	Chip Off
SHA-256	911D22BDE4CB6F7F4760503D7E15CA359B0F2EB139D8873DDB52E849AC2593D2
ID image	02_HTC_Desire_S_Chip_Off
Dataset	CFReDS
Phone model	HTC Desire S
Url	https://s3.amazonaws.com/cftt.cfreds.nist.gov/cfreds/mobile/CHIPOFF/HTC+Desire+S/HTC_Desire_S.img
OS version	2.3.5
Acquisition Method	Chip Off
SHA-256	6D6548F0CD125E30ADC73F8FD4D3FD4660430600719528FA258B2551850F89BC

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement No 833276

ID image	03_HTC_Desire_S_JTAG
Dataset	CFReDS
Phone model	HTC Desire S
Url	https://s3.amazonaws.com/cftt.cfreds.nist.gov/cfreds/mobile/JTAG/HTC+Desire+S/HTC_Desire_S_JTAG.bin
OS version	2.3.5
Acquisition Method	JTAG
SHA-256	9BBA24C280D13658754B0DFC841A49EBF1379CF26490F73F5836F06A96F3239D
ID image	04_HTC_One_Mini_Chip_Off
Dataset	CFReDS
Phone model	HTC One Mini
Url	https://s3.amazonaws.com/cftt.cfreds.nist.gov/cfreds/mobile/CHIPOFF/HTC+One+Mini/HTC_One_Mini.img
OS version	4.4.2
Acquisition Method	Chip Off
SHA-256	C2A92D06A34EA76DD766908EB8B63BE261238CDE9B7221286E7BAE676857A9FD
ID image	05_HTC_One_Mini_JTAG
Dataset	CFReDS
Phone model	HTC One Mini
Url	https://s3.amazonaws.com/cftt.cfreds.nist.gov/cfreds/mobile/CHIPOFF/HTCOne/HTCOneMini.bin

OS version	4.4.2
Acquisition Method	JTAG
SHA-256	74281AFE0901C5C8A878AFDFE18342371866F53913948C0174A998020F30E899
ID image	06_HTC_One_XL_Chip_Off
Dataset	CFReDS
Phone model	HTC One XL
Url	https://s3.amazonaws.com/cftt.cfreds.nist.gov/cfreds/mobile/CHIPOFF/HTC%20One%20XL/HTC_One_XL.img
OS version	4.1.1
Acquisition Method	Chip Off
SHA-256	B14E269FBEF3556979D1C92A8B7F9FE9C767531CD5E9A1486044EBD4D791F11F
ID image	07_HTC_One_XL_JTAG
Dataset	CFReDS
Phone model	HTC One XL
Url	https://s3.amazonaws.com/cftt.cfreds.nist.gov/cfreds/mobile/JTAG/HTC+One+XL/HTC_One_XL_JTAG.bin
OS version	4.1.1
Acquisition Method	JTAG
SHA-256	DECBC3DBB4E7043E2176F822B603B9248B7AD5B466B978C931AD0296DF57A89A

ID image	08_LG_K7_Chip_Off
Dataset	CFReDS
Phone model	LG K7
Url	https://s3.amazonaws.com/cftt.cfreds.nist.gov/cfreds/mobile/CHIPOFF/LG+K7/Chipoff.001
OS version	5.1.1
Acquisition Method	Chip Off
SHA-256	656D31B8973E55AC1AAE25D733020F007A43EBBEAC30D6BBED99DF4D07B7BD15
ID image	09_LG_E510_JTAG
Dataset	CFReDS
Phone model	LG Optimus
Url	https://s3.amazonaws.com/cftt.cfreds.nist.gov/cfreds/mobile/JTAG/LG+Optimus/LG_E510_OPTIMUS_HUB_JTAG.bin
OS version	>= 2.3
Acquisition Method	JTAG
SHA-256	6C503067C98C8953762781E60CA75980225209FDA1918ECFE52ACA678A960FA9
ID image	10_Moto_E_Chip_Off
Dataset	CFReDS
Phone model	Moto E
Url	https://s3.amazonaws.com/cftt.cfreds.nist.gov/cfreds/mobile/CHIPOFF/Moto-E/N115015+CHIP+OFF.001

OS version	5.1
Acquisition Method	Chip Off
SHA-256	6E7952D6394C62DC920330EC7793D5AE354E3AB92514B94310F2219ED386EB48
ID image	11_Samsung_S2_Chip_Off
Dataset	CFReDS
Phone model	Samsung S2
Url	https://s3.amazonaws.com/cftt.cfreds.nist.gov/cfreds/mobile/CHIPOFF/Samsung+S2/N115020.001
OS version	4.1.2
Acquisition Method	Chip Off
SHA-256	EE6374B6B29CC5F8D4F64BC7324AC2467B09568660B46584A1B40AC441FB4FA4
ID image	12_Samsung_S4_Chip_Off
Dataset	CFReDS
Phone model	Samsung S4
Url	https://s3.amazonaws.com/cftt.cfreds.nist.gov/cfreds/mobile/CHIPOFF/Samsung+S4/N116133.001
OS version	4.4.4
Acquisition Method	Chip Off
SHA-256	9397C6659130E2A1353DA225FE1154E3FAAAF3DD26576FD11204BDE9DE515D62

ID image	13_Samsung_S4_JTAG
Dataset	CFReDS
Phone model	Samsung S4
Url	https://s3.amazonaws.com/cftt.cfreds.nist.gov/cfreds/mobile/JTAG/Samsung+S4/samsungS4_M919.bin
OS version	4.4.4
Acquisition Method	JTAG
SHA-256	E2A6EDAC4450747E3C6E2770DFFAA8A920C9F0D03F261BABA5549AE6C31CAEC6
ID image	14_ZTE_Z970_Chip_Off
Dataset	CFReDS
Phone model	ZTE Z970
Url	https://s3.amazonaws.com/cftt.cfreds.nist.gov/cfreds/mobile/CHIPOFF/ZTE+Z970/Chipoff.001
OS version	4.4.4
Acquisition Method	Chip Off
SHA-256	92009D75C1EDA5CD2D5E58C079760DCF6F2547D2C1897ACD8407D5313E565F4E
ID image	15_LG_H790_UFED_NOUGAT
Dataset	Josh Hickman
Phone model	LG H790
Url	http://downloads.digitalcorpora.org/corpora/mobile/android_7.tar.gz

OS version	7.1.2
Acquisition Method	UFED 4PC
SHA-256	6FEDD6CD7CA05EFBF291CA5B12E1C563322F389B6E6E7A2817E817F01ACE78D0
ID image	16_LG_H790_UFED_OREO
Dataset	Josh Hickman
Phone model	LG H790
Url	http://downloads.digitalcorpora.org/corpora/mobile/android_8.tar.gz
OS version	8.1
Acquisition Method	UFED 4PC
SHA-256	56FBD00EF738EF8785775C0189106BB28BD1B1B550259F9CB1FB6234EC9815F0
ID image	17_GOOGLE_G013A_PIE
Dataset	Josh Hickman
Phone model	G013A Pixel 3
Url	http://downloads.digitalcorpora.org/corpora/mobile/android_9.tar.gz
OS version	9.0
Acquisition Method	UFED 4PC
SHA-256	EDF14AA84FF5A007D89F2EEA4EE9056AD4A57EBA5EFFC418B46CB7983F1B9D66

ID image	18_GOOGLE_G013A_10
Dataset	Josh Hickman
Phone model	G013A Pixel 3
Url	http://downloads.digitalcorpora.org/corpora/mobile/android_10/Non-Cellebrite%20Extraction/Pixel%203.zip
OS version	10
Acquisition Method	UFED 4PC
SHA-256	CA6918EF8B20486B6A5DED15609AC51318F377829480F93BE3BA15364A8AA00A
ID image	19_CROSSOVER
Dataset	Eoghan Casey
Phone model	Samsung SM-G925F
Url	https://drive.switch.ch/index.php/s/GYze8UHvQ1N46Cx
OS version	6.0.1
Acquisition Method	UFED 4PC
SHA-256	62765111E7195CE75C6CB255CD03AD3433D35ACFF31AF89CCBF07CE34CE1E17E
ID image	20_UFED_ANDROID_LGE_Nexus5
Dataset	Digital Corpora
Phone model	Nexus 5
Url	http://downloads.digitalcorpora.org/corpora/scenarios/2019-owl/Nexus5-Full/LGE%20Nexus%205%20Full%20Image.raw

OS version	6.0.1
Acquisition Method	Magnet Acquire
SHA-256	e823720450071337d8a1a519c76c049fddef9e4a90c14774d77a2945c0147681

Appendix A.2 iOS mobile data set

ID image	01_IPAD_IOS_9_3_5
Dataset	Champlain College
Phone model	iPad Third Gen
Url	https://drive.google.com/file/d/1-Uy4RZIGsLzlulir4fLxTNG7IeoDiCvh/view
OS version	9.3.5
Acquisition Method	iOS Full File System
SHA-256	Not available
ID image	02_IPHONE_IOS_13_4_1
Dataset	Josh Hickman
Phone model	iPhone SE
Url	http://downloads.digitalcorpora.org/corpora/mobile/ios_13_4_1/ios_13_4_1.zip
OS version	13.4.1
Acquisition Method	iOS Full File System

SHA-256	C2285139DED2E8F987C71CF4FD27586708EBF059B934E2665FA11E4D21B307D3
ID image	05_IPHONE_IOS_4_3_1
Dataset	CFReDS
Phone model	iPhone 3GS
Url	https://www.cfreds.nist.gov/mobile/cellebrite/iPhone%203GS/iPhone3GS%20Physical/iPhone3GS_4.3-4.3.1_Physical_Physical_23-10-12_03-21-58.UFD
OS version	4.3.1
Acquisition Method	iOS Physical
SHA-256	67FD82D3CC264A227B2DE8B3BE232FBC9394B96EA718B5252A119CED798ADE6C

Appendix A.3 Computer Windows data set

ID image	01_NARCOS_KOWHAI
Dataset	Digital Corpora
Url	http://downloads.digitalcorpora.org/corpora/scenarios/2019-narcos/Narcos-1.zip
OS version	Windows 10
Source type	Virtual Disk
Source size	30 GB
Acquisition method	FTK Imager
Format	Split DD (1.5 GB)

