Computers & Security 89 (2020) 101675

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Formal knowledge model for online social network forensics

Humaira Arshad, PhD[a,*], Aman Jantan, PhD[b], Gan Keng Hoon, PhD[b], Isaac Oludare Abiodun, PhD[b]

[a] *The Islamia University of Bahawalpur, Pakistan*
[b] *School of Computer Science, Universiti Sains Malaysia, Malaysia*

ARTICLE INFO

Article history:
Received 1 July 2019
Revised 28 October 2019
Accepted 16 November 2019
Available online 17 November 2019

Keywords:
Forensic automation
Knowledge model
Formal model
Forensic ontology
Online social network forensics

ABSTRACT

Currently, examining social media networks is an integral part of most investigations. However, getting a clear view of the events relevant to the incident from a large set of data, such as social media, is a challenging task. Automation of the forensic and analysis process is the only solution to manage large data sets and get useful information. However, automation in digital forensics is a technical issue with legal implications. The legal system accepts only those automated processes that are reproducible, explainable, and rigorously testable. Therefore, automated forensic processes must be based on formal theories, which are rare in digital forensics. This article explains a theoretical and formal knowledge model for forensic automation on online social networks. This model consists of an event-based knowledge model, which provides theoretical concepts that can assist in the construction and interpretation of the events related to the incident under investigation. The proposed model is implemented through an ontology to provide semantically rich and formal representation to the concepts. This article also describes the feasibility of legally acceptable automated analysis operators, based on a formal theory, for online social network forensics.

1. Introduction

Social network content is commonly analyzed in most investigations involving criminal offenses, and also in domestic and financial disputes. Law enforcement agencies and legal practitioners regularly access social network profiles for quickly getting information relevant to the individuals (i.e., victim, suspect, or witnesses) involved in an incident. However, the process of collecting and analyzing the information accurately and efficiently is a challenging task due to the massive data volumes and heterogeneity of social network content and structure. Therefore, the process of forensic collection is technically intricate. Furthermore, the process is also legally challenging due to privacy laws and shared ownership of data.

The current proliferation of digital devices in combination with extensive usage and online activities resulted in massive volumes of electronic data created by a single person on digital devices and social media profiles. Thus, analyzing and investigating the vast volumes of digital evidence without appropriate support of automated tools and methods is a challenging and time-consuming task. Hence, it creates cognitive challenges and massive workloads for investigators. Therefore, automated and reliable solutions are needed to assist legal practitioners and investigators. However, automation in digital forensics is not an entirely technical issue; all digital forensic processes or methods must comply with the legal requirements, which are not straightforward.

All approaches designed for automated collection and analysis of forensic evidence must have to satisfy some crucial requirements such as integrity, credibility, and reproducibility (Baryamureeba and Florence, 2004). Otherwise, these approaches are criticized in legal proceedings for lack of scientific foundations and rigorous testing (Arshad et al., 2018). Hence, nowadays, digital forensic practices are emphasizing on the use of proven and scientific theories instead of old investigative techniques that rely on investigative experience only. Thus, automated techniques such as data mining methods and the approaches based on natural language processing are not suitable for digital forensics due to the legal constraints of data provenance (Arshad et al., 2019a). These approaches are based on statistics and estimations, so they cannot demonstrate the origin and derivation of data.

Currently, few data mining approaches are being used for content analysis to identify a suspect or predict a crime on online social networks. These data mining approaches are based on statistics and probability analysis. These approaches are not suitable in

[*] Corresponding author.
E-mail addresses: humeraarshed@gmail.com (H. Arshad), aman@usm.my (A. Jantan).

https://doi.org/10.1016/j.cose.2019.101675
0167-4048/

digital forensics, mainly because of two reasons; first, these approaches are based on statistical analysis instead of any explainable or proven theory. Second, they lost the provenance of data during processing and pre-processing. Provenance denotes the origin and history of an object. In forensic analysis, it is essential to manage the provenance of data regarding people, entities, and activities involved in producing related data objects. Therefore, the evidence that is lacking provenance or is generated by unexplainable or unproven data analysis methods are rejected in the court of law.

Judicial processes always demand an explainable theory for the conclusions generated by automated methods. However, very few proven and formal theories exist in digital forensics (Arshad et al., 2019b; Chabot et al., 2015). Notably, the existing theories are not entirely suitable for explaining the automated forensic process on online social networks. A standard and formal definition of the analysis process helps to ensure the reproducibility of the investigation process and correctness of results. A formalized model helps to understand and interpret the results or evidence achieved from the automated process. Furthermore, the formalization of the process also ensures the completeness and evaluation of the analysis process.

This article describes a formal theoretical model to explain the forensic process for social networks. This model aims to formulate a theoretical model to explain the evidence finding and analysis process by automated methods. These methods would be trustworthy only if they are based on a formal and explainable theory, which is rigorously testable; therefore, the automated results and evidence would be admissible in a court of law. This work is focused on formulating a formalized knowledge model that will explain the results obtained through automated analysis. This article is explaining an event-based knowledge model for automated forensic analysis of online social network data to retrieve evidence. The proposed knowledge model is implemented through an ontology.

Section 2 of this article gives an overview of related works. Section 3 explains the proposed approach and provides formal definitions related to online social networks and forensics. Furthermore, it describes the proposed event-based knowledge model. Section 4 explains the implementation details through a case study. Section 5 discusses the results and future work.

2. Related work

The necessity of a suitable theory that acts as a scientific foundation in digital forensic science is always stated in the literature. This theory is needed to satisfy the legal and scientific demands to justify the facts derived as evidence (Arshad et al., 2019b). Few such theories have been presented, the most prominent among them are proposed by Gladyshev, Carrier, Cohen, and Chabot (Carrier and Spafford, 2004; Chabot et al., 2014; Cohen, 2010; Gladyshev and Patel, 2004). Few approaches, based on these formal theories, are also adopted for the analysis and reconstruction of digital evidence (Chabot et al., 2014; Gladyshev, 2004; Hargreaves and Patterson, 2012). However, the suggested approaches are mostly focused on temporal modeling, and their scope is limited for standalone systems. Furthermore, these approaches are not adequately generic; hence, they cannot be adapted for shared and distributed data on online social networks (OSNs).

An event-based knowledge model in digital forensics was initially proposed by Carrier (Carrier and Spafford, 2004) and subsequently followed by (Chabot et al., 2015; Schatz et al., 2004a, 2004b). Few other approaches, based on formal theories, are also presented for the analysis and reconstruction of digital evidence (Chabot et al., 2014; Gladyshev, 2004; Hargreaves and Patterson, 2012). Schatz's model is using standard rule and signature-based event correlation techniques (Schatz et al., 2004b) While the older models like Carrier's and Willassen's are based on cause and effect relationship that shows the change in the state of an object with respect to time (Carrier and Spafford, 2004; Willassen, 2008). Similarly, finite state machine approaches (Gladyshev and Patel, 2004; James et al., 2010) also use historical states of objects for modeling and comparison. A similar approach is followed in cloud forensics by Jian Wang, which is based on timed automata for event reconstruction (Wang et al., 2016).

However, most of these models are limited in capacity to store the amount of knowledge and, as a result, analysis and automation capabilities (Chabot et al., 2015). Another variant based on rule-based reasoning and semantics is presented by (Turnbull and Randhawa, 2015), they used RDF data stores and developed Par-For Forensic RDF reasoning system; a forward-chaining, rule-based reasoning system for RDF-based data stores. They described Event Mappers for social network mapping, for the computer starting up and turning off and locating evidence of clock tampering. This system is also limited to disk images and subjected to minimum testing. Yoan et al. also enhanced and implemented that system for computer-based forensics and timeline analysis (Chabot et al., 2015). These models are addressing the forensic modeling on standalone systems such as standalone device.

