IoT Crimes: Evaluation of Forensic Evidence

Prof. (Dr.) M.K. Nagaraj[*]

Abstract

The new dimensional needs in the transformative Information and Technology world play a very significant role in providing solutions to the technology-driven virtual crimes. The lurking and fragile areas of evidentiary e-data are fairly spread over to Information System, computer peripherals, network system and other manifestations of Internet. The forensic procedures involve the collection, collation and presentation of forensic evidence. The foremost task of identifying, preserving, retrieving and processing the magnetically encoded evidential electronic data requires copious analysis. Since the virtual crime is one against many, the digital detectives or forensic experts having the domain expertise with exceptional knowledge and superior skills can only handle it. The validated software, utilities and hardware tools need to be availed in transforming evidentiary electronic data into presentable forensic evidence. The digital footprints and forensic fragments or traces in the computer or network systems constitute the best virtual clues. It is necessary to proceed from volatile memory medium to non-volatile memory medium while collecting the digital or forensic evidentiary e-data owing to their memory status. Internationally agreed Search-Seizure protocols are required to be complied by the digital detectives and forensic specialists while carrying out search and seizure in the virtual environment. Acclimatization is inevitable for both digital detectives and forensic specialists in view of the ubiquitous nature of Internet in relation to both conventional and virtual crimes. The virtual crimes include; data-

[*] Author of this article is, now serving as an Adjunct Professor in KLE Law College, Bengaluru. He also provides free legal consultancy to the poor and the needy through MKLegal Consultancy Services.

related, technology-related, software-related and social media-related crimes. Primarily, virtual crimes are characterized as adversaries of Information Communication Technology (ICT) resulting in the emergence of cybercrimes, while Internet Wireless Technology (IWT) resulting in Voice over Internet Protocol (VoIP) crimes and other emerging technologies like; Google lens, Cloud Computing and Internet of Things (IoT) resulting in the specialized and IoT crimes. I made sincere effort to explore all relevant areas keeping in view the paradigm shifts in the digital or forensic evidence.

Prelude

The term 'forensic' is derived from the Latin word 'forum', meaning market place where the Romans conducted law courts. Forensic evidence is considered as scientific evidence or third evidence. Forensic science, also called "Criminalistics" is free from human intervention and error, while forensic evidence has a greater evidentiary value in as much as providing the standard proof as to the guilt or innocence of the accused charged in a crime. Hans Gustan Adolf, father of forensic science has developed this science. A paradigm shift has been noticed in the evidentiary regime with the emergence of virtual crimes as technology-driven crimes. The task of digital detectives and forensic specialists in the collection of digital or forensic evidence is felt absolutely essential. Forensic evidence not only assures accuracy but also establishes the link between the culprit and victim or with the crime scene. Normally, a criminal leaves behind him forensic fragments or traces after perpetrating the virtual crime. In the virtual environment, forensic traces or fragments include the digital footprints, logs and audit trails. The computer has its distinct and complex mode of recording information or electronic data as it performs variety of tasks. The computer system, network system and external storage devices contain the store of information.

Forensic science establishes the -

(a) identity of evidential electronic data in the Information System or Network system;

(b) proof of unauthorised access to the Information System; and

(c) proof of presence of audit trails, logs[1], digital footprints and forensic fragments while perpetrating the virtual crime.

Internet facility is mainly meant to facilitate e-commerce and on-line interactions, but grossly misused by the perpetrators to commit virtual crimes which may be classified as; (a) Data-related virtual crimes (b) Technology-related virtual crimes and (c) software-related virtual crimes. All prohibited acts and forbidden conduct in the cyberspace attracts criminal and civil liabilities respectively under the information Technology Act, 2000 (In short ITA). Conspicuously, Information Communication Technology (ICT) paved the way for the emergence of cybercrimes, while Information Wireless Technology (IWT)[2] resulted in the emergence of Voice over Internet Protocol (VoIP) crimes. IoT[3] Crimes are also added to the list of virtual crimes in the recent times. IoT Crimes are special category of virtual crimes which include; masquerading, eavesdropping, phishing, pharming, pocket sniffing etc.

Electronic burglary or plagiarism is also a common virtual crime perpetrated in the cyberspace. E-mail Crimes involving masquerading, eavesdropping spamming are now made punishable under the amended provisions of ITA in the wake of corporate companies facing frequent disruption to their e-business or e-commerce activity. Section-43(1) ITA specifically prescribes civil liability for causing disruption to any computer system of network system. Web Crimes like; on-line frauds, on-line cheating, on-line dissemination of pornographic content, on-line sale of pirated software and on-line forgery are occurring in the cyberspace. The perpetrators has to pay sizable compensation for causing loss to an electronic data. Section-45 ITA provides residuary penalty where no specific penalty is provided for a virtual crime. News Group[4] Crimes like; sharing of electronic data, sale of pornographic pictures & videos, exchange of secret messages, distribution of hacking software,

---

[1] Logs include OS logs, control logs, OS event logs, network application logs, server logs, e-mail logs, router logs etc.

