JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 10(3), SEPTEMBER, 2022
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com

Digital Forensic Investigation of Cyberstalking and Social Media Harassment using Network Forensic Analysis

Yiye J., Mustapha R., Ahmad A. M., Bassi H.
Computer science Department
Kaduna State University.

ABSTRACT
Cyber harassment committed on social media are becoming more difficult for forensic investigators to gather evidence by changing the default location of important system files and folders on the victim's machine. Social media has made life easy for people and organizations because of the numerous advantages it has but the fact from evidence shows that these technologies could be taken over and utilized to the advantage of criminals to commit a wide scale of havoc and crimes on the cyber world, Crimes committed over the internet are called cybercrime as cyber related criminal attacks become more predominant in today's technologically driven society. Hence the need for and use of digital evidence in courts is inevitable. Digital forensics is the science of identifying, extracting, analyzing and presenting the digital evidence that has been stored in the digital devices there by making it easy for perpetrators of such crimes to be accountable and successfully prosecuting them. The main aim of this work is to provide a digital forensic investigation in cyber-stalking and social media harassment. In order to achieve the intended aim three objectives have been formulated thus to design digital forensic model that will mitigate the rapid increase of harassment on social media and security challenges, compare the proposed digital forensic model to in investigation. From our result that live-box analysis, alongside dead-box analysis gave us gave five (5) sufficient evidences will enable investigators bypass the issue of false flag, save time and apprehend the criminal.

ARTICLE INFO
Article History
Received: March, 2022
Received in revised form: April, 2022
Accepted: May, 2022
Published online: June, 2022

KEYWORDS
Cyberstalking, Cybercrime, Digital Forensic investigation, Live box, Dead box

INTRODUCTION

In today's world, online social media has revolutionized the way people think and do things due to the internet; online social media is defined as the collective of online communication channels dedicated to community-based input, interaction, content sharing and collaboration. Also, it is defined as an integrated technology that allows users to generate their own content and share that content through various connections (Bureau of Justice Assistant, 2013). Social media is linked with web 2.0, a technology which it centers of interest is on collaboration, interaction and integration (Bureau of Justice Assistant, 2013). Various online social media tools exist with various characteristics, statistical data and function. Tools used in social media include social networking sites, blogs, photo and video sharing sites, WhatsApp, blackberry messenger, etc. Social media has been adopted by people around the world. Industries, companies and organization have recorded success by using the various tools to establish communication with customers and potential customers. According to Tassel (2006), "the popularity of social media shows the power and importance of user-created contents".

Social media is diverse from the traditional form of media in various ways due to new technology been involved. In traditional media, people have to wait for the next publication before they can receive information, with online social media news comes from the direct source in real time (Bureau of Justice Assistant, 2013). Online social media is used in different ways and organizations which do not use online social media are potentially behind. Social media has made life easy for people and organizations because of the numerous advantages but the fact from evidence shows that these technologies could be taken and

Corresponding author: Bass, H. ✉ bassi.haruna1@gmail.com ✉ Computer Science Department, Kaduna State University, Kaduna. *© 2022. Faculty of Technology Education. ATBU Bauchi. All rights reserved*

utilized to the advantage of criminals to commit a wide scale of havoc and crimes on the cyber world. Crimes committed over the internet are called cybercrime.

Most forensic investigators neglect the fact that when a person is being cyber stalked on social media, the stalker might have had direct access to the victims' machine through malware or script and might have changed important, necessary files or even hidden them to prevent forensic investigators from tracing their track. In recent times, stalkers have developed a technique called "False Flag, in which the actions are undertaken in ways to deceive the victim as to the nature of the perpetrator" (Tabatabai, 2015), they stalk their victim and leave a trail to deceive forensic experts whereas hiding the exact trace. More so they are now running malware from volatile memory making it difficult for forensic expert to detect or trace their track. Research carried out by Berkeley scientist shows that 93% of data actually never leaves a digital domain (Gubanov, 2013). The rapid increase in the number of Social Media users have paved great functionality for communication, however increased the rate of cyber stalking (cyber harassment) (Norulzahrah et al. 2011). Cyber harassment committed on social media are becoming more difficult for forensic investigators to gather evidence by changing the default location of important system files and folders on the victim's machine. There is no fixed location for some important system files and folders with lower administrative rights which makes it easy for stalkers to change default location and further complicate the search for forensic experts (Gubanov, 2013).