Likewise, the previous investigation process models such as (Baryamureeba and Florence, 2004; Carrier and Spafford, 2004; Ciardhuáin, 2004; Köhn et al., 2006; Palmer, 2001; Stephenson, 2002) are not suitable for the evidence collection from social networks. These models are mainly designed to provide a guideline for evidence collection to human investigators. Only a few investigation process models are ever presented for online social networks explicitly (Jadhao and Agrawal, 2016; Zainudin et al., 2011; Zainudin and Llewellyn-jones, 2011). These models are also minimal and do not address all the aspects of online social network (OSN) investigation, such as incident recognition, crime scene boundaries, and provenance management.

The significant lack of process and tools in OSN forensic domain is due to the inherent differences of the medium from stand-alone digital devices. In online social networks, the essential components of forensic analysis and collection are different from the single machine-based examination. Data on OSNs includes multiple users, machines, and several time zones are also involved. Although the data is arranged in chronological order, each OSN has different structure and service model and uses several heterogeneous data formats. Also the concepts based on finite states are not applicable in the social network domain, as the objects are only created or interacted by creating new objects, or they are deleted; they do not change their state in their life cycle, although the events are evolved with time. Therefore, the model proposed in this article is using temporal aspects and rule-based correlations in addition to the subject and object-based correlations that founded on online interactions.

3. Proposed knowledge modeling approach

Collecting digital evidence and conducting digital forensic investigations is an expert and challenging task. In traditional investigations, investigators collect and analyze the forensic evidence by using the formal theory of that domain. In digital forensics, the process of collecting and examining is more difficult due to the rapid and continuous appearance of new technologies such as smartphones, social networks, cloud computing and IoT (Internet of Things). These new frontiers of electronics data are increasing the difficulty of collecting the evidence and using them successfully in legal proceedings.

The forensic analysis is further complicated on OSN due to the intrinsic complexity of storage, heterogeneous or shared access to electronic data, diversity of computing platforms, and significantly due to the lack of a formal theory. Also, a manual analysis of data is not feasible to deal with the enormous volumes of data. Hence automated approaches are needed for the purpose.

The legally acceptable use of automated methodologies for data analysis demands a robust theoretical model for the digital forensics process. A comprehensive and formal theoretical model is needed to explain all types of data analysis and processing that are needed to achieve evidence. Since with digital data and devices, the investigators and legal participants cannot observe directly what is happening inside a digital device or how the data is accessed and how a conclusion is made. Therefore, a cohesive set of characteristics is needed that is explicitly specified for a specific domain (i.e., social networks) to explain the digital forensics process.

A clearly defined theoretical model for online social network (OSN) investigation is needed to explain all the necessary components and associations among the components. A formalized knowledge model helps to understand and interpret the results or evidence achieved from the forensic analysis process. Furthermore, the formalization of the collection, management, and analysis process simplifies the development of automated analysis operators. The modeling process also ensures the completeness and evaluation of acquisition and analysis process. This work follows a four steps approach to achieve this goal; the proposed approach is outlined below.

- First, it identifies the knowledge related to online social networks and formally define the entities related to social networks.
- Second, it explains an event-based knowledge representation model to explain the associations among the identified entities and the incident related to the investigation. This knowledge will be used to perform analysis on the data to find the most relevant information related to the incident. This step ensures the reproducibility of the process and aids in acquiring the needed creditability to the automated analysis process.
- Third, it builds an ontology for the formal representation of the knowledge model, which extracts the knowledge from heterogeneous sources of data and populates the knowledge model.
- Fourth, it suggests the formulation of analysis operators for the analysis of information related to the incident that is extracted and stored in previous steps.

3.1. Fundamental definitions of social network components

An online social network or a social networking service (SNS) provides a platform for individuals to build a social network (SN) or social relations to the other individuals; those have similar views or professional interests. Also, it allows connectivity with real-life friends, acquittances, colleagues, and family. Hence, social media (SM) is described as an extensive set of interactions. Collectively social network data refers to the content generated as a result of interactions on online social networks. An interaction is a significant concept in social media content and on OSNs. A few key concepts that are shared by most OSNs and used in this model are outlined below.

3.1.1. Social Graph

A social network is a social setup that consists of a set of individuals (social actors), collections of associations, and sets of social interactions among actors. In this model, *Social Graph SG* is a set of all the individuals, which are related to each other through a social network, $SG = \{sg_1, sg_2, sg_3 \ldots\ldots sg_n\}$. $\mathrm{SG_x}$ is the set of users that are related to a given person *x*,

$$SG_x = \{sg_1, sg_2, sg_3 \ldots\ldots sg_n | sg_i \in U \wedge \forall sg_i \alpha x\}$$

Where *i* varies from 1 to n. $i = \{1,2,3\ldots.n\}$.In a single social graph, *x* is the central node; however, *x* is also a subset of social graph SG_x;

$$x_{.} \subseteq \; SG_{x.}$$

3.1.2. Content

All the information posted or shared on OSN is mentioned as content in this model. The updates posted by a user in the forms of text (i.e., micro-blogs, messages), media (i.e., images, videos) or behavioral responses (i.e., likes) are part of the content. Likewise, the interactions that occur among users are also part of the content. Therefore, the content C is set of all the information, posted as *Updates D* and *Interaction It*, in addition to *Profile P* data, therefore total content is

$$C = D \cdot \cup \cdot P \cdot \cup \cdot It \cdot$$

Content is further classified as Interaction and activity .

Interaction**.** A social network is the space where a set of interactions $It = \{i_1, i_2, i_3 \ldots . i_n\}$ take place. An interaction is an exchange of communication among users on OSN. The interactions occur among the users by responding to the content through comments, forwarding or sharing behaviors, and tagging others.

Hence, an interaction in OSNs refers to the set of objects that are used by a subject (person) for communication (i.e., Tweet, Direct Message) with another subject or to respond to an object, which is communication, (i.e., reply, favorite) by another subject. Let *It* is the *Interaction* occurred among the *User x*, and his *Social Graph SG*

$$it_j = \left\{ i_j \in I | i_j \alpha x \wedge \alpha sg_x \right\}$$

Where *j* varies from 1 to n $j = \{1,2,\ldots.n.\}$.While α is the relationship that linked the *x* to the *i* and *i* is also be linked with the social graph.

Activity. Social network provider records every information associated with interaction is known as Activity A. This recorded information is described as metadata MD in this model. It includes all the environmental (i.e., device info, location info) and temporal (i.e., data and time) attributes associated with an interaction I and recorded by the OSN provider or digital devices.

$$MD \, \alpha \, It$$

md_i is the set of metadata attributes $\{d_1,d_2,\ldots..d_n\}$ that is related to single interaction I_i. For every *Interaction Ii* there exist a unique set of metadata md_i, $md_i = \{d_1,d_2,\ldots..d_n\}$, hence

$$\forall It_i \exists ! \; md_i$$

The symbol "∃!" shows uniqueness quantification in predicate logic, which means "there exists only one." *MD* is set of metadata sets $\{\mathrm{md_1,md_2\ldots\ldots md_n}\}$. Each subset md_i have set of metadata attributes $\{d_1,d_2,\ldots..d_n\}$. $md_i \subseteq MD$, *w*here *i* varies from 1 to *n* $i = \{1, 2,\ldots.n\}$.

