SUPREMO AMICUS

VOLUME 15 ISSN 2456-9704

CYBER FORENSICS: TRACING DIGITAL FOOTPRINTS TO UNTANGLE CYBER-CRIMES

By Vartika Prasad and Aditi Sharan
From Amity University, Noida

Abstract

Cyber forensics is the application of technological knowledge to resolve legal issues. It involves the investigation, analysis, authentication and recovery of digital evidence from a digital device or medium used to commit a crime.

With the advancement in technology, things have become more convenient with quick and easy digital access. However at the same time, cyber-crime has increased exponentially and has become a threat to society which needs to be resolved. The legislations such as the IT act, 2000 and the Indian Evidence Act, 1872 has codified laws which penalises any offender involved in cyber-crime, but the constant advancement in technology and the cunning yet intelligent brains of the offenders sometimes paves a way out.

Nevertheless, a criminal leaves footprints after commission of a crime. A cyber forensic expert is the one who traces the digital foot-prints left behind and further digs into the root of the crime committed in the cyber-space.

This research paper will cast light upon the techno-legal aspect of cyber forensics; steps involved in investigation into cyber-crime; pre-eminent role of cyber forensic experts and cyber forensic analysis tools, with an emphasis on email tracer, a cyber analysis tool, which helps track down an offender in the cyber space and other cyber-crimes related thereto. Further, the concept of email forensics will be discussed, which is an offshoot of cyber forensic in itself.

- Keywords: Cyber forensics; cyber-crime; techno-legal; digital footprints; cyber forensic expert; email tracer; email forensics

- **Research methodology:**

➢ **Primary sources: Interview; relevant statutes; Judgements; Newspaper articles**

➢ **Secondary sources: Books; Internet**

Introduction

In this 21st century of fast-paced technological advancement we might leave electronic traces behind while using the internet. Whatever someone does online they leave behind digital footprints that can easily reveal who they are, what they did, and when they did it. Therefore , as we live more and more of our lives online cyber forensics becomes more critical than ever to keep us safe because as technology becomes more advanced so do the criminal activities.

Cyber Forensics is a field that merges the elements of computer science and law to analyse and realize digital evidence from computer systems, computer networks, wireless communications and storage devices in a way that is acceptable in the court of law. It can be referred as the science of locating, collecting, protecting, analysing and reporting of digital evidence from electronic devices like computer systems, hard disk, mobile phones etc. that is used to commit a crime.

A cyber forensic expert can discover data in different ways that reside in a digital device that has been used to commit a cyber-crime. They can recover encrypted, deleted and damaged file Information using the appropriate tools and techniques. The recovered data is then used in solving the crime and plays an important role in litigation process. After the discovery of hidden files and recovery of deleted files an overall analysis containing an overview of the computer system displaying every conspicuous pattern is created by the forensic experts. The forensic expert then assists in investigation or litigation as a consultant.

In short, Cyber or Computer forensics is concerned with obtaining the proof of a cyber-crime or breach of policy in such a way that could lead to the prosecution of the criminal.

The Information Technology act, 2000 acts as the supreme legislation regulating cyber laws of India. The motto behind enacting the act was to facilitate and acknowledge e-commerce and to penalise the offenders who committed cyber-crimes. However with the boom in technology, cyber related crimes increased and a need was felt to amend the law, and with that, the information technology amendment act,2008, was passed by the parliament, so as to provide legal remedy to curb cyber-crimes. Further, the provisions of the Indian Penal code, 1860, Indian evidence act,1872, etc., were also amended, so as to make it pliant with technology[1] and support the admissibility of 'electronic documents/records' as digital or electronic evidence in court.

Section 2(1) (t) of the Information Technology Act, 2000 defines "electronic record" as, means "data record or data generated, image or sound stored, received or sent in an electronic form or micro-film or computer generated micro-fiche".

Further, According to Wikipedia, "an Electronic evidence is any probative information stored or transmitted in a digital form"[2], which is admissible in court and serves as proof against offenders in the cyber-space.

