Scope International Journal of Science, Humanities, Management and Technology. ISSN : 2455-068X

Vol.3 Issue 4 (2017) 157 - 161. Submitted 25/11/2017. Published 30/12/2017

Cyber And Network security

[1]R. Ganeshan, Assistant Professor, Dept of CSE, St. Joseph College of Engineering Sriperumbudur.

[2]Dr. Paul Rodrigues, Professor, Dept of CSE, Indra Gandhi College of Engineering and Technology. Chengalpattu.

Abstract:

Cybercrime has become more popular in the World of internet. The paper here will outline more on cyber and network forensics. There is lot of crime related cases nowadays that needs digital or electronic proof as a form of evidence. For evidence to be presented, certain procedures need to be followed from the collection of data to keeping it safe for the evidence time in a particular case. This paper shall try summarizes information relevant to security and cyber Forensics in general and how those cases are solved.

Keywords: Cyber, Forensics, Digital.

1. INTRODUCTION

We are living in a world of technology where computers are being used every day from personal use, social interaction to business wise. Most storage medium of information relies on electronic devices like hard disks and flash, as well as cloud storage. Also the trending of smartphone usage nowadays also increases the risk of cybercrime as most transactions and communication online is done over smartphones. That poses vulnerabilities to attackers online to steal information such passwords, credit and bank credentials, etc. The paper will then highlight basics associated with computer and network security. Also information beneficial to prosecutors as well as Law enforcement on the guidelines and procedures for making use of digital evidence as well as obtaining it. Also to ensure the collected evidence information is made admissible to be used in court. The paper will generalize on the world of forensics and how it all works. Both authors state computer security as about confidentiality and protection of information from exposure to unauthorized entities. One author mentioned it as related to the protection of information from damage to both hardware and software as together with services disruption Crimes commonly associated with cyber include credit card information, money theft, and industrial espionage. And many institutions like government and private are finding ways to prevent such attacks Also according to another researcher, 80% of US Companies has suffered these cyber- attacks las year and most of attack done via emails. Hundreds and hundreds of consumers have been victims of credit card number, email addresses and other personal information attack from online intruders. Research showed around $445 billion costs were exceeded each Method used for these studies or investigations were conducted via survey done from different writers under forensics. The study demonstrations were compiled from a collective of different authors‟‟ information. Existing papers and articles on the forensic topic made the research a success.

2. RELATED WORK

Forensics is termed as scientific methods or applications in association with the judicial system or court of laws. The purpose behind these methods is to unveil the digital evidence to be used in court for solving crime cases. This kind of technology wasn‟‟t practiced before therefore most criminals tend to get away with their criminal acts without valid proof to incriminate or prosecute them. During that time the oaths, confessions, testimonies from witnesses were the only determining factors of evidence Now with the

enhancement in the technological world forensics has brought new and advanced methods in a digital format for the investigation part. There are procedures and principals to be followed for performing or undertaking such crime investigations. Those include usage of certain measures like blood DNA printing, palm printing, foot prints and finger prints It is all about provision of digital evidence usually retrieved from digital devices like hard disks, cameras.

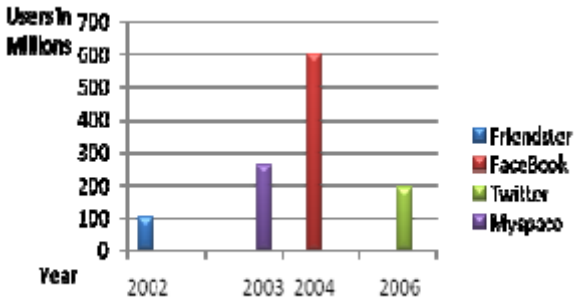

Fig.1.Social Network Analysis

Set of analysis techniques are used to achieve this by gathering data to be used as evidence. Each process done need to be documented until final report is produced. This starting from the onset which is crime scene until last stage. And the powerful ability behind computer forensics is that even damaged, deleted or lost data from devices can still be recovered. here comes the second step after acquisition step. Collected information from crime scene is then going to be analyzed for it to be able to be used as evidence. It also entails the use of methodologies and procedures that are even capable of retrieving the damaged/destroyed or deleted data from a device. The results here can be presented in either hardware or a soft copy format. those involve the violation of corporate polices commission of crime. This could be unlawful accessing of certain things like websites, also sabotage within an organization, etc. Unlike cyber forensics, network forensics mainly deals with the capturing of data, storing it as well as performing filtration analysis on data packets. For security purposes e ach packet of data passing is recorded. All form of communication on the web from email systems, web browsing to database queries. Capturing is done through usage of finger prints in post attack analysis. With network forensic it is possible to analyze how attack happened and the actual person who did it as well as the duration of the incident. Therefore network forensic is regarded as the powerful tool when it comes to network analysis.

