A BRIEF SURVEY OF MOBILE FORENSICS ANALYSIS ON SOCIAL NETWORKING APPLICATION

Nana Kwame Gyamfi
Computer Science Department, Kumasi Polytechnic-Kumasi, Ghana

Makafui Nyamadi
Computer Science Department, Ho Polytechnic, Ghana

Prince Appiah
Information Technology Education Department,
University of Winneba, Ksi-Ghana

Dr. Ferdinand Katsriku
University of Ghana, Department of Computer Science

Dr. Jama-Deen Abdulai
University of Ghana, Department of Computer Science

ABSTRACT

As mobile devices grow in popularity and presents in everyday life, it’s often involved in digital crimes and investigation as well. But rapid evolution of new form of online communication known as social networking has become a medium for real time activities which involve instant messaging and conversation or chatting, status, comment and share of information and ideals. A brief forensics analysis was done on some of the popular social media platform like Hi5 and Tagged. Activities on this platform were examined and how it’s potential for forensics investigation. This paper briefly discussed how relevant data would be gathering from the various activities/features used by the platform for crime investigation of suspects.

Keywords: Social Networking Forensics Investigation, Mobile Device, Suspects.

Cite this Article Nana Kwame Gyamfi, Makafui Nyamadi, Prince Appiah, Dr. Ferdinand Katsriku and Dr. Jama-Deen Abdulai, A Brief Survey of Mobile Forensics Analysis on Social Networking Application. International Journal of Computer Engineering and Technology, 7(4), 2016, pp. 81–86.

http://www.iaeme.com/ijcet/issues.asp?JType=IJCET&VType=7&IType=4
1. INTRODUCTION

In recent years, computer-related crimes were rampant in the system but now due to the increase of smart phones and more applications makes these devices a goldmine for forensic investigators. Potential evidence can be held on these devices and recovered with the right tools and examination methods. We have witnessed the rapid evolution of a new form of online communication known as social networking. By joining websites and rooms that offer these services, users can interact and socialize, share information and ideas, post status or comment and updates, participate in activates and events, upload files and photos and engage in real-time instant messaging and conversations. These operating chat rooms attract millions of people from all over the world. A study estimated that the number of unique users of online social networks worldwide was 830 million at the end of 2009, International Telecommunication Union (2009). This tells us that now we can estimate over 900 million people are now users of online social networks worldwide due to increasing of more social network applications.

In spite of being primarily used to communicate and socialize with friends, the diverse and anonymous nature of social networking applications makes them highly vulnerable to phishers, fraudsters, child predators, and other cyber criminals can register or connect to these chat rooms with fake identities, hiding their malicious intentions behind innocent appearing profile. It also encourages the publication of personal data, such as age, gender, habits, whereabouts and schedules. The wealth of personal information given to these chat rooms makes it possible for cyber criminals to manipulate this information to their advantage and use it to commit criminal acts. Other scurrilous activities that can be committed on these chat rooms include uploading illegal or inappropriate material, defaming, and stalking from Mutawa, Baggili and Marrigton (2012). The large number of criminal acts that can be performed through social networks via chat rooms raises the relevant of digital forensics in this area. Electronic evidence retrieves from social network via chat rooms activities on a suspect’s machine can be great assistance in investigating a criminal case by incriminating or proving the innocence of a suspect.

Likewise accessing social networking via chat rooms with desktop computers and laptops, subscribers can use their Smartphone’s to tap into these services. A survey conducted by Ruder Finn (a PR agency) showed that “91% of Smartphone users go online to socialize compared to only 79% of traditional desktop users”. It shows that 53% of Smartphone users use them to communicate with people on social networking via chat room sites.

Approximately half of Facebook users access Facebook through a mobile device, such as Smartphone or tablet. According to Facebook, these users are twice as active as users who do not access Facebook through a mobile device, Facebook (2013). Given that millions of users of social networks through Smartphone and Smartphone provide 24/7 access to these services when data is on, there is high risk of the abuse of these services by users with malicious attention. Therefore, when a forensic examination is performed on a suspect’s Smartphone, there might be a chance of finding evidence that supports criminal prosecution.

