Mobile and Forensics
Vol. 5, No. 2, September 2023, pp. 01-14
ISSN: 2714-6685 (online), 2656-6257 (print)
DOI: http://dx.doi.org/10.12928/mf.v5i2.8937

Social Media Metadata Forensic Ontology Model

[1]Ibnu Rohan Tuharea, [2,*]Ahmad Luthfi, [3]Erika Ramdani
[123] Master Program in Informatics, Faculty of Industrial Technology, Universitas Islam Indonesia
[1]ibnu.tuharea@students.uii.ac.id, [2,*]ahmad.luthfi@uii.ac.id, [3]erika@uii.ac.id
[*]correspondence email

Abstract

The escalating use of compact electronic gadgets, such as smartphones and smartwatches, along with social media platforms, has paved the way for a new dimension of criminal activities. Concurrently, advancements in digital forensics, a field that delves into digital evidence investigations, have become noteworthy. Researchers David Christopher Harrill and Richard P. Mislan devised a subdivision of digital forensics, named Small-Scale Digital Device Forensics (SSDDF), which is centered around examining miniature digital devices often used in criminal undertakings. This inclusion in the broader spectrum of Device Forensics has shed light on the unique difficulties posed by such appliances. In another stride forward, Edlira Kalemi and Sule Yildirim-Yayilgan demonstrated the application of ontology in social media forensics, scrutinizing how digital proof from these platforms can be court-admissible. Their work involved deciphering the inherent frameworks of the Android system tied to social media, facilitating the recognition and extraction of different categories of digital data like user accounts, messages, and photographs, proving instrumental in social media-related forensic probes. However, it is pertinent to mention that their investigations primarily concentrated on digital evidence available on social media platforms, overlooking the instrumental role of gadgets used by both criminals and victims. The process of extracting digital data from these devices remains pivotal in securing germane evidence from social media. Notwithstanding, the incorporation of the SSDDF subsection and demystifying Android system structures have made substantial contributions to augmenting digital forensic methodologies. These enhancements can considerably bolster the investigation process, allowing for the capture and analysis of critical digital evidence from compact electronic appliances and social media platforms. In conclusion, the advent of SSDDF with the elucidation of Android system structures and also the application of ontology in social media forensics have offered invaluable inputs to the discipline of digital forensics, with a promising potential to enhance the efficacy and productivity of forensic investigations, specifically when amassing significant digital evidence from small electronic devices and social media platforms, paving the way for more robust digital evidence handling in the future.

Keywords: Ontology, RDF, OWL, Social Media, Digital Forensic, Smartphone

INTRODUCTION

The usage of the Internet and social media is increasing year by year. According to data from We Are Social on digital resource usage in Indonesia in February 2022, as cited from *datareportal.com*, the total population in Indonesia is 277.7 million, with 73.7% (204.7 million) Internet users, and 68.9% (191.4 million) social media users, which is a 12.6% increase from January 2021. The most widely used social media platforms among individuals aged 16 to 64 are WhatsApp at 88.7%, Instagram at 84.8%, Facebook at 81.3%, TikTok at 63.1%, Telegram at 62.8%, and Twitter at 58.3% [1].

This proliferation has given rise to various social media phenomena and behaviors over time, impacting personal lives, communication dynamics, and even criminal activities. These include trend or phenomena such as self-disclosure by sharing information about their activities and

Article History: *Received August 26, 2023; Revised September 7, 2023; Accepted September 19, 2023*

personal issues [2], new behaviors like taking selfies, cyber warfare, online shopping, user personalization, and the culture of sharing [3], self-disclosure [4], phubbing [5], the use of social media for entertainment [6], cyberbullying [7], the spread of hoaxes [8], narratives of terrorism and radicalism [9], as well as other criminal cases related to social media.

In the realm of digital forensics, the process of ensuring the admissibility of evidence in court involves several stages [10]. These stages can vary in number and order based on different cases and opinions. However, four of them are particularly important: acquisition, research, analysis, and presentation [11]. In the context of social media, two primary sources provide digital evidence: the devices owned by victims or suspects (clients) and the service providers (servers). These sources are critical during the acquisition stage, which serves as the foundation for subsequent investigation and analysis.

As we delve further into the realm of digital evidence, researchers often turn to ontological models to establish knowledge bases supporting the analysis process. Notably, David Christopher Harrill and Richard P. Mislan introduced the *Small-Scale Digital Device Forensics (SSDDF)* ontology, which has been further incorporated into the Device Forensic sub-ontology by Nickson M. Karie, M.Sc, and Hein S. Venter, Ph.D [12]-[13]. These ontological models play a crucial role in structuring and organizing the digital evidence landscape.

While some ontologies have been developed to address digital forensics in the context of social media, a notable gap remains. This gap becomes evident when considering the work of Edlira Kalemi, Sule Yildirim-Yayilgan, Elton Domnori and Ogerta Elezaj, who developed the SMoNt ontology specifically related to this topic. The perspective they adopt focuses on the digital evidence found in social media metadata, which can be considered valid evidence in court. Despite the wealth of information provided by social media metadata forensics, including diverse entities such as user profiles, messages, status posts, photos, friends, groups, and more [14], [15], these studies do not delve into the crucial connection between digital evidence and the electronic devices used.