SHA-1	4d8e5041f47e0b0fc0eacc85d300661946537418
ID image	02_NARCOS_ESTEBAN
Dataset	Digital Corpora
Url	http://downloads.digitalcorpora.org/corpora/scenarios/2019-narcos/Narcos-2.zip
OS version	Windows 10
Source type	Virtual Disk
Source size	30 GB
Acquisition method	FTK Imager
Format	Split DD (1.5 GB)
SHA-1	576d20ffc835d98724e472c1714eaecff37f13d1
ID image	03_NARCOS_FREDRICKSEN
Dataset	Digital Corpora
Url	http://downloads.digitalcorpora.org/corpora/scenarios/2019-narcos/Narcos-3.zip
OS version	Windows 10
Source type	Virtual Disk
Source size	30 GB
Acquisition method	FTK Imager
Format	Spli DD (1.5 GB)
SHA-1	57c9a704b09fbb50118da57f62546824e062a73a

ID image	04_OWL
Dataset	Digital Corpora
Url	http://downloads.digitalcorpora.org/corpora/mobile/2019-owl/HD1.zip
OS version	Windows 10
Source type	Physical Disk
Source size	500 GB
Acquisition method	Ewfacquire
Format	E01
SHA-1	4bd21d6f93236006905212501549dd6d0813bb73
ID image	05_CROSSOVER
Dataset	Eoghan Casey
Url	https://drive.switch.ch/index.php/s/VBqsRZYDvBKIo0J
OS version	Not provided
Source type	Physical Disk
Source size	128 GB
Acquisition method	Tableau TD2u
Format	Split E01 (2.0 GB)
SHA-1	47cecff40ad74fb17e9a87dff4636034757e5ce2

Appendix A.4 USB Pen Drive data set

ID image	FALCON_LOGICUBE_R29_PC_E01_manner
Dataset	Mattia Epifani
Url	Not provided
File system	NTFS
Source size	56 GB
Acquisition method	Falcon Logicube
Format	Split E01 (4 GB)
SHA-1	Not provided
ID image	FALCON_LOGICUBE_R30_Pendrive_DD_manner
Dataset	Mattia Epifani
Url	Not provided
File system	NTFS
Source size	56 GB
Acquisition method	Falcon Logicube
Format	Whole disk
SHA-1	Not provided

Appendix B – CASE and Cyber items representation

In the Appendixes below the CASE representations of the main Cyber items described in the present deliverable are provided. The current CASE ontology version does not denote yet all kinds of Cyber items illustrated in the present document, so no "possible" representations have been deduced for the missing Cyber items.

Appendix B 1 - What is CASE?

The open-source Cyber-investigation Analysis Standard Expression (CASE) is a community-developed ontology designed to serve as a standard for interchange, interoperability, and analysis of investigative information in a broad range of cyber-investigation domains, including digital forensic science, incident response, counter-terrorism, criminal justice, forensic intelligence, and situational awareness.

CASE is being developed along with the Unified Cyber Ontology (UCO) that provides a format for representing all cyber artefacts. CASE, as a specific profile of UCO, provides support for cyber-investigations in any context, including criminal, corporate and intelligence. CASE and relevant portions of UCO build on the Hansken[19] data model developed and implemented by the Netherlands Forensic Institute (NFI).

The main aims of CASE are:

- to make interoperability between different tools and organisations possible;
- to automate normalization and combination of differing data sources to facilitate analysis and exploration of investigative questions (who, when, how long, where);
- to ensure all analysis results are traceable to their source(s) (Chain of Evidence) The power of such a standard is that it supports automated normalization, combination correlation, and validation of information, which means less time extracting and combining data, and more time analysing information.

An investigation generally involves many different tools and data sources, effectively creating separate store-room of information. Manually pulling together information from these various data sources and tools is time consuming, and error prone. Tools that support CASE can extract and ingest data, along with their context, in a standard format that can be automatically combined into a unified collection to strengthen correlation and analysis.

This opens up new opportunities for searching, contextual analysis, pattern recognition, machine learning, and visualisation. Furthermore, organisations involved in joint investigations can share information using CASE.

[19] https://www.forensicinstitute.nl/products-and-services/forensic-products/hansken.

CASE provides a standard language (ontology) for representing information collected, extracted, analysed and exchanged during investigations involving digital evidence

.

In a nutshell, CASE is a community-developed ontology to support:

- reporting of Cyber items;
- exchanging of Cyber items;
- tool validation (express ground truth);

in the context of:

- digital forensic science;
- incident response;
- counter-terrorism;
- criminal justice;
- forensic intelligence; and
- situational awareness.

Ultimately the benefits in using such a formalism/standard language are:

- to foster interoperability between different tools, organisations and countries;
- to strengthen the admissibility of the evidence, representing the provenance (chain of custody) to keep track of who handled digital evidence, when, where, how, etc. and lineage (chain of evidence), i.e., the set of tools and transformations that led from acquired raw data to the resulting product, highlighting the traceability of the potential digital evidence;
- to address and to solve the lack of standards for the representation of the forensics tools results;
- to provide trustworthy information: in a legal context, the evidence authentication process uses information about provenance, including evidence collection documentation, continuity of possession forms (chain of custody), audit logs from forensic acquisition tools, and integrity records, which all help establish the trustworthiness of digital evidence.

CASE implements UCO to represent certain types of information that transverse the cyber domain as core entities. They consist of a set of data and metadata for describing:

- People involved in the evidence life-cycle, from search and seizure to the report before the Court, technical and legal (subjects, victims, authorities, examiners, etc.);
- Surrounding information about Legal authorization (i.e. search warrant);
- Information about the Process/Lifecycle (i.e. seizing, acquisition, analysis, etc.);

- Information about the Chain of custody by identifying Who did What, When and Where from the moment the Evidence has been gathered/seized;
- Actions performed by people (seizing, acquisition, analysis, etc.);
- Source of evidence, that is physical objects involved in the investigative case (e.g.: hard disk, smartphone) but even digital source of evidence (i.e. memory dump);
- Description of the Objects inside the digital evidence and their Relationships (e.g. Contains, Extracted From, etc.)

Appendix B.2 - Cyber item Call: CASE-JSON-LD representation

The representation consists of the following Cyber items:

1. Phone Account
2. Phone Call

as illustrated below:

1	*{ "@id":"kb:phoneAccount-uuid-xxx",* *"@type":"uco-observable:CyberItem",* *"uco-core:facets":[{ "@type":"uco-observable:Account",* *"uco-observable:accountIssuer":"***_MOBILE_NETWORK_OPERATOR***", "uco-observable:isActive":"true"},* *{"@type":"uco-observable:PhoneAccount",* *"uco-observable:phoneNumber":"***{DFDM_CALL_IDENTIFIER}***",* *"uco-observable:name":"* **DFDM_CALL_name***" }*
4	*{ "@id":"kb:8f2b3c38-e2fa-11ea-9e34-acde48001122", "@type":" uco-observable:CyberItem",* *" uco-core:facets ":[{*

```
 "@type":"uco-observable:PhoneCall",

"uco-observable:callType":"{DFDM_CALL_DIRECTION}",

"uco-observable:startTime": {

        "@type":"xsd:dateTime",

        "@value":"},"{ DFDM_CALL_TIMESTAMP}"

},

"uco-observable:from":"kb:phoneAccount-uuid-xxx",

"uco-observable:to":"phoneAccount-yyy ",

        "uco-observable:duration":"{ DFDM_CALL_DURATION}",

         "uco-observable:allocationStatus":"":"{DFDM_CALL_STATUS}",

        "uco-observable:__outcome":"{DFDM_CALL_OUTCOME}" } ]}
```

Appendix B.3 – Cyber item Chat: CASE-JSON-LD representation

The representation (new properties in light blue), consists of the following Cyber items.

1. Application Name
2. Chat Account,
3. Chat Message
4. Chat Thread Message
5. File attached to the Message
6. Relationships of kind "attachment-of" between File and Message

as illustrated below:

1	{ "@id":"kb:chat-application-uuid-XXX", "@type":"case-core:CyberItem", "core:name":"{**DFDM_APP_NAME}**" "case-core:hasPropertyBundle":[{ "@type":"uco-observable:Application" }]}
2	{ "@id":"kb:chat-account-uuid-XXX ", "@type":"case-core:CyberIitem", "uco-core:Facet":[{ "@type":"uco-observable:Account", "uco-observable:accountIssuer": “{**DFDM_CHAT_SOURCE**}", "uco-observable:applicationIdentifier": {**DFDM_CHAT_IDENTIFIER**}, "uco-observable:isActive":"true" }, { "@type":"uco-observable:ApplicationAccount", "uco-observable:application":" kb:chat-application-uuid-XXX " }, { "@type":"uco-observable:DigitalAccount", "uco-observable:displayName":”{**DFDM_CHAT_NAME**}" }]}

3	{ "@id":"kb:chat-message-uuid-XXX ",
	"@type":"case-core:Cyber item",
	"uco-core:Facet":[{
	"@type":"uco-observable:Message",
	"uco-observable:messageText": "{DFDM_**CHAT_MSG_BODY**}",
	"uco-observable:application": "":"chat-application-XXX ", "
	uco-observable:sentTime": {
	"@type":"xsd:dateTime",

	"@value":"{**DFDM_CHAT_MSG_TIME_STAMP**}", "uco-observable:from": " **uuid-chat-account-uuid-XXX**}", "uco-observable:to": “**uuid-chat-account-uuid-YYY**"], "uco-observable:allocationStatus":"{**DFDM_CHAT_MSG_STATUS**}", "uco-observable:__outcome":"{**DFDM_CHAT_MSG_OUTCOME**}", "uco-observable:messageType":"**DFDM_CHAT_MSG_DIRECTION**" }]}

4	{ "@id":":01142ef8-e6d7-11ea-8c48-acde48001122",
	"@type":"case-core:Cyber item",
	"uco-core:Facet":[{
	"@type":"uco-observable:messageThread",
	"uco-observable:displayName":"NOT_PROVIDED",
	"uco-observable:messages":[{
	" olo:length ":"6",
	"olo:slot":[
	{ "olo:index":"1",
	"olo:item": {"@id":"":"kb:chat-message-uuid-XXX “ }
	},
	{ "olo:index":"2",
	"olo:item": {"@id":"":"kb:chat-message-uuid-YYY “ }
	},],
	"uco-observable:participants":[
	{“kb:chat_account_XXX “}
	{“kb:chat_account_YYY “}]
	}] }