3.1.3. User

Let $\mathrm{U} = \{u_1, u_2, u_3, \ldots..u_n\}$ is the set of individuals that represent themselves on OSN by creating a *Profile*. That profile provides basic information about that person, such as name, address, age, interests. The profile information is provided by the person and visible on OSN. A single individual is referred to as u_i and represented by the *Profile P* on online platforms. These two concepts are roughly similar in a social media context, hence, $u_i \approx$ *Profile.* Every user there exists only one profile on each social network.

$$\forall u_i \exists ! \, P$$

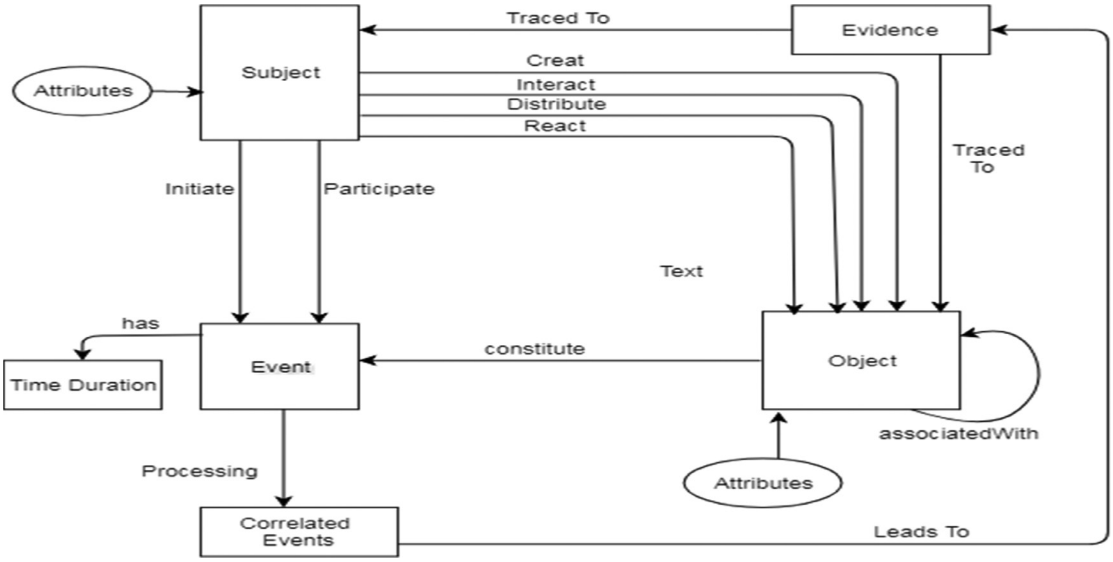

Fig. 1. Event-based online social network forensic knowledge model.

3.2. Event-based knowledge model for OSN

In digital forensics, an event-based knowledge model was initially proposed by Carrier (Carrier and Spafford, 2004) and subsequently followed by (Schatz et al., 2004a; Schatz et al., 2004b; Chabot et al., 2015). However, all these models are limited in capacity to store the amount of knowledge and, therefore, analysis and automation capabilities (Chabot et al., 2015). Yoan et al. also enhanced and implemented an event-based model for computer-based forensics and timeline analysis. These models are addressing forensic modeling only on closed systems such as standalone devices.

The model explained in this article is based on the event-based knowledge that is specifically designed for automated social media forensics and analysis. This model will be the first model to provide a theoretical foundation for social media forensics and evidence collection. This model allows a rich knowledge representation containing a broad set of entities and relations from the social media domain. The accurate representation of these entities will allow constructing automated analysis methods. In this section, a formal description of the model is presented; it is following similar notations as followed in existing works (Chabot et al., 2014).

Additionally, this model will help to generate results that are easily explainable in legal proceedings. It further allows reproducing and validating the investigative process. The process and procedure that cannot be validated are no longer useable in courts (Arshad et al., 2018). This section provides the formal definitions of the entities and relations first, from the domain that comprises the model. Then it introduces the set of analysis and correlation operators to manipulate the knowledge stored by the model. An outline of the proposed event-based model is given in Fig. 1.

An event is defined as a single action that occurred at any given time (Chabot et al., 2014). In this model, an event refers to the set of interactions (reply, likes, shares) that take place among several subjects (i.e., users) through various objects (i.e., image, video, tweets). Therefore, $E = \{e_1,e_2,\ldots e_n\}$ is the set of n events that take place at a crime scene. However, the crime scene concept is entirely different in OSN forensics. This work explains and reformalizes the concept of the crime scene on social networks. Furthermore, it describes all the essential components of OSN formally as part of formal modeling in this section.

3.3. Formal knowledge modeling

The entities involved in the event-based knowledge model are defined as follows.

3.3.1. Subject

Subjects initiate events on social networks. Subjects are representing the human actors or people in this model, let S be the set of subjects that are involved in an event, hence, $S = \{s_1,s_2,\ldots\ldots\ldots.s_n\}$.Therefore, S is a subset of users U that are related to an event E.

$$S \subseteq U \wedge S\alpha E$$

Each subject is referred to as s_i, where i varies from 1 to n, $i = \{1,2,\ldots\ldots n\}$. A set of attributes A_s describes the attributes which are associated with each subject. The attribute of a subject may be its name, age, or date of birth. The attribute can also be an email address or screen name.

$$A_s = \{a_1, a_2 \ldots\ldots a_n\}$$

Each subject s_i is related to a specific set of attributes, A_{si}. Where i varies from 1 to n. α_s is the relation that is connecting the subject with its attributes.

$$s_i\alpha_s A_{si}$$

3.3.2. Object

An event E may involve multiple objects in its life cycle. An object O in this model is representing an instance of communication on OSN. The object may refer to comment, reply, message, post, photo, video, or update. A set of attributes A_o describes each Object O.

$$A_o = \{a_1, a_2 \ldots\ldots a_n\}$$

The attribute a_i of an object may represent the unique id of the object, its URL, name, or description. Each Object *oi* is related to a specific set of attributes, $A_{oi,}$ hence,

$$o_i\alpha_o A_{oi}$$

Where i varies from 1 to n. α_o is the relation that is connecting the object with its attributes.

3.3.3. Event

An event takes place when a subject S performs an online activity on a social network by creating an object O at time T. These parameters define an atomic or single event. However, in a social network environment, most of the interactions involve multiple subjects and objects. Such as a subject S_1 created a Tweet that is an object O_1; this is identified as an event E_1. Subsequently, another subject, $S_{2,}$ replied, or liked that Tweet by creating a new object O_2 of reply. The reply action is classified as an event E_2.

Similarly, several subsequent events are expected over time. However, the event E_2 is created in response to event E_1. If the event E_1 is not created, event E_2 may not have existed. Therefore, it is necessary to preserve that association between the event E_1 and E_2.

