A PROTOTYPE ANALYSIS OF DIFFERENT FORENSIC METHODS IN SOCIAL MEDIA APPLICATIONS

[1]P. MARESWARA RAO, [2]K. RAJASHEKARA RAO
[1]Research Scholar, Rayalaseema University, Kurnool, Andhra Pradesh, India.
[2]Director, Usha Rama College of Engineering and Technology, Telaprolu,
Andhra Pradesh, India
Email: [1]mareshphd2017@gmail.com

ABSTRACT

Now a day's, usage of social online networks and other communication services has been increased and perform important role in human's day to day life. So all the users share their feelings in different formats like messages, audio, video, photographic usage on different types of events in real time data assessment. Whenever increasing social communication then forensic activities also increased to access user's personal data from online social network servers. Intuitively social forensics is a new field to investigate criminal and illegal user activities from user's communication networks like Face book, Whatsup, and other social networks in android and web oriented applications. Some of the law enforcement consultants significantly research on online user data to provide solution for criminal activities. So analysis and collect large amount of data from multiple online social networks is a challenging aspect in present days. In this paper, we give brief literature about different forensic analysis approaches and techniques used to investigate different types of forensic problems to identify criminal activities from both android oriented and web oriented applications. Our survey gives those techniques implementation procedure's to identify criminal forensics present in online social networks.

Keywords: *Online Social Networks, Face book, Twitter, Whatsup, Digital Forensic Analysis and Instance Messages and Email-Forensic Analysis.*

1. INTRODUCTION

Increasing online social networks has becoming social norm for different users to share their representations to other peoples, in present days for individual and company; enterprise oriented social networking (Face book, LinkedIn) services are increased to define efficient services between different user's. This was occurred because of increasing mobile device usage, internet connectivity to store high amount of data stored in committed usable portable devices. Because of increasing smart phone usage on the other hand increasing criminal activities investigations implemented by some of the terrorist groups and individual users in real time application developments. This procedure is used to growth and increase forensic data with increasing of large amount of crime investigation data, Social forensic and mobile device forensic is a new field to extract and take forensic data in different formats. The expressive growth of Online Social Networks (OSN) in communicative environment is favorably increased duo to increase of digital forensic in different data sharing communications. Digital forensic is a procedure to deal with legal or illegal collection digital forensic data from corporate, official and unofficial organizations. So, in this paper, we analyze and discuss the procedures of different techniques or approaches to detect forensic analysis in both web and android based application development. We also discuss forensic analysis procedure in different applications. This survey gives efficient analysis about forensic application development to detect different attributes in social forensics. We mainly investigate the study of email forensic, twitter forensic presentation on online social networks. Our research mainly to determine and presents forensic data evaluated by smart phones and online social applications, and also investigates research procedure on social media applications like: Face book, Windows and Android and other services.

2. SOCIAL FORENSICS

Digital forensic inquire about has been an important asset in unraveling criminal offenses regardless of its moderately youthful "age". Initially, the emphasis was on looking at points of interest put away on a PC, and a recuperating information document that suspects had expelled. Be that as it may, accordingly of the advancements of innovation and its utilization engendering to all parts of life, nowadays, advanced devices contain as it were a segment of the accessible client points of interest that could help the experts in settling criminal offenses. A considerable measure of associations happens in on the web open systems administration administrations and over advanced association's media, for example, messages, IM and VoIP frameworks. Clients get to data through these items and spare records about their arrangements in computerized plans. In that capacity, the vast majority of the information is put away on the web not on a particular framework. Subsequently, it is mandatory for "crime scene investigation" instruments to draw out points of interest put away on the web, what's more, not just draw out points of interest put away provincially on a framework. The objective of open "legal sciences" is to target open long range interpersonal communication and correspondence arrangements and draw out as much subtle elements as conceivable, with respect to the web exercises and interchanges of a suspicious. We will likewise show that computerized arrangements can be used to give associations of client subtle elements over administrations, i.e., perceive subtle elements shape distinctive arrangements that have a place with a similar client.