Cyber-Crimes and its Legal Implications :

Cyber-crimes have increased exponentially with the passage of time. With the wake in technology, the criminal minds have become sharp and cunning with several crimes being committed on the digital platform. Although, the technology is fast driven than the law, nevertheless, law finds the key to unlock such crimes and further prevent them.

The information technology act, with its 2008 amendment lays down almost every sort of cyber-crime and prevention from such crimes in term of punishments in its chapter XI.

1. Denial of Access:

DOS attack is used to make the online services unavailable to the user by flooding it with traffic from a variety of sources. Organizations such as commerce, banking, media, government and trade organizations are often targeted.

Legal implications:

[1] Wikipedia, The free encyclopaedia. Information Technology Act, 2000. Available from: https://en.wikipedia.org/wiki/Information_Technology_Act,_2000

[2] Wikipedia, The free encyclopaedia. Digital forensics. Available from: https://en.wikipedia.org/wiki/Digital_forensics

Section 43(e), 43(f) and 43(g) r/w section 66 of the IT act, 2000 lays down provision w.r.t., dos attack.[3] Section 65 of the IT act also punishes for tampering with computer source document.[4]

If a person without the consent of the owner or the in-charge of the computer system, disrupts or causes disruption of any computer, computer system or computer network[5] ; or denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means[6] ; or provides any assistance to any person to facilitate access to a computer , computer system or computer network , then he/she shall be held liable to be imprisoned for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.[7]

2. **Hacking:**

It usually refers to unauthorized intrusion into a computer or a network. A skilled programmer who performs hacking is known as a hacker. Hacking is done to alter systems. This hacker may alter the system or change the security features to commit fraudulent activities such as stealing personal/professional data, identify theft, Privacy invasion etc.

Legal implications:

The term hacking had a place under the IT act, 2000, pre 2008's amendment[8] . Hacking as under section 43 and 66 of the IT act[9] was removed after the amendment, so as to secure the interest of ethical and legal hacking done by experts in good faith. It drew a distinction between ethical hacking and malicious hacking, where malicious hacking is specifically known as cracking in layman's term.[10] Although, the IT act, 2000 does not cover the term hacking, it does lays down provision for unauthorised and malicious cracking/hacking under sections 43 and 66 of the act.

Section 43 r/w section 66 of the IT Act, 2000, applies to this particular offence.

Further, section 66 acts as an extension to section 43 of the act by stating that, "If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both ".[11]

Section 378 r/w 379 i.e., Theft and **405 r/w 406 i.e., criminal breach of trust,** of the Indian Penal Code, 1860 is also applicable for the offence of illegal hacking/cracking.

3. Identity theft:

It refers to impersonating a person in order to steal important data about that person such as credit card information, banking details etc. Identify thrives can use someone else's name whenever they commit a crime like drug trafficking, money laundering, smuggling or any cyber-crime.

Legal implications:

[3] India Tech Law. January 31, 2017. Denial of Service (DoS) attack and relevant Indian Laws. Access from: https://indiatechlaw.com/security/denial-of-service-dos-attack-relevant-indian-laws/

[4] Justice Yatindra Singh. Fifth edition. Universal law publishing co. Cyber laws. p 25

[5] Section 43(e). IT act, 2000.

[6] Section 43(f). IT act, 2000

[7] Section 43(g). IT act, 2000

[8] Information Technology (Amendment) Act, 2008 (Act No. 10 of 2009).

[9] Information Technology Act, 2000 (Act No. 21 of 2000).

[10] Ipleader. July 1, 2016. Laws Against Hacking In India. available from: https://blog.ipleaders.in/laws-hacking-india/

[11] Section 66. IT act, 2000

According to **section 66C** of the Information Technology Act, 2000, A person who fraudulently or dishonestly, uses **someone else's electronic signature, password or any other unique identification feature**, shall be punished with imprisonment for a term, which may extend to **three years** and shall also be liable to **fine which may extend to one lakh rupees**.

