ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 5, February 2016 in association with
HEERA COLLEGE OF ENGINEERING AND TECHNOLOGY, THIRUVANANTHAPURAM
Organizes
NATIONAL CONFERENCE ON ENGINEERING FOR LIFE (NCEL – 2016)
(12th -13th February 2016)

Evidence Extraction tool for Social Networking sites like facebook, twitter and LinkedIn

by Vidhya. J.A
Cyber Forensics and Information Security ER & DCI institute of Technology, Trivandrum

Abstract: **The usage of Social Network Sites has increased rapidly in recent years. Social networking consists of many computer networks and millions of people interact for multiple purposes. These networking services allow people to interact each other to build a network relationship. Government and business sectors also make use of economical consumer interaction using networks. Unfortunately, a majority of the users of these sites are young people; hence the sites also tend to attract online predators and others who would exploit the sites. This project focuses on the implementation of evidence extraction tool that can extract data from the three most popular Social Networking Sites (SNS), Facebook, Twitter, and LinkedIn. Understanding the capabilities of the tool can help forensic investigators to use the tool in the most effective way, so that they can produce repeatable results and admissible evidence to the court of law. The collected artifacts are analyzed for relevant artifacts. Some of the common SNSs artifacts that could be extracted from users computer includes: Online chat messages, wall post, status update, pictures, videos, GPS information, email, and web browsing history. The proposed framework will benefit law enforcement agents when crimes are committed.**

I. INTRODUCTION

Social Networking websites are widely used for people to openly exchange ideas and to interact publicly in cyber space. It would seem that the introduction of Social Networking Sites (SNSs) tapped into the human desire to be able to communicate with other like-minded individuals in a convenient and reasonably safe fashion, a desire that has manifest in young people in particular. Social networking sites are mainly populated by young people in their teens and twenties. SNSs were initially used for the purpose of promoting friendship. Criminal investigation can be complicated if the crime involves social networking technology because information can be posted on a number of different social network spaces, and if evidence found from these SNSs is not collected in the most timely and efficient way, other complications can be caused such as wrongful convictions. While the increase in the number of users in SNSs has resulted in

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 5, February 2016 in association with
HEERA COLLEGE OF ENGINEERING AND TECHNOLOGY, THIRUVANANTHAPURAM
Organizes
NATIONAL CONFERENCE ON ENGINEERING FOR LIFE (NCEL – 2016)
(12th -13th February 2016)

an increased number of crimes, there are limited studies focused on identifying the existing tools capability of extracting evidence from SNSs.

The aim of this project is to develop a digital forensic tool that have the ability to extraction artifacts from the three most popular Social Networking Sites (SNS), Facebook, Twitter, and LinkedIn. Understanding the capabilities of the tool can help forensic investigators to use the tool in the most effective way, so that they can produce repeatable results and admissible evidence to the court of law**.** The collected artifacts are analyzed for relevant artifacts and the hidden artifacts are also identified.

Some of the common SNSs artifacts that could be extracted from users computer includes: Online chat messages, wall post, status update, pictures, videos, GPS information, email, and web browsing history. It tries to retrieve the information posted on SNSs from the target hard disk. This project also aims to assist forensic investigators to identify existing tools capability to extract SNSs related evidence that resides on user's hard disk. All research has been carried out in the interest of gaining a better understanding of the capability of extraction tools that can retrieve the information posted on SNSs.

Digital forensics investigations require a vast knowledge of software and hardware in order to perform an effective investigation. Knowing the right tools for different investigation scenarios will not only save time but also helps to avoid unnecessary steps, and avoid inadvertent alteration of evidence. Investigators do not therefore, need to go back and re examine the evidence several times. The tools can help investigators easily identify where to look, what to look for, and how to look for the required evidence in a forensically sound manner. These aspects of forensic tools play an important role in the digital forensic environment, as the tools will immensely enhance the forensic investigation process. Social networking site investigation can be very useful and as the sites contain valuable, time stamped data and locations which can be used for finding relationships with crime or find actual suspects. Thus, when social networking sites are involved in a crime or other incidents, it is important for forensic examiners to know which tools can be used for their investigation process in order to retrieve relevant information effectively and accurately.