5	{ "@id":":uuid-file-attached-XXX ",
	"@type":"case-core:Cyber item",
	"tag":["_NOT_PROVIDED_"],
	"uco-core:Facet":[
	{
	"@type":"uco-observable:File",
	"uco-observable:fileName":"**{DFDM_CHAT_MSG_ATTACHMENT_FILENAME}**",
	"uco-observable:filePath":"**{ DFDM_CHAT_MSG_ATTACHMENT_FILENAME}**",
	"uco-observable: fileLocalPath":"**{ DFDM_CHAT_MSG_ATTACHMENT_URL}**",
	"uco-observable:extension":"{ DFDM_CHAT_MSG_ATTACHMENT_FILEEXTENSION}",
	"uco-observable:fileSystemType":"userdata (ExtX)",
	"uco-observable:isDirectory":"false",
	"uco-observable:allocationStatus":"allocated",
	"uco-observable:sizeInBytes": {
	"@type":"xsd:long",
	"@value":"_NOT_PROVIDED_"
	},
	"uco-observable:createdTime":"_NOT_PROVIDED_",
	"uco-observable:modifiedTime":"_NOT_PROVIDED_",
	"uco-observable:accessedTime":"_NOT_PROVIDED_"},
	{
	"@type":"uco-observable:ExtInode",
	"uco-observable:extInode":"_NOT_PROVIDED_",
	"uco-observable:extSGID":"_NOT_PROVIDED_",
	"uco-observable:extSUID":"_NOT_PROVIDED_",

	"uco-observable:extInodeChangeTime":"_NOT_PROVIDED_"},
	{
	"type":"ContentData",
	"hash":[
	{
	"@type":"uco-types:Hash",
	"uco-types:hashMethod":{
	"@type": "uco-core:HashNameEnum",
	"@value": "_NOT_PROVIDED_"
	},
	"uco-types:hashValue":{
	"@type": "xsd:hexBinary",
	"@value":"_NOT_PROVIDED_"
	}
	}
	]
	}

6	{ "@id":":f7a5de5c-f367-11ea-8d8d-acde48001122", "@type":"uco-observable:Relationship", "uco-observable:source":"**uuid-file-attached-XXX** ", "uco-observable:target “**uuid-chat-msg-XXX** ", "uco-observable:kindOfRelationship":"attachment-of", "uco-observable:isDirectional":"True", "uco-core:Facet": [

```
        {
                  "@type":"uco-observable:DataRange",
                  "uco-observable:rangeOffset":"{NOT_PROVIDED}",
                  "uco-observable:rangeSize":"{NOT_PROVIDED}"
        },
        {
                  "@type": "uco-observable:TableRelation",
                  "uco-observable:name":"{NOT_PROVIDED}"
}]      },
```

Appendix B.4 – Cyber item Contact: CASE-JSON-LD representation

The representation (new properties in light blue), consists of the following Cyber item:

1. Account

```
{ "@id":":phoneAccount-8f2aa638-e2fa-11ea-8e01-acde48001122",
      "@type":"case-core:CyberItem",
      "uco-core:Facet":[{
                "@type":"uco-observable:Account",
                "uco-observable:accountIssuer":"":"_MOBILE_NETWORK_OPERATOR”
                "uco-observable:isActive":"true"
},
      {
                "@type":"uco-observable:PhoneAccount",
                "uco-
                observable:phoneNumber":"{DFDM_CONTACT_PHONE_NUM}",
                "uco-observable:name":"{ DFDM_CONTACT_NAME}"
                "uco-observable:allocationStatus ":"{ DFDM_CONTACT_STATUS}”
      } ]}
```

Appendix B.5 – Cyber item Email: CASE-JSON-LD representation

The representation consists of two distinct Cyber items:

1. Email Account
2. Email Message
3. File attached to the Email
4. Relationships of kind “attachment-of” between File and Email

as illustrated below:

```
        {       "@id":":uuid-emai-account-XXX ",
                "@type":"case-core:CyberItem",
                "uco-core:Facet":[{
                        "@type":"uco-observable:Account",
                        "uco-observable:accountIssuer":"NOT_PROVIDED",
                        "uco-observable:isActive":"true"
        },
                {
                        "@type":"uco-observable:EmailAccount",
                        "uco-observable:emailAddress":"{DFDM_EMAIL_FROM / EMAIL_TO}"
                }
```

	]}

2	{ "@id":":4476b83a-e602-11ea-9bc0-acde48001122",
	"@type":"case-core:CyberItem",
	"uco-core:Facet":[
	{
	"@type":"uco-observable:EmailMessage",
	"uco-observable:application":"**{ DFDM_EMAIL_SOURCE}**",
	"uco-observable:sentTime":{
	"@type":"xsd:dateTime",
	"@value":"**{ DFDM_EMAIL_TIME_STAMP}**"},
	"uco-observable:fromRef":{"**uuid-email-account-XXX**"},
	"uco-observable:toRef":[{"**uuid-email-account-TO_01**"}, {"**uuid-email-account-TO_02**"}],
	"uco-observable:ccRefs**":[{" uuid-email-account-**}, {"**uuid-email-account-CC_02**"}],
	"uco-observable:bccRefs**":[{" uuid-email-account-BCC_01"}**, {"**uuid-email-account-BCC_02**"}],
	"uco-observable:body":"**{DFDM_EMAIL_BODY}",**
	"uco-observable:subject":"**{DFDM_EMAIL_SUBJECT}**",
	"uco-observable:allocationStatus ":"**{DFDM_EMAIL_STATUS}"**
	}]}

3	{ "@id":":uuid-file-attached-XXX ", "@type":"case-core:CyberItem", "tag":["_NOT_PROVIDED_"], "uco-core:Facet":[{ "@type":"uco-observable:File",

```
"uco-observable:fileName":" e_ATTACHMENT_FILENAME}",
"uco-observable:filePath":"{e_ATTACHMENT_FILENAME}",
"uco-observable:__fileLocalPath":"NOT_PROVIDED",
"uco-observable:extension":"{e_ATTACHMENT_FILEEXTENSION}",
"uco-observable:fileSystemType":"userdata (ExtX)",
"uco-observable:isDirectory":"false",
"uco-observable:allocationStatus":"allocated",
"uco-observable:sizeInBytes": {
"@type":"xsd:long",
"@value":"_NOT_PROVIDED_"
},
"uco-observable:createdTime":"_NOT_PROVIDED_",
"uco-observable:modifiedTime":"_NOT_PROVIDED_",
"uco-observable:accessedTime":"_NOT_PROVIDED_"},
{
        "@type":"uco-observable:ExtInode",
        "uco-observable:extInode":"_NOT_PROVIDED_",
        "uco-observable:extSGID":"_NOT_PROVIDED_",
        "uco-observable:extSUID":"_NOT_PROVIDED_",
        "uco-observable:extInodeChangeTime":"_NOT_PROVIDED_"},
        {
        "type":"ContentData",
        "hash":[
        {
                "@type":"uco-types:Hash",
```

	"uco-types:hashMethod":{
	"@type": "uco-core:HashNameEnum",
	"@value": "_NOT_PROVIDED_"
	},
	"uco-types:hashValue":{
	"@type": "xsd:hexBinary",
	"@value":"_NOT_PROVIDED_"
	}
	}
	]
	}
	]},

4	{ "@id":":f7a5de5c-f367-11ea-8d8d-acde48001122", "@type":"uco-observable:Relationship", "uco-observable:source":"**uuid-file-attached-XXX** ", "uco-observable:target “**uuid-email-msg-XXX** ", "uco-observable:kindOfRelationship":"**attachment-of**", "uco-observable:isDirectional":"True", "uco-core:Facet": [{ "@type":"uco-observable:DataRange", "uco-observable:rangeOffset":"NOT_PROVIDED", "uco-observable:rangeSize":"__NOT_PROVIDED" }, {

```
                                        "@type": "uco-observable:TableRelation",
                                        "uco-observable:name":"NOT_PROVIDED"
                        }]      },
```

Appendix B.6 – Cyber item FILE: CASE-JSON-LD representation

The representation (new properties in light blue), consists of the following Cyber item:

1. File

```
1    {
            "@id":":444bd28c-e602-11ea-baa1-acde48001122",
            "@type":"case-core:CyberItem",
            "tag":["Application"],
            " uco-core:Facet ":[
            {
                    "@type":"uco-observable:File",
                    "uco-observable:fileName":"{FILE_NAME}",
                    "uco-observable:filePath":"{FILE_PATH}",
                    "uco-observable:__fileLocalPath":"{FILE_LOCAL_PATH}",
                    "uco-observable:extension":"{FILE_EXTENSION}",
                    "uco-observable:fileSystemType":"EXT4",
                    "uco-observable:isDirectory":"false",
                    "uco-observable:allocationStatus":"allocated",
                    "uco-observable:sizeInBytes": {
                    "@type":"xsd:long",
                    "@value":"{FILE_SIZE}"
```

```
},
"uco-observable:createdTime":"{FILE_C_TIME}",
"uco-observable:modifiedTime":"{FILE_M_TIME}",
"uco-observable:accessedTime":"{FILE_A_TIME}"},
{
    "@type":"uco-observable:ExtInode",
    "uco-observable:extInode":"{FILE_INODE_NUM}",
    "uco-observable:extSGID":"{FILE_OWNER_GID}",
    "uco-observable:extSUID":"{FILE_OWNER_UID}",
    "uco-observable:extInodeChangeTime":"{FILE_INODE_M_TIME}"},
    {
    "type":"ContentData",
    "hash":[
    {
        "@type":"uco-types:Hash",
        "uco-types:hashMethod":{
        "@type": "uco-core:HashNameEnum",
        "@value": "MD5"
        },
        "uco-types:hashValue":{
        "@type": "xsd:hexBinary",
        "@value":"{FILE_MD5}"
    } ,
{       "@type":"uco-types:Hash",
        "uco-types:hashMethod":{
        "@type": "uco-core:HashNameEnum",
        "@value": "SHA-256"
```

```
                                        },
                                        "uco-types:hashValue":{
                                        "@type": "xsd:hexBinary",
                                        "@value":"{FILE_SHA}"
                              } } ]                                  }
                    ]}
```

Appendix B.7 – Cyber item Picture (EXIF): CASE-JSON-LD representation

The representation (new properties in light blue) consists of the following Cyber item:

1. File

1

```
{ "@id": "kb:digital_photograph1",
"@type": "uco-observable:CyberItem",
"uco-core:facets": [
{ "@type": "uco-observable:File",
"uco-observable:fileSystemType": "EXT4",
"uco-observable:fileName": "{DFDM_FILE_name}",
"uco-observable:filePath": "{DFDM_FILE_path}",
"uco-observable:__fileLocalPath": "{DFDM_FILE_localPath}",
"uco-observable:extension": "{DFDM_FILE_extension}",
"uco-observable:sizeInBytes": {
"@type": "xsd:long",
"@value": {DFDM_FILE_size}
} },
{ "@type": "uco-observable:ContentData",
"uco-observable:byteOrder": "BigEndian",
"uco-observable:magicNumber": "/9j/ww==",
"uco-observable:mimeType": "image/jpg",
"uco-observable:sizeInBytes": {
"@type": "xsd:long",
"@value": 35000
},
"uco-observable:dataPayload": "<base 64 encoded data of the file>",
"uco-observable:hash": [
{ "@type": "uco-types:Hash",
"uco-types:hashMethod": {
"@type": "uco-vocabulary:HashNameVocab",
"@value": "SHA256"
},
"uco-types:hashValue": {
"@type": "xsd:hexBinary",
"@value": {DFDM_FILE_sha1}
} } ] },
{ "@type": "uco-observable:RasterPicture",
"uco-observable:pictureType": "jpg",
"uco-observable:pictureHeight": "{DFDM_FILE_exifHeight},
"uco-observable:pictureWidth": "{DFDM_FILE_exifWidth},
"uco-observable:bitsPerPixel": 2 },
{ "@type": "uco-observable:EXIF",
```