The main aim of this work is to provide a digital forensic investigation in cyber stalking and social media harassment using network forensic and data mining. In order to achieve the intended aim, we investigated concrete evidences so as to avoid false flags and apprehend social media criminals. These evidences could also be used in a law court to file a suit against any social media harassment. We also identified already existing works and gaps which are related to social media harassment.

The rapid increase in the growth of computer use has become an expert tool for cyber criminals. The security tools available to mitigate such crimes are not effective enough due to the ease and availability of information on the internet to cyber criminals. Furthermore, the improvement in information technology and the vast internet users have given cyber criminals more opportunity to carry out their crimes (Govil & Jivika, 2007). According to Govil & Jivika, (2007) defines cybercrime as "any illegal activity arising from one or more internet components such as websites, chat rooms, email. Cybercrime is also defined as any criminal act dealing with computers and networks, which falls into a wide range of crimes committed using the internet such as; cyber bullying, cyber stalking, cyber harassment, hacking, identity theft, malicious software (Cross domain, 2015). Cybercrime is also seen as the use of a communication device through which a channel be it a laptop or mobile phones used directly or indirectly to commit a crime (Gunjan, et al., 2013)

RELATED WORKS

Aggarwal et al., 2005 Captured and recorded encrypted data which can be used as vital evidence in the investigation, using hardware-based acquisition or software-based acquisition from a remote computer. They were able to capture traces that the cyber stalker left on the victim's computer. They developed a proactive toolkit, in which he called Predator and Prey attack (PAPA) which was used to acquire data from a remote computer. lee et al., 2013 Identified forensic investigation Crime incidence digitally using the four stage models' crime scene investigation model was used which constitute four (4) stages recognition, identification, individualization and construction.

Spafford & Carrier, (2004) develop digital way of investigation, They Proposed the integrated digital invention process, which consists of 17 processes which are categorized into 5.

Zawoad et al., 2015, Built forensics Aware eco system for the Internet of Things (internet of things this is a system of interrelated computing devices that provide unique identifier and the ability transfer data automatically), to address the issue that the rapid increase of Internet of Things devices things which creates a new attack environment The use of internet of Things environment helps researchers obtain a clear understanding of specific machine.

Craig et al., 2020 explored age, gender, and cross-national differences in

Corresponding author: Bass, H. ✉ bassi.haruna1@gmail.com ✉ Computer Science Department, Kaduna State University, Kaduna. *© 2022. Faculty of Technology Education. ATBU Bauchi. All rights reserved*

adolescents' engagement in Social Media Use, then relationships between social media Use they describe engagement in the three types of Social Media Use (intense, problematic, and talking with strangers online) by age and gender and then in the perpetration and victimization of cyber-bullying. Relationships between SMU and cyber-bullying. Outcomes were estimated using Poisson regression (weighted in 166,647 from 42 countries).

METHODOLOGY

Digital Forensic Investigation Model for Social Network

We propose an extension of the work of Norulzahrah et al., 2011 by providing substantial evidence in digital forensic investigation. Their aim was to have a specific model which will be used in investigating crimes on social network. The proposed model comprises of all the process in social network. This model was divided into two parts shown in figure 1. Physical environment which includes various activities done before the commitment of the investigation. Digital environment, this involves carrying out the investigation of social network, as a result we will not have substantial forensic analysis with evidence to approach an investigation. therefore, it was drawn that live-box analysis be used alongside dead-box analysis to approach an investigation which would yield substantial evidence and also enable investigators bypass the issue of false flag, because they would actually have the opportunity of seeing ephemeral hidden evidence as seen in this research project. For digital forensic investigation to be undertaken, the forensic investigator should have the necessary skills and knowledge of digital forensic and must have an approved professional qualification, below is a digital forensic model.