Further, section **378 r/w section 379 i.e., 'theft'**, section **405 r/w section 406, i.e., 'criminal breach of trust'** and **section 420 i.e., 'cheating** and dishonestly inducing delivery of property' under the Indian Penal Code, 1860, is also applicable for the offence.

4. Child Soliciting & Abuse:

A person is below the age of 18 years is regarded as a child. Child soliciting and abuse takes place online by soliciting the children for the purpose of pornography. This type of crime is strictly prohibited by the law. Sometimes files containing illegal images are labelled incorrectly in order to trap individuals into visiting internet sites that they didn't intend to.

Legal implications:

According to section **67B of the IT Act, 2000**,

- Publishing or transmission, creating, facilitating, recording, collecting, seeking, browsing, downloading, advertising, promoting, exchanging or distributing, material **depicting children in obscene, indecent or sexually explicit manner, in an electronic form;**
- Further, **cultivating, enticing or inducing,** children to engage in online relationship with one another for sexually explicit act or in a manner that may offend a reasonable adult on the computer resource, shall be punished on **first conviction** with an **imprisonment of a term which may extend to five years** and with fine which may extend **to ten lakh rupees** and in the event of **second or subsequent conviction**, with an imprisonment, for a term which may extend **to seven years** and also with fine which may extend to **ten lakh rupee.**

In the case of **Raghuraj Singh v. Air Force Bal Bharti School (2001) 76**, filed in the Juvenile Court, Delhi, a class 12th student created a pornographic website with an intention of revenge from classmates and teachers, and listed the names of his 12 schoolmate's girls and teachers in sexually explicit manner. School authorities suspended him and the court charged him under S. 67 of I.T Act, S. 292-294 of IPC and Indecent Representation of Women Act.

5. **Pornography and its legal implications**

The IT act, 2000 lays down stringent provisions, w.r.t **'publishing or transmitting obscene material, punishable with an imprisonment, which may extend to 3 years and fine which may extend to five lakhs rupees on 1st conviction,** whereas on **second or subsequent conviction, the offender shall be liable with a fine and imprisonment which may extend to 10 lakhs rupees and 7 years respectively'**[12] and **'material containing sexually explicit act(s),** punishable with fine and

[12] Section 67. IT act, 2000

imprisonment which may extend to **10 lakh rupees and 5 years** respectively on first conviction and **10 lakh rupees and seven years** on **second or subsequent** conviction.’[13], in electronic form.

Further section 66E of the act[14] ensure, imprisonment which may extend **to three years** or fine not exceeding **two lakh rupees, or both** on the offender who **intentionally captures, publishes or transmits the image of a private area of any person** without his or her consent, violating the privacy of a person.

Section 354C i.e**., voyeurism,** and **section 293**, i.e., Sale, etc., of **obscene objects** to young person as under as under the, Indian penal code, 1860, are also applicable.

‘Voyeurism’ is the watching, capturing, or disseminating of a woman engaging in a private act.[15]

6. Ransomware:

It refers to the malicious use of software that blocks the victims data or threatens to publish the confidential data unless a ransom is paid to the person committing the crime. Ransomware attacks are carried out by injecting a Trojan disguised as a legitimate file which the user is tricked into opening or downloading.

The WannaCry is a ransomware attack that caused chaos across the world by infecting the computers run by windows operating system by encrypting the victim's data. This attack spread automatically through worms, without any participation from the victim's side. To decrypt the files, the attackers demanded a ransom payment of between $300 to $600 in Bitcoins within three days.[16]

Legal implications:

The offence is punishable under the IT act with an imprisonment for a term which may exceed to three years and with fine, under **Section 66A of IT Act, 2000**.

Section **383 r/w section 384** of the Indian Penal code, 1860 is also applicable for the particular offence. (extortion)

6. Email Spoofing and IP address spoofing:

Email spoofing is the process of creating a forged email address and sending emails which appears to have originated from a reliable source. Email spoofing is a very common cyber crime to trick the victims, as the information needed to make a forged email address is very easily available online. Therefore, we should always double check the sender's email address before opening the email or before downloading any data.