	"uco-observable:exifData": { *"@type": "uco-types:ControlledDictionary",* *"uco-types:entry": [{* *"@type": "uco-types:ControlledDictionaryEntry",* *"uco-types:key": "Make",* *"uco-types:value": "{**DFDM_FILE_exifManufacturer**}" },* *{ "@type": "uco-types:ControlledDictionaryEntry",* *"uco-types:key": "Model",* *"uco-types:value": "{**DFDM_FILE_exifModel**}" },* *{ "@type": "uco-types:ControlledDictionaryEntry",* *"uco-types:key": "Orientation",* *"uco-types:value": "Horizontal (normal)" },* *{ "@type": "uco-types:ControlledDictionaryEntry",* *"uco-types:key": "DateTimeDigitized",* *"uco-types:value": "{**DFDM_FILE_exifTimeCreation**}" },* *{ "@type": "uco-types:ControlledDictionaryEntry",* *"uco-types:key": "Latitude",* *"uco-types:value": {**DFDM_FILE_exifGpsLatitude**}" },* *{ "@type": "uco-types:ControlledDictionaryEntry",* *"uco-types:key": "LatitudeRef",* *"uco-types:value": "S" },* *{ "@type": "uco-types:ControlledDictionaryEntry",* *"uco-types:key": "Longitude",* *"uco-types:value": "{**DFDM_FILE_exifGpsLongitude**}" },* *{ "@type": "uco-types:ControlledDictionaryEntry",*

```
                "uco-types:key": "LongitudeRef",
                "uco-types:value": "W" } ] } } ] }
```

Appendix B.8 – Cyber item SMS: CASE-JSON-LD representation

The representation (new properties in light blue), consists of the following Cyber items:

1. Phone Account
2. Message

as illustrated below:

```
                {     "@id":":phoneAccount-8f2aa638-e2fa-11ea-8e01-
                      acde48001122", "@type":"case-core:Cyber item",
                      " uco-core:Facet":[{
                                "@type":"uco-observable:Account",
                                "uco-
                                observable:accountIssuer":"_MOBILE_NETWORK_OPERATOR",
                                "uco-observable:isActive":"true"
                },
                {
                                "@type":"uco-observable:PhoneAccount",
                                "uco-
                                observable:phoneNumber":"{SMS_IDENTIFIER}",
                                "uco-observable:name":"{SMS_NAME}"
                      }
               ]}
```

2	{ "@id":":446aa31a-e602-11ea-9ea1-acde48001122", "@type":"case-core:CyberItem", " uco-core:Facet":[{ "@type":"uco-observable:Message", "application**":"{SMS_SOURCE}**", "uco-observable:SMSmessage":"true", "uco-observable:messageText**":"{SMS_BODY}**", "uco-observable:allocationStatus":"**{SMS_STATUS}**", "uco-observable:_outcome":"**{SMS_OUTCOME}**", "uco-observable:from":{"phone-account-idXXX "}, "uco-observable:to":[{"phone-account-idYYY_01”},{” phone-account-idYYY_02”}, …], "uco-observable:sentTime":"**{SMS_TIME_STAMP}**"}] }

Appendix B.9 – Cyber item URL History: CASE-JSON-LD representation

The representation consists of the following Cyber items:

1. Web History Cyber item, as illustrated below:

1	{ "@id":":602fb8c6-e616-11ea-bad1-acde48001122", "@type":"case-core:CyberItem", "uco-core:Facet":[{ "@type":"uco-observable:WebHistory", "uco-observable:source**":"{DFDM_WEB_SOURCE}**", "uco-observable:url":"**{ DFDM_WEB_URL}**”, "uco-observable:title":"**{ DFDM_WEB_TITLE}**",

	*"uco-bservable:visitCount":"**{ DFDM_WEB_VISIT_COUNT}**",* *"uco-observable:visitTime":"**NOT_PROVIDED**",* *"uco-observable:typedCount":"0",* *"uco-observable:duration**":" NOT_PROVIDED**",* *"uco-observable:transitiontype**":"NOT_PROVIDED**",* *"uco-observable:searchterm":" **NOT_PROVIDED**",* *"uco-observable:lastVisited**":"{ DFDM_WEB_LAST_VISTED}**",* *"uco-observable:allocationStatus":"{ **DFDM_WEB_STATUS**}" }]}*

Appendix C – Axiom Artifact Reference: Table of Content

This list enumerates the Artifacts or Cyber items that Axiom forensic tool is able to detect and extract. The list includes the following 1.718 Artifacts broken down under the main mobile and computer operating system:

Windows	407 artifacts
Android	455 artifacts
iOS	361 artifacts
macOS	138 artifacts
Cloud	86 artifacts
Windows Phone	198 artifacts
Kindle	73 artifacts

Windows

Chat

Adium Chat

AIM

AIM Chat Messages

Chatroulette

Chatstep Messages

Google Talk

ICQ 10 Messages

ICQ Messages

iMessage Chats

iMessage Messages

KakaoTalk Chat Rooms - Windows

KakaoTalk Contacts - Windows

KakaoTalk Messages - Windows

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 833276

KakaoTalk Pictures

KakaoTalk Shared Pictures - Windows

Lync - OC Calls

Lync - OC File Transfers

Lync - OC Fragments

Lync - OC Messages

mIRC Chat Logs

MSN Protocol Fragments

Omegle

ooVoo Chat History

ooVoo Contact List

ooVoo Phone Book

Pal Talk

Pidgin Accelerators

Pidgin Accounts

Pidgin Buddies

Pidgin Chat

Pidgin Custom Smileys

Pidgin OTR Fingerprints

Pidgin OTR Users

QQ Chat

Second Life Chat

Skype Accounts

Skype Activity

Skype Calls

Skype Chat Messages

Skype Chatsync Messages

Skype Chatsync Messages Carved

Skype Contacts

Skype File Transfers

Skype Group Chat

Skype IP Addresses

Skype Media Cache

Skype SMS

Skype Voicemails

TorChat

Trillian

WeChat Messages

WhatsApp Messages - Windows

Windows Live Messenger - MSN

Windows Live Messenger Chat - Mac

Windows Viber Calls

Windows Viber Chat Messages

Windows Viber Contacts

Windows Viber Group Members

Windows Viber Messages

World of Warcraft Chat

Your Phone Contacts

Your Phone Devices

Your Phone Pictures

- Your Phone SMS - MMS
- Zoom Chat Messages
- Zoom Meeting Messages
- Zoom User Accounts

Cloud

- Carbonite Log File
- Dropbox
- Dropbox Configuration Data
- Flickr
- Google Docs
- Google Drive
- OneDrive
- SharePoint Discussions
- SharePoint Recycle Bin
- SharePoint Shared Documents

Documents

- Calc Documents
- CSV Documents
- Excel Documents
- Hangul Word Processor
- Impress Documents
- PDF Documents
- PowerPoint Documents
- RTF Documents
- Text Documents

Word Documents

Writer Documents

E-mail

EML- X Files

Gmail Email Fragments

Gmail Webmail

GMX Webmail

Hotmail Webmail

Hushmail Fragments

Hushmail Inbox

Mailinator Inbox Access

Mailinator Snippets

MBOX Emails

Offline Gmail webmail

Outlook Appointments

Outlook Contacts

Outlook Journals

Outlook Messages

Outlook Notes

Outlook Tasks

Outlook Web App Email Fragments

Outlook Web App Inbox

Outlook Webmail Inbox

Windows Mail

Email

Calendar Events - ICS

Encryption

Encrypted Files

Encryption - Anti-forensics Tools

Media

Audio

Carved Video

Pictures

RealPlayer Library Assets

RealPlayer Video History

Videos

VLC Recently Played Files

Web Video Fragments

Memory

Active Network Info - sockets

API Hooks - apihooks

Clipboard - clipboard

Command History - cmdscan

Connection Scan - connscan

Dynamically Loaded Libraries - dlllist

Files - filescan

Hidden Processes - psxview

Hidden - Residual Modules - modscan

Hidden - Terminated Processes - psscan

Image Info - imageinfo

LDR Modules - ldrmodules

Loaded Kernel Modules - modules

Malware Finder - malfind

Network Connections - connections

Network Connections - sockscan

Network Info - netscan

Open Handles - handles

Process Security Identifiers - getsids

Processes - pslist

Timeline - timeliner

Mobile Backups

iOS Address Book Backup

iOS Calendar Events

iOS Call Logs Backup

iOS Device Information

iOS Dropbox App Backup

iOS iMessage - SMS - MMS Backup

iOS Kik Messenger Backup

iOS Notes

iOS WhatsApp Media Messages Backup

iOS WhatsApp Messages

Operating System

AmCache Device Containers

AmCache Driver Binaries

AmCache Driver Packages

AmCache File Entries

AmCache File Entries - Legacy

AmCache Pnp Devices

AmCache Program Entries

AmCache Program Entries - Legacy

AmCache Shortcuts

Autorun Items

Cortana Person Reminders

Cortana Place Reminders

Cortana Time Reminders

File Associations

File Signature Mismatch - Audio

File Signature Mismatch - Container

File Signature Mismatch - Document

File Signature Mismatch - Picture

File Signature Mismatch - Video

File System Information

IME Suggestions - Japanese

Installed Microsoft Programs

Installed Programs

Jump Lists

Keyword Searches

Known DLLs

LNK Files

MRU Folder Access

MRU Opened - Saved Files

MRU Recent Files And Folders

MRU Run Commands

MUICache

Network Interfaces - Registry

Network Profiles

Network Share Information

Network Usage - Application Data

Network Usage - Connections

Operating System Information

Prefetch Files - Windows 8 - 10

Prefetch Files - Windows XP - Vista - Sette

Recycle Bin

Remote Desktop Protocol

Scheduled Tasks

Shellbags

Shim Cache

SRUM Application Resource Usage

SRUM Energy Usage

SRUM Energy Usage - Long Term

SRUM Network Connections

SRUM Network Usage

SRUM Push Notification Data

Startup Items

System Services

Timezone Information

USB Devices

User Accounts

UserAssist

UsnJrnl

Virtual Machines

Windows Event Logs

Windows Logon Banner

Windows Notification Center

Windows Timeline Activity

Peer-to-Peer

Ares Download Folder

Ares Downloads

Ares Incomplete Downloads

Ares Search Keywords

Ares Shared Files

Bitcoin Address

Bitcoin Debug Logs

Bitcoin Logged Queries

eMule GUIDs

eMule Search Keywords

eMule Shared Files

eMule Shared Folders

Frostwire

Gigatribe Chat Messages

  - Gigatribe Shared Files
  - Limerunner Shared Files
  - Limewire Shared Files
  - Limewire - Frostwire
  - Luckywire Shared Files
  - Shareaza GUIDs
  - Shareaza Library Files
  - Shareaza Search Keywords
  - Shareaza Search Results
  - Torrent Active Transfers
  - Torrent Feeds
  - Torrent File Fragments
  - Usenet Binary Files

