Journal of Advances and Scholarly Researches in Allied Education
Vol. 16, Issue No. 2, February-2019, ISSN 2230-7540

Case Study on Cyber Crime by Performing Forensic Examination on Social Networking Sites

Dr. Rakesh Kumar Ray*

Assistant Professor, Department of Forensic Science, Swami Vivekananda University, Sagar, MP

Abstract* – Crimes in this digital world are of various sorts and the one among is Cyber-crime. As everything is digitized, there is fast increment being used of internet and in the meantime increasingly number of cyber-crimes happens that raised by the aggressors. A portion of the cyber-assaults are hacking, banking frauds, and email spamming and so forth. So as to research these fraudulent exercises, the examination organizations (requirement law) should utilize innovation which is a critical part Also the Mobile gadgets are progressively used to get to social media and texting services, which enable users to speak with others effectively and rapidly. In any case, the abuse of social media and texting services encouraged directing various cybercrimes, for example, cyber stalking, cyber bullying, slander spreading and sexual harassment. In this manner, cell phones are a significant evidentiary piece in digital examination. The principle point of this paper is to display an overview of the developing cybercrime issue and surveys the burdens of over employments of social networking sites. This paper additionally classes a few kinds of cybercrimes that may cause exploitation by these social networking sites. It incorporates few case studies indicating how the individual data is stolen if somebody's profile is as of now enrolled on any social networking sites for either monetary addition or antihuman exercises like illegal tax avoidance and terrorist action separately.

***Keywords:* Cybercrime, Social Networking, Decryption; Cracker; Hackers, Social Media, User, Forensic Examination, Case Study**

---------------------------------x---------------------------------

1. INTRODUCTION

The rapidly growth of social media and texting applications encouraged advancement of numerous genuine cybercrime and malicious exercises. Cybercriminals are continually changing their techniques to target quickly developing social media and texting users. The abuse of social media and texting in cell phones may permit cybercriminals to use these services for malicious purposes, for example, spreading malicious codes, getting and scattering classified data and so on. Numerous social media and texting suppliers have stretched out their services to portable stages which decline the circumstance as users are in danger of losing significantly progressively private data. Copyright encroachment, cyber stalking, cyber bullying, slander spreading and sexual harassment are getting to be not kidding dangers to social media and texting portable users. Hence, it isn't unexpected to defy with various sorts of cell phones during assortment of forensics examination cases. Cell phones are presently a significant wellspring of forensic remainders applicable to user's social media and texting exercises. Notwithstanding, distinction between cell phones command forensics examiners to create modified strategies and methods for examination of various phones.

The ancestor of the present internet ARPANET was structured as a correspondence framework that would enable analysts to get to data from different computers around the nation, along these lines enabling data to flow all the more uninhibitedly. Later this extended over the breaking points and came to every single point on glob and now daily's computer and the internet have progressed toward becoming interwoven into our day by day lives. The utilization of the internet is exceptionally fundamental since they can assemble and impart data to different people just as the diminishing expense and size of computers regardless of where people are situated on the globe. Subsequently, encourages business at domestic to worldwide dimension. Nonetheless, this new innovation has carried with it much headway which makes our lives simpler however sadly it has likewise prompted progressions in crime.

Figure 1: Forensic Investigation of Cyber Crime

The all-inescapable role of internet and computers and the systems can be checked from the look of a paper on some random day, on the lives of the residents, organizations and governments world over. Number of lottery tricks, fake profiles on social networking websites and, wholesale fraud for fake banking transactions and so on., have progressed toward becoming updates on day by day schedule and, are influencing expanding number of conventional natives. Business enterprises are getting to be focuses of frauds by insiders, business espionage and, intellectual property robberies making huge harms notorieties of the organizations and, possibly gigantic money related misfortunes. At last, the dangers of cyber fear-based oppression and, espionage are nearer to reality than were whenever before. The Wiki spills scene of distributing of the characterized discretionary communications in public space is a pointer to the things to come in future. At last, Governments and regimes are being ousted, through the sheer intensity of internet and social networks, as a stirring power. While a portion of these demonstrations may not be delegated Cyber Crimes all around, as Law Enforcement Officers, it winds up important to comprehend and research the occurrences as and when revealed. During the exchange all through this manual, the word 'Cyber Crime(s)' is utilized and would mean equivalent to a Computer Crime and additionally Digital Crime for convenience, except if expressly expressed.