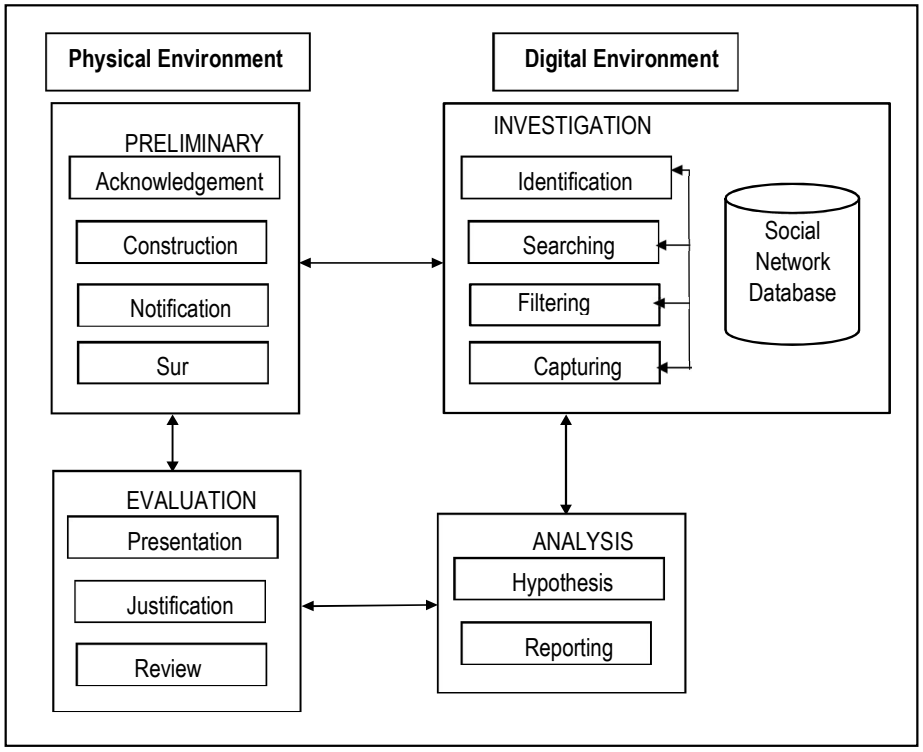

Figure 1 Digital Forensic Investigation Model for Social Network adopted from (Norulzahrah et al., 2011)

Creating the Victims Facebook Account

Facebook was chosen as the social media site. This is because Facebook is known to be the most widely used social media site, and this is where majority of people meet to make new friends, keep up with the activities of

Corresponding author: Bass, H. ✉ bassi.haruna1@gmail.com ✉ Computer Science Department, Kaduna State University, Kaduna. *© 2022. Faculty of Technology Education. ATBU Bauchi. All rights reserved*

their friends, etc. Facebook is known to have over five hundred million people (Vargas, 2010). Table 3.0 shows the user Facebook profile page requirements for the purpose of anonymity in this project, the name Eve Janeth was used, and she does not have any profile picture.

Table 1.0 Details of Victim social media account on Facebook

Facebook Name	Eve Janeth
Joined Facebook	September 20, 2015

Installing the Stalkers Machine

The software to be used for stalking the victim would be a Kali Linux and a Windows 7 operating system. This is because, the stalker is categorized as a vindictive stalker, one who has a very good knowledge of computer and is being able to execute his/her activities through malicious codes, viruses, Trojan, etc. kali Linux is a Linux based advanced operating system, which is used for penetration testing (Offensive Security, 2015), by advanced security personnel, but has now been compromised by cyber criminals (Cyber Stalkers) due to the free availability of information on the internet available.