- **Social Networking**
  - Bebo Live Chat
  - Facebook
    - Facebook Chat
    - Facebook Email Snippets
    - Facebook Email
    - Facebook Pages
    - Facebook Status Updates - Wall Posts - Comments
  - Instagram Pictures
  - Instagram Posts
  - LINE Pictures
  - LinkedIn Emails

MySpace Chat - Messages

MySpace Chat - User Info

MySpace Inbox Messages

Sina Weibo Carved Searches

Sina Weibo Microblogs

Sina Weibo Search History

Twitter

VK Wall Posts

VK Web Messages

Web Related

360 Safe Browser Archived Keyword Search Terms

360 Safe Browser Archived Web History

360 Safe Browser Autofill

360 Safe Browser Autofill Profiles

360 Safe Browser Bookmarks

360 Safe Browser Cache Records

360 Safe Browser Cookies

360 Safe Browser Current Downloads

360 Safe Browser Current Session

360 Safe Browser Current Tabs

360 Safe Browser FavIcons

360 Safe Browser History Index

360 Safe Browser Last Session

360 Safe Browser Last Tabs

360 Safe Browser Logins

- 360 Safe Browser Saved Credit Cards
- 360 Safe Browser Shortcuts
- 360 Safe Browser Top Sites
- 360 Safe Browser Web History
- 360 Safe Browser Web Visits
- Ashley Madison - Backpage Ads - Craigslist Ads - Plenty of Fish
- Bing Toolbar - Map History
- Bing Toolbar - Search History
- Chrome
    - Chrome Archived Keyword Search Terms
    - Chrome Archived Web History
    - Chrome Autofill Profiles
    - Chrome Autofill
    - Chrome Bookmarks
    - Chrome Cache Records
    - Chrome Cookies
    - Chrome Current Session
    - Chrome Current Tabs
    - Chrome Downloads
    - Chrome Extensions
    - Chrome FavIcons
    - Chrome History Index
    - Chrome Keyword Search Terms
    - Chrome Last Session
    - Chrome Last Tabs

Chrome Logins

Chrome Saved Credit Cards

Chrome Shortcuts

Chrome Sync Accounts

Chrome Sync Data

Chrome Top Sites

Chrome Web History

Chrome Web Visits

Edge Cache Data

Edge Extensions

Edge Favorites

Edge Last Session

Edge Reading Lists

Edge Top Sites

Edge - Internet Explorer 10-11 Content

Edge - Internet Explorer 10-11 Cookies

Edge - Internet Explorer 10-11 Daily - Weekly History

Edge - Internet Explorer 10-11 Dependency Entries

Edge - Internet Explorer 10-11 Downloads

Edge - Internet Explorer 10-11 Main History

Firefox Add-ons

Firefox Bookmarks

Firefox Cache Records

Firefox Cookies

Firefox Downloads

Firefox FavIcons

Firefox FormHistory

Firefox Input History

Firefox Private Browsing History

Firefox SessionStore Artifacts

Firefox Web History

Firefox Web Visits

Flash Cookies

Google Analytics First Visit Cookies

Google Analytics First Visit Cookies Carved

Google Analytics Referral Cookies

Google Analytics Referral Cookies Carved

Google Analytics Session Cookies

Google Analytics Session Cookies Carved

Google Analytics URLs

Google Analytics URLs Carved

Google Maps

Google Maps Tiles

Google Toolbar

Internet Explorer Cache Records

Internet Explorer Cookie Records

Internet Explorer Cookies

Internet Explorer Downloads

Internet Explorer Favorites

Internet Explorer InPrivate - Recovery URLs

Internet Explorer Leak Records

Internet Explorer Main History

Internet Explorer PrivacIE Records

Internet Explorer Typed URLs

Internet Explorer Weekly History

IP Addresses - Audio - Video Calls

Malware - Phishing URLs

Opera Archived Keyword Search Terms

Opera Archived Web History

Opera Autofill Profiles

Opera Bookmarks

Opera Cache Records

Opera Cookies

Opera Current Session

Opera Current Tabs

Opera Downloads

Opera History Index

Opera Last Session

Opera Last Tabs

Opera Logins

Opera Saved Credit Cards

Opera Search Field History

Opera Shortcuts

Opera Top Sites

Opera Typed History

Opera Web History

Pornography URLs

Rebuilt Webpages

Safari Bookmarks

Safari Cache Records

Safari Downloads

Safari History

Safari iCloud Devices

Safari iCloud Tabs

Safari Last Session

Safari Top Sites

WebKit Browser Session - Tabs - Carved

WebKit Browser Web History - Carved

XBox 360 Internet Explorer Cache Records

XBox 360 Internet Explorer Daily History

XBox 360 Internet Explorer Favorites - Recent - Featured Items

XBox 360 Internet Explorer Weekly History

XBox Internet Explorer Main History

Android

Advanced Search Tools

Dynamic Application Finder

Chat

AIM Buddies

AIM Messages

Android Burner Conversations

Android Burner Numbers

Android Google Hangouts Messages

Android Kik Messenger Attachments

Android Kik Messenger Contacts

Android Kik Messenger Messages

Android Messages

Android MMS

Android MMS - UFED Agent

Android SMS

Android SMS - UFED Agent

Android SMS - MMS - Content Provider

Android SMS - MMS - Google Play Services

Android Telegram Chats

Android Telegram Contacts

Android Telegram Messages

Android TigerText Messages

Android Tinder Accounts

Android Tinder Matches

Android Tinder Messages

Android Tinder Photos

BlackBerry Messenger Contacts

BlackBerry Messenger File Transfers

BlackBerry Messenger Invitations

BlackBerry Messenger Locations

BlackBerry Messenger Messages

BlackBerry Messenger Profile

Cake Local User Account

Cake Messages

Discord Messages

Facebook Messenger Calls

Facebook Messenger Groups

Facebook Messenger Messages

Facebook Messenger Users Contacted

Glide Messages

Glide Users

Google Duo Calls

Google Hangouts Cached Images

Google Hangouts Voice Calls

Grindr Buddies

Grindr Messages

GROWLr Chat Messages

GROWLr Notes

Gtalk Contacts

Gtalk Message

imo Contacts

imo Messages

Jott Groups

Jott Messages

KakaoTalk Calls

KakaoTalk Chat Rooms

- KakaoTalk Detected Wifi
- KakaoTalk Friends
- KakaoTalk Messages
- Life360 Circle Members
- Life360 Local User Account
- Life360 Messages
- Life360 Places
- Life360 Trip Locations
- QQ File Transfers
- QQ Local Users
- QQ Messages
- Samsung Text Message Logs
- Signal
  - Forensic notes
    - Signal for Android
  - Artifacts
  - Signal Group Members
  - Signal Local User
  - Signal Messages
- Skype Accounts
- Skype Activity
- Skype Calls
- Skype Chat Messages
- Skype Chatsync Messages
- Skype Contacts

Skype Emotions

Skype File Transfers

Skype Group Chat

Skype IP Addresses

Skype Notifications

Slack Channel Messages

Slack Channels

Slack Direct Messages

Slack Files

Slack Users

Slack Workspaces

TamTam Messenger Channels - Android

TamTam Messenger Contacts

TamTam Messenger Conversations - Android

TamTam Messenger Groups - Android

TamTam Messenger Messages - Android

Textfree Attachments

Textfree Contacts

Textfree Groups

Textfree Messages

TextMe Calls

TextMe Messages

TextNow Calls

TextNow Chat

TextNow Contacts

- TextNow Groups
- TextNow Profile
- TextPlus Calls
- TextPlus Messages
- Touch Experiences
- Touch Friends
- Touch Local User
- Touch Messages
- Verizon Messages Messages
- Viber Messages
- WeChat Friends
- WeChat Messages
- WhatsApp
    - Artifacts
    - Android WhatsApp Chats
    - Android WhatsApp Contacts
    - Android WhatsApp Groups
    - Android WhatsApp Live Locations
    - Android WhatsApp Messages
    - Android WhatsApp Profile Pictures
    - Android WhatsApp User Profiles
    - WhatsApp Accounts Information
- Your Phone Companion Info
- Zalo Contacts
- Zalo Groups

Zalo Messages

Zalo Profiles

Zoom Chat Messages

Zoom Meeting Messages

Zoom User Accounts

Cloud

Android Dropbox

Android Dropbox Account Info

Documents

Evernote Accounts

Evernote Contacts

Evernote Notes

Evernote Work Chat

Excel Documents

Hangul Word Processor

PDF Documents

PowerPoint Documents

RTF Documents

Text Documents

Thinkfree Office Viewer Files

Word Documents

E-mail

Android Emails

Android Gmail Conversations

Android Yahoo Mail Attachments

Android Yahoo Mail Emails

Android Yahoo Mail User Accounts

Gmail Emails

Outlook Accounts

Outlook Appointments

Outlook Contacts

Outlook Messages

Internet of Things

Amazon Alexa Audio Activity

Amazon Alexa Cached Audio

Amazon Alexa Device Information

Amazon Alexa Tasks

Amazon Alexa User

Amazon Alexa Web Resource

Fitbit Floors

Fitbit Heart Rate

Fitbit Profiles

Fitbit Sleep

Fitbit Steps

Pebble Activity Information

Pebble Applications

Pebble Calendar Events

Pebble Contacts

Pebble Detected Android Applications

Pebble Device Information

- Pebble Notifications
- Pebble Physical Characteristics
- Pebble Weather Locations

Media

- AMR Files
- Android Snapchat Accounts Information
- Android Snapchat Event Logs
- Android Snapchat Friends
- Android Snapchat Photo Transfers
- Android Snapchat Received Images
- Android Snapchat Received Snaps
- Android Snapchat Sent Snaps
- Android Snapchat Stories
- Audio
- Carved Video
- Pictures
- Snapchat Chat Messages
- Snapchat Group Members
- Snapchat Memories
- Snapchat Received Videos
- Videos