Forensic examination of mobile devices like Smartphone is challenging. Smartphone are always active and are constantly updating data, which can cause faster loss of evidentiary data. Second, the operating system (OS) of Smartphone are generally closed source, with the notable exception of Linux-based Smartphone like android, which make creating custom tools to retrieve evidence a difficult task for forensic examiners from Mutawa, Baggili and Marrigton (2012). Smartphone vendors tend to release OS updates very often, making it hard for forensic examiners to keep up with examination methods and tools required to forensically examine each release. Not only, is variety of properties hardware of Smartphones another issue faced by forensic examiners from M. Zarouni (2006).

This paper focuses on a brief survey on forensic analyses on two main widely used social networking applications on Smartphone: Tagged and Hi5. Activities on these platforms are briefly explained and how it would be used for forensics investigation.
2. RELATED WORKS
Mobile devices have become widespread, mobile forensics becomes more and more important as mobile devices are often found in crime scenes. Consider that more and more people are using mobile devices in their daily lives. An average consumer may use several of the following items: Cellular phone, smartphone, MP3 player, digital camera and External USB drive according to Andrew Martin (2008). This devices mention was used by Andrew Martin (2008), provided the various tools, thus would be used by an investigator for analysis. They document in details the methodology used to examine mobile electronics devices for the data critical to security investigations. The methodology encompasses the tools, techniques and procedure need to gather from common devices. From their research mainly on the devices, but this paper is all about analysis on applications used by mobile users on their phone such as networking applications. Since GSM is with world’s largest system for mobile communication today and also lay the foundation for the future UMTS, it is important to recognize the need to study the methods and fools for forensic analysis of the GSM systems, Roshan, Thankur and Bhupenda (2012). It was their ideal that available data retrieved form the mobile user SIM have a great potential to be used as evidence. Not knowing this social networking applications activities can not be retrieved from the SIM card or GSM system. , Roshan, Thankur and Bhupenda (2012) Explain very well on phone contents for evidence. The following contents of modern mobile phones can have value as evidence:

- **IMEI**: IMEI or 'International Mobile Equipment Identity' is a unique 15-digit number assigned to all cellular devices. We can use this number to block a mobile phone from being used by another person or phone company if it has been lost or stolen.

- **Short Dial Numbers**: Short/Speed dial is a function available on many telephone systems allowing the user to place a call by pressing a reduced number of keys. This function is particularly useful for phone users who dial certain numbers on a regular basis. In most cases, the user stores these numbers in the phone's memory for future use.

- **Text Messages**: Text messaging, or texting, is the act of composing and sending brief, electronic messages between two or more mobile phones, or fixed or portable devices over a phone network.

- **Settings** (language, date/time, tone/volume etc): Phone configuration, such as the network connections in use, screen resolution, memory use, battery life, domain settings for email accounts you've set up and which version of Windows Phone software is running.

- **Stored Audio Recordings**

- **Stored Computer Files**

- **Logged incoming calls and dialed numbers**

- **Stored Executable Programs**

- **Stored Calendar Events**

- **GPRS, WAP and internet settings**: General packet radio service (GPRS) is a packet oriented mobile data service on the 2G and 3G cellular communication system's global system for mobile communications(GSM). GPRS was originally standardized by European Telecommunications Standards Institute (ETSI) in response to the earlier CDPD and i-mode packet-switched cellular technologies. It is now maintained by the 3rd Generation Partnership Project (3GPP). Wireless Application Protocol (WAP) is a technical standard for accessing information over a mobile wireless network. A WAP browser is a web browser for mobile devices such as mobile phones that uses the protocol. The Internet is the global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link billions of devices worldwide. It is a network of networks that consists of millions of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies. The Internet carries an extensive range of information resources and services, all from Wikipedia.
However, direct analyst of the memory could plausibly reveal other hidden information such as deleted text messages, Roshan, Thankur and Bhupenda (2012).