[2] Wacking or wireless hacking is done by eavesdropping technique on a wireless networking system to steal sensitive information.

[3] Abbreviated for, of IoT is Internet of Things.

[4] NewsGroups include; alt.hackers, alt.security, comp.security.unix etc.

sharing of credit card details are highly dangerous to the society as well as the nation. Phreaking[5] Crimes implies making free calls by circumventing the telecommunication network system are seen occurring across the globe. Availing the technique of masquerading or shoulder surfing, the terrorists accomplish their evil task of collecting intelligence to carry out cyber attacks against a sovereign nation.

Virtual crimes or on-line crimes are perpetrated in the cyberspace[6]. In all virtual crimes, the digital detectives and forensic specialists inclusive of the corporate detectives are required to comply with internationally accepted standards of search-seizure protocols[7]. G-8 Group consisting of advanced industrial countries required scrupulous compliance to the standard forensic procedures in the recovery of digital or forensic evidence and also prescribed superior skills, exceptional knowledge and familiarisation of relevant laws as qualifications to the digital detectives and forensic specialists. They are also required to desist from comprehensive seizure or to disrupt e-commerce activity, while the corporate detectives need to adopt the technique of 'trap & trace approach' to crack down the virtual perpetrators. The digital or forensic evidence should retrieve digital or forensic evidentiary data by resorting to distinct techniques and proven methods as recognized by the international conference held at Melbourne (Australia) in 1996.

Rules & Traits of Digital Detectives & Forensic Specialists

The digital detectives and forensic specialists need to comply with the following twelve commandants -

1) Not to resort to 'overstepping role'[8].

2) To avoid comprehensive seizure.

---

[5] Phreaking literally means hacking of the phone to steal free telephone calls.

[6] Cyberspace is also termed as 'network of Networks', 'Odd Neo World' and 'invisible space' of virtual reality.

[7] International standards and procedures have been laid down by the International Electro-Technical Commission (IEC) and Joint Technical Committee (JTC) in the task of collection of technical evidence in virtual crimes.

[8] Overstepping role implies going into too much of technicalities than what is necessary for investigation of the virtual crime.

3) Not to disrupt e-business or e-commerce activity.

4) To follow 'order of volatility'[9].

5) To keep the computer and other storage devices away from the strong or low magnetic fields to prevent the loss of electronic data[10].

6) To prevent incompetent persons to handle the digital or forensic evidential data.

7) To follow the 'chain of custody'[11] by the digital detectives.

8) To avail only the proven validated software in the collection and collation of forensic evidence.

9) To subject the digital evidentiary data for forensic analysis.

10) To comply with internationally agreed search-seizure protocols[12].

11) Not to boot the computer before commencing the task of collecting the forensic evidence as it wipes out the temporary files.

12) The digital detectives must equip themselves with the sterile 'virtual kit' comprising of clean boot Compact Disks (CDs), software, virus scan software, utility software, backup software, imaging software etc., before commencing the detective task.

Above all, the digital detectives must possess outstanding knowledge and exceptional skills with real-time situation tasks to effectively solve the virtual or specialized crimes. The Central Government is vested with powers to make rules within the scope of Section-81 ITA on matters relating to security procedures & practices, authentication procedures, licencing procedures and mode & method procedures of encryption. International Organization on Computer Evidence (IOCE) which was set up in 1995 has formulated standards and protocols on computer evidence by evolving effective methods.

---

[9] Order of volatility means proceeding from volatile media to non-volatile media in the retrieval of forensic evidentiary data.

[10] The safe range of magnetic fields vary up to 45 degrees Centigrade and 20% of humidity.

[11] Chain of custody means the digital diary of recording events within the scope of Section-172 Cr. PC.

[12] Protocols refer to internationally agreed standard procedures and norms.

Forensic Chain of Evidence

The digital detectives and forensic specialists are required to maintain the 'Chain of Custody' or forensic chain of evidence, referring to the virtual digital case diary of investigating sleuths in a virtual crime within the scope of Section-172 Code of Criminal Procedure, 1973 (In short Cr. PC). It is also a method of sequencing the source of digital evidence, date & time of retrieval, software or utilities availed in the process. Mr. A. Ahmed at the Tokyo conference held in September 2002 has proposed the forensic chain of evidence model covering access to audit trails, logs and headers[13]. John R. Vacca defined the chain of custody as "A road map that shows how the forensic evidence was collected, collated, analysed and preserved in order to be presented as forensic evidence in the court." Hence, it is a precise forensic procedure to ensure accurate auditing of the forensic evidential data. Any modifications done to the original electronic data at the time of retrieving the forensic evidentiary electronic data tend to destroy its integrity and trustworthiness. The chain of custody is a means to demonstrate trustworthiness of forensic evidence since it involves adoption of proven technology as well as new approach. The digital detectives and forensic specialists need to demonstrate their proven skills and abilities in so far as adoption of 'steps' involved in it, is concerned. The chain of custody ensures integrity and accuracy to the forensic evidence as it clearly specifies how evidential electronic data is converted into forensic evidence based on the digital footprints and forensic fragments or traces. The BAIT[14] being a powerful intrusion detection software helps the digital detectives and forensic specialists to trace the chain of custody of all persons possessing the stolen electronic records. However, they need to necessarily resort to 'calibration' which implies the steps adopted towards ensuring accuracy and reliability of procedures involved in the chain of custody. Electronic data retrieved and transmitted in electronic or optical means fulfils the reliability of forensic evidence.