Not many ontologies associate social media with electronic devices, even though in digital forensics, one of the three crucial stages in investigations is acquisition [11]. This stage involves collecting electronic devices from suspects and/or victims as evidence, which is then acquired as digital evidence. While the existing research landscape boasts separate ontologies for digital devices and social media, a conspicuous void remains when it comes to integrating these critical aspects in the field of digital forensics. This gap hinders the holistic and efficient examination of digital evidence in cases that involve both small-scale electronic devices and social media platforms. Bridging this gap has the potential to revolutionize the way digital forensics is conducted, offering investigators and law enforcement agencies a comprehensive tool to navigate the complex interplay between devices and social media data. By developing a unified ontology, this research strives to address this critical gap and contribute to the advancement of digital forensics, ultimately enhancing our capabilities in investigating criminal activities in the digital age.

Therefore, this research aims to develop a new ontology model that can map both sides of forensics: the small-scale electronic device aspect using the SSDDF subclass, which defines classes for device types (cell phones, smartphones, tablet computers, notebook computers, and others), and the social media data aspect within the social media forensics subclass. By combining these two classes, the small-scale electronic device aspect defined in the SSDDF subclass and the social media data aspect within the social media forensics subclass, the research aims to create a unified ontology. The outcome of this research is expected to map the relationship between mobile devices and social media metadata in the hierarchy of ontology classes and objects.

METHODS

In this research, we implement experimental method to map the ontology. In the subsequent phase of the research, a case study was conducted involving the interaction between the suspect's account (Garry Swihart), who uses a Samsung Galaxy Mega 2 Android device, and the victim's account (Norah Nolan), who uses a Samsung Galaxy J1 Ace Android device.

Case Study Implementation

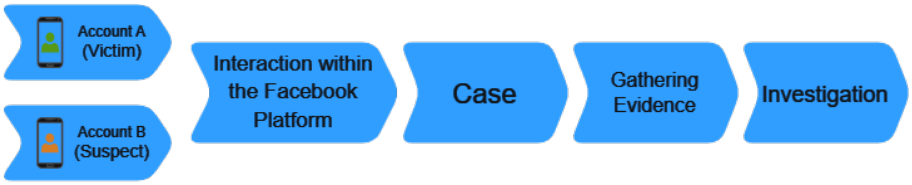

Figure 1. Case study implementation scheme

As mentioned before and depicted in Figure 1:

1. **Devices and Accounts**
   a. **Account A (Victim – Fictitious):** Norah Nolan, a fictitious individual, portrayed as a regular user of social media platforms, using a Samsung Galaxy J1 Ace Android device, which serves as her primary means of accessing and engaging with online content.
   b. **Account B (Suspect – Fictitious):** Garry Swihart, a fictitious character, depicted as an individual with potential suspicious activities on social media, using a Samsung Galaxy Mega 2 Android device as his main tool for interacting with others on digital platforms.
2. **Interaction within the Facebook Platform:** The initial contact occurred when the fictitious suspect (Garry Swihart) initiated a friend request to the fictitious victim (Norah Nolan) on the Facebook platform. Subsequently, he extended an invitation to join a group titled "Branded Bags & Accessories," where he held the position of group administrator. This initial interaction marked the commencement of their communication within this social media ecosystem.
3. **Case*:*** Within the Facebook group "Branded Bags & Accessories," the fictitious suspect (Garry Swihart) strategically posted content aimed at capturing the attention of the fictitious victim (Norah Nolan). These posts were designed to pique her interest, and as a result, she engaged by commenting on several of them. This initial interaction within the group led to further communication through private messages.
4. **Investigation*:*** In response to the escalating interaction between the fictitious victim (Norah Nolan) and the fictitious suspect (Garry Swihart) through private messages, investigators initiated the process of gathering evidence. This involved meticulous collection and preservation of all pertinent digital communications, including text messages, multimedia files, and associated timestamps. The investigation's objective was to construct a comprehensive timeline of the interactions, identify potential evidence of any illicit activities, and scrutinize the intentions and actions of both fictitious parties involved.

Device Conditions and Limitations

This research involved the use of two Samsung Android smartphones: Samsung Galaxy Mega 2 and Samsung Galaxy J1 Ace. These devices differ in terms of their software specifications. The Samsung Galaxy Mega 2 has the latest ROM (Baseband G750HXXU1ANI5) and runs on Android version 4.4.4 (KitKat). On the other hand, the Samsung Galaxy J1 Ace has the latest ROM (Baseband J11FXXU0AQE1) and operates on Android version 5.1.1 (Lollipop).

These devices where choosen is to maximize completeness of data acquisition opportunities by utilizing rooting methods on the Android KitKat and Lolipop version platform. For more detailed

information, please refer to Table 1, which provides a comprehensive overview of these specifications.

Table 1. Map of the device in the case study

Brand & Type	Device Code	Android Version	Username	Role
Samsung Galaxy Mega 2	vasta3g	4.4.4 (Kitkat)	Norah Nolan	Victim
Samsung Galaxy J1 Ace	j1acevelte	5.1.1 (Lolipop)	Garry Swihart	Suspect

In the case of the two devices, the following conditions can be observed:

1) **for the Android KitKat version (used by the victim)**
   The *Facebook* application (*com.facebook.katana* or as FB) is not available in the Play Store. However, as an alternative, *Facebook Lite* (*com.facebook.lite* or as FBL) is available as a lightweight version of the regular *Facebook* application. Therefore, *Facebook Lite* has become a convenient choice for installation
2) **for the Android Lollipop version (used by the suspect)**
   The FB is still available in the Play Store. Hence, there are no obstacles encountered, unlike in previous Android versions.