Therefore, this model is introducing the multilevel concepts of an event; primary event E_p and sub-event E_s. The primary event would be the first event that triggers the initiation of sub-events. Therefore, the primary event E_p will be initiated by the primary subject by S_p by creating original object $O1$ at time t_1.

$$E_{p=}eInitiatedByS_p \wedge ecreatedO_1 \wedge O_1createdAtT_1$$

The sub-event E_s is created in response to primary event E_p by a secondary subject $Ss_.$ A sub-event E_s is initiated when a secondary subject S_s interacted with an already existing object O_1 by creating an object O_2 at time T_2.

$$E_s = SsparticipatedIne \wedge SsinteractedWithO_1 \wedge SscreatedO_2 \\ \wedge O_2createdAtT_2$$

$$Ep\cdot = \sum\nolimits_{\mathrm{i}=1}^{\mathrm{n}} Es$$

However, in this case, the time T_1 of creation O_1 must be earlier. Therefore, T_2 is higher than T_1.

$$T_1 \cdot \le \cdot T_2$$

Moreover, each set of sub-events E_s is derivable from primary event $E_{p.}$

$$E_s \cdot \vdash \cdot E_p$$

E_p is the set of primary events that are initiated independently. E_s is the set of sub-events that are related to an already existing primary event. In general, an event E must consist of one primary event and may have multiple secondary events.

$$\forall E \ \exists! Ep \ \vee \sum_{i=1}^{n} Es$$

3.3.4. Evidence

Digital forensics defined footprint as a sign of a previous activity or a piece of information that can be used to reconstruct the criminal activity (Morelato et al., 2013). In online social networks, the content updated on platforms is used as evidence of specific activities and conditions. Hence, an interaction or an object that indicates an illicit activity or proof of a particular fact is defined as evidence in this model. Let E be a set of all the evidence related to an investigation, an evidence ev $\in E$, ev is defined as,

$$ev = \{ev \cdot \in \cdot E \cdot \wedge \cdot e \cdot v \cdot \in \cdot O \cdot | \cdot o \cdot \alpha \cdot S\}$$

Hence an evidence ev that is an element of evidence E must also be an element of a set of objects extracted from the information extraction zone (IEZ). The Object must be related to a subject involved in the incident and part of IEZ.

3.3.5. Relations

A relation is used to link the entities presented in the event-based models, such as in Fig. 1. This model is identifying a few significant relations; those are identified and explained in this section.

Subjects Relations Subjects relation σ_s represents two types of relations to link an event $e \epsilon E$ with a subject $s \epsilon S$. Here "ϵ" shows set membership, e is a single event that is an element of set E, which shows total events. The relation is defined as:

$$\sigma_{\cdot s=} \cdot s \cdot hasInitiated \cdot e \cdot \vee \cdot s \cdot participatedIn \cdot e$$

a.Relation of initiation**.** *s hasInitiated e* means that a subject s has initiated an event by creating a post, or updating some content on the social network.

b.Relation of participation**.** *s participatedIn e* means that a subject has participated in an already initiated event such as by posing a reply or comment, by using a liking feature.

Objects Relations Objects relation σ_o represents three types of relations to relate an event $e \epsilon E$ with an object

$$o \cdot \epsilon \cdot O$$

The relation is defined as*:*

$$\sigma_o = (shasinteracted \cdot o \cdot \vee \cdot s \cdot hasdistributed \cdot o \cdot \vee \cdot s \cdot \\ hasreactedo) \cdot \wedge \cdot (screatedo)$$

Relation of Creation A subject initiated an event e by creating an object; therefore, o does not exist before the start of event e.

Relation of Interaction When a subject $s \epsilon S$ is interacted with an existing object $o \epsilon O$ in event $e \epsilon E$ by creating a new object o_1. Such as reply, comment on an existing object. The addition of new object $o_1 \epsilon O$ will be linked to the event e as a sub-event.

Relation of Distribution The relation of distribution occurs when an already existing object $o \epsilon O$ is shared or posted by a new subject S_2 again on the social network.

Relation of Reaction The relation of reaction occurs when a subject S responds on an already existing object $o \epsilon O$ by using a predefined interaction behavior of like or dislike or other, on the social network.

4. Events relations

Events relation σ_e consists of relations that used to link two events

$$e1 \epsilon E \text{ and } e2 \epsilon E$$

4.1. Relation of composition

In composition, one event $e \epsilon E$ consists of other events (e_2, e_3) ϵ E. As explained in the context of primary and secondary events.

$$e_1composese_2 \vee e_2composese_3$$

Each event e, either primary or secondary, *is* initiated by a subject S by creating an object O at time T.

$$E = \{S, O, T\}$$

The relation of composition implies a set of constraints. First is the temporal constraint, the event e_1 that is composed of another event must exist before the comprising events such as e_2, e_3. If t_1 is the time of creating o_1 hence initiating e_1, and t_2 and t_3 are the time of creating objects related to e_2, e_3 then it implies that:

$$t_1 \le t_2 \le t_3$$

The second constraint is, e_1 *composes* e_2, e_3 then if e_1 is destroyed or deleted all the comprising events such as e_2, e_3 will also cease to exist.

4.2. Relation of correlation

The correlation between two events e_1, e_2 means that e_1 is associated with e_2 based on multiple criteria and (e_1, e_2) ϵ $E_.$ They may be related through common subjects in two separate events, shared objects in two events, or they may have temporal proximity.

Let e_1 is an event $e_1 = \{s_1,o_1,t_1\}$ and $e_2 = \{s_2,o_2,t_2\}$ so these events are correlated if

$$s_1 \equiv s_2 \vee o_1 \equiv o_2 \vee (t_1 \wedge t_{2)} \subseteq P$$

Where s_1 and s_2 are identical and set of $(s_1,s_2,) \subseteq S$, $(o_1,o_2,) \subseteq O$. S and O represent the set of subjects and objects, respectively. P is a time interval specified by the incident. Hence, the event e_1 or e_2 are correlated if s_1 or s_2 refer to the same person if o_1 and o_2 refer to the same object, or they can be related if the time t_1 and t_2 belong to a given interval.

5. Evidence relation

σ_{t} is a relation used to link an evidence *ev* with an entity *en*. An entity consists of an event, a subject, an object hence, $en \subseteq \{E \times S \times O\}$. A function Trace is introduced which ensures that the evidence deduced by the automated operators are traced back to a given entity

$$Trace(en \subseteq \{E \times S \times O\}) = \{Ev \subseteq Tr | ev\sigma_t en\}$$

For example, an offensive behavior inferred by analysis of the online content of a subject *x* must be traced back to specific events and objects (i.e., comments, image, profile) created by *x*. The *Trace* function must also provide all the related attributes of subject and object.

5.1. Correlations and analysis operators

After the collection and preservation of the required part of data from the social network, it becomes a static environment that contains the digital footprints. Then the goal is to reconstruct a timeline containing the events that are more relevant and significant in the context of the incident under investigation. Selecting the most relevant events and ordering them in chronological order is a challenging task. As the data collected from OSN is immense and diverse; hence, it is complicated for examiners to filter and sort the data in a useful way.

This approach has identified the underlying relationships among the entities of the data and formulated a few analysis operators. These operators will identify the relations between events, to filter or highlight the most relevant fact. These analysis operators are based on correlation assumptions, and these correlations are explained in the rest of this section. The following function gives the correlations between two events $e_1 \ \epsilon \ E$ *and* $e_2 \ \epsilon \ E$:

$$\begin{aligned} Correlation(e_1, e_2) = {} & Correlation_T(e_1, e_2) + Correlation_I(e_1, e_2) \\ & + Correlation_S(e_1, e_2) + Correlation_O(e_1, e_2) \\ & + Correlation_{RB}(e_1, e_2) \end{aligned}$$

Correlation (e_1, e_2) can be weighted to give more significance to one type of correlation function such as in a cyberbullying investigation; more weight can be assigned to the object and subject-based correlations as compared to temporal correlation. However, the choice of assigning weights and priorities is exceedingly dependent on the type of investigation.

Furthermore, the aim of the current article is not to propose analysis functions for each type of investigation. It aims to propose a model that can explain the suitability of a formal knowledge model in explaining the automated analysis of forensic data from online social networks. Presently, the following correlation is proposed and explained for the purpose.