---

[13] "The Forensic Chain of Evidence Model", By A. Ahmed, at http:// www.dis.unimelb.edu.au/staff/atiffAhmedACIS.pdf, visited on 21.06.2004.

[14] BAIT stands for Binary Audit Identification Transfer.

Evaluation of Forensic Evidence in IoT Crimes

IoT (Internet of Things) Crimes are currently afflicted in the Internet society. Masquerading, Phishing, Pharming, Piggybacking, Eavesdropping, Spiking. Chipping, Cross Scripting, Phreaking, Google lens, Quantum Computation, Cloud Computing, Big Data, Digital Marketing and Pocket Sniffing are all IoT Crimes emerging out of IoT technology. Pocket Sniffing Crimes are perpetrated by installing the pocket sniffer program to monitor electronic data traffic and stealing electronic data. The digital detectives and forensic specialists need to exercise due diligence and exhibit endurance and perseverance in the detection of IoT crimes. Internet being ubiquitous in nature, any intruder can loop-in from any part of the globe. The digital detectives and forensic specialists need to avail Gopher Software[15] to monitor the activities of perpetrators in the cyberspace. CERN which was later developed by Switzerland as world wide web (www) by linking Gopher sites as standard information service on the internet for accessing via hyper text browsers facilitated the users to navigate Information Super-I Way of the cyberspace. With the introduction of www and browsing software, computer resources on the internet can be accessed via hypertext browsers.

Prominent IoT Crimes

(i) *Masquerading* is an IoT Crime that implies assuming false identity of a genuine user by impersonation to gain unauthorised access to Information System (IS)[16] or networking system. Since masquerading constitutes both 'identity theft' and 'cheating by impersonation' under IoT Crimes, they are made punishable under Section 66E and Section 66D ITA respectively. Masquerading is also called 'shoulder surfing', 'Social engineering, 'vishing' or 'spoofing the identity' of the genuine user so that

[15] Gopher is a shared protocol in the Internet as it allows every subscriber to access the public domain information on the Internet which is run by the Gopher server.

[16] Article-2(f) of the UNCITRAL Model Law on Electronic Commerce, 1996 defines Information System as "a system for generating, sending, receiving, storing or otherwise processing data message".

the cyber perpetrator can steal confidential or personal information and even resort to commit 'cyber insider trading' in the corporate sector. Therefore, Masquerading is considered at a grave virtual crime more specific to the corporate world. Conspicuously, masquerading is a combination of VoIP (Voice over Internet Protocol) crime and phishing. Outsider becomes an insider the moment he assumes the identity of a genuine user by means of shoulder surfing or by means of espionage. Masquerading could be:- 1) One user masquerading another user, wherein the cyber attacker diverts the attention of the genuine user by concealing his identity and 2) One Information System masquerading another Information System by means of vishing or spoofing. In R vs. Gold & Another[17], the U.K. Court convicted Mr. Gold & Mr. Shifreen for gaining unauthorised access to the British Telecommunication Network by stealing the passwords allotted to its subscribers by resorting to phishing attacks and availing free telecommunication services without billing. In the instant case, the digital detective and forensic expert have produced forensic evidence about the password trafficking by the perpetrators successfully. In R vs. Whitley[18], Mr. Whitley has assumed the identity of Alan Dolby and hacked the Joint Academy Network (JANET) by spoofing his identity and altered electronic data. Mr. Whitley was charged for causing damage and blocking access to authorised users, thereby causing disrupting. Here again, the digital detective and the forensic specialist collected the spoofed Internet Protocol (IP) address and audit trails as forensic evidence and secured conviction.

Masquerading by impersonation arises once the perpetrator assumes the perfect combination of identifiable characters of the genuine user. Impersonation can be detected by discovering the legitimate access card holder by using the technique of 'tailgating'. Hackers being the predators of computer technology resort to masquerading or spoofing[19] as if they are genuine users to avail services by deception. Mr. Andrew Miffleton, a member of Darkside Hackers Group (DHG) has hosted a

---

[17] 1988 AC 1063.

[18] (1991) 93 Cr. App. Rep. 25.