Data Acquisition

After implementing the case study, we proceeded with data acquisition from both devices using the following methods:

1) **Rooting both devices using magisk***,* to ensure comprehensive access to the device's data and applications, we utilized the Magisk rooting method. Magisk is a suite of open-source software for customizing almost all version of Android with more than 260 contributors on the project development [16], [17], especially to it root feature. Rooting allows for elevated privileges, enabling the extraction of meaningful data that might otherwise be inaccessible [18]
2) **Conducting the acquisition of both devices using the dd method***,* employed this method to create a bit-by-bit copy of the device's storage. This approach ensures acquiring more data [19], including text messages, images, application data, and system files.
3) **Transferring the acquired data from the Android Debug Bridge (ADB) shell to the host computer using nc (Netcat) command installed by Busybox.** ADB is the open-source tools to run command-line operation such as installing and debugging apps in the android device [20]. it can access dd command in the android device also. ADB is a common tool when like [18], [19], [21]. Busybox is a set of tiny UNIX programs for small or embedded systems [22], we use it to install and then run nc command (Netcat) in both devices to perform networking operation. Once the data acquisition process was complete, the acquired data, in the form of '.dd' files, was transferred from the ADB shell to the host computer with nc command. This step is essential for further analysis and examination of the collected digital evidence.
4) **The transferred data acquisition results are in the .dd file extension.** The acquired data from both devices was saved in '.dd' file format, a raw extension well known for acquisition disk image in digital forensics.

Challenges and Limitations

In the case study, we discovered several challenges and limitations:

1) **Data Limitations for FB and FBL***,* one notable challenge was the limited scope of acquired data from Facebook (FB) and Facebook Lite (FBL). While FB provided contact and local media data that could be obtained as evidence, FBL had more restricted data access, offering only contact data.

2) **Inclusion of Messenger (FBM)**, another challenge involved integrating an additional application, Messenger (*com.facebook.orca* or FBM). While Messenger offers specific functions and features for sending messages between FB users, extracting data regarding private messages or conversations between the two accounts presented its own set of challenges.

These challenges and limitations influenced the data collection process and should be considered when interpreting the findings of this research. They underscore the complexities and nuances involved in digital forensics and the acquisition of data from social media platforms.

RESULT AND DISCUSSIONS

Practical Application of SSDDF Ontology

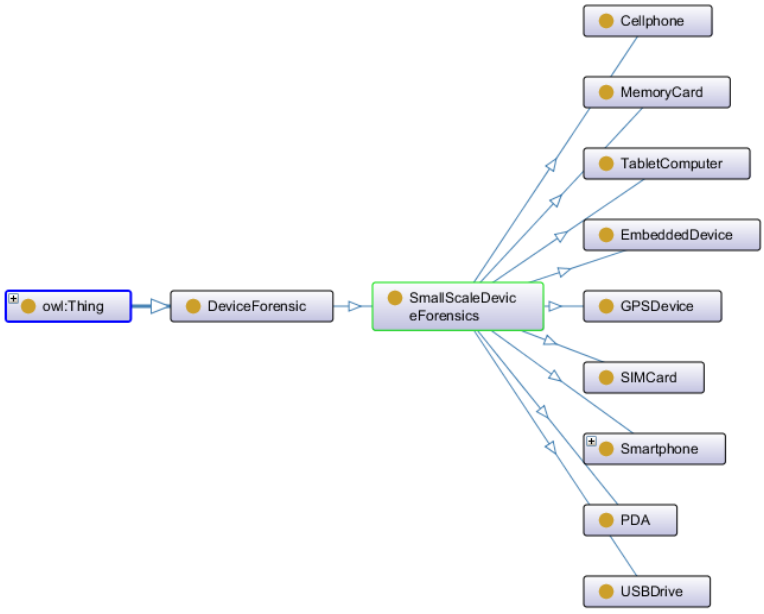

Figure 2. SSDDF ontology

In Figure 2, we present the Small-Scale Digital Device Forensic (SSDDF) Ontology, a crucial component of our research that plays a central role in categorizing and organizing digital evidence from small-scale digital devices. This ontology serves as the foundation for our exploration of digital forensic investigations on devices such as *smartphones*, *memory cards*, and *embedded systems*.

In this section, we illustrate the practical utility of the Small-Scale Digital Device Forensic (SSDDF) ontology in real-world digital forensic investigations. The SSDDF ontology serves as a valuable tool for law enforcement agencies and forensic experts, enhancing their capabilities in the following ways:

1) Streamlined Data Analysis: The SSDDF ontology provides a structured framework for organizing and categorizing digital evidence obtained from small-scale digital devices. By leveraging predefined classes and relationships, investigators can efficiently analyze data, leading to quicker insights.

2) Cross-Device Correlation: In multi-device investigations, the SSDDF ontology allows investigators to correlate data from various sources. For example, it enables linking evidence from smartphones, memory cards, and embedded devices to reconstruct a comprehensive timeline of events.

3) Enhanced Data Retrieval: With well-defined classes and properties, the ontology simplifies data retrieval. Investigators can quickly locate relevant information, such as chat histories, media files, or user profiles, leading to more effective case resolutions.

4) Integration with Existing Tools: The SSDDF ontology can be integrated with existing digital forensic tools and software, making it accessible and user-friendly for forensic experts. This integration streamlines the investigative process without requiring extensive retraining.

Development of Small-Scale Digital Device Forensic Ontology

Developing an ontology for Small-Scale Digital Device Forensic (SSDDF) based on data acquisition can be done. In the Android system, there are several storage blocks, namely mmcblk0 representing internal storage and mmcblk1 representing external storage (if available), as shown in Figure 3.