While email spoofing revolves around the user, IP spoofing is performed to attack a network. The attacker generally sends a message with a fake or spoofed IP address to the victim to make it look like the message has originated from a reliable source. Thus is done to steal the victim's personal information such as banking details.

Legal implications:

Section 66D of the IT act, 2000, applies in case of email and ip address spoofing.

[13] Section 67A. IT Act, 2000

[14] IT act, 2000

[15] Section 354C. IPC, 1860.

[16] csoonline.com. Josh Fruhlinger. August 30th,2018. What is WannaCry Ransomware, how does it infect and who was responsible? Available from: https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html

Any person, who cheats by personating via any communication device or computer resource cheats by personating, shall be punished with imprisonment, which may extend to three years and shall also be liable to fine which may extend to one lakh rupee.[17] Ipc- 465(2 yrs) or fine, 468(7yrs+fine)

7. Phishing:

Phishing is a cybercrime in which the victims are lured into providing their sensitive information such as banking details, credit card details, passwords etc. by masquerading as a reliable entity in an electronic communication. It's one of the oldest types of cyberattacks and is becoming increasingly sophisticated with time.

Legal implications

The crime of Phishing is no-where defined in the IT act, nevertheless, **Section 66A(c)** covers the offence with an imprisonment of 3 years with fine. Further, **section 420 of** IPC is also applicable.

Cyber Forensic Investigation Process

A cyber forensic investigation is digging into and analysing the digital footprints left behind by the offender. Eoghan Casey, a forensic researcher defines it as 'a number of steps from the original incident alert through to reporting of findings'[18].

The provisions of the code of criminal procedure, provides for the basic structure of investigation into the crime. Cyber-crime investigation, requires both technical and legal skills, nevertheless, it is more technical then legal in nature[19]

The power to investigate a cyber-crime lies with the police, not below the rank of an inspector.[20] Almost every police departments in India have a cyber-crime investigation cell, under whose authority, the cyber forensic experts along with police, untangles cyber-crimes. Such cyber-crime cells are usually equipped with a Cyber Lab having cyber forensic capabilities such cyber forensic analysis tools, forensic servers, portable forensic tools for on-site examination.[21]

There are technically four steps involved in the cyber forensic investigation namely, Search and seizure; Acquisition; Analysis and Reporting.

1. Search and seizure

The search and seizure should be done with compliance to the provisions as established in the code of criminal procedure and IT act, 2000. A police officer, not below the rank of an inspector may enter any public place, and further, search and arrest without warrant.[22]

The cyber forensic expert handles the technical details, while the investigating officer i.e., the police handles the legal formalities on site.

First, the set-up is **labelled and photographed** so as to aid legal and technical process. All the connectors and plugs should be labelled properly so as to ensure easy and accurate re-assembly. Thereafter, the system should be **checked if turned on or on sleeping mode and**

[17] Section 66D. IT act, 2000

[18] Wikipedia, The free encyclopaedia. Digital forensic process. Available from: https://en.wikipedia.org/wiki/Digital_forensic_process

[19] Sodhganga. Chapter IV. Investigation into crime. p. 122. Access from: http://shodhganga.inflibnet.ac.in/bitstream/10603/203654/9/09_chapter%204.pdf

[20] Section 78. IT act, 2000.