3. PROPOSED SYSTEM

The interest of social networking web sites has been increased and many research papers have been published. Some of them discussed the security issues of social networking, analyzing the privacy and the risks that threat the online social networking web sites. The article [7] identifies the security behavior and attitudes for social network users from different demography groups and assess how these behaviors map against privacy vulnerabilities inherent in social networking applications. In the article [8], the researcher highlights the commercial and social benefits of safe and well- informed use of social networking web sites. It emphasizes the most important threats of the users and illustrates the fundamental factors behind those threats. Moreover, it presents the policy and technical recommendations to improve privacy and security without compromising the benefits of the information sharing through social networking web sites. author addresses security issues, network and security managers, which often turn to network policy management

services such as firewall, intrusion, perfusion system, antivirus and data lose. It addresses security, framework to protect corporation information against the threats related to social networking web sites.

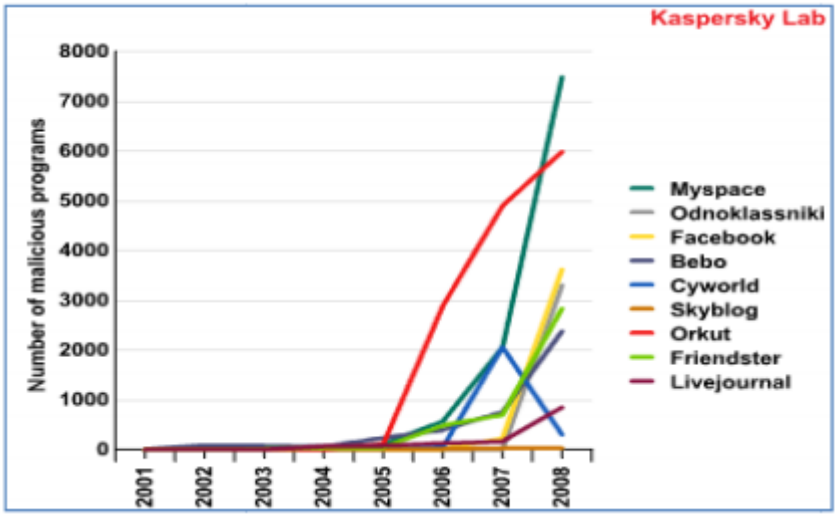

Fig.2.Data base on networks

Also many other scientific research papers have been published where the new technology and strategies were discussed related to the privacy and security issues of social networking websites. Generally, there are two types of security issues: One is the security of people. Another is the security of the computers people use and data they store in their systems. Since social networks have enormous numbers of users and store enormous amount of data, they are natural targets spammers, phishing and malicious attacks. Moreover, online social attacks include identity theft, defamation, stalking, injures to personal dignity and cyber bulling. Hackers create false profiles and mimic personalities or brands, or to slander a known individual within a network of friends.

4. ANALYSIS

Nowadays, millions of internet users regularly visit thousands of social website to keep linking with their friends, share their thoughts, photos, videos and discuss even about their daily-life. Social networks can be traced back to the first email which was sent in 1971 where two computers were sitting right next to each other. In 1987 Bulletin Board System exchanged data over phone lines with other users and lately in the same year the first copies of early web browsers were distributed through Usenet. Geocities was the first social website founded in 1994. Theglobe.com launched in 1995 and gave people the ability of interacting with others, personalize and publish their files on the Internet. In 1997, the America on Line (AOL) Instant Messenger was lunched. Unlike cyber forensics, network forensics mainly deals with the capturing of data, storing it as well as performing filtration analysis on data packets. For security purposes e ach packet of data passing is recorded. All form of communication on the web from email systems, web browsing to database queries. Capturing is done through usage of finger prints in post attack analysis.

With network forensic it is possible to analyze how attack happened and the actual person who did it as well as the duration of the incident. Therefore network forensic is regarded as the powerful tool when it comes to network analysis communication from storage mediums to online charts (via network) as well as cloud storage, email systems should be kept as secure as possible.