3. RELATED WORK

Social Forensic Artifacts

A substantial amount of scholarly works is accessible significant to crime scene investigation research of long range informal communication locales (SNSs). This scholarly works is confined to criminology of SNSs connected through PCs or portable workstation frameworks as it were. Confined reviews likewise exhibited in regards to SNS confirmation elaboration assets and their abilities. Specialists have investigated some unmistakable data names created in different LinkedIn sites. In the wake of assessing the main source of different cross web sites these chose names are used in defined made representation catchphrase inquiries to draw out evidence. Some important artistic works portrayed the procedures of recovering and recovering Face book or MySpace moment talk data from hard plate [4].

Legal sciences specialists can find huge long range interpersonal communication verification from cell phones. Advanced crime scene investigation by sensible buy of iPhone 4S said Face book or MySpace database is situated in the framework stockpiling [5]. These data incorporates data with respect to name and telephone data of as of late interfaced companions. If there should arise an occurrence of Tweets, separate postings are accessible containing data like client record data, connections and late tweets alongside individual timestamps. LinkedIn data can likewise be removed from the capacity. Besides, sensible pictures of Android working framework and Ms window's cell phones said these savvy devices synchronize the essential Face book or MySpace data with telephones connect with rundown. In this way connect with. Database is analyzed to draw out Face book or MySpace pertinent data is most reliable presentation [6]. Device stores like Tweets and LinkedIn refreshes and in some cases secret passwords in plain. Then again, comparable data in BlackBerry contraptions was inaccessible.

Smart phone Forensics:

Techniques for information buy and criminological relations in regions of real presentations amid in earlier researches in this field. Flow artistic works around there, especially Burnette's examination with respect to BlackBerry, more often than not identifies with the normal data evacuation techniques for moderately more established sorts of cell phones and portrayal of the product programs and also the equipment hardware that can be found in the chose evacuation method [3]. Besides, starting work examines different research strategies, for example, examination utilizing cell test systems and recognizing relics through editor representations. With reliable progression of time, further abstract works was created and gives essential/starting outlines and speculations identifying with measurable assessment of late cell phones contraptions. More extensive idea of the relic's general stockpiling areas in cell phones, the used advancements and assets, and the included administration procedures is accessible in the current abstract works. Content and media data, logbook/scheduler sections, images and recordings, contacts, telephone logs, messages and history in web data are a portion of the sorts of information that may be retrieved from the cell phones stockpiling.

After completion of this work thought more reliable presentations with particular brands of late cell phones and delineated the procedures to extract different kind of different data specifications especially from storage space.

Two expansive sorts of relative approaches are included in social occasion relics from iPhone contraptions, i.e. real and sensible process. Jail breaking gadget is utilized as a part of the physical process. In spite of the fact that iPhone can be effortlessly modified by jail breaking however this approach defines appropriate small changes to the data in the framework. Then again, contemporary techniques are presently created which acquire may photo of the framework. Since this approach does not require iPhone escape, it is reviewed with reliable finest techniques for iPhone data. In addition, Science & Technology with National Institute (NIST) have likewise evaluated this strategy. Besides, two genuine and sensible strategies are utilized to draw out relics from Mobile android working framework and Ms Windows with boosted devices in reliable presentations. Measurable photo of the framework can be gotten by utilizing gadget. Root/regulatory benefits are, be that as it may, required in this real procedure. For all time intended for measurable assessment which includes the recuperation parcel on telephone's memory storage card defines and utilized to dedicated evacuation assets. This strategy can be utilized as a part of both Android working framework and Ms Windows cell phones. The following sections describe techniques used for different social applications in different problems.

4. EMAIL FORENSIC ANALYSIS METHOD FOR ONLINE SOCIAL NETWORKS

We study the problem of email forensic with different parameters based on network communication analysis, in this study; we observe the relationship between criminal organizations with communication network, and also study the forensic data analysis with relationships between members with their organization abilities.