[19] Spoofing could be e-mail spoofing, web spoofing of IP spoofing.

webpage for the use of his fellowmen of the group to resort to masquerading. This group has caused loss to VERIO, Inc. to the extent of 90,000 dollars. The digital detectives of Federal Bureau of Investigation (FBI) busted the entire racket and secured conviction up to 21 months imprisonment and a provision for the restitution of loss caused to VERIO, Inc. The forensic evidence on Platform as a Service (PaaS) and spoofing have been successfully proved by the forensic specialist. In a spoofing incident, the perpetrators have set up a false Automated Teller Machine (ATM) in public places and shopping malls which accepted ATM card the moment the user entered his PIN code. The ATM returned the card on the ground of malfunctioning of the machine, but the cyber fraudsters cloned the card and used the duplicate one to purchase merchandise goods in the telemarketing. In another incident the cloned smart card was used by the fraudsters and purchased jewels worth Rs.9,00,000/- from Navaratna Jewellery shop at Bengaluru.

Acts of masquerading or spoofing, or industrial espionage by the internet intruders are made punishable even in the United States of America. In the U.S. vs. Barth[20], the court held that accessing and viewing electronic data stored in the Information System amounts to the violation of privacy right of a corporate company or an individual. This judgment has facilitated the digital detectives and forensic specialists to proceed against the perpetrators resorting to masquerading. If such an electronic data is voluntarily or openly uploaded by the genuine user, he/she cannot exercise the right of privacy as held in the U.S. vs. Lyons[21].

A criminal gang named 'AFT-13' developed MethBot Robot Browser that masquerades or spoofs all necessary interactions for initiating, carrying out and competing with advertisement transactions. Russia-based hackers registered more than 60,000 domains and 250,267 Universal Resource Locators (URLs) impersonating high profile websites like; ESPN, CBS Sports, FOX News, Huffington Post and sold fake videos on 'Ad-Slots'. The perpetrators have obtained 'video-ad-inventory' by deception to display in its fake media websites for the sake of dollars

[20] 26 F. Supp. 2d. 928, 936-37 (W.D. Tex. 1998.

[21] 1992 F. 2d. 1029, 1031-32 (10th Cir. 1993.

by giving an impression that 'ad content' is being viewed by the legitimate website visitors. In reality, the video-ads were viewed with the help of MethBot by fake viewing. This kind of automated software program mimics the user who is viewing the video. The digital detectives and forensic specialists have carried out investigation in a copious manner and proved the spoofing techniques adopted by the group. Necurs is one of the largest BotNets with 6.1 million Bots that is capable of causing loss in terms of millions of dollars. FlokiBot is a financial malware which is sold in DarkWeb or DarkNet Market to grab 'point of sale data' through aggressive spear phishing. 'explorer exe', a malicious code is used for tracking and stealing electronic data or information from the memory. Zeus code has been used since 2013 to construct a 'citadel malware' to steal banking and financial information, especially in Canada, Brazil and the USA. The forensic specialists need to possess knowledge and skills to counter these BotNets to bring home the guilty. Lizaard Stresser IoT BotNet which is part of 400 GPPS DDoS attacks can hijack 1,300 Internet accessible video cameras and the targeted Banks. Internet attackers are shifting to Object Linking & Embedding (OLE) to spread malware by placing the malicious code. Any Time Money containing entries in the 'till rolls' indicate all transactions forming the real or direct forensic evidence. The digital detectives and forensic specialists have succeeded in tracking the forensic traces & fragments, audit trails and system logs.

(ii) *Phishing* is another IoT Crime which implies fraudulently acquiring passwords, price-sensitive information and credit card details for financial gain by resorting to masquerading technique. Recently, the Computer Emergency Response Team-India (CERT-In) has issued an advisory regarding the potential attacks from the Chinese army in the guise of free COVID 19 test. The Chinese cyber warriors are set to carry out phishing attacks against India. One may recall the memory that China has stolen the U.S. nuclear secrets from the Los Alamos National Laboratory resulting in the dismissal of its scientist Dr. Wen Ho Lee for leaking and mishandling the classified data. In the National Association of Software & Services Companies (NASSCOM) vs. Ajay Sood & Ors[22],

[22] 199 (2005) DLT 596: 2005 (30) PTC 437 Del.

the Delhi High Court declared phishing as an illegal act which entails grant of injunction and liable for damages. Phishing Crimes are perpetrated by acquiring the sensitive information like; passwords, credit cards, bank accounts, billing & payment details and cyber insider trading by means of spoofing or vishing. Phishing fraud is also perpetrated fraudulently by acquiring passwords, credit card details by means of spoofing for financial gain. The digital detectives and forensic specialists depend on electronic traces like IP headers to track down such IoT Crimes.