Having knowledge about forensics also helps knowing that it doesn"t only applies to crime investigations but also to other matters like social ones. That could be family disputes investigations, work place disputes, transport or even fire incidents.

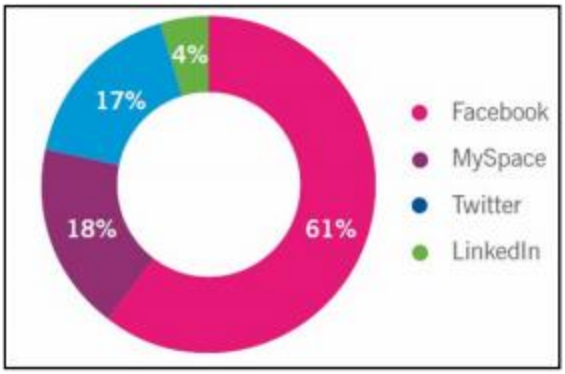

Fig.3.Analysis

And finally when it comes to choice of best forensic tools, with that forensic background knowledge this will allow or help you make the right choice that could actually benefit you. Choosing best techniques and tools would lead to successful resolving of a case even though challenges are always there, those that could be from technological compatibility and limitations.

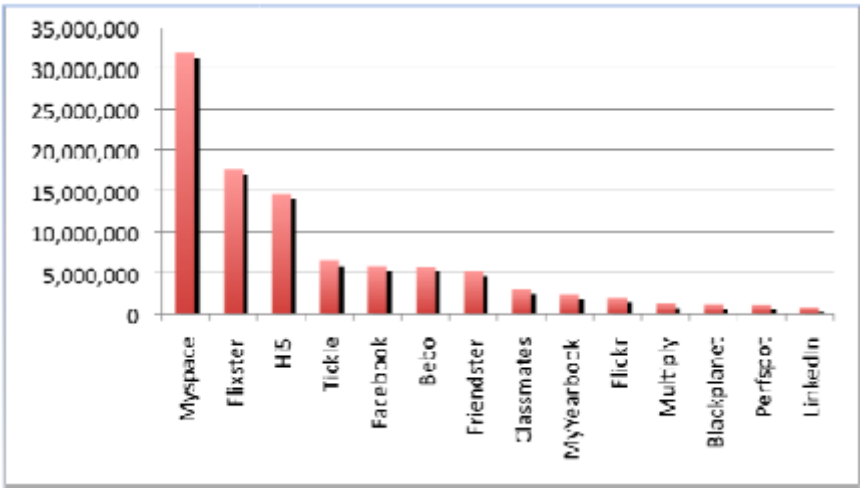

Fig.4.Output data

here comes the second step after acquisition step. Collected information from crime scene is then going to be analyzed for it to be able to be used as evidence. It also entails the use of methodologies and procedures that are even capable of retrieving the damaged/destroyed or deleted data from a device. The results here can be presented in either hardware or a soft copy format.

CONCLUSION

And finally when it comes to choice of best forensic tools, with that forensic background knowledge this will allow or help you make the right choice that could actually benefit you. Choosing best techniques and tools would lead to successful resolving of a case even though challenges are always there, those that could

be from technological compatibility and limitations. Having knowledge about forensics also helps knowing that it doesn‟t only applies to crime investigations but also to other matters like social ones. That could be family disputes investigations, work place disputes, transport or even fire incidents.

REFERENCES

[1] Katie Macdonald, „Why is Home Network Security Important", Digicert, 1.801.701.9600, 22 September, 2015

[2] Jager et al., "Network Security assessment-An Important Task in Distribution Systems with dispersed generation", 22 September 2009

[3] Marilyn Miller, "Crime Scene Investigation Laboratory Manual", Elsevier, 28 January 2014

[4] Yizhen Huang et al., "Learning from Interpolated images using neural networks for digital forensics, IEEE, 2010

[5] Binti et al., "Digital Forensics & CyberSecurity",IEEE,11.1109/WorldCIS.20 15.7359428, 2015

[6] Jones et al., "Information Security and Digital Forensics in the World of Cyber Physical Systems", IEEE, 10.1109/ICDIM.2016.782979526 January 2017

[7] Choi et al.2016, "Introduction to a Network Forensics Systems for Cyber IncidentsAnalysis",IEEE,10.1109/ICACT.2 016.7423270, 03 March 2016.