[21] Cyber crime cell, Delhi Police. About cyber-crime EOW. Access from: http://www.cybercelldelhi.in/

[22] Section 80. IT act, 2000

thereafter be powered down through operating system and then **unplugged,** so as to **protect** it from **any loss of e-evidence**. After turning off, the device should be disconnected from any **network connections.** Thereafter, the device is be **dismantled into separate components**. Lastly, **seizure of the device**, its software, operating system etc., should be accomplished.[23]

2. Acquisition

Once the device and data is recovered, the **expert images, duplicates, and replicates** it.[24] The duplication is usually done via a write blocking device and is known as acquisition or imaging. The software imaging tools such as TrueBack, EnCase, FTK Imager etc., are used for duplication and further the image is verified using hash function or SHA.[25]

3. Analysis

Analysis involves recovery of e-evidence through different techniques and tools such as Encase, FTK etc., Different types of data such as, chats, images, internet history, email, or documents can be recovered, from within the operating system, depending upon the nature of investigation. Keywords, type of files, deleted spaces etc., gives clues in analysis[26]. Further, conclusions are reached via the recovered data.[27]

4. Reporting

The final step of investigation is the **preparation of report** of the acquired e-evidence and further submitting it to the authority, who prepares a **charge sheet** to be submitted in the court. The forensic expert also acts as an **expert witness** and present and explains the evidence in court.

According to **Section 65-A, the contents of electronic records can be proved and is admissible in accordance with the provisions of Section 65-B (2),** which lays down the requirements to be fulfilled for an electronic evidence to be admissible in the court of law.[28]

<u>Role of Forensic Experts</u>

Forensic experts are able to decrypt the password protected documents and encrypted files used by cyber criminals to make the files unreadable in order to conceal the digital evidence. Experts can retrieve deleted computer files and emails. Downloaded files and website visits can be identified that can be used for further investigation of the crime scene.

[23] Sodhganga. Chapter IV. Investigation into crime. p.116-117. Access from: http://shodhganga.inflibnet.ac.in/bitstream/10603/203654/9/09_chapter%204.pdf also see: http://www.indiancybersecurity.com/downloads/cci/method%20of%20investigation.pdf

[24] Sodhganga. Chapter IV. Investigation into crime. p.121. Access from: http://shodhganga.inflibnet.ac.in/bitstream/10603/203654/9/09_chapter%204.pdf

[25] Wikipedia, The free encyclopaedia. Digital forensic process. Available from: https://en.wikipedia.org/wiki/Digital_forensic_process

[26] Justice Yatindra Singh. Fifth edition. Universal law publishing co. Cyber laws. p 38

[27] Wikipedia, The free encyclopaedia. Digital forensic process. Available from: https://en.wikipedia.org/wiki/Digital_forensic_process

[28] Dr. Avtar Singh. 22nd Edition.Central law publications. Principles of the Law of evidence , p 323.

Roles & responsibilities of a cyber-forensic expert during the forensic investigation are:

1. Protection of the digital device from data corruption, tampering, damage, or any kind of cyber-attacks.
2. The forensic expert ensures that the digital device is not damaged in any way.
3. Discovery of hidden, encrypted, deleted, and password protected data.
4. Data recovery, data analysis and proving a printout of the overall analysis of digital evidence.
5. Providing testimony and acting as an expert consultant to provide information about the corrupted digital system.
6. The forensic expert has vast amount of knowledge about the different type of formats in which the evidence can exists.

Computer Hacking Forensic Investigator

The detection of hacking attacks, extracting electronic evidence to report a crime and carrying out audits to prevent future attacks is known as Computer Hacking Forensic Investigation. CHFI investigators have high level expertise to use a variety of methods for discovering the data residing in a computer system that can be used as digital evidence.

A CHFI certified professional has an expertise in various skills. Some roles & responsibilities of the CHFI are mentioned below [29]

- Performing incidence response, evidence collection, forensics, and digital forensic acquisitions.
- Ensuring that the investigation is handled with confidentiality.
- Identifying the origin of incidence.
- Checking the computer hard disk drives and storage media thoroughly in order to recover data beneficial for the investigation.
- Responsibility of conducting audit trails and evidence integrity mechanisms in order to prevent the data from any sort of modifications by internal or external entities.
- Collecting information from different operating systems such as Windows, Mac and Linux.
- Using forensic technology methods
- Executing anti-forensics detection processes.
  - Identification of data, images and activities required for internal investigations.
  - Being able to recover deleted files and encrypted files.