Current review identified with legitimate association correspondence contact focus on email interchanges content examination, for example, EMT and MET. The two instruments predominantly assess the data activity and my own particular message subject to give choice help to investigate. Another student proposed a strategy to my own particular delicate substance and idea powerless to recognizable proof message confirmation utilizing help vector machine learning strategies [13]. In any case, these review for email "crime scene investigation" is not locked in the whole program structure. It is difficult to accomplish broad email scientific perform without framework structure. So investigation of the structure for email "crime scene investigation" is vital to email confirmation examination. Parsons, A et.al [14] planned and connected an extensive programming gadget set called IEFAF to help analysts accumulate hints and verification in a review "legal sciences" for email correspondence. The structure offers a few functionalities, for example, email sparing, changing, looking, questioning and email account limitation. The IEFAF accomplishes a settled "legal sciences" and investigation for email correspondence and has a decent sensible significance. In any case, IEFAF gadget can't acquire a confounded email arrange affiliation investigation. Email forensic data representation procedure is as shown in figure 1.

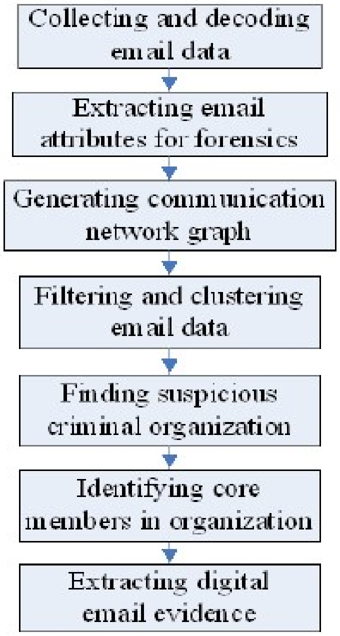

Collecting and decoding email data
Extracting email attributes for forensics
Generating communication network graph
Filtering and clustering email data
Finding suspicious criminal organization
Identifying core members in organization
Extracting digital email evidence

Fig .1. Framework Module Analysis In Different Steps.

As per this structure, we accumulate email data from email clients (e.g. Foxmail, a China version of the email client programming). Diverse clients may utilize distinctive email stockpiling data structure and email alternatives business techniques. We have to find the connection between email information records and email alternatives. In any case, likewise we have to individual out each and every personal mail to individual email data representation thought different areas. So we can get all the client idea data. As per distinctive email technique structure necessities with different web interfaces Binhex and other websites, we can interpret all data. For every email idea, we can draw out its elements be required for email 'crime scene investigation', and store email highlights into the MySQL information source. The above instances for the most part incorporate from manage, to manage, cc, point, acquired, date with different formations. Using these relations, we can contemplate and find the reliable relations between a few email choices. Furthermore the investigator can recoup the predetermined email fitting to the case. Next we construct an association graph of email records' messages, in which the vertices imply email thought and a trained favorable position is set up from a hub with from manage to another hub with to manage. The quantity of email between from manages and to manage is as the benefit of comparing preferred standpoint. In the email "criminology" structure, it is essential to find lawful organizations and their essential individuals.

5. ANALYZING CRIMINAL SOCIAL NETWORKS

In this section, we describe the criminal activities in different criminal organization at online social networks, to identify forensic system analysis using Criminal Leader Identifiers (CLDRI), this technique identify influence member operations in criminal organization.