5.1.1. Interaction based correlations

It is observed in various studies that all online associations expressed by users on OSNs are not similar. Some of the associations are more important or personal than others (Dindia and Canary, 1993). Notably, the significance of a social association is perceived by exchange and transitivity of interaction among people (Krackhardt and Kilduff, 1999). A study shows that most users tend to interact with a smaller subset of friends and usually have no interactions, with almost 50% of their OSN contacts (Wilson et al., 2009). Therefore, only a few interactions are significant and more critical than others. Hence, this model is introducing the concept of sorting and prioritizing interactions to build a graph that is based on the interactions from one person to another; this graph would be a subset of the social graph.

5.1.2. Temporal correlations

Social media content is always chronologically ordered. A unique timestamp is associated with each object that indicates the time of creating that object, which is recorded by the platform. It is argued in this model that temporal aspects of data are crucial to understanding the interaction behaviors in social network forensic analysis and should be judged more carefully.

As the social network content is a sequence of discrete-time data, it can be manipulated as time-series data. The proposed model allows us to process the temporal data separately from content, but still, it can be associated with the social network data. Therefore, it is reasonable to apply a time series analysis on this data. Time series analysis can reveal useful statistics and meaningful characteristics of the data. It is well documented in various studies that temporal patterns of communication such as daily time of online activity and frequency of communication, the difference in a pattern on weekends and trends of mobile phone usage can be viewed as representations to sleeping and waking behaviors of a person (Nimrod, 2015; Aledavood et al., 2015b).

In forensic analysis, these kinds of patterns can be used to identify the time zones and approximate geographic area of the person posting the content. Mostly, usage patterns are unique for individuals, and they tend to maintain these patterns (Aledavood et al., 2015a; Randler et al., 2016). Hence, by scrutinizing these rhythms, they may help to compare the identity of an anonymous user with a known user and thus to find the identity. In this model, the following assumptions are defined for the temporal aspects:

- Temporal proximity may reveal a relatedness among the events. The lesser the relative difference, *difference* (e_1,e_2,t_1,t_2), among the two events, the higher the relatedness.
- Repetition of social activity at the specific time also reveals a relatedness among the events or subjects, *pattern*(e_1,e_2), and the subject's actual lifestyle.
- A specific time interval may represent the relatedness of two different events. If two events e_1 and e_2 are transpired in a time interval from, t_1 to $t_{2,}$ it is given by *interval* $(e_1,\ e_{2,}t_{1,}t_2)$.

5.1.3. Subject and object correlation

These two correlations quantify the relatedness concerning the shared subjects and objects involved in an event.

- The relatedness between two events e_1 and e_2 increases proportionally with several common subjects participating in the events. The correlation is measured by the cardinality of common subjects S among the events.

  $$\text{correlation}\,(e_1, e_2) = \frac{|\text{Se1} \cap \text{Se2}|}{\max(|\text{Se1}|,\, \text{Se2}|)}$$

- The relatedness between two subjects s_1 and s_2 increases proportionally with several objects they shared or interacted with

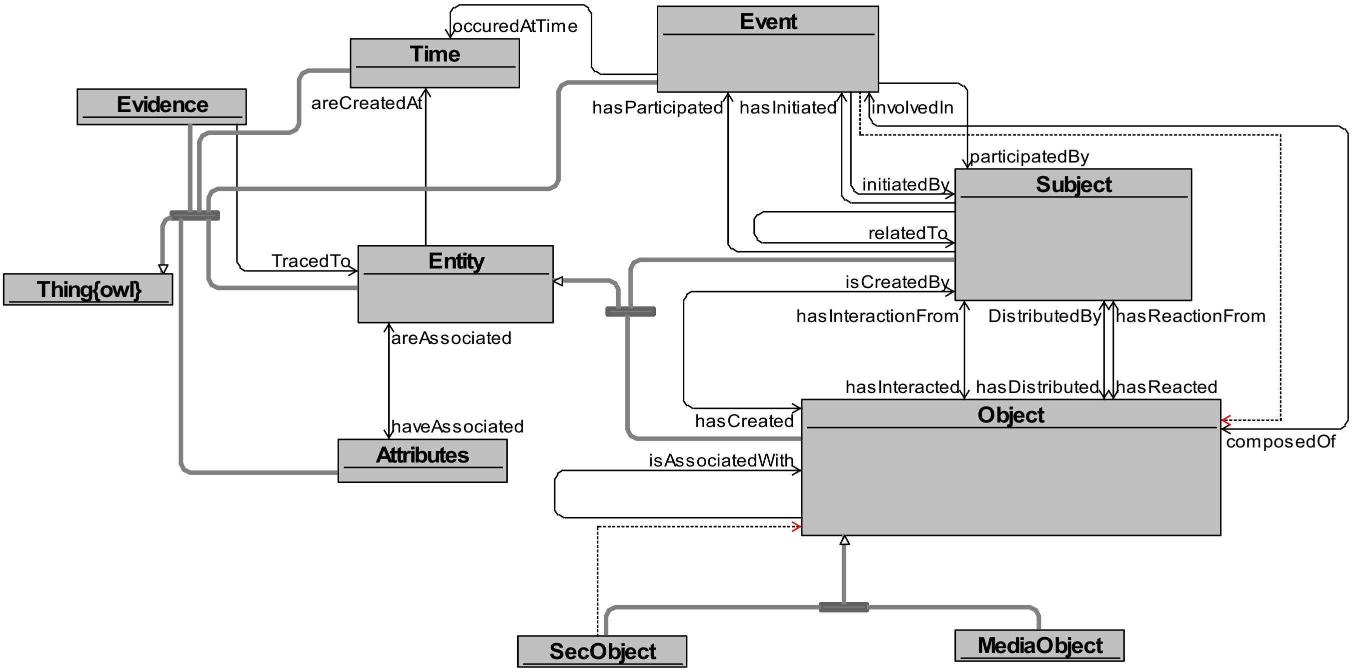

Fig. 2. Ontology implementation for the event-based model.

the subject, s_1 may like, comments, or share the object O_{s2} created by s_2 and vice versa. The *correlation* is measured by the cardinality of common objects O among the subjects.

$$\text{correlation } (s_1, s_2) = \frac{|\text{Os1} \cap \text{Os2}|}{\max(|\text{Os1}|, |\text{Os2}|)}$$

$|\text{S}_\text{e}|$ and $|\text{O}_\text{e}|$ gives the number of subjects and objects or frequency, not the subjects or objects themselves, in the equation mentioned above.

5.1.4. Rule-based correlation

In addition to the previous aspects such as subject, object, and time, rules based on expert knowledge in social behaviors can also be used to correlate events. Rule-based correlation is high if the events satisfy the rule or lower otherwise.

$$\text{correlation } (e1, e2) = \sum_{r=1}^{n} rule_r(e1, e2)$$

Therefore, the higher the number of rules satisfied by the events, the higher the correlation among them. It is possible to assign higher values to rule-based correlation to give more emphasis on expert knowledge.

6. Implementation and evaluation

The concepts of knowledge model are formally implemented through an ontology named "Event-based forensic Integration Ontology for Online Social networks" (EFIOSN). An outline of the ontology is given in Fig. 2.

6.1. Case study

This section aims to illustrate the working and usage of the knowledge model by using an example of social media defamation case and analyze the incident by using the proposed model to infer new knowledge. This work has conducted a theoretical investigation to illustrate the capabilities of the proposed knowledge model. The case involves a defamation attempt initiated against a victim named Anna, on an online social media platform. The investigators believe that the suspect identified with the social media profile named "Bill" is using a fake identity, and the real person impersonating as "Bill" is most probably a member of the victim's online social network.