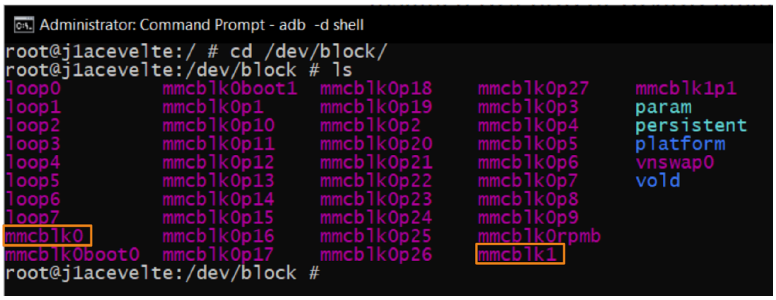

Figure 3. Block internal storage (mmcblk0) and external storage (mmcblk1) on the Samsung Galaxy J1 Ace device.

In the internal storage, we can explore the userdata partition along with its contents ("data", "media", and "system") to search for findings related to the Facebook applications (FB, FBL, and FBM) as shown in Figure 4. Within the "data" folder, we can find all data associated with installed applications, specifically for Facebook, each application has a consistent package name (folder) starting with *com.facebook* followed by the package name for each respective application.

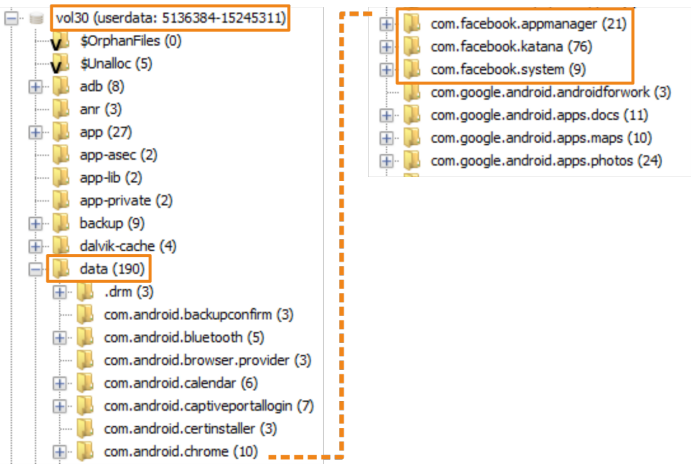

Figure 4. User data partition structure and Facebook application package list.

From the structure of the folders and the files found, a lot of data was discovered that indicates the presence of log files and databases representing the activities of both accounts, as obtained from the implementation of the case study. Some of these findings can be observed in Table 2.

Table 2. Findings of digital evidence

App Code	File	File Path	Description
Samsung Galaxy Mega 2 (vasta3g)			
com.facebook.lite	fblite_database.db	/vol_vol30/data/com.facebook.lite/databases/fblite_database.db	This database contains critical data from Facebook Lite, including user profiles, messages, and activity logs.
com.facebook.orca	msys_database_100090534141448	/vol_vol30/data/com.facebook.orca/databases/msys_database_100090534141448	The Messenger system database, which holds chat histories, attachments, and contact information.
Samsung Galaxy J1 Ace (j1acevelte)			
com.facebook.katana	app_uploads	/vol_vol30/data/com.facebook.katana/app_uploads	A directory where the Facebook app uploads media files, including photos and videos shared by users.
com.facebook.katana	contacts_db2	/vol_vol30/data/com.facebook.katana/databases/contacts_db2	A database that stores contact information from the Facebook app, aiding in contact tracing and connections analysis.
com.facebook.katana	local_media_db	/vol_vol30/data/com.facebook.katana/databases/local_media_db	This database houses locally stored media files shared on Facebook, offering insights into user media preferences.
com.facebook.katana	authentication	/vol_vol30/data/com.facebook.katana/app_light_prefs/com.facebook.katana/authentication	Authentication preferences data, crucial for understanding user login patterns and security measures. system
system	accounts.db	/vol_vol30/system/users/0/accounts.db	The system-level accounts database that holds information about user accounts on the device.

Based on the findings above, it can be concluded that SSDDF ontology needs to add several more structured classes to map the findings into the ontology. Essentially, we raise the competence question of "How to map the Small-Scale Digital Device Forensic ontology?" This is an initial assumption, considering the complexity of the existing data structure within the devices.

The presence of storage blocks representing mmcblk0 (Internal) and mmcblk1 (External) storage suggests that the primary focus of the exploration process should be on Internal storage. External storage, on the other hand, is optional as it involves removable media.

Furthermore, within the internal storage, the presence of the data, media, and system folders raises the hypothesis that there is a need for separate classes to map these directories for clearer identification and categorization. As a result, the competence question can be further divided and refined as follows:

1) How to map based on the nature of Internal and External storage?

Justification: The inclusion of classes to distinguish between internal and external storage elements (e.g., Internal and External classes) is crucial for precise data categorization. Digital forensic investigations often involve differentiating between data stored within the device's internal memory and data on removable external storage (e.g., memory cards). This distinction aids investigators in focusing their analysis on relevant data sources and ensures that the ontology accurately reflects the nature of the storage medium.

2) ***How to map the important structures present in internal storage?***

Justification: Internal storage within small-scale digital devices contains various critical structures (e.g., data, media, system) that require separate mapping. These structures are key to organizing and categorizing digital evidence effectively. By including classes such as data, media, and system, we ensure that investigators can precisely identify and access these essential components during the forensic analysis. This granularity enhances the ontology's utility in reconstructing digital timelines and extracting pertinent information.