The structure of CLDRI, a framework can be developed from Mobile Data Communications (MDC) that connected to a related organization. In such a system, a vertex symbolizes a legitimate (i.e., a guest/beneficiary) and an advantage symbolizes a course of messages between two lawbreakers (e.g., phone cell phone calls, points of interest, and so forth.). The heap of an advantage connecting two vertices symbolizes assessment between two reliable vertices to access successive social networks. An edge's bodyweight demonstrates the social quality of the vertices connected by the side. The correspondence records are accumulated either straight from mobile phones that have a place with the con artists or eventually from cell organize suppliers. We connote a framework made with MDC as N = (V, E), where V is a (limited) arrangement of vertices speaking to lawbreakers, and E is a (limited) arrangement of sides connecting vertices. More often than not, partners of a lawful organization, who hold focal parts in the organization, are engaged by criminal agents for disposal or checking [3, 18]. This is on the grounds that these fundamental partners, for the most part, perform key and imperative parts in the organization by getting to be authorities who issue directions to individuals or capacity as watchmen, who get and spread points of interest and items to different individuals. Dispensing with these principle partners is well on the way to disturb the organization and put it out of organization. In subsection A, we fabricate a framework that perceives these persuasive partners by recognizing the vertices speaking to them in a framework showing the legitimate association. We can find the analysis of different attributes in social networks with weights of each object can be used the following equation

$$w(v_k)=\frac{\left|\sum_{i=1}^{|v_k^E(in)|}|(v_i,v_k)|+\sum_{j=1}^{|v_k^E(out)|}|(v_k,v_j)|\right|}{\sum_{i=1}^{|v_k^E(in)|}0.8|(v_i,v_k)|+\sum_{i=1}^{|v_k^E(in)|}0.6|(v_i,v_k)|}$$

$w(v_k)$ is the weight of the attributes with vertex consideration.

$|(v_i,v_k)$ number of incoming with respect to crime incidents applications

$|(v_k,v_j)$ number of outgoing messages with respect crime reports.

By using above equation to define incoming and outgoing relations between different users with different attributes in edges and vertexes.

6. TWITTER SPAM ANALYZER USING FORENSIC METHOD

In this section, we discuss about designing framework to analyze twitter spammers email and different types of spammers in data sharing in communication framework data representations. The following forensic implementation procedure to define twitter spam in fallowing ways. System 'forensics' method comprises of Catching, Collection, Planning, Purchase, Maintenance, Evaluation, and Research with coverage in reliable data presentations. In network communications, different forensic data presentations in [6, 7] i.e. System Traffic Research &amp; Log Files. Email Spammer data extraction procedure as shown in figure 2.

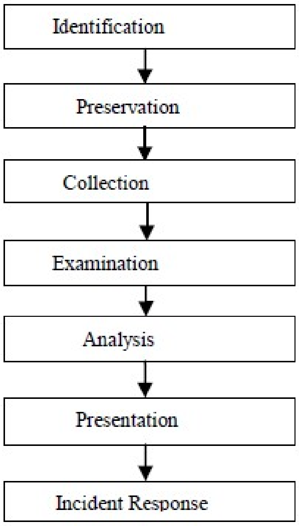


Fig .2. Network Email Spam Forensic Steps.

Spam detection device the harmful customers World health organization pollute the information in reliable and genuine customers and consecutive reason for risk to the protection and comfort of social networking sites. Spammers are supposed to be to 1 of the following classes:

A. Spam Network with Communication: In present years with open media sites is amazingly incredible. The people connect with their companions and talk or offer transmitting material with them. Locales like Facebook or myspace, tweets are continually among awesome twenty most considered sites on communication [4]. Shockingly open media links don't offer tough check frameworks, and it's basic demonstration kind of a man and put into individual's system of have confidence in [5]. The serious advancement of unsought messages has convinced the event of different garbage filtration techniques. Uncovered anyway it may be workable for spammers to workmanship centered garbage by making a speculation the data available in on-line open long range informal communication sites.

B. Spam Email Presentation: This email presentation gives best cooperation inside the web to talk with each other. Subsequently of expanding the colossal improvement with quality indexed email spam presentations. Email garbage, however for the most part known as uninvited extensive messaging, is that the "traditional" assortment of garbage. Spammers utilize a clear crevice inside the email strategy to counterfeit the from field of member degree email, so the main proficient data on the country of the email is that the coming innovation inside the email headers. Indeed, even the innovation is commonly shocking and ought not to be useful in distinguishing the criminal. Hence, spammers still capacity completely secretly without worrying of steadily being charged.