Digital forensics is a vehicle organizations used to provide good and trustworthy evidence and processes from Grobler, Louwrens and solms (2012). Current DF models concentrate on reactive investigation with limited reference to DF readiness and live investigation from Grobler, Louwrens and solms (2012). Their study discussed the goals for comprehensive DF management framework that will:

- Prepared organizations for DF investigations by proactive identification and the availability of enough admissible evidence, and the restructuring of relevant processes to be forensically sound;
- Use DF tools and techniques to enhance governance framework in organizations;
- Gather and analyze live evidence during ongoing attacks; and
- Successfully investigation incidents to determine the root-cause of an incident and successfully prosecute a perpetrator from Grobler, Louwrens and solms (2012).

The Federal Bureau of Investigation has highlighted the issue of growing crimes involving handheld devices in their computer crime survey from A. Ramabhadran (2009). The PDA family mainly includes palm devices, windows mobile devices (Pockets PCs) and Linux based devices, among these, Windows mobile devices are gaining more popularity of late, as the base on the popular Microsoft Window operating systems and offer a familiar look and feel from A. Ramabhadran (2009). But their believe here that, most people are patronizing windows mobile devices has now chant to more people using the Linux based Android OS. According to A. Ramabhadran (2009), the discrepancies between computer forensics and mobile electronic device forensics exist due to various factors including:

- Wide range of hardware model and accessories.
- Variety of different embedded operating systems.
- Short product cycle with new models emerging very frequently.
- Extreme orientation towards mobility.
- File system residing in volatile memory on certain devices while in non-volatile on some others.
- Hybrid devices with advanced networking and communication features.
- Suspending processes when off or idle, while the device being active in background.

Moreover, all these challenges focused on the devices internal and external components but not considering the applications run on them, this paper through more light on how forensics analysis would done on social media platform of Tagged and Hi5.

3. SOCIAL NETWORKING APPLICATIONS

For the past two decades, on the field of technology has grown rapidly with a lot of innovation. Technology is solving a lot of problems which is beyond human imagination. It is obvious that these developers on the field of technology have come out with a networking application, popularly known as social media. It has often proven to be double-edged sword breeds crime from M. Zarouni (2006). Starting from sending text messages from mobile devices to other devices, but now with access to internet, many people can share ideas and information through these social networking applications. These social networking applications come with a particular activity to perform others too come with integration of different activities. The following are examples of social networking applications, Facebook, Kik, Hi5, Tango, Skype, eBuddy, Whatsapp, Imo, Tagged, Bebo, Tagword, Ning, Black planet, Power.com, Heello, Netlog, Orkurt, LikeAlittle, Dot429, MeetMe, Pizco, Talent Splash, Google plus, path, Noteleaf and Twitter just to mention few. With internet provide by mobile service providers, mostly these applications are run on our smart phones. On this paper we concentrate on activities performed by the users on Tagged and Hi5 social media and it relation for digital forensics investigation.
4. SOCIAL NETWORKING FEATURES ON TAGGED AND HI5

1. **Registration:** Initially, all these social networking applications required registrations to login in, and login out. The survey conduct truly spells it out, because we were not able to get access to this platform activity unless you register. During registration few details are required from you. We also notice that you can register to the Tagged and Hi5 via other social media platforms like Facebook. Not only, also available in multilingual for registration.

2. **Friends Networks:** Moreover, one of the major reasons why most people join this platform is looking for friends all over the world. Tagged and Hi5 gives it members free will to search the kind of friends they want to network with. Descriptions, interest, hometown, countries, age range etc, are used by members of this popular social networking platform for searching friends and sending friend requests. Users can also send friend request via e-mails to other users. When a person receives a friend request, he may accept it or decline it, or block the user altogether. If a user accepts another user as a friend the two will be connected directly. The users friends name will be appear on his/her friends list vice versa [7].