Cyber Stalking the Victim through Social Media Scenario

Maxwell shipping UK was incorporated in the year 2010, as one of the leading shipping companies in the UK. William Sam, was an employee of this company, he worked in the human resource department. William Sam has a Bachelor of Science in Computer Science and a Master of Science in Computer security, although he never had the opportunity to continue in this field, as he was employed in the human resource department of Maxwell Shipping Company. In 2013 Eve Janeth was employed into the human resource department of Maxwell Shipping Company. Eve Janeth was in the same department with Williams and both knew themselves. As years went by, they became familiar with each other as work partners. Eve looked for a house and William told her there is a spare room in the shared apartment he lives, and eventually Eve moved into the room. On September 19, 2015, Eve Janeth was promoted to deputy manager human resource. William became angry and jealous because he has been in that department long before Eve was employed and yet he was not promoted. He decided to do everything possible to her to be demoted or even sacked. Then he decided to pursue and stalk her through social media, because he could be anonymous and she would not know the actual identity of him. September 20, 2015, he created a Facebook account with the Name Henry Yappy and then he searched for her name on Facebook and sent her a friend request Eve saw the request and accepted the friend request, since Facebook is a platform to meet new people and she never knew the consequences of accepting a stranger on both parties started communicating through Facebook which resulted in the victim asking the stalker for a software application which would enable her win lottery often which can be seen the command msfconsole, which is a metasploit framework that is used to exploit vulnerability, was issued. The next is to issue the exploit to be used. The exploit to be used is MS013_071_THEME, which is a vulnerability known in all versions of Microsoft windows which allows a remote malicious code to be executed on the windows theme of the system, thereby creating a back door or an open port for an attacker to have administrative access to the system (CVE, 2013). However, for an attack to be possible the user of the machine must be convinced to un the application. The command uses exploit/windows/fileformat/ms13_071_theme The next is to set the payload with the command set payload windows/meterpreter/reverse_tcp, which is used to inject VNC DLL via a reflective loader to connect back to the remote machine used by the attacker (Offensive Security, 2015) Next is to set the IP address of the machine to grant access to when the exploit is executed. The command set lhost 192.168.181.129 was issued From the chat below between Henry Yappy and Eve Janeth it shows that Henry has sent the link to Eve and she has clicked on it, downloaded the software and run it Once the software has been executed by Eve, then the attacker which is William now has full access to her computer without her knowing The next is to issue the command sessions –l to view the

Corresponding author: Bass, H. ✉ bassi.haruna1@gmail.com ✉ Computer Science Department, Kaduna State University, Kaduna. *© 2022. Faculty of Technology Education. ATBU Bauchi. All rights reserved*

connection details and the port number which has been opened on the remote computer for the attacker to have remote access. Then the command sessions –I 1 was issued to begin the connection.

Cyber Stalking the Victim

After having full remote access to the victim's computer, the attacker had to browse throw the remote computer documents to find any valuable file that can be used against the victim. There was a picture which the victim did not want anyone to see, because it is sensitive and can damage her personality if seen by people. Because the attacker has full access to the computer remotely, he browsed through the computer changing directories till he got to the directory c:\users\Johanna\Pictures\desert.jpg and came across an image file named Desert.jpg for the attacker to view the file the command was issued Desert.jpg and then the command run VNC was issued to enable him view the screen of the victim's computer to see the file opened and take a screen shot of it as a copy. Virtual Networking Computing (VNC) is used to enable a graphical user interface (GUI) of a windows machine on a Linux machine (Richardson, 2013).

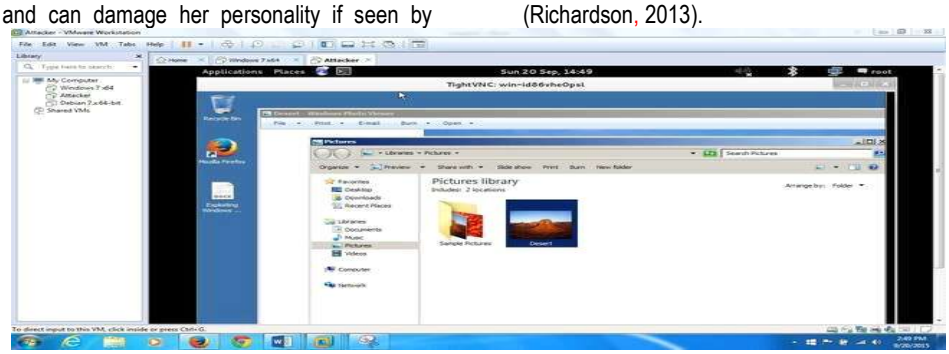

Figure 2: Victims screen displaying from the attacker's machine showing the image fi

Next the victim closed the opened le by terminating the process with the command taskkill /IM dllhost.exe.