(iii) *Pharming* is also an IoT Crime which implies acquiring of domain names on websites illegally and re-directing the Internet traffic from one website to another website, wherein the Domain Names System (DNS) server converts the website's name into Internet Protocol (IP) address[23]. Pharming arises if any malicious code is introduced through electronic mail, thereby modifying the DNS cache. Then the perpetrators meddle with the DNS server and redirect it to the fake or wrong website. It is inevitable for the digital detectives and forensic experts to secure the DNS server against pharming attacks. Internet Service Provider (ISP) has no liability to inform the Internet users whether the DNS server is prone to pharming attack or not. Pharming Crimes are perpetrated by exploiting the Domain Names System (DNS) server software, acquiring domain names or cyber squatting and redirecting electronic data traffic from one website to another. Cybersquating is not recognized as criminal offence under the ITA.

It is rather incumbent for forensic specialists to avail the Secure Socket Layer (SLL) to prevent both phishing and pharming crimes. Integrity of information or electronic data is also assured by the application of SLL.

(iv) *Piggybacking* being an IoT Crime, it implies gaining unauthorised access to Information System by activating the terminal circuits and the network controls from the remote control. Jumping over the firewalls and by breaking the security controls and password trafficking for the purpose of 'identity theft' is committed by the perpetrator. Once they gain

[23] Example of IP Address is IP 24 94 200 54.

access to the network system, they can commit specialized virtual crimes. The digital detectives and forensic specialists set to make analysis of server logs, audit trails and collect forensic evidence to bring home the perpetrators into the virtual crime net. Audit trails discloses brute force hacking.

(v) *Eavesdropping* is an IoT Crime which is also known as 'wire tapping of telecommunication services'. In some countries, eavesdropping is allowed in the interest of the society and integrity of the Sovereignty of the State after obtaining prior permission. It is a cause of great concern for developing countries because advanced countries can flick electronic data or information from the remote locations. Eavesdropping can also be resorted by the digital detectives or forensic specialists for monitoring conversations or maintaining electronic surveillance over the telecommunication of electronic data traffic. The U.S. Electronic Wiretapping Act allows wire tapping by the investigating agencies. Even Denmark and Germany have provisioned for wire tapping under the Criminal Procedural Code and Administration of Justice Act respectively. In India, interception is allowed under the Telcom Regulatory Authority of India Act of 1997, The Telcom Regulatory Authority of India (Access to Information) Regulations, 2005 and Indian Telegraph Act, 1885 with the prior permission of the government in the interest of the sovereignty, security and integrity of the nation. The substituted provision of Section-69 ITA by Act 10 of 2008 w.e.f. 27.10.2009 empowers the Controller to issue directions for interception, decryption and monitoring information through computer resources. In reality, eavesdropping amounts to violation of privacy rights of a person which is punishable under Section-66E ITA, while Section-72 prescribes punishment for both privacy and the breach of confidentiality. The digital signature is a technical solution against acts of eavesdropping which also prevents the bugging of radio frequency emanations and picking up emanations from the remote terminals, micro-wave or satellite signals. Certifying authority signs the digital signature which assures authenticity, integrity, confidentiality and non-repudiation of electronic document.

Eavesdropping being wiretapping of telecommunication services through which electronic data is tapped by the perpetrators, The

perpetrators resort to eavesdropping with a self-centred motive to illegally extract information or electronic data, even by resorting to espionage activity. The Federal Bureau of Investigation (FBI) termed the Microdot Technology developed by the Germans as enemy's masterpiece of espionage. The forensic specialists need to monitor the security controls and security performance matrix and performing the security impact analysis. The digital detectives can seek assistance from the Controller appointed under Section-17 ITA.

(vi) *Cloud Computing* is the latest global trend in the Information Communication Technology (ICT) management which existed in the form of 'magic cookies' earlier. Magic cookies were under the public domain information of a Gopher Server which was prone to abuse in those days. Gopher server ensures public domain information of the site concerned, which could be abused by the virtual perpetrators. The Cloud Service Providers (CSPs) include; Amazon Simple Service, Amazon Web Services, Google App Engine, Microsoft Azure Services Platform and Peer-to-Peer Network based on Bit Torrent or Skype have enabled the users to access to ICT resources. The chief elements of cloud computing include; Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). All these enable access to ICT resources. In the Cloud Computing, the right to privacy figures as a prominent issue which is now recognized as a constitutional right[24]. In the U.S. vs. Kennedy[25], the court held that the search of Kennedy's computer by a private person i.e. computer repairer did not violate his right of privacy. The Google Lens cannot process or further process the information of private persons without their consent. The CSPs process the customers information which needs to be protected under the Data Protection Principles[26]. The United Kingdom has enacted the Data Protection Act in 1984 and amended from time to time, apart from evolving Data Protection Principles. An organizational and technical data

---

[24] In Retired Justice Puttaswamy v. Union of India, the Supreme Court of India in their judgment on August 24, 2017held that privacy is a constitutional right.

[25] 81 F. Supp. 2d. 1103, 1112 (D. Kan. 2000.