C. Spam Content Relation: Content shelling incorporates dynamical the sensible read the instructions for material representations. Information investigation strategies are now utilized on garbage recognizable proof issues [4]. Based on content garbage recognizable proof is that the robotized of distinguishing proof of spammers idea as garbage and it works fortified finding the styles inside the material and by recognizing an email. Amid this paper we appear to displayed logical technique for agent spam workers. Intentions of Spammers:

a) Dissipate creation
b) Open up infections
c) Phishing assaults
d) Bargain framework name

7. FORENSIC EXAMINATION ON SMART PHONES

In this section, we discuss about how much data generated in social networks on smart phones with preferable data operations in mobile smart phones. This analysis is represented on identifying if information generated by public networking real time applications on mobile phones to be processed and recovered from the storage space of reliable presentations. The study technique implemented was to forensically analyze and check out activities performed on top three well known public networking apps; Face book or My Space, from our frequent smart phones; iPhone, Android operating system, Windows and BlackBerry. Law providing causes and regulators in an presented criminal activity or legal criminal equalization to retrieve data or proof with direct access to the public networking companies. Although, these companies are suitable sources in collecting electronic facts are reliance on these suppliers due to power and collaboration representations [7]. But analyzing smart data representation for getting electronic proof has its own importance like confirmation and approval of proof from unique resources. The following modules describe the examination of different services of forensic analysis in online social networks.

7.1. Test Procedure: The tests performed amid assessment are isolated into four noteworthy activities. To start with activities require the application establishment taken after by various conditions for executing general exercises. The following stride identifies with sensible buy and at last looking at the gained points of interest [8]. These activities as appeared by the flowchart in Fig. 3. Each stage is thought independently in taking after circumstances:

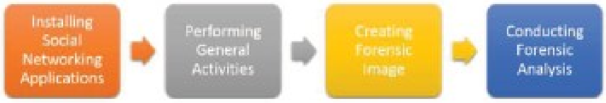

Installing Social Networking Applications
Performing General Activities
Creating Forensic Image
Conducting Forensic Analysis

Fig .3. Phases Of Social Network Crime Analysis.

1) Installation for different Applications: There are public networkings applications are set up on each smart phone system. Equalization tests are performed based on latest versions to different instructions present with time of these studies. Test information is reliable presentation of Face book and My Space data analysis, Tweets and LinkedIn services for executing typical actions on these applications.

2) Techniques: This stage is concerning executing natural and common activities on the chosen mobile phones via public internet reliable applications for acquiring typical user generated contents. Thus, assumed traditional pursuits with different status updates, feedback as well as picture and video content, mail and instance messages were performed.

3) Logical Acquired Information: In this stage is targeted at acquiring a sensible picture storage space. The acquired picture should be carefully privacy and music, making it qualified with considerable legal formations. Data stability and security was assured by reliable protecting procedures of 'forensics' research described by NIST so that gathered artifacts are appropriate in the court of law. Similar to connection oriented data purchase in stable representations, it is true for smart phone with well suited representations records of non-active details records may be like details in slack space. Connection oriented image of every chosen smart system was acquired by using particular resources with accurate configurations as these smart phones have unique Operating Systems surroundings. Approaches involved in collecting these pictures and relevant details are later explained in these studies.

4) Technical Analysis: This analysis and assessments were performed on the grouped images of the chosen mobile phones in the 4th stage for evaluating if details with actually operated in the storage then it is acquirable presentation. Also the assessments help to evaluate the number of retrieval details, its storage space in the storage and the benefits or calculation of data. All assessments were evaluated with different approaches resources for evaluating the acquired sensible pictures, finding unique signatures details specially evaluated with public networking applications.

8. FORENSIC ANALYSIS OF DIFFERENT SOCIAL APPS.

In this section, we discuss three type's social applications and their faced forensic activity from different services in resource sharing between computer organizations. National Institute of Science & Engineering (NIST) defines those forensic data representations in social application developments like Face boon, Viber and Skype artifacts in different services. NIST defines three stages to define forensic presentation in social applications.