RESULT

Search warrant to physically search the suspect physical crime scene

1. Use of forensic tools to capture the volatile and non-volatile memory
2. Examine and analyze the different Images acquired for evidence that can lead to the apprehending of the suspect in the crime committed
3. An appropriate digital forensic report about the investigation will be produced

Corresponding author: Bass, H. ✉ bassi.haruna1@gmail.com ✉ Computer Science Department, Kaduna State University, Kaduna. *© 2022. Faculty of Technology Education. ATBU Bauchi. All rights reserved*

Example 1: Regional Computer Forensics Lab • 4455 Genesee Street, Cheektowaga, NY 14225

REQUEST FOR SERVICE

CASE INFORMATION:			***RCFL Case #:***
Submitting Person/ID#:		Date:	Agency Case #:
Submitting Agency:		Service: **Field Lab Tech**	Case Title:
Agency Property Tag #:		Suspect's Name:	
Case Agent:		Phone #:	
DDA/AUSA Assigned:		Phone #:	
Date Seized:		Case/Crime Type:	
Location Seized:		Pending Court Dates:	
Site #:		Date Analysis Needed:	
Suspect In Custody:	**Yes/No**	Expected Evidence Return Date:	
Narcotics Related:	**Yes/No**	Number of Computers Anticipated:	
Type of Seizure: (Circle) **Search Warrant Probation Parole Consent Admin Fed. Grand Jury Other:**			
Has this evidence been previously viewed and/or accessed by anyone? (Explain)			
Are you aware of any privileged information contained within evidence? (Explain)			
Do you want Standard Case Related Search Strings run against evidence? **Yes/No** (Circle Requested Searches) **Child Porn Narcotics Financial Crimes Internet Crimes Extortion Other:**			

SERVICE REQUESTED: ***(Requests for Field Service must be received at least 2 business days prior to the search.)***

INSTRUCTIONS:

a. Please prepare one form for each search site (address).
b. Please provide ***ALL*** requested information and note any unusual circumstances in the Service Request area.
c. Please attach an Evidence Custody Form listing each individual container or package of submitted evidence.

RCFL USE ONLY	
Date Case	**Received By:**
Case Priority:	**Priority Established By:**

Figure 3: Approval form to undertake an Investigation adopted from (National Institute of Justice, 2004)

This process involves the forensic investigators carrying out incidence response, to survey the physical crime scene (computer). Incidence Response, involves sending a forensic investigator to the crime scene to perform a dead-box or live-box approach. But in this case, Live-box and Dead-box approach will be used.

Live-box

The method to be used is the software-based acquisition, which involves using software to acquire a memory dump of the RAM (volatile memory) whilst the computer is still running. This is to ensure that all suspicious process is not lost. The software used was FTK image software, which has the capability to capture both volatile memory and Nonvolatile memory.

Dead-Box

This method involves capturing the image of the computer whilst its shutdown or turned Although this process can also reveal potential evidence in the crime but some vital evidence such as ephemeral evidence will be

During the process of analyzing the information retrieved by the tool, Facebook chat tab was visited and examined, and then a suspicious information was retrieved

Sender name = n/a

Senders ID = 1000010078516859

Message = ok let me send you the link.

Further analyses continued and Facebook URLs tab was visited and suspicious information was retrieved.

URL = http://192.168.181.129 , https://www.facebook.com/messages/1000010078516859. The last digits relate to the same sender's ID retrieved. This became even more suspicious. The forensic investigator continued with the analyses and Firefox downloads was visited and another suspicious information was retrieved.

File name: msf.scr

Downloaded source: file:////192.168.181.129/vXrBzd/msf.scr Saved to: file///c:/Users/Johanna/Downloads.

After viewing this information, it became clear that a file was downloaded from the IP address 192.168.181.129 and it was saved to C:\Users\Johanna\Downloads. But the details about this file downloaded had not yet been analyzed. Up till this moment, the forensic investigator, does not know exactly who sent the message "ok let me send you the link" and the computer with the IP address "192.168.181.129". Further analysis continued and then Firefox session store artifacts tab was analyzed and then a suspicious

Corresponding author: Bass, H. ✉ bassi.haruna1@gmail.com ✉ Computer Science Department, Kaduna State University, Kaduna. *© 2022. Faculty of Technology Education. ATBU Bauchi. All rights reserved*

information relevant to the investigation was retrieved.

Title: Henry Yappy – messages
URL:
https://www.facebook.com/messages/1000010078516859

Further analysis carried out on the Firefox web history tab was analyzed and the information retrieved was shown below

URL = file:////192.168.181.129/vXrBzd/msf.scr

From this information it was clear that the victim visited the url above.