Mobile

- Activity Manager History
- Camera History
- Google Play Application Details

- Google Play Installed Applications
- Google Play Searches
- Last Known Locations
- SIM Card ICCID
- SIM Card IMSI
- SIM Card Phone Numbers
- SIM Card Service Providers
- SIM Card SMS Messages
- Wi-Fi Profiles

Operating System

- Accounts Information
- Android Call Logs
- Android Call Logs - UFED Agent
- Android Contacts
- Android Contacts - UFED Agent
- Android Device Information
- Android KeyStore
- Android Usage History
- Android Usage History - Dumpsys
- Android User Dictionary
- Application Activity - Android
- Application Power Usage
- Bluetooth Devices
- Calendar Events
- Calendar Events - UFED Agent

  - Chrome
  - Android Downloads
  - File Signature Mismatch - Audio
  - File Signature Mismatch - Container
  - File Signature Mismatch - Document
  - File Signature Mismatch - Picture
  - File Signature Mismatch - Video
  - File System Information
  - Installed Applications
  - Wi-Fi Logs - Android

- **Peer-to-Peer**
  - Torrent Active Transfers
  - Torrent Feeds
  - Torrent File Fragments
- **Social Networking**
  - Android Instagram Following
  - Android Instagram Posts
  - Android Instagram Users
  - Android Meet24 Cache Records
  - Android Meet24 Cookies
  - Android Whisper Posts
  - Facebook
    - Android Facebook Messages
    - Android Facebook Pictures
    - Facebook Contacts

- Facebook User - Friends

Foursquare Check-ins

Foursquare Locations

Foursquare Searches

Instagram Direct Messages

Instagram Group Members

Instagram Media

Instagram Profiles

LINE Chats

LINE Contacts

LINE Messages

LINE Pictures

Sina Weibo Posts

Sina Weibo Private Messages

TikTok Contacts

TikTok Messages

TikTok Videos

Twitter Direct Messages

Twitter Tweets

Twitter Users

VK Messages

VK Users

Whisper Messages

Transportation and Travel

OnStar RemoteLink Accounts

OnStar RemoteLink Hotspot Info

OnStar RemoteLink Recent Location Searches

OnStar RemoteLink Remote Commands

OnStar RemoteLink Saved Places Of Interest

OnStar RemoteLink Saved Wireless Carrier

OnStar RemoteLink Vehicle Diagnostics

OnStar RemoteLink Vehicle Info

Uber Payments

Uber Trips

Web Related

Aloha Browser Autofill

Aloha Browser Bookmarks

Aloha Browser Downloads

Aloha Browser History

Android Browser Bookmarks

Android Browser Search Terms

Android Browser Web History

Android Firefox Bookmarks

Android Firefox Web History

Android Google Maps

Autofill

Brave Bookmarks

Brave Cookies

Brave Downloads

Brave Favicons

- Brave Keyword Search Terms
- Brave Top Sites
- Brave Web History
- Brave Web Visits
- Browser Activity
- Calc Vault Browser Bookmarks
- Calc Vault Browser History
- Chrome
  - Android Archived Web History
  - Android Autofill
  - Android Chrome Autofill Profiles
  - Android Chrome Favicons
  - Android Chrome Logins
  - Android Chrome Saved Credit Cards
  - Android Chrome Top Sites
  - Android Chrome Web Visits
  - Android Downloads
  - Chrome Bookmarks
  - Chrome Cache Records
  - Chrome Cookies
  - Chrome Keyword Search Terms
  - Chrome Sync Accounts
  - Chrome Sync Data
  - Chrome Web History
- Dolphin Browser Bookmarks

Dolphin Browser History

Ecosia Autofill

Ecosia Bookmarks

Ecosia Cookies

Ecosia Downloads

Ecosia Favicons

Ecosia Keyword Search Terms

Ecosia Logins

Ecosia Top Sites

Ecosia Web History

Ecosia Web Visits

Firefox Cache Records

Firefox Cookies

Firefox FormHistory

Google Analytics First Visit Cookies

Google Analytics First Visit Cookies Carved

Google Analytics Referral Cookies

Google Analytics Referral Cookies Carved

Google Analytics Session Cookies

Google Analytics Session Cookies Carved

Google Analytics URLs

Google Analytics URLs Carved

Iron Browser Autofill

Iron Browser Bookmarks

Iron Browser Cookies

Iron Browser Downloads

Iron Browser Favicons

Iron Browser Keyword Search Terms

Iron Browser Logins

Iron Browser Top Sites

Iron Browser Web History

Iron Browser Web Visits

Kiwi Browser Autofill

Kiwi Browser Bookmarks

Kiwi Browser Cookies

Kiwi Browser Downloads

Kiwi Browser Favicons

Kiwi Browser Keyword Search Terms

Kiwi Browser Top Sites

Kiwi Browser Web History

Kiwi Browser Web Visits

Lunascape Autofill

Lunascape Bookmarks

Lunascape Cookies

Lunascape History

Malware - Phishing URLs

Naver Web History

Opera Autofill

Opera Bookmarks

Opera Cookies

Opera Downloads

Opera Favicons

Opera Keyword Search Terms

Opera Top Sites

Opera Web History

Opera Web Visits

Pornography URLs

Puffin Browser Bookmarks

Puffin Browser History

Rebuilt Webpages

Reddit Accounts

Reddit Posts

Reddit Recently Visited Subreddits

Samsung Browser Archived Keyword Search Terms

Samsung Browser Archived Web History

Samsung Browser Autofill

Samsung Browser Autofill Profiles

Samsung Browser Bookmarks

Samsung Browser Cache Records

Samsung Browser Cached Thumbnails

Samsung Browser Cookies

Samsung Browser Current Session

Samsung Browser Current Tabs

Samsung Browser Downloads

Samsung Browser Favlcons

Samsung Browser History Index

Samsung Browser Keyword Search Terms

Samsung Browser Last Session

Samsung Browser Last Tabs

Samsung Browser Logins

Samsung Browser Media History

Samsung Browser Saved Credit Cards

Samsung Browser Saved Pages

Samsung Browser Shortcuts

Samsung Browser Tabs

Samsung Browser Top Sites

Samsung Browser Web History

Samsung Browser Web Visits

Sleipnir Autofill

Sleipnir Bookmarks

Sleipnir Cookies

Sleipnir Search Terms

Sleipnir Web History

UC Browser Bookmarks

UC Browser Cookies

UC Browser Downloads

UC Browser History

WebKit Browser Session - Tabs - Carved

WebKit Browser Web History - Carved

Whale Autofill

Whale Bookmarks

Whale Cookies

Whale Downloads

Whale Favicons

Whale Keyword Search Terms

Whale Logins

Whale Top Sites

Whale Web History

Whale Web Visits

Yandex Autofill

Yandex Bookmarks

Yandex Cookies

Yandex Downloads

Yandex Favicons

Yandex Keyword Search Terms

Yandex Logins

Yandex Shortcuts

Yandex Sync Data

Yandex Top Sites

Yandex Web History

Yandex Web Visits

WebRelated

Baidu Searches

Baidu Web Visits

iOS

Advanced Search Tools

Dynamic Application Finder

Chat

AIM Buddies

AIM Messages

BlackBerry Messenger Contacts

BlackBerry Messenger File Transfers

BlackBerry Messenger Invitations

BlackBerry Messenger Locations

BlackBerry Messenger Messages

BlackBerry Messenger Profile

Discord Messages

Facebook Messenger Calls

Facebook Messenger Groups

Facebook Messenger Messages

Facebook Messenger Users Contacted

Glide Messages

Glide Users

Google Duo Calls

Google Hangouts Voice Calls

Grindr Buddies

Grindr Messages

GROWLr Chat Messages

GROWLr Notes

iOS Burner Conversations

iOS Burner Numbers

iOS Google Hangouts Cached Images

iOS Google Hangouts Contacts

iOS Google Hangouts Messages

iOS Kik Messenger Attachments

iOS Kik Messenger Messages

iOS Kik Messenger Users

iOS Telegram Channel Chats

iOS Telegram Chats

iOS Telegram Messages

iOS Telegram Users

iOS Textfree Cache Records

iOS TigerText Messages

iOS Tinder Accounts

iOS Tinder Matches

iOS Tinder Messages

iOS Tinder Photos

iOS WhatsApp Messages

Life360 Circle Members

Life360 Local User Account

Life360 Messages

Life360 Places

Life360 Trip Locations

LINE Contacts

LINE Local Users

LINE Messages

LINE Pictures

ooVoo Chat History

ooVoo Contact List

ooVoo Phone Book

QQ File Transfers

QQ Local Users

QQ Messages

QQ Messages Carved

Signal Contacts

Signal Group Members

Signal Local User

Signal Messages - iOS

Skype Accounts

Skype Activity

Skype Calls

Skype Chat Messages

Skype Chatsync Messages

Skype Contacts

Skype Emotions

Skype File Transfers

Skype Group Chat

Skype IP Addresses

Skype Notifications

Skype SMS

Skype Voicemails

Slack Channel Messages

Slack Channels

Slack Direct Messages

Slack Files

Slack Users

Slack Workspaces

TamTam Messenger Channels - iOS

TamTam Messenger Contacts - iOS

TamTam Messenger Conversations - iOS

TamTam Messenger Groups - iOS

TamTam Messenger Messages - iOS

Textfree Attachments

Textfree Contacts

Textfree Groups

Textfree Messages

TextMe Calls

TextMe Messages

TextNow Calls

TextNow Chat

TextNow Contacts

TextNow Groups

TextNow Profile

TextPlus Calls

- TextPlus Messages
- Viber Messages
- WeChat Friends
- WeChat Messages
- WhatsApp
    - Artifacts
    - iOS WhatsApp Chats
    - iOS WhatsApp Contacts
    - iOS WhatsApp Groups
- Zalo Contacts
- Zalo Groups
- Zalo Messages
- Zalo Profiles
- Zoom Chat Messages
- Zoom Meeting Messages
- Zoom User Accounts

Cloud

- iOS Dropbox
- iOS Dropbox Carved

Documents

- Excel Documents
- PDF Documents
- PowerPoint Documents
- RTF Documents
- Text Documents

Word Documents

E-mail

Apple Mail

Apple Mail Fragments

Gmail Emails

iOS Yahoo Mail Contacts

iOS Yahoo Mail Messages

iOS Yahoo Mail User Accounts

Outlook Appointments

Outlook Contacts

Outlook Messages

Encryption

Best Secret Folder Configuration Data

Internet of Things

Amazon Alexa Audio Activity

Amazon Alexa Device Information

Amazon Alexa Tasks

Amazon Alexa User

Amazon Alexa Web Resource

Apple Health Distance

Apple Health Floors

Apple Health Steps

Fitbit Activity Log

Fitbit Floors

Fitbit Profiles

- Fitbit Sleep
- Fitbit Steps
- Nest Location Configuration
- Nest Temperature Adjustment
- Nest User
- Pebble Activity Information
- Pebble Calendar Events
- Pebble Physical Characteristics
- Pebble Steps
- Pebble Weather Locations