6.1.1. Data extraction

At the start of the investigation, the investigators identify the initial scope of data extraction from the online social network. The data is collected from the given OSN, Twitter, in this case, for the period, including the reported offense. In this case study, the data is collected for 35 days, from the suspect, victim, and a few of the related contacts from their social graph. The extracted data at this stage consists of online objects posted by users. A simplified example is explained for demonstration purposes, as shown in Fig. 3.

6.1.2. Mapping and instantiation

The next step after data extraction is populating the ontology using the result of the extraction process. Instances for events, subjects, and objects are created from the extracted data to populate the ontology and corresponding RDF files. The links between each entity are instantiated according to the formal properties defined in the EFIOSN ontology. The associations among events, sub-events, subjects, and objects are deduced from the type of the objects created.

A simplified example of the instantiation process is given in Fig. 4. The example explained in Fig. 4 is showing only four primary events to avoid complexity. It also shows that three sets of sub-events are associated with primary events.

E1: Event E1 is initiated when the subject Bill created a Tweet.
SE1. A set of sub-events are generated when other subjects are subsequently interacted, by responding, reacting, or distributing the primary Tweet (id = 1). The objects that are created as a result of interaction with the primary object are considered as sub-events (SE1) of primary event E1.

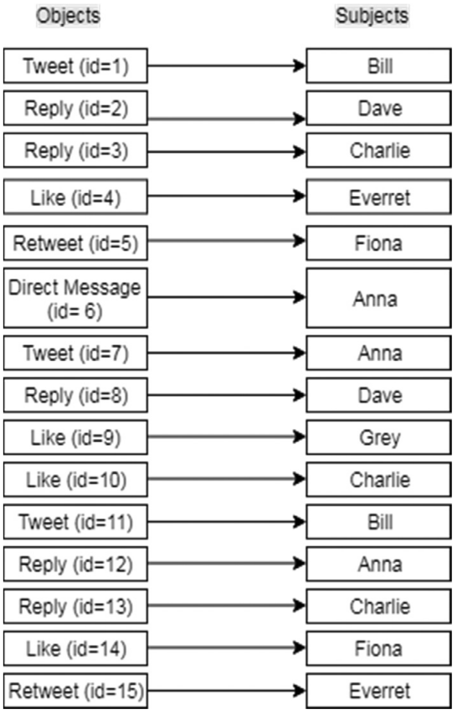

Fig. 3. The sample of extracted objects and subjects.

E2: Event E2 is initiated when the subject Anna has created a direct message that is sent to Bill**.** This event has no sub-events.

E3: Event E3 is initiated when the subject Anna created a Tweet.

SE3. A set of sub-events is associated with the Tweet (id = 7) and primary event E3.

E4. Event E4 is initiatedlist when the subject Bill created another Tweet.

SE4. A set of sub-events created as a result of interactions with primary Tweet (id = 11) is associated with primary event E4.

6.1.3. Knowledge enhancement

After the instantiation and populating the data in ontology, the next step is to deduce knowledge from the extracted data. This stage is mainly valuable to improve the results of the analysis steps as it helps in filtering the most relevant knowledge about the entities, and it may discover some new knowledge. For instance, in this case, the investigators will be more concerned about gathering evidence of defamatory material posted by the suspect. Hence, they can sort the events that are initiated or participated by the suspect only by using subject correlations as given in 3.3.3 and 3.4.3.

These events can be filtered additionally for selecting those events where the victim is mentioned, or the events where both suspect and victim have participated. In this case, both E_1 and E_4 are examined for the illegal content, and the participants (subjects) that encouraged the content verbally and involved in the distribution of the content are identified. In this example, event, E1, and E4 show the participation of Anna, Dave, Charlie, Fiona, and Everett. Fiona and Everett have participated by sharing the offending content on their profiles, so they are of immediate interest to the investigators. A closer inspection of the retweets by Anna, Dave, and Charlie showed that Anna and Dave had protested the content,

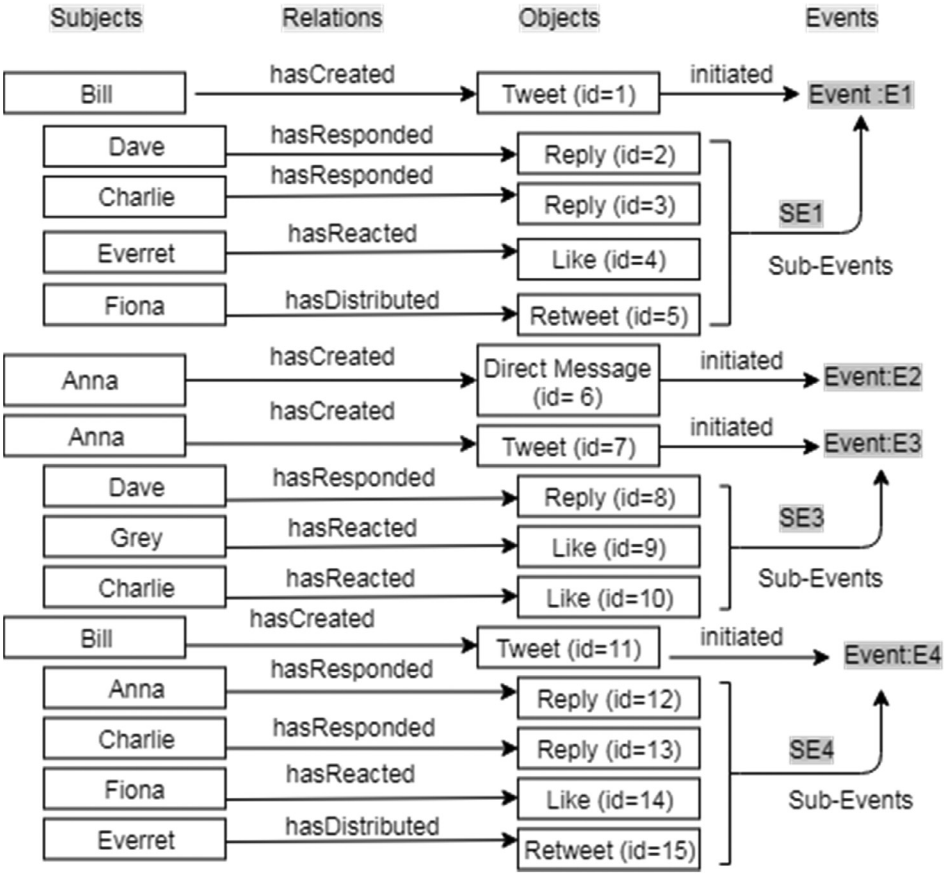

Fig. 4. Data Instantiation and Mapping.

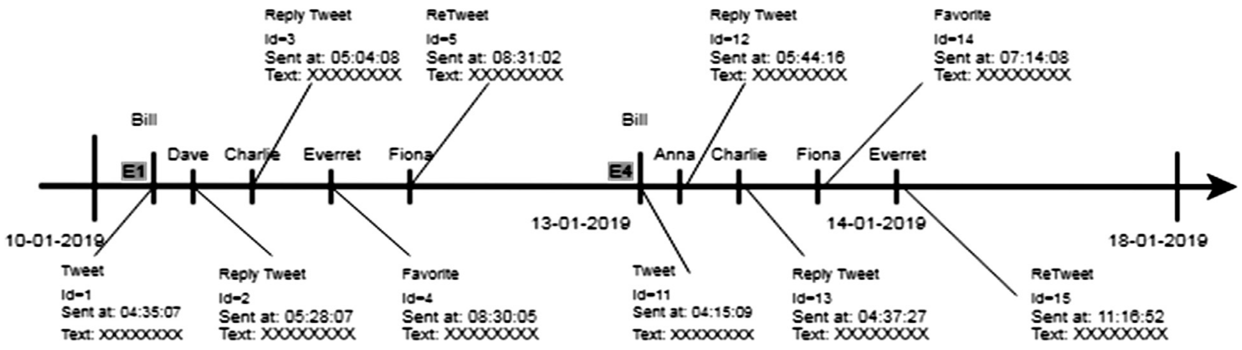

Fig. 5. Timeline of the sample events.

but in both events, Charlie is encouraging the suspect. The scope of the investigation will be expanded and included the Fiona, Charlie, and Everett.