Capturing

This phase involves the relevant data which will eventually be used in the investigation. There was suspicious evidence which was gathered using the IEF tool. The table below shows evidence that's is eventually needed for the investigation

Evidence 1
The sender's ID 1000010078516859 indicates that, who so ever sent the message ok let me send you the link "eventually has the ID and the person who received the message has the Receiving ID 1000010087396830. Also, from the list of evidence gathered it is clear that the victim was visiting facebook frequently, because it was only facebook social network that turned up during the search.

Evidence 2
Facebook urls: this indicates all possible urls that was visited on facebook social network. Carefully analyzing the url list, the address http://192.168.181.129/ http://www.facebook.com/messages/1000010078516859, it indicates the victim visited a link which was sent to her as a message during a chat conversation with the suspect which is yet to be apprehended. Also, the ID at the end of the url link which is "100010078516859", also matches the same ID as evidence 1, which indicates that whosoever the victim had a chat with the IP address 192.168.181.129 was the person who sent the message as indicated in evidence 1.

Evidence 3
Firefox Download: this shows a list of files downloaded from the internet with the possible locations and the url of the downloaded file. Carefully analyzing this tab, a file with the name "msf.scr" was discovered. Also the url at which the file was downloaded from was shown file:////192.168.181.129/vXrBzd/msf.scr, the location at which the file was downloaded was shown file:////c:/Users/Johanna?Downloads and the download status of the file was shown "Downloaded". From this it indicates that the user visited a link and downloaded a file, although the authenticity of the file is not be verified yet. Again, the IP address in the url of the downloaded file corresponds to the IP address in Evidence 2, which indicates the person with the IP address or the person who had a chat with the victim in evidence 2 sent this file to the victim.

Evidence 4
Firefox Session Store Artifacts: this is a service on Mozilla Firefox that stores a firefox session while a user is using it to surf the internet and if the system is shutdown or the browser crashes, the session store artifact will restore the users browsing session back (Mozilla, 2014). Carefully analyzing this tab, a url was shown https://www.facebook.com/messages/1000010078516859 also the title of the session was "Henry Yappy – Messages/1000010078516859". From the first information, the ID corresponds to previous ID in evidence 1 and 2. The second information has an Id at the end which corresponds to evidence 1 and 2 and also carries a name. This indicates that the person who sent the message or potentially sent the link is Henry Yappy. The next step was to search the victim's face book account for more evidence such as recent friends added, conversation the victim had with people and so on with focus more on the name Henry Yappy. Going through the victim's friend list, the name Henry Yappy was seen and then further investigation went on to see the messages both parties had. Eventually the exact message discovered in Evidence 1 was seen on the conversation as shown in Appendix D. Also, the link discovered was also seen, which was sent to the victim as a lottery software, which eventually did not work as said in the message sent by the victim to the

Corresponding author: Bass, H. ✉ bassi.haruna1@gmail.com ✉ Computer Science Department, Kaduna State University, Kaduna. *© 2022. Faculty of Technology Education. ATBU Bauchi. All rights reserved*

suspect. It became clear to the investigator that this was the person who sent the link.

Evidence 5

Firefox Web history: this shows a list of url visited by the victim. Careful analyses showed a url file:////192.168.181.129/vXrBzd/msf.scr the number of times the victim visited the url was shown as "1". Also, if the victim typed the link was also shown as "No'. From this, it indicates that the victim clicked on the link sent to her through a chat conversation with the potential victim in evidence 4.

Pro-discover Tool

This tool is used to examine an image of a hard disk for any possible non-volatile file on the system. It is able to detect any deleted file of if possible hidden files.