3) ***How to map the structures present in external storage?***

Justification: While the primary focus lies on internal storage, external storage (e.g., memory cards) remains a potential source of digital evidence. Including classes to map external storage ensures that investigators can account for and analyze data stored on removable media when relevant. This flexibility accommodates diverse scenarios in digital forensic investigations, where external storage may contain valuable information related to the case.

By providing these justifications, we aim to clarify the rationale behind the selection and inclusion of specific classes and properties within the SSDDF ontology. These additions are designed to align with the practical requirements of digital forensic analysis, facilitating more efficient and effective investigations.

Implementation of Competency Questions

Competency questions play a pivotal role in defining the scope and structure of the SSDDF ontology. These questions guide the ontology's development and help ensure it effectively addresses the needs of digital device forensic analysis.

Initially, the SSDDF ontology's original class structure serves as a foundation. Subsequently, based on the competency questions, additional class structures are meticulously created to enhance the ontology's relevance and utility.

For instance, let's delve into the first competency question: "How to map based on the nature of Internal and External storage?" This question prompts the creation of classes dedicated to distinguishing between internal and external storage elements, ensuring precise data categorization and retrieval.

The resulting ontology, as depicted in Figure 5, provides a visual representation of how these classes are integrated to address this specific competency question.

Figure 5. *Addition of a class for the first competency question in the SSDDF ontology.*

For the second competency question, the classes that can be mapped are shown in Figure 6.

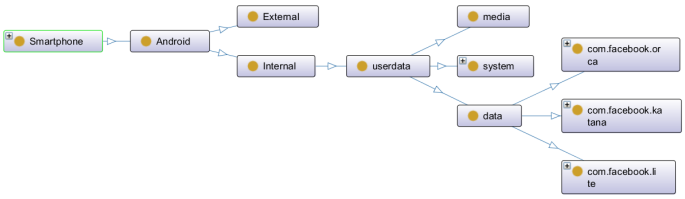

Figure 6. *Class addition for the second competency question in the SSDDF ontology.*

For the third competency question, the classes that can be mapped are depicted in Figure 7.

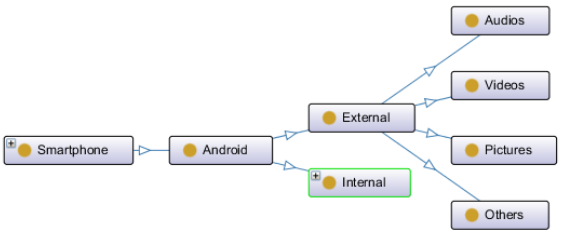

Figure 7. *Class addition for the third competency question in the SSDDF ontology.*

From the implementation of the three competency questions above, the complete SSDDF can be visualized in Figure 8.

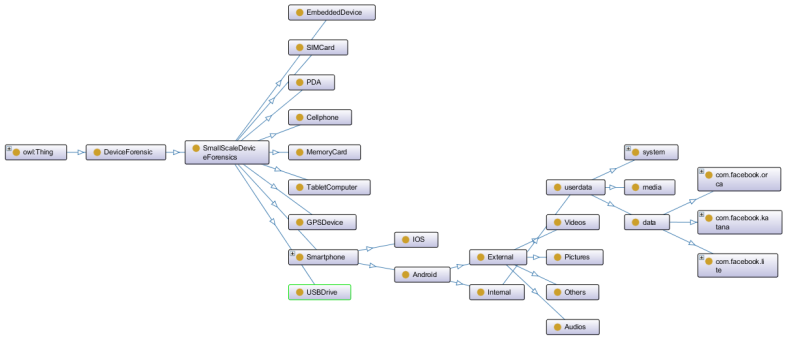

Figure 8. *The SSDDF ontology.*

Integration with existing ontologies, such as the *Social Media Evidence* ontology, offers a holistic approach to digital device forensic analysis. In this research endeavor, the SSDDF ontology [12], [13] seamlessly converges with the established *Social Media Evidence* ontology [14], [15], creating a unified and comprehensive knowledge framework.

The motivation behind this integration is to leverage the strengths of both ontologies. While SSDDF excels in structuring digital device forensic data, the *Social Media Evidence* ontology specializes in capturing metadata and contextual information from social media platforms. The amalgamation of these domains enriches our ability to derive meaningful insights from digital evidence.

Methodologically, this integration involves mapping relevant classes and properties from each ontology to ensure compatibility and data interoperability. By doing so, we can seamlessly correlate digital device data with social media activity, enhancing the depth and breadth of forensic analysis.

However, it's essential to acknowledge that this integration is not without its challenges. These include reconciling differences in class definitions, handling overlapping properties, and maintaining ontology consistency. Nevertheless, the benefits far outweigh these challenges.

In conclusion, Figure 9 provides an overview of the resulting integrated ontology. This collaborative effort between SSDDF and the *Social Media Evidence* ontology opens new avenues for advanced digital device forensic investigations.