This process will significantly eliminate irrelevant events and deduce new knowledge, such as the identification of new subjects or suspects in this case. This step is also significantly helpful in narrowing the focus of investigation on a few specific subjects and objects from the bulk of data.

6.1.4. *Timeline construction and analysis*

The final step is to formulate a timeline that establishes the temporal sequence of the events involved in an incident. Although the social media data is already arranged in chronological order, the timeline obtained from the social media platform includes all the irrelevant data. Hence this step is also focused on finding the correlations among the related events. The correlated events are then extracted and arranged in a timeline. Several timelines can be generated by using various parameters due to the flexibility that exists in the current model because of using semantics and ontologies. These timelines will summarize the data related to any specific aspect, such as temporal proximity or specific subject. So, the investigators can compare and evaluate the useful aspects of knowledge.

Fig. 5 is showing a timeline that is extracted from the events that are generated by the suspect Bill. As in this case study, the suspect is responsible for generating offensive content. Therefore, the timeline contains the events that are initiated by Bill, such as *Event* E_1, and *Event* E_4 are initiated when the suspect created a Tweet. These events are initiated by a common subject and are sorted by using the subject correlation. The subsequent events related to E_1 and E_4 are revealing the participation of other individuals in these events. As these participants are shared among the correlated events hence again, the subject correlation and event correlation are involved. In this case, the investigators are interested in those participants who are liking or distributing the content because this behavior shows the hostility of the participants towards the victim. The participants that are linking and distributing the content might be the close associates of the suspects, or either one of them is impersonating by using the fake identity.

The investigators will interpret the results, after correlating the events, in the context of the reported incident. In this case, event E1 indicates that Dave has replied with neutral comments, and Charlie and Everett seem to like the content, and Fiona participated by spreading the illicit content by using the "Retweet" feature. Likewise, in event E_4, Dave and Anna seem to be offended by the content, but the response by Charlie and Fiona indicates a liking for the content, and Everett redistributed the content. A more and less similar pattern is observed in other events. It indicates that Charlie, Everett, and Fiona seem to be participating with the suspect. The correlation results of interaction frequency explained in 3.4.1, show a closer relationship among Charlie, Everett, and Fiona. A closer inspection of temporal patterns, writing statistics, and profile aspects can lead to finding the similarity between the Bill and one of the individuals from the suspect group. In this case study, we find that Bill and Charlie are showing very similar temporal activity patterns, and language used by them in their Tweets also shows a close statistical match. These similarities lead to the probability that the same person operates both profiles. However, this possibility is not direct evidence, but it gives a specific focus to the investigators to search for the more extensive evidence for linking the identities of the preparators by searching the physical devices of the identified suspect or through corroborating witnesses.

The timeline analysis will give the events that are related to the incident under investigation only. This process also helps to sort a few individuals of interest among the whole social graphs of the suspect and victim, which may contain hundreds of people. Therefore, the investigators can focus on a significantly smaller set of data for further analysis and evidence collection.

7. Conclusion and future work

The massive volume of data to process and the heterogeneity in the content and social network structure are the most critical challenges in social media forensic investigations. The automated approaches are necessary to manage the large volumes of data and the vast scope of OSN investigations. However, the commonly used data mining approaches are not suitable for forensic processing because of legal issues. These approaches cannot sufficiently explain the sequence of execution and logical reasoning to support the generated results.

The knowledge model proposed in this article is providing the formal definitions of the entities involved in an incident and explain the possible correlations among them. This work mainly explains the probable correlation among the events and entities. The use of correlated events, in this model, is helping to filter the information most relevant to the incident. In this model, the subjects and objects are the central concepts that are initiating the events. The events are grouped into primary and secondary events; this classification is based on the type of object involved in an event instead of temporal differences or cause and effects like Chabot's and Carrier's model. Chabot's model is using the temporal differences and similarity of durations for correlating the events, and Turnbull is also using rule-based correlations (Chabot et al., 2015; Turnbull and Randhawa, 2015). However, the content in social network includes discrete-time series; therefore, the correlations cannot be described through durations and overlapping periods.

The case study presented in this article has shown the relevance of this model. It is observed from the example that the process has reduced the number of resultant events and objects that are subjected to further analysis. In actual, this process significantly reduced the number of entities and sped up the analysis process. In this case study, we collected 43 objects created by the suspect and 89 objects that are created by the victim. We manage to obtain 14 Tweets by using the subject and object correlations. Closer inspection reveals that nine among those 14 Tweets are containing the offending material posted by the suspect, and the other 5 Tweets also contain abusive content mostly posted by the victim.

The use of that model would allow the automated process to suitably extract, analyze, and interpret the forensic data. The results generated by the automated processes are reasonably explainable by using a formal knowledge model. This formalization of concepts explained the involvement of subjects as initiator, participator, or observer by inferring that information from the type of objects they created. Notably, the objects created by subjects can be traced back to the original content on OSN to validate the provenance of data evidence. Furthermore, the use of semantically rich representation through ontology provides the formalism to the model, and use of several semantic aspects (i.e., temporal similarities or differences, connections, relatedness based on activities or shared objects) allows building sophisticated analysis processes for OSN forensic investigations.

In the future, we aim to develop a platform-specific ontology such as for Twitter or Facebook, the detail of the hybrid semantic data model is given in our previous work (Arshad et al., 2019a). The next step is to formulate the advanced analysis operators based on the entities and correlations given in this article and test them on a large volume of data. The correlations identified in this model will be used to formulate analysis operators that consist of semantic queries, mathematical computations, and visualizations. The knowledge model given in this article will be used to test and validate the implementation and explain the automated results. This model would also help to test the linking between the generated results and the originating data items so that they would be legally acceptable as evidence.

Declaration of Competing Interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Aledavood, T., Lehmann, S., Saramäki, J., 2015a. On the digital daily cycles of individuals. Front. Phys. 3. doi:10.3389/fphy.2015.00073.

Aledavood, T., López, E., Roberts, S.G.B., Reed-Tsochas, F., Moro, E., Dunbar, R.I.M., Saramäki, J., 2015b. Daily rhythms in mobile telephone communication. PLoS ONE 10, e0138098. doi:10.1371/journal.pone.0138098.

Arshad, H., Jantan, A., Hoon, G.K., Butt, A.S., 2019a. A multilayered semantic framework for integrated forensic acquisition on social media. Digit. Investig. 29, 147–158. doi:10.1016/j.diin.2019.04.002.

Arshad, H., Jantan, A., Omolara, E., 2019b. Evidence collection and forensics on social networks: research challenges and directions. Digit. Investig. 28, 126–138. doi:10.1016/j.diin.2019.02.001.

Arshad, H., Jantan, A.B.A.B., Abiodun, O.I.O.I., 2018. Digital forensics: review of issues in scientific validation of digital evidence. J. Inf. Process. Syst. 14, 346–376. doi:10.3745/JIPS.03.0095.