3. **Media Upload and Sharing:** Users on this platform can also upload photos, files, videos and other media on their walls for their friends to see. Restrictions can also be set for those you want to show your upload and status to.

4. **Instant Messages:** Aside sending message via emails to friends on this social networking platform, users are able to chat with their friends when they are online at the same time. Many people make fun of using this platform for instant messages to their business partners, friends and relatives for relevant conservations.

5. **Update Status:** in addition, most users on this platform update their current status via this platform to their friends. Example status like “I am not fine dudu”, will tell the user friend that he/she is sick. Updating status, help friends to know the kind of mood their friend found him in at the moment.

4.1. Other Features

**Free web space:** Each member is provided free web space to publish content.

**Free web address:** Each member gets a unique web address that becomes the identity of that individual or business. The members can then use their web address or url to promote themselves or their business.

**Build Profile:** Members are provided web space to build their profiles. The profiles serve a dual purpose: one, they allow friends or contacts to identify members from their profiles; and two, the data entered by the members is used by Social Networking Sites to connect with other members who have a similar background.

**Upload content:** The Social Networking Sites allow members to upload text messages, photographs, audio and video files free of cost. All posts are arranged in descending order with the last post coming first. Further, all content is published in real time, and becomes visible instantly.

**Build conversations:** Content posted by members can be browsed and commented upon by all members who form part of the community. Content can also be tagged from third party sites on subjects that interest the group.

**E-mail:** Members can send e-mails to each other. The Social Networking Sites also send e-mail alerts whenever a member is tagged in a third party post. This enables members to learn when a fellow member has connected to them.

**Create Pages:** Members are allowed to create pages where they can post articles or photographs related to a theme. The pages can also be used to promote businesses.

4.2. Forensics Analysis on Social Networking Applications

Turn increase of social networking application on our mobile devices, motivated us to study how this application can be used to involve in criminal case. A survey was done on these two social media already stated. However, massive observation was done to come out how these social networking applications can be involved in many crimes. The study was done with three months. Analyzing how features of these social networking applications will relevant to criminal cases for evidence. We get ourselves involve by
registering to these social media platforms. The following information was gathered based on the features provided by the platform, for forensics investigation.

1. **Registration:** An individual can register to this social media site several times, if the person owns more than two e-mail addresses. On the ground of this, any one who involved in criminal cases, social media platform registration details should be check. For the fact, people can register and pretend as they are women, children etc. we strongly believe that people with cases at the law court with fake social media profile information should hold responsible. Because anyone who hides identity intends to join for different reason.

2. **Friend’s networks:** Culprit who has registered on this social media kind of friends can help for investigation. There is a saying that “show me your friend and I will tell you your character”. Analysis like the kind of friends the culprit indulge himself with, the age range of his friends, area and location too are very important.

3. **Instant message:** Crime suspects, social media instant message with his other friends will be a vital evidence for the law court. Recently, most people communicate to their friends through this media, reasons being that the GSM system will not be able listen to their conservation. There should be a tool to analyze all kind of chat involve by the culprit with his friends. Data gathering from conversation before crime scene, on the accused social media can be question for more investigation.

4. **Update Status:** Most people show their moods to the public through status update. Accused suspect of a criminal case social networking application status before and after the scene can be check to collect evidence. In a nutshell, we insist that forensics investigator should take notes of activities perform suspects, they should account various actions too that go on there too. Not only, will their mobile device depict the accurate evidence to the law court.

5. **CONCLUSION**

Always looking at the components of the cell phones, both external and internal components for forensic investigation, the author proposed for critical investigation on culprit social media applications activities. Due to the fact that this application on mobile devices is used for so many activities, which were briefly explain. In future we need more forensic tools that can analyze data on culprit social media platform for evidence, looking at it activities perform since joined the media.

**REFERENCE**