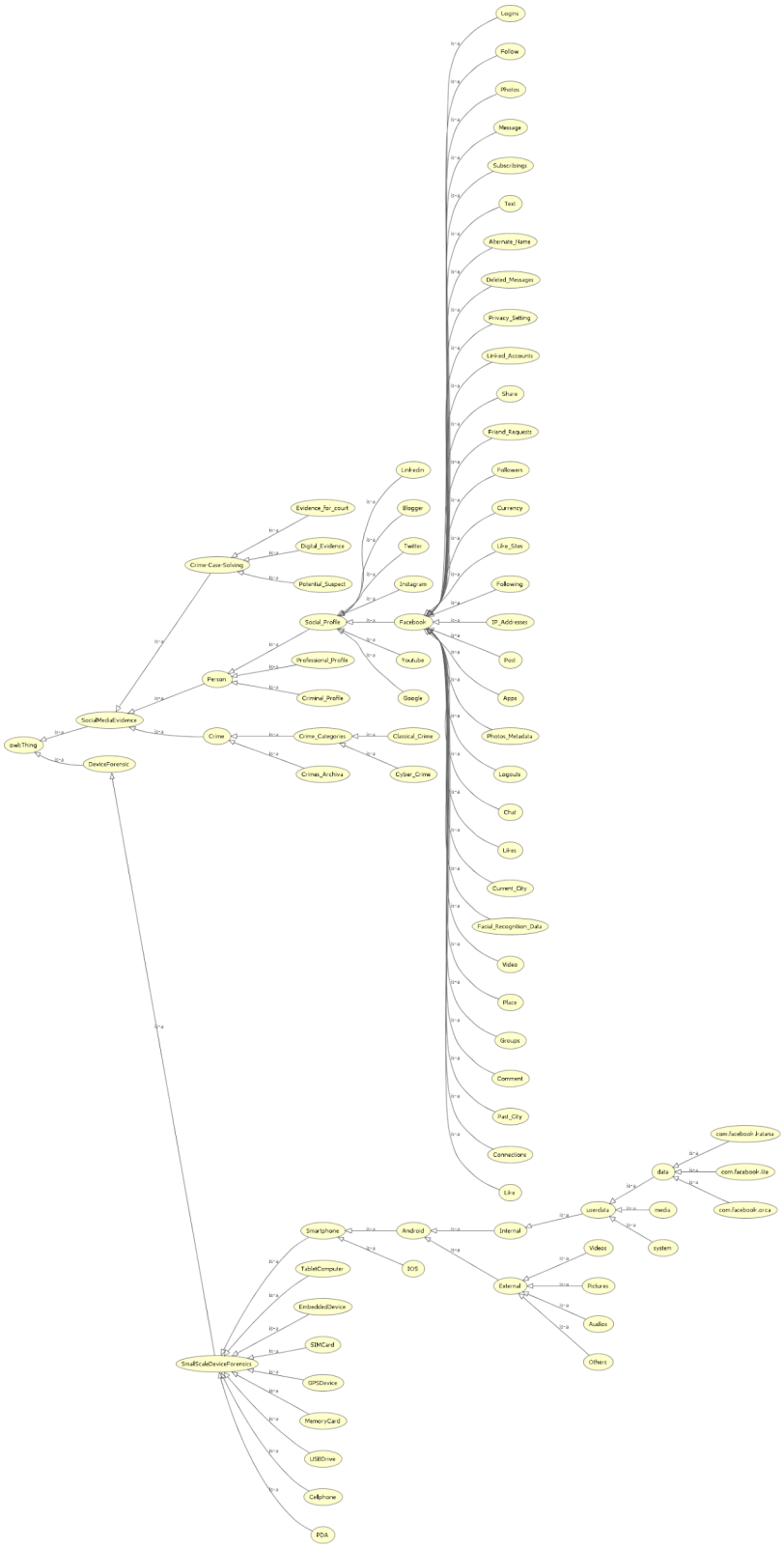

Figure 9. *The overall ontology.*

Class Structure

There are two major classes in ontology, *DeviceForensic* and *SocialMediaEvidence*. Each of them has its sub-classes :

1) *DeviceForensic: SmallScaleDeviceForensics, Cellphone, EmbeddedDevice, GPSDevice, MemoryCard, PDA, SIMCard, Smartphone, Android, External, Audios, Others, Pictures, Videos, Internal, userdata, data, com.facebook.katana, com.facebook.lite, com.facebook.orca, media, system, IOS, TabletComputer, USBDrive.*
2) *SocialMediaEvidence: Crime, Crime_Categories, Classical_Crime, Cyber_Crime, Crimes_Archiva, Crime-Case-Solving, Digital_Evidence, Evidence_for_court, Potential_Suspect, Person, Criminal_Profile, Professional_Profile, Social_Profile, Blogger, Facebook, Alternate_Name, Apps, Chat, Comment, Connections, Currency, Current_City, Deleted_Messages, Facial_Recognition_Data, Follow, Followers, Following, Friend_Requests, Groups, IP_Addresses, Like, Like_Sites, Likes, Linked_Accounts, Logins, Logouts, Message, Past_City, Photos, Photos_Metadata, Place, Post, Privacy_Setting, Share, Subscribings, Text, Video, Google, Instagram, Linkedin, Twitter, Youtube.*

The *DeviceForensic* ontology and the *SocialMediaEvidence* ontology offer distinct yet interconnected frameworks for digital forensic investigations. The *DeviceForensic* ontology primarily focuses on organizing and categorizing data acquired from small-scale digital devices, encompassing information related to storage, files, and device characteristics. Conversely, the *SocialMediaEvidence* ontology specializes in handling evidence originating from social media platforms, including user profiles, messages, connections, and online activities.

In many digital forensic cases, investigators encounter scenarios where evidence retrieved from small-scale digital devices, such as smartphones or memory cards, intersects with social media activity. For instance, a suspect's smartphone may contain chat histories, multimedia files, or location data relevant to a social media-related investigation. By employing both the *DeviceForensic* and *SocialMediaEvidence* ontologies in tandem, investigators gain the ability to seamlessly correlate and analyze evidence originating from these disparate yet interconnected sources.