Media

- AMR Files
- Audio
- Carved Video
- iOS Snapchat Conversations
- iOS Snapchat My Story
- Live Photos
- Pictures
- Snapchat Chat Messages
- Snapchat Received Videos
- Videos

Mobile

- SIM Card ICCID
- SIM Card IMSI
- SIM Card Phone Numbers

SIM Card Service Providers

SIM Card SMS Messages

Operating System

Apple Accounts

Apple Contacts - iOS

Apple Keychain Generic Passwords

Apple Keychain Internet Passwords

Apple Keychain Saved Credit Cards

Apple Maps Trips

Apple Notes

Apple Notes - Voice

Application Install States

Application Permissions

Bluetooth Devices

Cached Locations

Calendar Events

File Signature Mismatch - Audio

File Signature Mismatch - Container

File Signature Mismatch - Document

File Signature Mismatch - Picture

File Signature Mismatch - Video

File System Events

File System Information

Installed Applications

iOS App Cache

iOS Call Logs

iOS Device Information

iOS iMessage - SMS - MMS

iOS Maps

iOS PowerLog App Usage

iOS PowerLog Process Data Usage

iOS PowerLog Timezone Information

iOS Snapshots

iOS Spotlight

iOS User Shortcut Dictionary

iOS User Word Dictionary

iOS Voice Mail

KnowledgeC Application Activities

KnowledgeC Application Focus

KnowledgeC Application Install States

KnowledgeC Device Lock States

KnowledgeC Device Orientation States

KnowledgeC Device Plugged-in States

KnowledgeC Do Not Disturb Usage

KnowledgeC Media History

KnowledgeC Safari History

KnowledgeC Screen Backlight States

KnowledgeC Siri UI Usage

Network Usage - Application Data

Network Usage - Connections

- Owner Information
- Screen Time Synced Applications
- Screen Time Usage
- Seen Bluetooth Devices
- Significant Locations
- Significant Locations Visits
- SIM Card Activity
- Siri Message Search Suggestions
- Wallet Passes
- Wallet Payment Cards
- Wallet Transactions
- Wi-Fi Profiles

Peer-to-Peer

- Torrent File Fragments

Social Networking

- Facebook
  - iOS Facebook Friends
  - iOS Facebook Messages
- Foursquare Check-ins
- Foursquare Locations
- Instagram Direct Messages
- Instagram Group Members
- Instagram Media
- Instagram Profiles
- iOS Whisper Posts

Sina Weibo Posts

Sina Weibo Private Messages

TikTok Contacts

TikTok Messages

TikTok Videos

Twitter Direct Messages

Twitter Friends

Twitter Tweets

VK Messages

VK Users

Whisper Messages

Yik Yak Notifications

Yik Yak Yaks

Transportation and Travel

Lyft Account Information

Lyft Last Known Location

Lyft Rider Payment Details

OnStar RemoteLink Hotspot Info

OnStar RemoteLink Remote Commands

OnStar RemoteLink Saved Wireless Carrier

OnStar RemoteLink Searches

OnStar RemoteLink Vehicle Diagnostics

OnStar RemoteLink Vehicle Info

Uber Accounts

Uber Cached Locations

- Uber Locations
- Uber Payments
- Uber Profiles
- Uber Rider Payment Details
- Uber Trips
- Waze Events
- Waze Favorites
- Waze Places

Web Related

- Brave Tab History
- Brave Web History - iOS
- Browser Activity
- Chrome
  - Chrome Archived Keyword Search Terms
  - Chrome Archived Web History
  - Chrome Autofill Profiles
  - Chrome Autofill
  - Chrome Bookmarks
  - Chrome Cache Records
  - Chrome Cookies
  - Chrome Current Session
  - Chrome Current Tabs
  - Chrome Downloads
  - Chrome FavIcons
  - Chrome History Index