The motivation of the project ranging from the popularity of SNSs to the lack of supported digital forensic tools available to conduct investigation on SNSs. Digital forensic investigators are relying on digital forensic tools to extract evidence from digital devices in order to examine evidence more effectively and in a forensically sound manner. Tools and techniques in digital forensics have been developed in recent years due to an increase in the number of digital crimes. Even though there are many digital forensic tools developed to extract evidence from digital devices, these tools do not yet appear to support extracting evidence from SNSs such as Facebook, Twitter and LinkedIn.

II.SOCIAL NETWOKING SITES

Social networking sites are an important communication medium. Just like emails and

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 5, February 2016 in association with
HEERA COLLEGE OF ENGINEERING AND TECHNOLOGY, THIRUVANANTHAPURAM
Organizes
NATIONAL CONFERENCE ON ENGINEERING FOR LIFE (NCEL – 2016)
(12th -13th February 2016)

instant messaging, social networking sites are excellent place for companies, businesses and governments to interact with the public and their customers. These social networking sites become an important communication medium for many organizations and people. Christo Ananth et al. [6] discussed about Reconstruction of Objects with VSN. By this object reconstruction with feature distribution scheme, efficient processing has to be done on the images received from nodes to reconstruct the image and respond to user query. Object matching methods form the foundation of many state- of-the-art algorithms. Therefore, this feature distribution scheme can be directly applied to several state-of- the-art matching methods with little or no adaptation. The future challenge lies in mapping state-of-the-art matching and reconstruction methods to such a distributed framework. The reconstructed scenes can be converted into a video file format to be displayed as a video, when the user submits the query. This work can be brought into real time by implementing the code on the server side/mobile phone and communicate with several nodes to collect images/objects. This work can be tested in real time with user query results. Currently there are many criminal cases that are related to social networking sites or the use of social networking sites in order to commit crime. With the popularity of social media, many people are willingly publicizing where they live, their religion, their medical status, their friends, personal email addresses, phone numbers, photos of themselves and status updates, which informs people where they are and what they doing.

Criminals can use these social networking sites to commit crimes. For example, a terrorist group may use a social networking site such as Google Plus (location-based social networking website) to identify popular locations for bombing, while drug dealers can use social networking sites in order to communicate with other dealers or their customers. SNSs are rapidly growing, and spread quickly because of their characteristics and the development of cutting edge technologies such as smart phones. In other words, SNSs induce large numbers of people to create and share information, provide a place where people can express their own feelings, and enables people to check and update information anytime without geographical barriers. These characteristics of SNSs induce people to use SNSs often, and it is expected that this trend will most likely to continue (Boyd & Ellison, 2007). As more people in the world's Internet population visit social networking sites, this also indicates that evidence we can collect from these websites is likely to grow as time spent on social networking sites is growing more. The most popular social networking websites used include - Facebook, Twitter, LinkedIn, MySpace and Google Plus.

III.EVIDENCE EXTRACTION

SNS are online forums in which users come together at their convenience to share information in the form of digital text, graphics, links, or sometimes just to chat. Social Networking Sites (SNS) are defined as a web based services that users to create a public or semi-public profile allowing sharing and connections with other users. SN Sites are an important communication medium providing organizations, businesses and governments with a means to interact with the public. Everyone uses Social Networking Sites (SNS) to surf the internet.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 5, February 2016 in association with
HEERA COLLEGE OF ENGINEERING AND TECHNOLOGY, THIRUVANANTHAPURAM
Organizes
NATIONAL CONFERENCE ON ENGINEERING FOR LIFE (NCEL – 2016)
(12th -13th February 2016)

Majority of the users of these sites are young people. Many people willingly (or with personal interest) publicize:

- where they live
- their religion
- their medical status
- their friends
- personal email addresses
- phone numbers
- photos
- Status updates - informs others where they are and what they are doing.