The integration of device data with social media evidence facilitates a comprehensive and enriched contextual analysis of digital evidence. This synergy allows investigators to delve deeper into the circumstances surrounding a case. For instance, device data might reveal the timestamp of a photo, while social media data can provide insights into the user who shared it on a social platform. This combined context is invaluable for building a complete and accurate narrative of events, potentially uncovering critical details that might be missed when analyzing each type of evidence in isolation.

By forging a link between the *DeviceForensic* and *SocialMediaEvidence* ontologies, investigators can adopt a unified approach to digital forensic investigations. This unified framework empowers them to organize, analyze, and draw connections between evidence, regardless of whether it originates from a digital device or a social media platform. This simplifies the investigative process and enhances efficiency, ultimately leading to more effective and insightful results.

In essence, the integration of these two ontologies offers a cohesive and comprehensive solution for digital forensic experts and law enforcement agencies. It allows them to tackle the complexities of modern investigations that involve both digital devices and social media platforms, facilitating a more holistic and thorough examination of digital evidence. This approach opens up new avenues for advanced digital device forensic investigations, where evidence from various sources can be interconnected and analyzed within a unified framework.

Object Properties Structure

In the object properties, several properties have been added to enrich the knowledge within the ontology, such as: *administrator, advocate_of, as_account_in, author_of, bank_account_of, check_in, co_author, comment, current_work, dislike, education, eyewitness_of, family_relations, followed, geolocation, going_to, has_additional_item, has_advocate, has_attended, has_author, has_bank_account, has_blocked, has_brother, has_cousin, has_criminal_profile, has_device, has_eyewitness, has_father, has_husband, has_juror, has_mother, has_officer, has_political_status, has_religion, has_sister, has_wife, has_witness, hash_value, inspector_of, interested_in, is_closed, is_open, is_part_of, is_private, is_public, juror_of, like, location, member, mentioned, mentioned_by, officer_of, ownedby, owns, participate_same_riot, past_work, photo_of, published_emotions, published_status, same_organisation, share_via, stored_in, subscribe, tagged, tagged_by, talking_about, transferred_amount, transferred_by, transferred_to, uses_app, vality_url, video_of, visited, witness_to*.

Data Properties Structure

In the data properties structure, the researcher has added several properties, such as *directory*, *has_app*, and *parent_directory*. These three properties will be useful when mapping individuals related to *DeviceForensic*.

CONCLUSIONS

In this research, we exhibit the evolution of pre-existing ontologies as an aid to systematically categorize digital evidence located on both server and client endpoints. In this manner, the ontological framework can function as an advanced procedural methodology in the rigorous scrutiny of case files pertaining to social media incidents. We employed the sophisticated capabilities of the Social Media Digital Evidence Ontology, enabling us to meticulously organize data derived from the server-side service provider. In our pursuit for detail-oriented and specific mapping, we took into consideration the enhancement and subsequent deployment of the Small-Scale Digital Device Ontology (SSDDF). This was primarily to delineate the storage architecture within Android smartphones more explicitly, and concurrently, to organize data originating from mobile apparatuses, hereby referred to as clients.

Our contributions in this study have been twofold. Firstly, we harnessed the sophisticated capabilities of the Social Media Digital Evidence Ontology, enabling us to meticulously organize data derived from the server-side service provider. This ontological framework has emerged as a robust procedural methodology for rigorously scrutinizing case files related to social media incidents. Secondly, recognizing the need for explicit delineation of storage architecture within Android smartphones, we introduced the Small-Scale Digital Device Ontology (SSDDF). SSDDF plays a pivotal role in categorizing digital evidence obtained from mobile apparatuses, often referred to as clients.

The practical implications of our research are profound. With the deployment of SSDDF, forensic investigators and law enforcement agencies gain a structured framework for organizing and categorizing digital evidence extracted from small-scale digital devices. This empowers them with the ability to efficiently analyze data, leading to quicker insights, more effective cross-device correlation, and enhanced data retrieval. Moreover, SSDDF seamlessly integrates with existing digital forensic tools, eliminating the need for extensive retraining and streamlining the investigative process.

Looking ahead, there is an imminent need for additional research aimed at mapping storage systems spanning an array of mobile device platforms. These range from iOS-based smartphones and smartwatches to *Unmanned Aerial Vehicles (UAVs)* and beyond. Such advancements will serve to enrich the existing ontological infrastructure. Furthermore, a concerted effort to expand

research development on the practical implementation of *SparkQL* is crucial. This will effectively substantiate the intricate interlinkages between server and client data, thereby shedding light on the complex dynamics of data interactions within the digital ecosystem.

The complexities of integrating data from both server and client endpoints are not to be underestimated. Our ontological frameworks, including SSDDF, offer a structured approach to navigating these challenges. They provide a foundation for comprehending the intricate interplay between data sources, enhancing the depth of digital forensic analyses.

In closing, our research reaffirms the critical role of ontological frameworks in the realm of digital forensics. These frameworks not only categorize and organize digital evidence but also pave the way for more efficient, effective, and holistic investigative practices. As the digital landscape continues to evolve, embracing ontological methodologies becomes increasingly imperative for cybersecurity, law enforcement, and the broader field of digital forensics. Our work sets the stage for advanced investigations where digital evidence from diverse sources can be interconnected and analyzed within unified frameworks, ultimately contributing to a more secure and informed digital environment.