8.1. Identification: In electronic measurable examination, acknowledgment of confirmation could mean a stroll through of the criminal activity field and distinguishing any segments or application meriting choice. In this examination nonetheless, it was pre-set up that Face book or MySpace, Skype and Viber application relics were to be examined. Subsequently, a picture of the troublesome circle produce (particularly the create keeping ms windows 10 establishment) was perceived for determination.

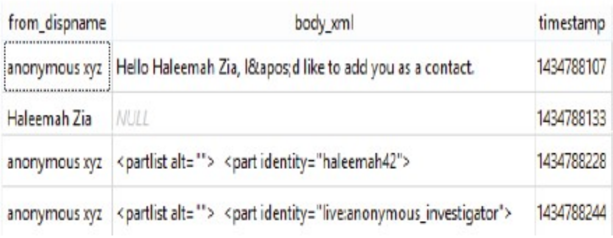
8.2. Collection: We make reference to our system for getting the troublesome circle produce picture as the accumulation arrange. We utilized FTK Imager for buy reason (and also for assessment as portrayed in this document). The choice showed up because of the truth that FTK picture processed with the speediest and most proficient picture gadget [4]. The plate measurement, as depicted in region 3 was purposely kept to 25 GB. A crude (dd) a little bit at a time (physical) picture was procured what's more, spared onto another segment create on a similar program. The acknowledgment of relics and their assessment was effectively performed over the stay program. In any case we picked to play out the entire assessment system on storage room medias picture in order to reflect a genuine life circumstance whereby respectability conservation is of huge significance. To further protect the unwavering quality, we utilized electronic hashes of the gathered confirm framework with organization. The photo was looked into for Face book or MySpace, Skype and Viber curios in this stage. The relics were examined and related in buy to examine their adequacy in any real world case. Comes about for each application are portrayed beneath.

1) Face book or MySpace Artifacts: Most of the Face book or MySpace relics were found from an indistinguishable area from in screen 8.1 [2]. Number of SQLite information source data, for example, Buddies, Experiences, Companion Demands, Information, Decals were found at the place AppData Local Packages Face book. Face book 8xx8rvfyw5nntLocalState*Face book IDDB. The greater part of these documents were rapidly reasonable through the DB Web program for SQLite

2) Viber Artifacts: Viber relics were found at the place AppDataLocalPackages2414FC7A. Viber-Free Phone Calls Text p61zvh252yqyrLocalStateviber. They were existing individual data inside the posting and furthermore in an information source by the name of viber.db. When we inquired about the documents inside guardian's registry containing Viber relics, messages were found in "/shared/exchanged" posting however were spared secured and subsequently not comprehensible. For us, they were rapidly identifiable to be SMS messages as they connected with the timings at which we played out our content informing activity. Also, stickers and pictures exchanged amid the discourse were show decoded in individual records inside a similar posting. An energizing the truth was that the shopper profile pictures of all contacts of A were immediately held in another posting despite the fact that we didn't use As thought to perceive any of these pictures.

3) Skype Artifacts: The place AppDataLocal PackagesMicrosoft.SkypeApp kzf8qxf38zg5cLocalState contained an information source with name primary.db that uncovered confirm for different activities. The thought improvement, call span, name and Skype ID of individuals among whom the exchange

occurred and specific timestamps were all recouped.



from_dispname	body_xml	timestamp
anonymous xyz	Hello Haleemah Zia, I&apos;d like to add you as a contact.	1434788107
Haleemah Zia	NULL	1434788133
anonymous xyz	<partlist alt=""> <part identity="haleemah42">	1434788228
anonymous xyz	<partlist alt=""> <part identity="live:anonymous_investigator">	1434788244

Fig .4. Face book, Viber and Skype applications with syntaxes in anonymous data representations.