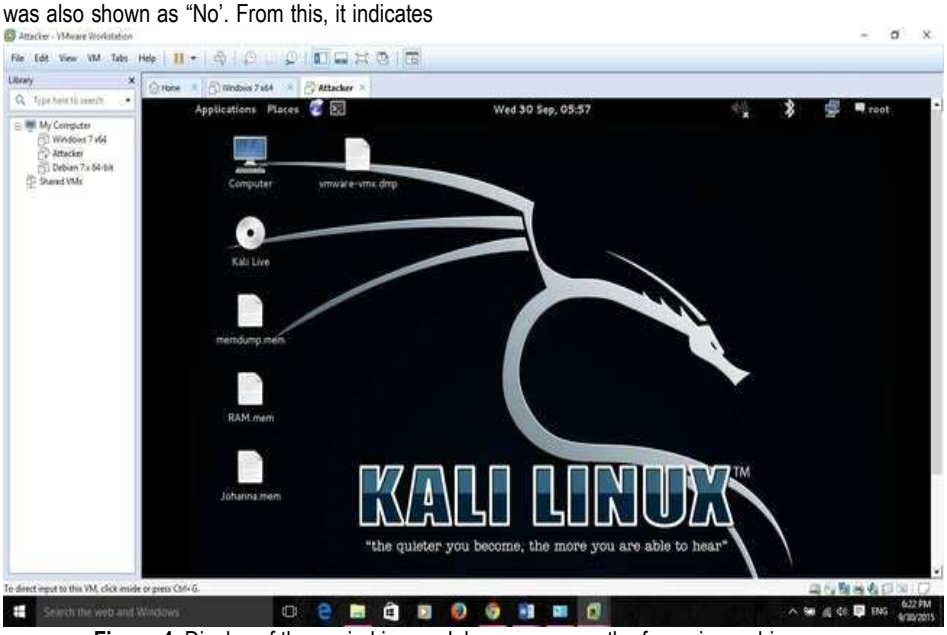

Figure 4. Display of the copied image Johanna.mem on the forensic machine

.

Investigating the Real Owner of the Facebook Profile Henry Yappy

From all evidence gathered and analyzed it is clear that the perpetrator is Henry Yappy, but who is Henry Yappy is yet to be known, because since cyber stalking is not committed physically, it means the stalker would definitely be in a different or remote location. To find the list of open network connections to the victim's computer at the time the volatile memory was captured the following command was issued as shown.

volatility netscan –profile=Win7SP1x64 –f Johanna.mem

The IP address of the victim computer (local Address), the port number using the service, the remote IP address the service is connecting to and the port number. Hence, we can deduct from this that the process yappy.scr is linked to the remote ip address 192.168.181.129 and port number 4444.

Carefully analyzing both the victims IP address and the IP address discovered, it can be seen that they are on the same network. This indicates the suspect is actually connected to the network of the victim; therefore, we can conclude that the victim is on the same building as the suspect.

Investigation on the Suspect Machine

Investigation on the suspect machine was not done as a result of time constraint. However, the step or process for the investigation to occur is using GeoIP tools to locate the IP address, however in this case scenario the suspect was on the same network as the victim having an appropriate approval to retrieve suspect information from theISP (Internet Service Provider).

Corresponding author: Bass, H. ✉ bassi.haruna1@gmail.com ✉ Computer Science Department, Kaduna State University, Kaduna. *© 2022. Faculty of Technology Education. ATBU Bauchi. All rights reserved*

Table 2.0 Digital Forensic Investigation Report by Justina Yiye

Investigator	JUSTINA YIYE (Abc Intelligence)
Examiner	JUSTINA YIYE
ID	Mcs/csc/scs/0008/2016
Department	Computer Science
Subject	Digital Forensic Investigation and Examination Report
Offences	Cyber stalking, Hacking, Data theft, Use of Malicious software, Email spam, scam
Suspect	Henry Yappy
Start Date	JANNUARY, 2020
End date	APRIL 9, 2021

DISCUSSION

This research identifies the various types of cyber stalkers, the approach, techniques and tools being used to stalk their victims on online social media. The issue of false flag was discussed which is becoming a new way cyber stalker use to deceive forensic investigators during investigation. The lack of substantial evidence in digital forensic investigation was as a result of using only the dead-box forensic analysis to approach an investigation. therefore, it was drawn that live-box analysis be used alongside dead-box analysis to approach an investigation which would yield substantial evidence and also enable investigators bypass the issue of false flag, because they would actually have the opportunity of seeing ephemeral hidden evidence as seen in this research project. For digital forensic investigation to be undertaken, the forensic investigator should have the necessary skills and knowledge of digital forensic and must have an approved professional qualification.