- **Cyber Crime**

Cybercrime has an extensive definition that incorporates any crime directed by means of the Internet, network or digital device. Catching digital proof, for example, that found on phones, GPS devices, computers, tablets and network servers, is pivotal to examining and solving cybercrimes. Cybercrime is just a sub-set of regular crime where ICTs are utilized as a vehicle or apparatus to carry out customary criminal offenses. This definition holds fast to the basics of legitimate understanding connected to traditional criminal offending. Legislators ought to be careful to abstain from making 'sui generis' lawful classifications of cybercrime offenses by fitting laws to meet changes in technology.

The semantics of 'cybercrime' point to a legitimate and specialized wonder that banishes crime associated with the cyber area. Such movement is completely unique to conduct considered 'deceptive' or 'illegal' which does not in itself add up to 'criminal conduct'. The creator declares that criminal equity procedures should possibly be locked in when a course of conduct is resolved to be genuinely criminal and warrants indictment. Key to most lawful frameworks is the guideline of 'nullum crimen sine lege', which means regardless of how destructive the conduct, it can't be arraigned except if it is officially denied by law.

Types of cybercrime

- **Crimes targeting computer systems**

√ Hacking

√ Denial of Service (DoS) attack or Distributed Denial-of-Service (DDoS) attack

√ Spreading viruses and malware

√ Website defacement

√ Cyber terrorism

√ Spoofing

√ Skimming

√ Pharming

√ Spamming

- **Crimes in which computer systems are used as tools/instruments**

√ Financial fraud

√ Data modification

√ Identity theft and its misuse

√ Cyber bullying/Stalking

√ Data theft

√ Pornography

√ Theft of trade secrets and intellectual property

√ Espionage on protected systems

- **Social Networking**

A social networking service is a stage to assemble social networks or social connection among individuals who, for instance, share interests, exercises, backgrounds, or genuine connections. Network service comprises of a portrayal of every user that is called profile, his/her social connections, and an assortment of extra services. Social networking sites enable users to share thoughts, pictures, posts, exercises, events, and interests with individuals in their network. Some social networking sites are Facebook, Twitter, Gmail, yahoo, Indyarocks, Orkut and so forth.

- **Social Networking based Application: An Alert**

The applications utilized by the smart phone users like whatsapp, line, viber, we visit, genuine guest and so forth are additionally exceptionally dangerous since the organization of that server can without much of a stretch locate the careful area of any contact number present in the phone of the user of any such application.

Computer/Cyber forensics is a rising practice to find proof from digital devices, and indict criminals in a courtroom. The expression "Computer Forensics" was begat in 1991 in the main training session held by the International Association of Computer analytical Specialists (IACIS) in Portland, Oregon, USA. Like customary forensics, Computer forensics is a science, and utilizations specialized skills, tools and programs.

A few examples of cybercrime are: monetary burglary through e-banking, erotic entertainment, information taking, information control, hacking, splitting and so forth. The motivation behind this paper is to investigate territories identified with cybercrime which may happen through social networking sites and to survey criminological speculations that have been connected to the study of cases of cybercrime and furthermore proposed a few apparatuses and strategies to shield ourselves from these dangers. The hacker and crackers are the people who get access into a framework or into a network with no approval. Essentially utilized systems by the con artists include observation in other word one can say foot printing (gathering information about the focused-on individual is called foot printing). It includes three systems dumpster diving in this procedure trickster uses to experience the injured individual's garbage and attempts to assemble valuable information about the person in question. The second system is social engineering it is a specialty of persuading individuals to reveal sensitive information. The third is shoulder surfing it is a strategy where assailant spies over the injured individual's shoulder and attempt to take sensitive information of the unfortunate casualty which is shown on the screen of the person in question.

2. LITERATURE REVIEW

Nishesh Sharma (2017) - Cyber forensic proof gathered in one nation isn't allowable in foreign courts. Government policies and cyber laws from various areas should try endeavors to determine clashes and issues emerging due to multi-jurisdiction examinations. There is a necessity for training of examination agencies and judicial members. There exists a need to create examination methods like Cyber Forensic Examinations to gather digital proof and to correct Indian Cyber laws to coordinate the speed of technological progress.