Chrome Keyword Search Terms

Chrome Last Session

Chrome Last Tabs

Chrome Logins

Chrome Saved Credit Cards

Chrome Shortcuts

Chrome Top Sites

Chrome Web History

Chrome Web Visits

Dolphin Browser Bookmarks

Dolphin Browser History

Ecosia Bookmarks

Ecosia Current Tabs

Ecosia Web History

Google Analytics First Visit Cookies

Google Analytics First Visit Cookies Carved

Google Analytics Referral Cookies

Google Analytics Referral Cookies Carved

Google Analytics Session Cookies

Google Analytics Session Cookies Carved

Google Analytics URLs

Google Analytics URLs Carved

iOS Google Map Coordinates

iOS Safari Cache

iOS Safari Recent Search Terms

Malware - Phishing URLs

Pornography URLs

Puffin Browser Bookmarks

Puffin Browser History

Rebuilt Webpages

Reddit Accounts

Reddit Posts

Reddit Recently Visited Subreddits

Safari Bookmarks

Safari History

Safari iCloud Devices

Safari iCloud Tabs

Safari Tabs

WebKit Browser Session - Tabs - Carved

WebKit Browser Web History - Carved

Whale Autofill

Whale Bookmarks

Whale Cookies

Whale Downloads

Whale Favicons

Whale Keyword Search Terms

Whale Logins

Whale Top Sites

Whale Web History

Whale Web Visits

Yandex Autofill

Yandex Bookmarks

Yandex Cookies

Yandex Downloads

Yandex Favicons

Yandex Keyword Search Terms

Yandex Logins

Yandex Shortcuts

Yandex Sync Data

Yandex Top Sites

Yandex Web History

Yandex Web Visits

macOS

Chat

iMessage Archived Chats

iMessage Archived Messages

iMessage Chats

iMessage Messages

Skype Accounts

Skype Activity

Skype Contacts

Skype Group Chat

Documents

CSV Documents

Excel Documents

PDF Documents

PowerPoint Documents

RTF Documents

Text Documents

Word Documents

Email

Calendar Events - ICS

Media

Audio

Carved Video

Pictures

Quicktime Player History

Videos

VLC Recently Played Files

Web Video Fragments

Operating System

Apple Accounts

Apple Contacts - macOS

Apple Contacts Groups

Apple Keychain Generic Passwords

Apple Keychain Internet Passwords

Apple Notes

Bash Sessions

Bluetooth Devices - macOS

CoreAnalytics

Daily Logs - Disk Status

Daily Logs - Local System Status

Daily Logs - Network Interfaces Status

Deleted Accounts

Dock Items

File Signature Mismatch - Audio

File Signature Mismatch - Container

File Signature Mismatch - Document

File Signature Mismatch - Picture

File Signature Mismatch - Video

File System Events

File System Information - APFS

Finder MRU

Finder Sidebar Items

Installed Applications - macOS

KnowledgeC Application Activities

KnowledgeC Application Focus

KnowledgeC Application Install States

KnowledgeC Device Lock States

KnowledgeC Device Orientation States

KnowledgeC Device Plugged-in States

KnowledgeC Media History

KnowledgeC Safari History

KnowledgeC Screen Backlight States

Login History

Menu Bar Apps

Network Interfaces - macOS

Network Profiles - macOS

Network Utilities

Operating System Information - macOS

Quick Look Thumbnails

Recently Used Items

Recovery Account Information

Resumed Apps - macOS

Spotlight Shortcuts

Startup Items - macOS

Trash Items

USB Connection History

User Accounts - macOS

Volume Information

Wi-Fi Logs

Web Related

Chrome Archived Keyword Search Terms

Chrome Archived Web History

Chrome Autofill

Chrome Autofill Profiles

Chrome Bookmarks

Chrome Cache Records

Chrome Cookies

Chrome Current Session

Chrome Current Tabs

Chrome Downloads

Chrome Extensions

Chrome FavIcons

Chrome History Index

Chrome Keyword Search Terms

Chrome Last Session

Chrome Last Tabs

Chrome Logins

Chrome Saved Credit Cards

Chrome Shortcuts

Chrome Sync Accounts

Chrome Sync Data

Chrome Top Sites

Chrome Web History

Chrome Web Visits

Firefox Add-ons

Firefox Bookmarks

Firefox Cache Records

Firefox Cookies

Firefox Downloads

Firefox FavIcons

Firefox FormHistory

Firefox Input History

Firefox Private Browsing History

Firefox SessionStore Artifacts

Firefox Web History

Firefox Web Visits

Google Analytics First Visit Cookies

Google Analytics First Visit Cookies Carved

Google Analytics Referral Cookies

Google Analytics Referral Cookies Carved

Google Analytics Session Cookies

Google Analytics Session Cookies Carved

Google Analytics URLs

Google Analytics URLs Carved

Google Maps

Google Maps Tiles

Malware - Phishing URLs

Pornography URLs

Rebuilt Webpages

Safari Bookmarks

Safari Cache Records

Safari Downloads

Safari History

Safari iCloud Devices

Safari iCloud Tabs

Safari Last Session

Safari Top Sites

WebKit Browser Session - Tabs - Carved

WebKit Browser Web History - Carved

Cloud

Chat

Cloud Google Hangouts Messages

Cloud Slack Channels

Cloud Slack Messages

Cloud Slack Users

Cloud Slack Workspaces

Cloud

Cloud Dropbox Files

Cloud Facebook Messenger Messages - Warrant Return

Cloud Google Activity

Cloud Google Calendar Events

Cloud Google Chrome Autofill

Cloud Google Chrome Bookmarks

Cloud Google Chrome Browser History

Cloud Google Chrome Extension Settings

Cloud Google Chrome Extensions

Cloud Google Chrome Search Engines

Cloud Google Chrome Sync Settings App Settings

Cloud Google Chrome Sync Settings Apps

Cloud Google Chrome Sync Settings Preferences

Cloud Google Connected Apps

Cloud Google Contacts

Cloud Google Drive Files

Cloud Google Keep

Cloud Google Passwords

Cloud Google Recent Devices

Cloud Google Tasks

Cloud iCloud Mail

Cloud Instagram Account Actions - Warrant Return

Cloud Instagram Comments - Warrant Return

Cloud Instagram Direct Shares - Warrant Return

Cloud Instagram Direct Stories - Warrant Return

Cloud Instagram Followers and Following - Warrant Return

Cloud Instagram Photos - Warrant Return

Cloud Microsoft Teams Messages

Cloud Microsoft Teams Teams

Cloud Office 365 Audit Logs

Cloud Office 365 Outlook Calendars

Cloud Office 365 Outlook Contacts

Cloud OneDrive Files

Cloud SharePoint Content

Cloud SharePoint Documents

Cloud Sharepoint Site Pages

Cloud Snapchat Account Information - Warrant Return

Cloud Snapchat Friends - Warrant Return

Cloud Snapchat Group Chat Messages - Warrant Return

Cloud Snapchat IP History - Warrant Return

Cloud Snapchat Messages - Warrant Return

Cloud WhatsApp Backups

G Suite Drive Events

G Suite Login Events

iCloud Backups

iCloud Drive Files

iCloud Photos

E-Mail

Cloud Google Gmail Messages

Cloud IMAP - POP Emails

Cloud Office 365 Hotmail - Outlook Emails

Email

Cloud MBOX Emails

Media

Cloud Google Photos

Cloud Google Photos - AXIOM

Social Networking

Cloud Facebook Audit Logs - Warrant Return

Cloud Facebook Friend Requests - Warrant Return

Cloud Facebook Friends

Cloud Facebook Friends - Warrant Return

Cloud Facebook Messenger Messages

Cloud Facebook Messenger Messages - Warrant Return

Cloud Facebook Photos - Warrant Return

Cloud Facebook Posts

Cloud Facebook Profile Info

Cloud Facebook Status Updates - Warrant Return

Cloud Facebook Timeline

Cloud Facebook Wallposts - Warrant Return

Cloud Instagram Direct Messages

Cloud Instagram Posts

Cloud Instagram Posts - AXIOM

Cloud Twitter Direct Messages

Cloud Twitter Posts

Cloud Twitter Posts Public

Cloud Twitter Users

Cloud Twitter Users Public

Transportation and Travel

Cloud Google Timeline Locations

Windows Phone

Advanced Search Tools

Dynamic Application Finder

Chat

Lync - OC Calls

Lync - OC File Transfers

Lync - OC Fragments

Lync - OC Messages

Skype Accounts

Skype Calls

Skype Chat Messages

Skype Chatsync Messages

Skype Chatsync Messages Carved

Skype Contacts

Skype File Transfers

Skype Group Chat

Skype IP Addresses

Skype SMS

Skype Voicemails

Documents

Excel Documents

PDF Documents

PowerPoint Documents

RTF Documents

Text Documents

Word Documents

E-mail

Gmail Email Fragments

Gmail Webmail

Hotmail Webmail

Hushmail Webmail

Mailinator Inbox Access

Mailinator Snippets

Offline Gmail webmail

Outlook Appointments

Outlook Contacts

Outlook Journals

Outlook Messages

Outlook Notes

Outlook Tasks

Outlook Web App Email Fragments

Outlook Web App Inbox

Outlook Webmail Inbox

Windows Phone Emails

Media

Audio

Carved Video

Pictures

Videos

Web Video Fragments

Mobile

SIM Card ICCID

SIM Card IMSI

SIM Card Phone Numbers

SIM Card Service Providers

SIM Card SMS Messages

Operating System

File Signature Mismatch - Audio

File Signature Mismatch - Container

File Signature Mismatch - Document

File Signature Mismatch - Picture

File Signature Mismatch - Video

Jump List Dest List Entries

Jump List Shortcut Entries

LNK Files

Network Share Information

Operating System Information

Prefetch Files - Windows 8 - 10

Prefetch Files - Windows XP - Vista - 7

Shellbags

Startup Items

Timezone Information

USB Devices

User Accounts

Windows Event Logs

Windows Phone Call Logs

Windows Phone Contacts

Windows Phone Contacts Carved Fragments

Windows Phone SMS - MMS

Social Networking

Bebo Live Chat

Facebook

Facebook Chat

Facebook Email Snippets

Facebook Email

Facebook Pages

Facebook Pictures

Facebook Status Updates - Wall Posts - Comments

Instagram Pictures

Instagram Posts

LinkedIn Emails

MySpace Chat - User Info

MySpace Live Chat

Sina Weibo Carved Searches

Sina Weibo Microblogs

Sina Weibo Search History

Twitter

Web Related

360 Safe Browser Archived Keyword Search Terms

360 Safe Browser Archived Web History

360 Safe Browser Autofill

360 Safe Browser Autofill Profiles

360 Safe Browser Bookmarks

360 Safe Browser Cache Records

360 Safe Browser Cookies

360 Safe Browser Current Downloads

360 Safe Browser Current Session

360 Safe Browser Current Tabs

360 Safe Browser FavIcons

360 Safe Browser History Index

360 Safe Browser Last Session

360 Safe Browser Last Tabs

360 Safe Browser Logins

360 Safe Browser Saved Credit Cards

360 Safe Browser Shortcuts

360 Safe Browser Top Sites

360 Safe Browser Web History

360 Safe Browser Web Visits

Bing Toolbar - Search History

Browser Activity

Chrome

Chrome Autofill

Chrome Web Visits

Edge Cache Data

Edge Extensions

Edge Favorites

Edge Last Session

Edge Reading Lists

Edge Top Sites

Edge - Internet Explorer 10-11 Content

Edge - Internet Explorer 10-11 Cookies

Edge - Internet Explorer 10-11 Daily - Weekly History

Edge - Internet Explorer 10-11 Dependency Entries

Edge - Internet Explorer 10-11 Downloads

Edge - Internet Explorer 10-11 Main History

Firefox Bookmarks

Firefox Cache Records

Firefox Cookies

Firefox Downloads

Firefox FavIcons

Firefox FormHistory

Firefox Input History

Firefox Private Browsing History

Firefox SessionStore Artifacts

Firefox Web History

Firefox Web **Visits**

Flash Cookies

Google Analytics First Visit Cookies

Google Analytics First Visit Cookies Carved

Google Analytics Referral Cookies

Google Analytics Referral Cookies Carved

Google Analytics Session Cookies

Google Analytics Session Cookies Carved

Google Analytics URLs

Google Analytics URLs Carved

Google Maps

Google Maps Tiles

Google Toolbar

Internet Explorer Cache Records

Internet Explorer Cookie Records

Internet Explorer Cookies

Internet Explorer Downloads

Internet Explorer Favorites

Internet Explorer InPrivate - Recovery URLs

Internet Explorer Leak Records

Internet Explorer Main History

Internet Explorer PrivacIE Records

Internet Explorer Typed URLs

Internet Explorer Weekly History

Malware - Phishing URLs

Opera Archived Keyword Search Terms

Opera Archived Web History

Opera Autofill Profiles

Opera Bookmarks

Opera Cache Records

Opera Cookies

Opera Current Session

Opera Current Tabs

Opera Downloads

Opera History Index

Opera Last Session

Opera Last Tabs

Opera Logins

Opera Saved Credit Cards

Opera Search Field History

Opera Shortcuts

Opera Top Sites

Opera Typed History

Opera Web History

Pornography URLs

Rebuilt Webpages

Safari Bookmarks

Safari Cache Records

Safari Downloads

Safari History

Safari Last Session

Safari Top Sites

WebKit Browser Session - Tabs - Carved

WebKit Browser Web History - Carved

Kindle

Advanced Search Tools

Dynamic Application Finder

Chat

AIM

AIM Chat Messages

Skype Accounts

Skype Calls

Skype Chat Messages

Skype Chatsync Messages

Skype Contacts

Skype IP Addresses

Cloud

- Android Dropbox
- Android Dropbox Account Info

Documents

- Excel Documents
- PDF Documents
- PowerPoint Documents
- RTF Documents
- Text Documents
- Word Documents

E-mail

- Android Emails
- Android Gmail
- Samsung Email Logs

Media

- Audio
- Carved Video
- Pictures
- Videos

Mobile

- Android Kik Messenger Attachments
- Android Kik Messenger Contacts
- Android Kik Messenger Messages
- SIM Card ICCID
- SIM Card IMSI
- SIM Card Phone Numbers

  - SIM Card Service Providers
  - SIM Card SMS Messages
- **Operating System**
  - Accounts Information
  - Android Downloads
  - File Signature Mismatch - Audio
  - File Signature Mismatch - Container
  - File Signature Mismatch - Document
  - File Signature Mismatch - Picture
  - File Signature Mismatch - Video
  - File System Information
- **Social Networking**
  - Android Instagram Posts
  - Android Instagram Users
  - Android Sina Weibo Posts
  - Android Sina Weibo Private Messages
  - Facebook
    - Android Facebook Pictures
    - Facebook Contacts
    - Facebook User - Friends
  - Twitter Tweets
  - Twitter Users
- **Web Related**
  - Google Analytics First Visit Cookies
  - Google Analytics First Visit Cookies Carved

Google Analytics Referral Cookies

Google Analytics Referral Cookies Carved

Google Analytics Session Cookies

Google Analytics Session Cookies Carved

Google Analytics URLs

Google Analytics URLs Carved

Google Maps

Google Maps Tiles

Kindle Silk Web History

Malware - Phishing URLs

Pornography URLs

Appendix D – Forensics Tools List Survey from LEA partner of the INSPECTr Consortium

INSPECTr LEA Tools	Tool Type	LEA1	LEA2	LEA3	LEA4	LEA5	LEA Total
EnCase	Computer Forensics	1	1	1	1	1	5
UFED (Cellebrite) for Phones	Mobile Forensics	1	1	1	1	1	5
Axiom (Magnet Forensics)	Digital Forensics	1	1	1	1		4
FTK Imager	Acquisition	1	1	1		1	4
MacQuisition	Acquisition	1	1	1	1		4
XRY	Mobile Forensics	1	1	1	1		4
DVR Examiner	CCTV	1		1	1		3
Griffeye Digital Investigator	Digital Forensics	1	1	1			3
Passware	Password cracking		1	1	1		3
Volatility	Memory Analysis		1	1		1	3
X-Ways	Digital Forensics		1	1	1		3
ADF Triage / Digital Investigator	Digital Forensics	1	1				2
Autopsy (freeware)	Digital Forensics	1				1	2
Berla	Automotive		1	1			2
Blacklight	Mac Forensics	1	1				2

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 833276

Forensic Explorer (GetData)	Digital Forensics	1			1		2
FTK	Computer Forensics			1	1		2
Maltego	OSINT		1			1	2
Nirsoft	Memory Analysis			1		1	2
Oxygen	Mobile Forensics		1		1		2
Palladin	Toolsets	1		1			2
Aid4Mail	Digital Forensics				1		1
Android photo forensics	Mobile Forensics				1		1
Arsenal Image Mounter (freeware)	Digital Forensics	1					1
Belkasoft	Digital Forensics				1		1
Caine Linux (freeware)	Digital Forensics	1					1
Chainalysis	Blockchain		1				1
Elcomsoft	Decryption		1				1
FiRST	Live Date Forensics			1			1
Gigatribe Forensic tools from Eric Zimmerman (freeware)	Digital Forensics	1					1