The information source incorporated a few stages, for example, Movie cuts, Calls, Information, Records, Participants and so forth. The "calls" table uncovered insights with relational the telephone calls made. It uncovered the time postage stamps, Skype id of both individuals, regardless of whether video was permitted or not, sound stage, regardless of whether it was an approaching call or not and so forth. The "contacts work area uncovered insights about companion questions. At the point when investigated for the name "Haleema" numerous Skype clients with this username were point by point in the work area. The "messages" work area (Fig. 4) uncovered timestamps and members' IDs. The standard Skype idea which presents to the beneficiary was likewise observable in this work area. Contrasted and viber.db, the circumstance ID in Skype's information source was select and henceforth couldn't be associated with the stages to draw out any basic points of interest. A recognizable impression of information recovery from Face book, Skype and Viber. The numbers demonstrate the presume's subtle elements that an analyst would attempt to show signs of improvement while making a wrongdoing story. For Face book or MySpace, points of interest are incorporated inside various data relations for Viber and Skype, found to be in various tables of similar information source. Face book or MySpace is perceived for new presented networks while Viber and Skype for their contact highlights.

By observing this analysis from different approaches with different types of forensic activities in social networks. So in our research, we need to develop these type applications to detect forensic evaluation on different types of social media applications in relevant social data streams. In our research, we develop different data mining algorithms like classification and clustering and other approaches available in data classification procedures to extract forensic data evaluation for different data solutions. In our approach, we also develop different privacy and security techniques to reduce criminal activities in social or mobile phone forensic analysis.

9. CONCLUSION

In this paper, we introduce social forensic definitions on digital communication systems. We also discuss different authors opinion regarding social and mobile forensic data analysis with different crime activities in real time applications in related work. And also discuss Face boon, Viber, Skype digital artifact procedures to extract forensic data via messages and audio and video files sharing between different users in communication network. And also discuss about email spam forensic data analysis in social applications. Crime activities in online social networks also presence in real time application development. As further improvement our research, we introduce different data mining application to detect forensic data presentation in social media applications. And also we implement different privacy and security approaches to analyze and detect criminal activities in social media applications.

REFERENCES

[1] YanHua Liu, GuoLong Chen, Lili Xie, "An Email Forensics Analysis Method Based on Social Network Analysis", 2013 International Conference on Cloud Computing and Big Data.

[2] Kamal Taha, Paul D. Yoo, "A System for Analyzing Criminal Social Networks", 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining.

[3] Fazeel Ali Awan, "Forensic Examination of Social Networking Applications on Smart phones", 2015 Conference on Information Assurance and Cyber Security (CIACS) ©2015 IEEE.

[4] Asma Majeed, Haleemah Zia, Rabeea Imran and Shahzad Saleem," Forensic Analysis of three Social Media Apps in Windows 10", 978-1-4673-9268-6/15/$31.00 ©2015 IEEE.

[5] Ankita M. Ghate, L. G. Malik, " Survey on Designing Framework for Analyzing Twitter Spammers using Forensic Method", International Conference on Pervasive Computing (ICPC), -1-4799-6272-3/15/$31.00(c)2015 IEEE.

[6] Haggerty, J. (2010). Digital Forensics Investigations of Social Networks: Learning from Other Disciplines. Paper presented at the Centre for Security, Communications and Network Research. University of Plymouth.

[7] Coyle, C. L., & Vaughn, H. (2008). Social Networking: Communication revolution or evolution? Bell Labs Technical Journal.13(2).13-17.

[8] Juan Martinez-Romo , Lourdes Araujo Expert Systems with Applications 40 (2013) 2992–3000 "Expert Systems with Applications"

[9] Norulzahrah Mohd Zainudin, Madjid Merabti"Online Social networks As Supporting Evidence: A Digital forensic Investigation Model and Its Application Design." 2010 International conference on Digital Forensic.

[10] M. McCord, M. Chuah, Spam Detection on Twitter Using Traditional Classifiers, ATC'11, Banff, Canada, Sept 2-4, 2011, IEEE.