With the increase in the number of users in SNSs has resulted in an increased number of crimes. Due to the popularity of Facebook and its potential for being misused, the main objective of this study is to findEVIDENCE EXTRACTION TOOL FOR SOCIAL NETWORKING SITES LIKE FACEBOOK, TWITTER AND LINKEDIN

This project focuses on the implementation of evidence extraction forensic tool that can extract data from the three most popular Social Networking Sites (SNS):

- Facebook
- Twitter
- LinkedIn

The artifacts to be collected include:
Facebook Artifacts:

- Make friends, Upload photos, post videos, get news, tag friends, view friend's status.
- The artifacts extracted from face book activities includes:
  - User personal information
  - post and comments
  - Chat details
  - Pictures and videos

Twitter Artifacts:

- Online social networking service that enables users to send and read short character messages called "tweets".
- Artifacts extracted for twitter activities :
  - Posted tweets
  - Photos
  - Friends
  - Timestamps
  - Contents of tweets

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 5, February 2016 in association with
HEERA COLLEGE OF ENGINEERING AND TECHNOLOGY, THIRUVANANTHAPURAM
Organizes
NATIONAL CONFERENCE ON ENGINEERING FOR LIFE (NCEL – 2016)
(12th -13th February 2016)

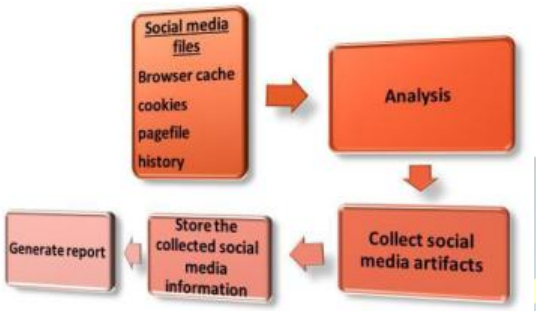

Fig 1 Block diagram of the proposed framework

Figure 5.1 shows the block diagram of the proposed system. Social media files such as browser cache, pagefile, web history and cookies acquired and analyzed. After analysis the artifacts related to social media will be collected and store the data in a temporary location .Also report is generated. These are basic steps involved in the proposed tool.

IV.ARTIFACTS AND LOCATION POTENTIAL EVIDENCE

Internet history analysis is a primary technique and involves examining and analyzing a suspect's Internet activity. This is usually achieved by investigating the Web browser used by a suspect to access and interact with the World Wide Web (WWW). All of the well known Web browsers such as Mozilla Firefox, Google Chrome, and Microsoft Internet Explorer (IE) save detailed information of activities in a cache, in the internet history list and in cookies in order to improve the user experience and save browsing time .Table 1 displays various Internet artifacts specifically related to SNS evidence which may be discovered on a suspect's operating system used to interact with a SNS. Possible artifact locations that include files or disk areas are also presented.

Table 1: Social Network Artifacts and Location of Potential Evidence

- User photos and email address
- career profiles and update details
- Job seeker's information
- Recruiter's details
- Contacts
- Inbox
- Company details

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 5, February 2016 in association with
HEERA COLLEGE OF ENGINEERING AND TECHNOLOGY, THIRUVANANTHAPURAM
Organizes
NATIONAL CONFERENCE ON ENGINEERING FOR LIFE (NCEL – 2016)
(12th -13th February 2016)

Artifacts	Description	Primary data location
Internet History	List of websites URLs visited	Browser Database (eg. index.dat)
Cookies	Cookies data	Browser profile file, Browser cache
Web pages	Web site data and files. such as html	Browser cache, pagefile.sys files
Images	Pictures and other images, such as jpeg images	Browser cache, pagefile.sys file, user folder, local settings
Videos	Video files	Browser cache ,pagefile.sys, Users folder, local settings, temporary internet files
Downloads	Material downloaded from SNS	Browser cache, temporary Files
Location	Users location stored on SNS	Browser cache file, user folder, pagefile.sys files.
Chat	Messages sent and received	Temporary Internet files
Wall Post and Status update	Possible to collect location information from the status update	Temporary Internet files, pagefile.sys file

The proposed system focuses on the implementation of evidence extraction forensic tool that can extract data from the three most popular Social Networking Sites (SNS).In this system study phase the input files need for the proposed tool is mentioned. The social media files includes :

Cookies

- web sites run in a stateless mode: no connection contains information about the state of the session
- **cookies** are used by a web site to store values on the client that create a web session (e.g., items in your shopping cart); in a unless you have changed your file viewing settings to show hidden and system files.
- Pagefile.sys is a windows system files, acts as swap file and was designed to improve performance.
- The size of the pagefile is around 1.5 to 3 times the size of the RAM. Pagefile.sys is a file that is used by Microsoft Windows to store frames of memory that do not currently fit into physical memory.