REFERENCES

[1] We Are Social, "Digital 2022: Indonesia - DataReportal - Global Digital Insights," *DateReportal*, 2022. https://datareportal.com/reports/digital-2022-indonesia (accessed Sep. 15, 2022).

[2] P. Qurrota Ayun, "Fenomena Remaja Menggunakan Media Sosial dalam Membentuk Identitas," *CHANNEL Jurnal Komunikasi*, vol. 3, no. 2, pp. 1–16, Oct. 2015, doi: 10.12928/channel.v3i2.3270.

[3] Mulawarman and A. D. Nurfitri, "Perilaku Pengguna Media Sosial beserta Implikasinya Ditinjau dari Perspektif Psikologi Sosial Terapan," *Buletin Psikologi*, vol. 25, no. 1, pp. 36–44, Jun. 2017, doi: 10.22146/buletinpsikologi.22759.

[4] A. Sagiyanto and N. Ardiyanti, "SELF DISCLOSURE MELALUI MEDIA SOSIAL INSTAGRAM (Studi Kasus Pada Anggota Galeri Quote)," *Nyimak (Journal of Communication)*, vol. 2, no. 1, pp. 81–94, Aug. 2018, doi: 10.31000/nyimak.v2i1.687.

[5] R. Aditia, "Fenomena Phubbing: Suatu Degradasi Relasi Sosial Sebagai Dampak Media Sosial," *KELUWIH: Jurnal Sosial dan Humaniora*, vol. 2, no. 1, pp. 8–14, Apr. 2021, doi: 10.24123/soshum.v2i1.4034.

[6] Y. N. Bulele and T. Wibowo, "ANALISIS FENOMENA SOSIAL MEDIA DAN KAUM MILENIAL: STUDI KASUS TIKTOK," *Conference on Business, Social Sciences and Innovation Technology*, vol. 1, no. 1, pp. 565–572, 2020, [Online]. Available: http://journal.uib.ac.id/index.php/cbssit

[7] M. Rifauddin, "Fenomena Cyberbullying pada Remaja," *Khizanah al-Hikmah : Jurnal Ilmu Perpustakaan, Informasi, dan Kearsipan*, vol. 4, no. 1, pp. 35–44, Jun. 2016, doi: 10.24252/kah.v4i1a3.

[8] R. Pakpahan, "ANALISIS FENOMENA HOAX DIBERBAGAI MEDIA SOSIAL DAN CARA MENANGGULANGI HOAX," *Konferensi Nasional Ilmu Sosial & Teknologi (KNiST)*, vol. 1, no. 1, pp. 479–484, Mar. 2017, Accessed: Sep. 17, 2022. [Online]. Available: http://seminar.bsi.ac.id/knist/index.php/UnivBSI/article/view/184

[9] R. Rustandi, "Analisis Framing Kontra Narasi Terorisme dan Radikalisme di Media Sosial (Studi Kasus pada Akun @dutadamaijabar)," *Jurnal Komunikatif*, vol. 9, no. 2, pp. 134–153, Dec. 2020, doi: 10.33508/jk.v9i2.2698.

[10] M. Nur Faiz, W. Adi Prabowo, and M. Fajar Sidiq, "Journal of Informatics, Information System, Software Engineering and Applications Studi Komparasi Investigasi Digital Forensik pada Tindak Kriminal," vol. 1, no. 1, pp. 63–70, 2018, doi: 10.20895/INISTA.V1I1.

[11] D. Ranđelović and D. Stojković, "Possibilities of autopsy tool use for forensic purposes," *Nauka, bezbednost, policija*, vol. 17, no. 3, pp. 19–33, 2012.

[12] D. C. Harrill and R. P. Mislan, "A Small Scale Digital Device Forensics ontology," *Small Scale Digital Device Forensics Journal*, vol. 1, no. 1, pp. 1–7, 2007.

[13] N. M. Karie and H. S. Venter, "Toward a general ontology for digital forensic disciplines," *J Forensic Sci*, vol. 59, no. 5, pp. 1231–1241, 2014, doi: 10.1111/1556-4029.12511.

[14] E. Kalemi and S. Yildirim-yayilgan, "Ontologies for Social Media Digital Evidence," no. January, 2016.

[15] E. Kalemi, S. Yildirim-Yayilgan, E. Domnori, and O. Elezaj, "SMoNt: An ontology for crime solving through social media," *Int J Metadata Semant Ontol*, vol. 12, no. 2–3, pp. 71–81, 2017, doi: 10.1504/IJMSO.2017.090756.
[16] "Download Magisk Manager Latest Version 26.3 For Android 2023." https://magiskmanager.com/ (accessed Sep. 18, 2023).
[17] "GitHub - topjohnwu/Magisk: The Magic Mask for Android." https://github.com/topjohnwu/Magisk (accessed Sep. 18, 2023).
[18] M.-R. Boueiz, "Importance of rooting in an Android data acquisition," in *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, IEEE, Jun. 2020, pp. 1–4. doi: 10.1109/ISDFS49300.2020.9116445.
[19] H. H. Lwin, W. P. Aung, and K. K. Lin, "Comparative Analysis of Android Mobile Forensics Tools."
[20] "Android Debug Bridge (adb) | Android Studio | Android Developers." https://developer.android.com/tools/adb (accessed Sep. 18, 2023).
[21] T. Almehmadi and O. Batarfi, "Impact of Android Phone Rooting on User Data Integrity in Mobile Forensics," in *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, IEEE, May 2019, pp. 1–6. doi: 10.1109/CAIS.2019.8769520.
[22] "BusyBox." https://www.busybox.net/ (accessed Sep. 18, 2023).