Vicky Nanjappa, (2012) - according to the information of National Crime Record Bureau, given during recent years, the enlisted cases under IT Act are 3682 and the conviction rate is 7% for example the enrolled cases are expanding and the conviction rate is declining. The expansion in announced cases is multiple times. As indicated by Advocate Pawan Duggal, a cyber-crime master and senior promoter of Supreme Court, more often than not electronic proof is neither caught in the correct manner nor is it held and saved in the way required to be valuable in law.

Urvashi Sharma Mishra (2018) - Utilization of computers in the space of law is later and kept to the surface dimensions as it were. Be that as it may, the new methods and kinds of crimes, known as cyber-crimes heading off to the extraordinary dimensions of terrorism through the channels of financial offenses at both national and universal dimensions demonstrate the current interface of law and cyber forensics deficient and slacking both in principle just as by and by. Such regions might be of crime examination and preliminary in the official courtrooms, along these lines making humble advances in this field as enactment of Information Technology Act and revisions in this law just as in the Code of Criminal Procedure and Indian Evidence demonstrating to be to a great extent deficient and lacking to deliver to the present needs. Such needs are accomplishing over 80% feelings like in the created world, logical examinations and confirmation of proof in the courts through cyber forensics methods and technology. For the reason, the co-activity of law and cyber forensics must turn out to be extremely close to be coupled together appearing to one order.

3. DATA ANALYSIS AND RESULT

♦ **Case study: 1**

An officer of a steel plant named Akash shrivastava of Jabalpur was browsing on his PC in his office a popup of 'Facebook notification' came. He enthusiastically tapped on that connect to join the visit or see the new post in his profile yet he found that it is a promotion of another social networking site he declined it and went to break room to take his lunch. When he returned, he found that his everything arrangements and all information identified with organization working and marketing strategies are erased and, thusly, he was in loss of Rs 5, 00,000.

While examination it is discovered that the popup of 'Facebook talk' was containing a contaminated connection that have a fix record covered up in it of a software considered net transport through which the representative of a similar organization affronted this crime, with the assistance of this software he hacked his manager's computer and carried out this crime

Variables of this case: fake link 'facebook', netbus tool.

In this case the enthusiasm of Mr. Akash Shrivastava in facebook which is a social networking site made him an unfortunate casualty, thus numerous social networking sites and their fake pages with popup are accessible on internet which may supportive to the crackers or hackers.

"Know from subordinates and friends in financial issue."

♦ Case study: 2

A businessperson actuated internet banking for him, after some days he found that all his record balance Rs. 7,50,000 has been moved to a record through internet banking.

After the examination guilty party admitted his offense when showed up in the court and advised to the court that he was really a companion of the victim. One day the victim's house cleaner was dumping some paper pieces at dump yard through dumpster diving he found an envelope having information in regards to the affirmation of enactment of internet banking likewise notice that the new user ID and secret phrase has been sent to your enlisted email account. That envelope was stolen by the charged. Through shoulder surfing he saw that the victim uses to spare his everything ID and passwords in his drama program. In his first endeavour to get the ID and secret key he found that the victim's workstation was ensured with a secret phrase and a clue proclamation for that secret word, which was "include jay after your senior sibling's closest companion's name". Here he had exploited social networking site called facebook; initially, he opened victim's profile then he gone to his senior sibling's profile where he checked the rundown of dear companions and found just one name 'Surya'. He endeavoured commonly with various secret word like 'Suryajay, Surajjay, Prabhakarjay and so forth." finally he got the secret key as Sunjay from that point he had stolen the mail id password word and from that point he moved cash by login in internet banking site of the bank and moved all the cash to another record.

Variables of this case: Dumpster diving, shoulder surfing, Facebook profiles, Hit and trial method.

As in above case social networking sites are additionally useful to assemble sensitive information like phone no., address, photographs, companions and so forth particularly when victim is a female.

♦ Case study 3

One day an MMS went to a girl to be specific Divya Kapoor, containing her vulgar photo pursued by a SMS inside a moment. The charged was blackmailing the girl for money in lieu of publically showing the photo through web.