Computer Forensic Tools

Computer forensic tools(CFT's) are used by forensic experts to conduct the investigation process by collecting data from the computer systems, to analysing the data for obtaining information that may not be immediately obvious and for making a true copy of that data such that it can be used in legal proceedings.

Types of Data:

1. Active Data is the data that we can see with our naked eyes like programs, data files, and files used by the operating system. It is the easiest type of data to discover.

[29] Hackernoon.com. Michael Warne. August 29th , 2018. CHFI-The Ultimate Ticket to Computer Forensics. Available from: https://hackernoon.com/chfi-the-ultimate-ticket-to-computer-forensics-35e1973997ad

2. Archival Data is the data that has been backed up and stored in hard drives, CDs, backup tapes, floppies etc.
3. Latent Data is the data that can be obtained using only specialised tools and software such as deleted or partially overwritten data. It's very hard to obtain latent data as it is very costly and time consuming.[30]

   Some popular computer forensic tools are: [31]

1. EnCase Software

It is a widely used and reliable tool developed by guidance software. It consists of a single software having multiple packages and supports a variety of operating systems. The user can write scripts for automated tasks. It can also perform file signature analysis. It has MD5 message-digest encryption algorithm, a database to crack encrypted files with passwords. It usually supports windows platform but can analyse any other operating system. It has a built-in imager with software Write blocker which allows only read instructions and blocks all the write instructions it helps to prevent the evidence from any kind of modifications by unauthorised entity. Encase provides very good results for disk imaging, volume image and memory and logical files.

2. FTK Imager

Forensic Toolkit or FTK imager provides a data preview and imaging tool that allows to view the discovered information in window explorer. It can examine files and folders on local and network drives, and can also review the content of memory dumps. The software is developed by AccessData. Its is a free tool and occupies around 30mb of memory and also provides support for different file systems. It safely mounts forensic image as a physical device or logically, as a drive. FTK imager can be used to recover deleted files. This tool has built in MD5 calculator ensuring integrity, the deleted files can be searched easily using this tool.

3. Sleuth Kit

The Sleuth kit is a very popular open-source tool that provides a command line interface. It has built-in commands to investigate the disk images. The Sleuth kit examines volumes of data, and allows the content to be accessed manually or automatically. The entire tool is written in C language library. It can be used to investigate Linux, Windows, Mac, Solaris and some other operating systems. It also supports Unicode and ASCII structure. It provides wide access to metadata and file attributes and also provides an extensive investigation of file systems. It also provides additional features such as keyword searching and timeline analysis.

4. DEFT

Digital Evidence & Forensics Toolkit or DEFT contains a bundle of popular free forensic tools including tools for mobile and network forensics, data recovery, and hashing. It is Ubuntu based live operating system along with a collection of several forensic tools. It provides best windows forensic tools. It is very stable and professional and is widely used by police, military etc.

5. Volatility

It is one of the popular tool in memory forensics, it is a fast and comprehensive

[30] newyorkcomputerforensics.com. The Computer Forensics Process. Available from: https://newyorkcomputerforensics.com/computer-forensics-process/

[31] geekflare.com. Chandan Kumar. February 17th,2018. 23 Free Forensic Investigation Tools for IT Security Expert. Available from: https://geekflare.com/forensic-investigation-tools/

open-source tool built in python coding language, it reduces complexity in the whole extraction process while remaining independent of the target system. It can be used to investigate the content of RAM. Malware present in the RAM can be identified by experts using volatility. It is available for different operating systems such as windows, Mac, Linux.

6. CAINE

Computer Aided Investigative Environment or CAINE, is a user friendly way to create reports for your investigations. It contains a variety of useful forensic tools. It executes on an Ubuntu based live CD and consists of a collection of forensic tools. It provides the user with a complete forensic environment that organizes existing software tools as software modules and to provide a friendly graphical interface. It has user friendly interface and tools it has a built in blocker so there's no possibility of accidental damage to evidence. Caine provides an optimized environment which is a good example of resource management. It has the ability to generate and export report so the user gets essential summary of the case.