Baryamureeba, V., Florence, T., 2004. The enhanced digital investigation process model. Asian J. Inf. Technol. 5, 790–794.

Carrier, B., Spafford, E., 2004. An event-based digital forensic investigation framework. Digit. forensic Res. Work 1–12. doi:10.1145/1667053.1667059.

Chabot, Y., Bertaux, A., Nicolle, C., Kechadi, M.T., 2014. A complete formalized knowledge representation model for advanced digital forensics timeline analysis. In: Digital Investigation. Elsevier, pp. S95–S105. doi:10.1016/j.diin.2014.05.009.

Chabot, Y., Bertaux, A., Nicolle, C., Kechadi, T., 2015. An ontology-based approach for the reconstruction and analysis of digital incidents timelines. Digit. Investig. 15, 83–100. doi:10.1016/j.diin.2015.07.005.

Ciardhuáin, S., 2004. An extended model of cybercrime investigations. Int. J. Digit. Evid. 3, 1–22. doi:10.1504/IJESDF.2010.033780.

Cohen, F., 2010. Toward a science of digital forensic evidence examination. In: IFIP Advances in Information and Communication Technology. Springer Berlin Heidelberg, pp. 17–35. doi:10.1007/978-3-642-15506-2_2.

Dindia, K., Canary, D.J., 1993. Definitions and theoretical perspectives on maintaining relationships. J. Soc. Pers. Relat. 10, 163–173. doi:10.1177/026540759301000201.

Gladyshev, P., 2004. Formalising event reconstruction in digital investigations 212.

Gladyshev, P., Patel, A., 2004. Finite state machine approach to digital event reconstruction. Digit. Investig. 1, 130–149. doi:10.1016/j.diin.2004.03.001.

Hargreaves, C., Patterson, J., 2012. An automated timeline reconstruction approach for digital forensic investigations. In: Digital Investigation, pp. S69–S79. doi:10.1016/j.diin.2012.05.006.

Jadhao, A.R., Agrawal, A.J., 2016. A digital forensics investigation model for social networking site. In: Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies - ICTCS '16. ACM Press, New York, New York, USA, pp. 1–4. doi:10.1145/2905055.2905346.

James, J., Gladyshev, P., Abdullah, M.T.M., Zhu, Y., 2010. Analysis of evidence using formal event reconstruction. Digit. Forensics Cyber Crime 31, 85–98. doi:10.1007/978-3-642-11534-9_9.

Köhn, M., Olivier, M., Eloff, J., 2006. Framework For a Digital Forensic Investigation. ISSA.

Krackhardt, D., Kilduff, M., 1999. Whether close or far: social distance effects on perceived balance in friendship networks. J. Pers. Soc. Psychol. 76, 770–782. doi:10.1037/0022-3514.76.5.770.

Morelato, M., Beavis, A., Tahtouh, M., Ribaux, O., Kirkbride, P., Roux, C., 2013. The use of forensic case data in intelligence-led policing: The example of drug profiling. Forensic Sci. Int. doi:10.1016/j.forsciint.2013.01.003.

Nimrod, G., 2015. Early birds and night owls: differences in media preferences, usages, and environments. Int. J. Commun. 9, 133–153.

Palmer, 2001. DIGITAL forensic research conference a road map for digital forensic research a road map for digital forensic research.

Randler, C., Wolfgang, L., Matt, K., Demirhan, E., Horzum, M.B., Beşoluk, Ş., 2016. Smartphone addiction proneness in relation to sleep and morningness–eveningness in German adolescents. J. Behav. Addict. 5, 465–473. doi:10.1556/2006.5.2016.056.

Schatz, B., Mohay, G., Clark, A., 2004a. Generalising event forensics across multiple domains. In: Australian Computer Network and Information Forensics Conference, pp. 1–9.

Schatz, B., Mohay, G., Clark, A., 2004b. Rich Event Representation for Computer Forensics, 2004. Asia Pacific Ind. Eng. Manag. Syst., APIEMS, pp. 1–16.

Stephenson, P., 2002. End-to-end digital forensics. Comput. Fraud Secur. 2002, 17–19. doi:10.1016/S1361-3723(02)00914-4.

Turnbull, B., Randhawa, S., 2015. Automated event and social network extraction from digital evidence sources with ontological mapping. Digit. Investig. 13, 94–106. doi:10.1016/j.diin.2015.04.004.

Wang, J., Tang, Z., Shao, W., Jin, X., 2016. A formal model of events reconstruction for cloud forensics. RISTI - Rev. Iber. Sist. e Tecnol. Inf. 2016, 45–55.

Willassen, S., 2008. Hypothesis-based investigation of digital timestamps. IFIP Int. Fed. Inf. Process. 285, 75–86. doi:10.1007/978-0-387-84927-0_7.

Wilson, C., Boe, B., Sala, A., Puttaswamy, K.P.N., Zhao, B.Y., 2009. User interactions in social networks and their implications. In: Proceedings of the Fourth ACM European Conference on Computer Systems - EuroSys, 09, p. 205. doi:10.1145/1519065.1519089.

Zainudin, N.M., Llewellyn-jones, D., 2011. A digital forensic investigation model and tool for online social networks. 6th IEEE Annu. Work. Digit. Forensics Incid. Anal. WDFIA 2011.

Zainudin, N.M., Merabti, M., Llewellyn-jones, D., 2011. Online social networks as supporting evidence&nbsp;: a digital forensic investigation model and its application design. In: Res. Innov. Inf. Syst. (ICRIIS), 2011 Int. Conf., pp. 1–6. doi:10.1109/ICRIIS.2011.6125728.

Humaira Arshad: She is Assistant Professor in the Department of Computer Sciences & IT at the Islamia University of Bahawalpur, Pakistan. She joined the faculty of Computer Sciences & IT in 2004. Previously, she holds a Master's degree in information technology from National University of Science and Technology (NUST), Pakistan. She has completed her Ph.D. at School of Computer Science in Universiti Sains Malaysia. Her areas of Interest are Digital & Social Media Forensics, Information Security, Online Social Networks, Cybersecurity, Intrusion Detection, Reverse Engineering and Semantic Web.

Aman Bin Jantan: He is an Associate Professor at the Faculty of School of Computer Sciences in Universiti Sains Malaysia. He got his Ph.D. and Master's degrees from Universiti Sains Malaysia. He has published over fifty articles in reputable journals and some of them has won local, national and international recognition. His research interest amongst others are; Artificial Intelligence, Cybersecurity, ICT application to National Security, Cryptography, Forensic, Computer & Network Security, E-Commerce/Web Intelligence, Compilers Design & Development Techniques.

Gan Keng Hoon: She is a senior lecture at the Faculty of School of Computer Sciences in Universiti Sains Malaysia. She got her Ph.D from Ph.D., University of Malaya (UM), Malaysia, and Master's degrees from Universiti Sains Malaysia. She has published over thirty articles in reputable journals and conferences, some of them has won local, national and international recognition. Her research interests mainly focus on semantically rich contents/documents/texts resulted from massive tagging and annotations by various levels of users. In general, studies are focused on automated contents building, platform development for structured text processing, and working applications of such contents.

Oludare Isaac Abiodun: He is a Senior Lecturer in Bingham University Kadope, Nigeria. Currently he is doing his PhD at School of Computer Science in Universiti Sains Malaysia. He also holds a Ph.D. in Nuclear and Radiation Physics from Nigerian Defence Academy, Kaduna. His research interests are; Computer Science, ICT application to National Security, Security Management, Artificial Intelligence & Robotics, Cybersecurity & Digital Forensic, Terrorism & Society, Cryptography, Nuclear Security.