CONCLUSION AND FURTHER WORKS

This research still has room for improvement. It is not a full and detailed approach when it comes to digital forensic investigation. Although it has created a pathway for more research to be done in some areas such as social network forensics and network forensics which was highlighted briefly in this research and therefore can be researched further.

Evidence gathered was done using the appropriate digital forensic standards; the tools used are approved digital forensic tools. The chain of custody form was filled to preserve the integrity of the evidence. The suspect committed different computer and cyber related crimes and hence the appropriate punishment for such crimes should be given to the suspect

REFERENCE

Aggarwal, S. H. P. K. L. &. M. J., 2005. Systematic Approaches to Digital Forensic Engineering. IEEE Article.

Brian D. Carrier, E. Spafford, 2004. "An Event-Based Digital Forensic Investigation Framework" Published 11 August 2004 Computer Science Paper Digital Investigation.

Bureau of Justice Assistant, 2013. Social Media: Article Getting Started, An Introduction to social media

Cambridge Dictionary, 2013. stalker.

Carrier, B. &. G. J., 2004. A Hardware-Based Memory Acquisition Procedure for Digital Investigations.

Casey, E., 2004. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. Academic Press, Inc.6277 Sea Harbor Drive Orlando, FL United States ISBN:978-0-12-374268-1 London, Academic Press.

Cross domain, 2015. Cybercrime. Paper cybercrime cross domain solution

Csweb Inc, 2007. Hash Function. https://cseweb.ucsd.edu/~mihir/cse207/w-hash.pdfCVE, 2013. MS13-071 - Important: Vulnerability in Windows Theme File Could Allow Remote Code Execution (2864063) - Microsoft Security Bulletin MS13-071

Davis, M., Bodmer, S. & Lemasters, A., 2010. Hacking Exposed Malware & Rootkits. s.l.:McGraw Hill.

Dewing, M., 2012. Social Media: An Introduction, Ottawa: Library of Parliament Canada Parliamentary Information and Research Service.

Corresponding author: Bass, H. ✉ bassi.haruna1@gmail.com ✉ Computer Science Department, Kaduna State University, Kaduna. *© 2022. Faculty of Technology Education. ATBU Bauchi. All rights reserved*

Govil, J. & Jivika, G. G., 2007. Ramifications of Cyber Crime and Suggestive Preventive Measures. IEEE International Conference on Electro/Information Technology Michigan, IEEE.

Gunjan, V. K., Kumar, A. & Avdhanam, S., 2013. A Survey of Cyber Crime in India, New Delhi: IEEE.

Henry C. Lee and Elaine M. Pagliaro 2013 "Forensic Evidence and Crime Scene Investigation". J Forensic Investigation, September 2013 Vol.:1, Issue:2.

Jose Antonio Vargas, Sep 20, 2010, "The Face of Facebook" profile of Mark Zuckerberg Zuckerberg founding Facebook. *Journal of Digital Investigations.*

Matt Richardson 2013, "Getting Started with BeagleBone: Linux-Powered Electronic Projects With Python and JavaScript (1st Edition)" (9/18/13) on Amazon.com.

Shams Zawoad, Ragib Hasan 2015. "Towards Building a Forensics Aware Eco System for the Internet of Things" Conference: 12th IEEE International Conference on Services Computing (SCC), I o T security. DOI:10.1109/SCC.2015.46

Van Tassel J. 2006 Digital right management: Protecting and monitoring content, Burlington, MA and Oxford Focal Press.

Wendy Craig, Meyran Boniel-Nissim, Nathan King, Sophie Walsh, 2020 "Social Media Use and Cyber-Bullying: A Cross-National Analysis of Young People in 42 Countries" May 2020, Journal of Adolescent Health 66(6): S100-S108. DOI:10.1016/j.jadohealth.2020.03.006

Yuri Gubanov 2013, Retrieving Digital Evidence: Methods, Techniques and Issues, 2012-2013 by Forensic Focus for digital forensic and e-learning forensic. yug@belkasoft.com

Corresponding author: Bass, H. ✉ bassi.haruna1@gmail.com ✉ Computer Science Department, Kaduna State University, Kaduna. *© 2022. Faculty of Technology Education. ATBU Bauchi. All rights reserved*