[26] Mrs. K.S. Shere made a permanent recommendation to enact Data Protection Act, but so far no such Act is put in place in India.

security measures are required to be ensured by the CSPs at all costs. In Cloud Computing, the legal responsibility for electronic data processing lies on the user who enlists services of a CSP. It is incumbent to realise that the third party is authorised to process the personal electronic data or even further processing of the processed electronic data. In the Recording Industries Association of America (RIAA) vs. Napster, Inc[27], the defendant company has provided the platform[28]for its 70,000 subscribers to freely download MP3 music files. Napster Inc. being a peer-to-peer music files, Application Service Provider (ASP) need to exercise control over it. The plaintiff and other companies have obtained injunction from the court against the defendant company in 2001 with court orders to stop providing the platform as a Service (PaaS) for downloading MP3 music files by the subscribers. The court also imposed heavy fine on Napster, Inc. to make good the loss suffered by RIAA. Similarly, software piracy has become a common feature by misusing the Software as a Service (SaaS) by soft lifting[29]. Software piracy deprives the software developers of their incentives for their inventions. The digital detectives and forensic specialists need to search Electronic Bulletin Boards (EBBs) which facilitates copying of the software. EBBs also facilitate hackers to hunt for specific information. Sometimes, the software developers also insert 'maintenance hooks' in the software to extort money from the users or buying companies. Information as a Service (IaaS) facilitates the subscribers or users to perpetrate plagiarism of proprietary electronic data or digital asset where copyright and patent right subsist, except for the fair use. In Grant vs. Allen[30], the court held that clandestinely downloading of computer program and using it for monetary gain amounts to electronic burglary or plagiarism. Cloud computing is utilized illegally as far as client's electronic data or information is concerned.

(vii) *Pocket Sniffing* Crime being a network monitoring program, it is installed to monitor the electronic data traffic from the public access to internet or websites. Pocket Sniffing facilitates the cyber terrorists to

---

[27] 239 f. 3d. 1004 (9th Cir. 2001).

[28] Platform as a Service (PaaS) is one of the components of cloud computing.

[29] Soft Lifting is unauthorized use and distribution of software among others.

[30] JC 71, January 20, 2011.

insert software programs from the remote network location to monitor electronic 'data packets' transmitted electronically in electronic form in the cyberspace. User name and password are obtained by the perpetrators to steal the electronic data or information and to perpetrate virtual crimes. The digital detectives need to remember always that every electronic document gets divided into small segments called "packets" at the source point and assemble at the destination point. The packets traverse electronically in electronic form[31]via telecommunication network or the satellite. The cyberpunks[32] are capable of intercepting electronic data packets traversing in the cyberspace and pass on the sensitive information to the terrorist organizations or enemy country. In addition, they also perpetrate Electronic Fund Transfer (EFT) or On-line Fund Transfer (OFT) frauds. Electronic Data Interchange (EDI)[33] ensures secure electronic communication from one computer to another computer in a structured format. EDI assures greater accuracy and certainty in all e-commerce transactions. Section-66F was inserted by 2008 amendment w.e.f. 2009 to ITA to make the offence punishable with life imprisonment. In America, Justice G. Donald Haneke has authorised the Federal Bureau of Investigation (FBI) to install the key board sniffing device to sneak into the system of the suspect Nicodemo S. Scarfo at Belleville, New Jersey, USA on May 10, 1999. The digital detectives and forensic specialists need to track the network server logs and audit trails to detect such specialised virtual crimes.

(viii) *Big Data*

Normally, big data contains broad-based information, but the basic problem lies in its absence of security audits. What happens if any virtual perpetrator fabricates e-data to undermine the quality of big data? How to check them out from the task of processing the big data? These simple

---

[31] Section-2(1) (r) ITA defines electronic form as "any information generated, sent, received or in media, magnetic, optical, computer memory, micro film, computer generated micro fiche, or similar device.

[32] Cyberpunks are experts in intercepting electronic data packets during their transmission and perpetrate on-line banking and financial frauds.

[33] Article-2(b) of UNCITRAL Model Law on Electronic Commerce, 1996 defines EDI as "electronic transfer from computer to computer of information using and agreed standard structure of information.

queries need to be clarified. Big Data technologies need to provide additional security layer protection to e-data. Generally, sensitive data is stored in the cloud without encryption. Inside it, IT professionals and greedy business rivals can mine the data to sell it for their benefits. Unauthorised changes to metadata that results in the wrong data sets forms an impediment to unearth security breaches. Data items falling under prohibitions like; medical records, names, e-mails etc., for medical research should not be processed. Science Soft has raised certain concerns about the Big Data security issues depending on perimeter security i.e. points of entry and exit in the data protection. Privacy to personal data is all the more significant.