The exploring group found that the photograph was altered by utilizing tool trick photography and the photo of that girl was downloaded from her unsecured face book profile.

Variables of this case: Facebook profile, Photo editor software, Mobile phone.

In this manner, uploading her photo on the internet particularly in social networking sites made her victim.

4. CONCLUSION

With cybercrimes (i.e., any criminal demonstration managing computers and networks) on the ascent and undermining authoritative information, just as the expanded utilization of digital devises by the overall public, the examination of digital proof turns into an essential component at numerous crime scenes. From the above dialog unmistakably the social network services are implied useful for society yet regularly these are dangerous if not verified. Particularly the adolescence and young ones should mindful of the disadvantages of the much of the time employments of social networking sites and ought to dependably be cautious and verified in case of their confidential information. With the help of certain instruments, software and a few systems like encryption decryption component, utilization of an Antivirus, Antitrozen pony, and net specialty apparatus bar for program which counter strikes the phishing assaults, in cyber cafes check for the key loggers, check the network protocol composed before the URL and so forth. One should avoid potential risk in utilizing phone application uncommonly VVIPs Intellectual brains which might be followed by GPS framework by the servers and furthermore prevent these people structure hostile to social or against terrorist activities.

In that capacity, there is a need to examine the current legitimate regime identifying with use and acceptability of cyber forensics in crime examination and trial. For the reason, different devices and procedures utilized for plate and device forensics ought to be broke down. These apparatuses and methods can be made progressively valuable in criminal examination and preliminary. The examination of the arrangements of law where under these Cyber Forensic apparatuses can be utilized by the examination agencies and the courts in law authorization ought to likewise be finished.

Cybercrime research will be a significant zone of study for future criminologist as we move more remote into the digital age, who knows, there might be multi day in the far future when the quantity of cybercrimes carried out exceeds the quantity of conventional crimes perpetrated.

5. REFERENCES

1. Tiwari R.K., Sastry P.K., Ravi Kumar K.V. (2002). Computer crime and computer forensics 1: pp. 89-97, pp. 113-116.

2. Dernadette S.H. & Clemens M. (2004). Cybercrime (A reference handbook) 1: pp. 247.

3. Stephension P. (1999). Investigating Computer related crime. CRC press, BocaRaton London, Newyork, Washington DC. pp. 82-83.

4. Singh Y.K. (2005). Cybercrime and law. Shree publisher and distributers 1: pp. 1-2, pp. 8-9, 28.

5. Mishra R.C. (2005). Cybercrime impact in the new millenniums. Authors press 1: pp. 1-2, 57, 29.

6. Khanuja H.K. & Adane D.S. (2012). A framework for database forensic analysis. Computer Science & Engineering. 2012 Jun 1;2(3): pp. 27.

7. Vicky Nanjappa: ‘Cyber Crime – 1600 arrested, only 7 convicted’, Rediff Business News, http://www.rediff.com/money/report/tech-cyber-crime-1600-arrested-only-7-convicted/20121211.htm

8. Ashish (2015, February 27). *Carving out the Difference between Computer Forensics and E-Discovery*. Retrieved from http://articles.forensicfocus.com/2015/02/27/difference-between-computer-forensics-and-e-discovery/

9. S Mahaboob Hussain, Prathyusha Kanakam, A.S.N. Chakravarthy (2017). "Inhibiting Cognitive Bias in Forensic Investigation Using DNA Smart Card with IOT", International Journal of Control Theory and Applications 10 (14), pp. 251-255.

10. Barbara, J. (2015, February 17). *Streamlining the Digital Forensic Workflow: Part 3*. Retrieved from http://www.forensicmag.com/articles/2015/02/streamlining-digital-forensic-workflow-part-3

11. Nishesh Sharma (2017). ‘Cyber Forensics in India – A Legal perspective’, Universal Law Publishing

12. Urvashi Sharma Mishra (2018). “Application of Cyber Forensics in Crime Investigation”, [Volume 5, Issue 3, July – Sept 2018] e-ISSN 2348 –1269, Print ISSN 2349-5138

Corresponding Author

Dr. Rakesh Kumar Ray*

Assistant Professor, Department of Forensic Science, Swami Vivekananda University, Sagar, MP