Browser Cache

The cache is where web page components can be stored locally to speed up subsequent visits. Browser caching is a mechanism where files retrieved from websites that have already visited are stored on a specific location on a hard disk. The main purpose of caching is that the web pages that were visited earlier can be loaded much faster when this web page is visited again in a later stage. The browser usually compares the data of the web page that is remotely available on the Internet with the one that is hold locally in the caching folder. When this web page has not changed, the cache will be used or parts of the cache and otherwise the web page is downloaded again, displayed and possibly cached. When the web browser is closed the web cache remains stored on that specific location of the hard disk. This will gives the investigator about the details what a user was looking at online. The information that the browser cache contains are the following:

- Identifies websites which were visited
- Provides the actual files the user viewed on a given website
- Cached files are tied to a specific local user

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 5, February 2016 in association with
HEERA COLLEGE OF ENGINEERING AND TECHNOLOGY, THIRUVANANTHAPURAM
Organizes
NATIONAL CONFERENCE ON ENGINEERING FOR LIFE (NCEL – 2016)
(12th -13th February 2016)

sense, they can be used to track you, as each one contains a username.

- Two types of cookies: session and persistent
- session cookies are stored in memory
- persistent cookies are stored on disk

Pagefile

Windows uses part of your hard drive space as virtual memory. It loads what it needs to load into the much faster RAM (random access memory) memory, but creates a swap or page file on the hard drive that it uses to swap data in and out of RAM.

account

- Timestamps show when the site was first saved and last viewed

IV. CONCLUSION

Digital forensics investigations require a vast knowledge of software and hardware in order to perform an effective investigation. They are relying on digital forensic tools to extract evidence from digital devices in order to examine evidence more effectively.

REFERENCES

[1] *Ahmed Rafea, Nada A. Mostafa* ,"Topic Extraction in Social Media "on 2013

[2] Brian Cusack,Edith Cowan University and Jung Son ,AUT University, "Evidence Examination Tools for Social Networks"on 2012.

[3] Guo, Y., & Slay, J. (2010). Data Recovery Function Testing for Digital Forensic Tools. Advances in Digital Forensics VI. 297-311. Springer Boston.

[4] Ana Gainaru, Stefan Daniel Dumitrescu, Stefan Trausan-Matu "Politehnica" University of Bucharest, Department of Computer Science Bucharest, Romania (2010)," Toolkit for automatic analysis of chat conversations" on 2010.

[5] M. Huber, M. Mulazzani, E. Weippl, G. Kitzler, and S. Goluch. Friend-in-the-middle attacks: Exploiting social networking sites for spam.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 5, February 2016 in association with
HEERA COLLEGE OF ENGINEERING AND TECHNOLOGY, THIRUVANANTHAPURAM
Organizes
NATIONAL CONFERENCE ON ENGINEERING FOR LIFE (NCEL – 2016)
(12th -13th February 2016)

Internet Computing, 2011.

[6] Christo Ananth, M.Priscilla, B.Nandhini, S.Manju, S.Shafiqa Shalaysha, "Reconstruction of Objects with VSN", International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Vol. 1, Issue 1, April 2015, pp:17-20

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

[8] Ravi Kumar Jain, B. (2007). Web Browser as a Forensic Computing Tool. ICFAI Journal of Information Technology. 47-57.

[9] Boyd, D. M., & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication. 13(1). 210-230.

[10] Carrier, B. D., &Spafford, E. H. (2004). An Event-based Digital Forensic Investigation framework. Paper presented at the Digital Forensic Research Workshop, West Lafayett , Purdue University, USA.

[11] Casey, E. (2002). Handbook of computer crime investigation : forensic tools and technology: San Diego, Calif. ; London : Academic, 2002.

[12] Casey, E. (2004). Digital evidence and computer crime : forensic science, computers and the Internet: London ; San Diego, Calif. : Academic Press, c2004.