Forensic Methods of Detection

The digital detectives and forensic specialists resort to certain proven detective methods to crack down the specialized virtual crimes which include -

a) Classifying & Clustering Method (CCM) is more feasible for forensic specialists to classify & cluster the forensic evidential data found in the database[34] which is required for the purpose of investigation of a virtual crimes. In a database, both proprietary electronic data and general data are present. Flat File Database (FFD) is required to be searched by the digital detectives and forensic experts to find evidential data. The network database contains general information, financial information and proprietary data. The 'data mart' in the data warehouse of an organization is a repository of a specific group of electronic data. The repository electronic evidentiary data present in the computer peripherals is also of immense value from the viewpoint of forensic evidence. Computer is no more a computing tool but a repository of evidence tool also. The data mining tools facilitate the digital detectives to display data patterns and to find the groups in the large amount of data is called 'clustering of data'. In the case of a protected system[35], classified and unclassified electronic data are stored. In 1999, two hackers from the U.S. and Australia have

[34] Database contains store of electronic information.

[35] Section-70 ITA punishes even for gaining access to the protected system.

hacked into the Baba Atomic Research Centre (BARC) at Mumbai and disturbed the unclassified data as they could not access the classified data. The hackers intended to get classified information from the BARC soon after the Phokran nuclear test by India.

b) Backtracking Method facilitates the forensic experts to analyse server logs from the targeted or victim computer to the source computer from where an attack has been made. The backtrack method or tracking back from server to server helps the forensic specialist to trace the origin of attack. This is known as "backward journey from the targeted computer to the source computer from where hacking was done[36]. Without the knowledge of the hacker, both original and modified medical prescription remained in the Information System (IS) in the form of 'ambient data'[37] which was recovered by the FBI sleuths and prosecuted the perpetrators. Ambient data is the best forensic evidence even in the stock scams, financial frauds, IoT crimes and other specialized virtual crimes. Backtrack software identifies the chain of events leading to the identification of the source computer.

c) Prying Eyes Method is of great utility to the digital detectives and forensic experts in which the Global Positioning System (GPS) chip is embedded beneath the skin of a person or animal and equipment, vehicle, aeroplane, boat, drone or any other object[38]. It is worth mentioning that the U.S. has come out with and advanced GPS chip called the "Digital Angel" as an effective tracking device. PGP encryption software helps the corporate detectives to shield the company's Information System (IS) against Prying Eyes or cyber surveillance. The digital detectives need to

---

[36] The Federal Bureau of Investigation (CBI) Cracked the cyber homicide in Smith Hospital vs. Rover Hospital case, wherein the Smith Hospital authorities have hacked into the computer system of Rover Hospital with the help of a hacker and administered lethal dosage of medicines to a targeted patient undergoing treatment in Rover Hospital different from what was prescribed by the doctor. After killing the patient, the hacker has restored the medical prescription back to its original position. The cyber homicide was committed with a malafide intention to bring disrepute to the Rover Hospital.

[37] Ambient data is forensically used to describe electronic data stored in non-traditional storage device or format of the computer without the knowledge of the perpetrator.

[38] Object may include; Cell Phone, Satellite Phone, Walkie-Talkie. Briefcase, Bullet Proof Jacket etc.

verify encryption of financial data which is necessary for electronic data traffic to pass through firewalls as access control security.

d) Cryptanalysis Method facilitates the digital detectives and forensic experts to have a breakthrough of steganography, thereby detecting embedded data or hidden secret messages. In this task, they need to avail validated software tools[39]. It is pertinent for the forensic specialists that 138,547 bytes can be hidden in the image file where stego-tools are used. The forensic expert may break into it and view & restore the hidden secret e-message in the innocent-looking digital image and succeed in extracting such electronic data. The header of electronic message points out the computer cracker (perpetrator) with additional cryptanalysis[40].

e) Link Analysis Method helps to detect major banking frauds and money laundering cases . The digital detectives and forensic experts need to retrieve the link analysis charts for evaluating the forensic evidence. In money laundering cases, the link analysis charts depicts the relation as to primary and secondary links[41].

Availing of Forensic Software

The digital detectives and forensic experts need to avail validated software in the collection of digital or forensic evidence. They should run the program from the short-term memory on the volatile media and burn on to write-once optical media to prevent tampering of critical electronic data and also to preserve the forensic evidential electronic data in the long term memory storage medium after making a copy. They cannot analyse the forensic evidential data on the original, It is also necessary that they should verify validation of software before its use[42].

---

[39] http://www.jjtc.com/steganography/toolmatrix.htm.

[40] "Exploring Steganography: Seeing the Unseen" Article by Neil F. Johnson and Sushil Jajodia, George Mason University, 21st April 2002 at http://www.isse.gmu.edu/-/njohnson/r20260.pdf.

[41] "Computer Evidence: A Forensic Investigation Hand Book". Bly Edward Wilden, P.47 & 48, London Street, Sweet & Maxwell.

[42] "Software is the New Tool for Catching the Crooks" at http:///.govexec.com/dailyfed/0100/0127.htm, visited on 17,06,2004.