7. LastActivityView

To know the last user actions and events that occurred on a machine, the LastActivityView is the appropriate tool. The information it uncovers can be easily exported to an HTML file. It is for windows Operating system. It collects information from various sources on a running system and displays a log of actions made by the user and the events occurred in the computer.

8. HxD

It is a user friendly low level hex editor that can be used on a raw disk or main memory. It has a variety of features, including exporting file, file shredding, and splitting of files. It is a free tool it is simple hex editor of disk image and RAM. It is very useful to analyse disk or file systems manually. It can handle file of any size directly provides access to specified address.

9. Mandiant Redline

In order to examine a specific host, Mandiant Redline will do that by collecting a huge amount of information on running processes, drivers, file systems, meta-data, event logs, and many other elements. It is a free tool that provides host investigative capabilities to users to find malicious activities by memory and file analysis. Using it we can analyse the process that was running on the system when the memory image was a acquired. It shows full details about the process such as the process id, path arguments and user names.

10. PlainSight

It is a live CD that allows to perform forensic tasks such as gathering data on USB device usage, accessing internet histories, hashes, extracting password and many more. It has a comprehensive forensic environment with powerful open source tools which allow the investigator to grab vital information from the target system. It also provides essential information about the storage devices.[32]

<u>A Peek into Email Forensics and Email Tracer, A Cyber-Forensic Analysis Tool</u>

The study of the source of electronic mail as evidence is Email forensics which helps identifying and process the actual sender and

[32] www.hackread.com. Maria Thomas. July 4th, 2018. Top 7 Most Popular and Best Cyber Forensics Tools. Available from: https://www.hackread.com/top-7-cyber-forensic-tools/

recipient of a message, the date, time and location of the email.[33]

Email spoofing is quite a common cyber-crime, in which the sender sends emails to its victims using fake email address. Email Tracing is method can be used to deal with such crimes. Tracing is performed to get information about actual sender of an email. It shows the path traced by mail It works by analysing the email header which is a part of the sender's email address. After analysing the email header it gives the sender's IP address that can be used to find the culprit's location and other information. [34]

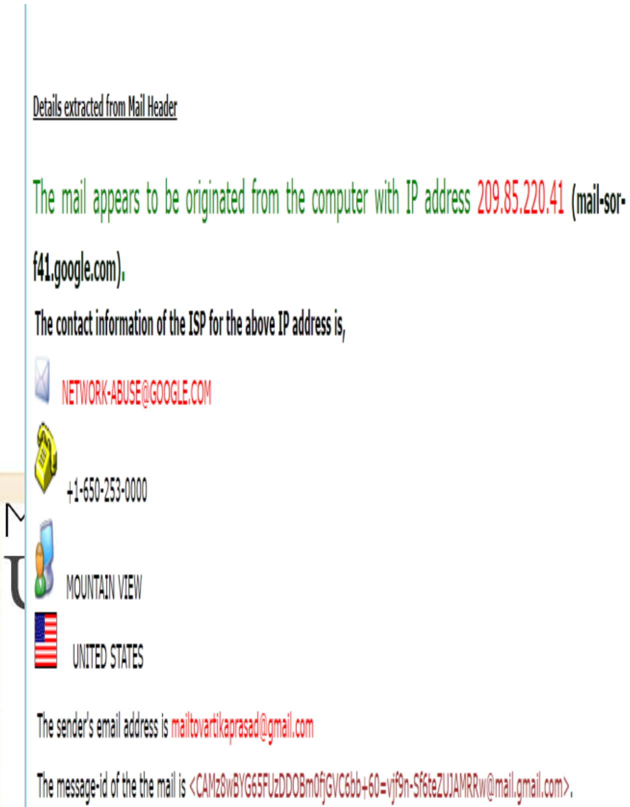
Step by step process of tracing an E-mail.