[11] Ms.S.M.Nirkhi,Dr. R.V.Dharaskar" Analysis of online messages for identity tracing in Cybercrime Investigation2010"

[12] Jeremy Davis,Joe MaclLean,David Damper" Methods of information hiding and detection in file systems." 2010 Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering.

[13] Ying Zhu, Member, IEEE" Attack Pattern Discovery in Forensic Investigation of Network Attacks2011"Ieee Journal On Selected Areas In Communications, Vol. 29, No. 7, August 2011

[14] Parsons, A. "Windows 10 Forensics: Conclusion" - Computer & Digital Forensics Blog, 2015, April 30. Retrieved June 22, 2015, from http://computerforensicsblog.champlain.edu/2015/04/30/windows- 10-forensics-conclusion/

[15] Parsons, A. "Windows 10 Forensics Part 2: Facebook Forensics", - Computer & Digital Forensics Blog, 2015, April 1. Retrieved June 21, 2015, from http://computerforensicsblog.champlain.edu/2015/04/01/windows-10-facebook-forensics/

[16] Viber: Number of registered users 2015 — Statistic. (n.d.). Retrieved June 21, 2015, from http://www.statista.com/statistics/316414/vibermessenger- registered-users/

[17] Baca, M., Cosic, J., & Cosic, Z. "Forensic analysis of social networks (case study"), Information Technology Interfaces (ITI), Proceedings of the ITI 2013 35th International Conference on (pp. 219-223). IEEE.

[18] Al Mutawa N, Al Awadhi I, Baggili I, Marrington A. *Forensic artifacts of Facebook's instant messaging service*. In: Proceedings of the 2011 International Conference for Internet Technology and Secured Transactions (ICITST); 2011. p. 771–6. Abu Dhabi, UAE.

[19] Bader M, Baggili I. *iPhone 3GS forensics: logical analysis using apple iTunes backup utility*. Small Scale Digital Device Forensics Journal September 2010; 4(1).

[20] Kubasiak R, Morrissey S, Varsalone J. Macintosh OS X, iPod, and iPhone forensic analysis DVD toolkit. Burlington, MA: Syngress; 2014.

[21] Pattillo, N. Youssef, and S. Butenko, "Clique relaxation models in social network analysis," in *Handbook of Optimization in Complex Networks*. Springer, 2012, pp. 143–162.

[22] Taha, K. "Determining the Semantic Similarities among Gene Ontology Terms". *IEEE Journal of Biomedical and Health Informatics (IEEE JBHI)*, 2013, Vol. 17, Issue 3, pp. 512 - 525.

[23] Taha, K., Homouz, D., Al Muhairi, H., and Al Mahmoud, Z. "GRank: A Middleware Search Engine for Ranking Genes by [502] Relevance to Given Genes". *BMC Bioinformatics* 2013, 14:251, doi:10.1186/1471- 2105-14-251.

[24] Tversky A: Features of Similarity. Psycholog. Rev 1977, 84:327-352.

[25] Taha, K. and Elmasri, R. "SPGProfile: Speak Group Profile." *Information Systems (IS)*, 2010, Elsevier, Vol. 35, No. 7, pp. 774-790.

[26] Taha, K. and Elmasri, R. "BusSEngine: A Business Search Engine." *Knowledge and Information Systems: An International Journal (KAIS)*, 2010, LNCS, Springer, Vol. 23, No. 2, pp. 153-197.

[27] Taha, K. and Elmasri, R. "CXLEngine: A Comprehensive XML Loosely Structured Search Engine." DataX'08 (Database technologies for handling XML information on the web), Nantes, France, March 2008.

[28] Taha, K. *"*Determining Semantically Related Significant Genes". *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, 2014, Vol. 11, issue 6, pp. 1119 - 1130.

[29] Taha, K. "GRtoGR: A System for Mapping GO Relations to Gene Relations". *IEEE Transactions on NanoBioscience*, 2013, Vol. 12, Issue 4.

[30] U. Glsser, Estimating Possible Criminal Organizations from Cooffending Data. Public Safety Canada, 2012.