1. Open your Gmail Account.
2. Open google, search for cyber forensics online email tracer.

http://www.cyberforensics.in/OnlineEmailTracer/index.aspx

3. Open the mail for which you want to find the information about the actual sender.
4. Click on "more" on top right hand corner next to reply button, a drop down menu appears, click "show original".
5. At the bottom right corner, an option of "copy to clip board" appears, click on the button.
6. Open to cyber forensics online email tracer page in a different tab, paste the copied content to the space provided.
7. The sender's IP Address and the path traced by mail appears on the below the pasted content as depicted below.

The image below shows the IP address of the sender.



Details extracted from Mail Header

The mail appears to be originated from the computer with IP address 209.85.220.41 (mail-sor-f41.google.com).

The contact information of the ISP for the above IP address is,

✉ NETWORK-ABUSE@GOOGLE.COM

☎ +1-650-253-0000

MOUNTAIN VIEW

UNITED STATES

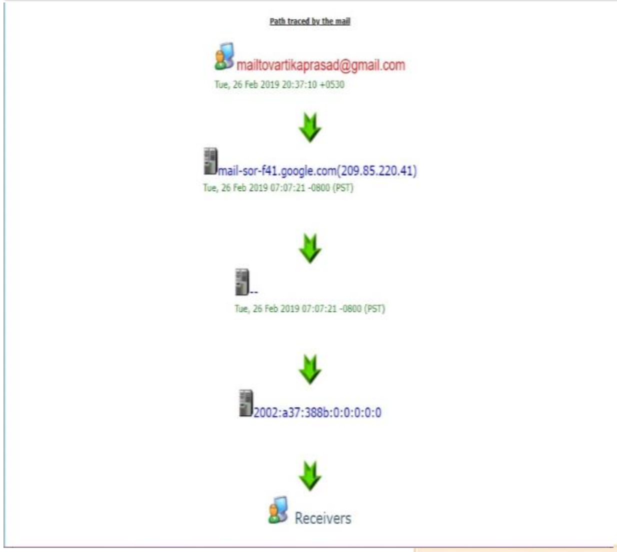
The sender's email address is mailtovartikaprasad@gmail.com

The message-id of the the mail is <CAMz8wBYG65FUzDDOBm0fjGVC6bb+60=vjf9n-Sf6teZUJAMRRw@mail.gmail.com>.

The image shows the path traced by the mail.

[33] UKEssays. November 2018. Cyber Crime And Evolution Of Cyber Forensics Information Technology Essay. [online]. Available from: https://www.ukessays.com/essays/information-technology/cyber-crime-and-evolution-of-cyber-forensics-information-technology-essay.php?vref=1

[34] cyberforensics.in. Online EmailTracer. Available from: http://www.cyberforensics.in/OnlineEmailTracer/index.aspx



Path traced by the mail

mailtovartikaprasad@gmail.com
Tue, 26 Feb 2019 20:37:10 +0530

mail-sor-f41.google.com(209.85.220.41)
Tue, 26 Feb 2019 07:07:21 -0800 (PST)

--
Tue, 26 Feb 2019 07:07:21 -0800 (PST)

2002:a37:388b:0:0:0:0:0

Receivers

Conclusion

The IT act has become a key to untangle cyber-crimes, post 2008 amendment, nevertheless, the technological advancements and the quick and cunning brains of the criminals, sometimes paves a pay out of the grips of law. Cyber cells have been formed in almost every police department of the country.

Almost every police departments in India have a cyber-crime investigation cell, wherein the cyber forensic experts along with police, untangles cyber-crimes with the help of several computer forensics tools, following a systematic mechanism of search & seizure, acquisition, analysis and reporting.

However, In the case of Dilipkumar Tulsidas Shah v. UoI [W.P.(C).No. 97 of 2013], it was observed that, "Conventional investigative methods unsuited to dealing with complex cyber- crimes are nevertheless being followed, leading to police harassment of citizens." Many other writ petitions as of Tulsidas, are also being filed to seek formulation of an appropriate regulatory framework for effective investigation of cyber-crimes.

*****