Following are a few software tools that can be availed by the forensic specialists in ensuring the validation of the forensic evidence -

- GetSlack software facilitates to retrieve ambient data from the unallocated space or file slack.
- GetSwap software is a forensic utility that helps to capture and analyse swap files.
- Gethtml is a filtering software that automatically identifies and reconstructs HTML documents in the internet scenario.
- GetGif is a filtering software that automatically identifies and constructs gif files.
- HexSearch is a forensic utility availed to find the binary data patterns associated with the headers of electronic documents.
- FileList software facilitates in the disk cataloguing to evaluate the use of computer and timelines.
- xTree Pro Gold helps to trace and retrieve hidden files.
- Magellan software helps to retrieve graphic files and provides as online directory of Internet sites. It also restores the damaged electronic files.
- Hasher Software (Program) verifies the data integrity
- SafeBack is an ideal forensic tool for mirror imaging the deleted electronic data, fragments of electronic files and audit trails.
- SnapBack and DIBS facilitates to perform the bit-stream image copy of the HDD.
- EnCase being the forensic utility software, it identifies and listings of system files, re-constructs images, depicts timelines and enables to view electronic records. All hidden, erased, compressed, encrypted and password protected files can be subjected for forensic analysis.
- AnaDisk detects the hidden partitions in the HDD and FDD and evaluate the random memory dumps.
- E-mail Tracer analyses e-mail headers.

- ILook Image Investigator software facilitates the forensic specialists to view images which is also known as the 'best known forensic imaging'.
- E-mail Pro Gen facilitate to search e-mail addresses which can also verify the user names of the e-mail server.
- iConnectFree software helps to receive e-mails and voice mails.
- RealSecure Server Sensor (RSS) software facilitates to monitor servers.
- Data Interception by Remote Transmission (DIRT) is a powerful remote control monitoring software for securing the forensic evidence.
- WebSpider software creates searchable indices of websites within the database.
- Alta Vista[43] ensures the precise search through the web index to obtain full text of thousands of News Groups.
- The Key Board Sniffing device helps to know the password of a computer or internet.
- Sniffit is a network Pocket Sniffer that tracks down e-data packets transmitted under the network protocols.
- The Norton Disk Editor Viewer, a component of Norton Utility enables the digital detectives to view electronic content in its entirety on the computer screen.
- Fast File Undelete software recovers deleted files.
- UNERASE facilitates to preserve integrity of evidential electronic data.
- DOS Undelete software restores erased files.
- Drive Lock is a solution to the hot key used by the perpetrators.
- Graphics software is availed in the detection of morphing of photographs, videos or digital images to commit cyber morphing by the perpetrators.

[43] One of the old Crawler-based search engines which has a large index of web pages.

Forensic Evaluation of Evidentiary Data

Forensic evaluation of digital evidence is essential in the task of collecting the mute evidence or true evidence. The circumventing efforts of the cyber perpetrators to hide evidentiary data and to delete files can be countered by the digital detectives and forensic specialists by availing forensic software like; EnCase, Digital Imaging Backup System (DIBS), SafeBack, TrueBack and ILook . The digital detective and forensic specialist need to subject the 'targeted computer' and the 'source computer' to forensic analysis in the task of retrieving the evidentiary e-data. The recovery of forensic fragments and digital footprints from the computer or network system, date & time stamps stored in the hidden 64-bit of the system's clock together constitute the best evidence. The date & time of creation, modification and restoration assumes significance. If an electronic file is deleted and moved to the recycle bin, an 'index entry' is created so as to indicate its original location, name and date of deletion. File Date Time Extractor (FDTE) software helps to recover e-data from 64-bit date & time allocated space. Since the date & time stamps are computer generated e-data, they form the best evidence.

A wide range of technological, logical and legal requirements is inevitable in the identification, analysis, preservation and processing of evidentiary electronic data. The forensic evidence constitutes the proof of fact in the all legal issues. The digital signature assures reliability and speed with precision, while Electronic Data Interchange (EDI) assures accuracy and certainty in all e-commerce or e-business transactions.

Electronic documents comprising of digital or forensic evidentiary e-data assures primary evidentiary status under the Section-62 Indian Evidence Act, 1872[44] (In short IEA). The forensic experts are now able to solve the problem of Lack of Visual Evidence (LOVE). An admission made with reference to the contents of e-record in electronic form[45] is relevant under the amended Section-22(A) IEA. In order to admit digital or forensic expert's evidence under Section-45 IEA,

---

[44] Sectopm-29A of the Indian Penal Code, 1860 read with Section-2(1) (t) ITA defines an electronic document.

[45] Section 2(1) (r) ITA defines an electronic form.

it must be shown that an expert possess specialized knowledge and required skills as held in State of Himachal Pradesh vs. Jail Lal & Another[46]. The Supreme Court of India in NCT of Delhi vs. Sunil & Another[47] held that even if the voluntary statement of the accused is inculpatory under Section-27 IEA, his/her voluntary statement given before the digital detective while in the police custody forms the relevant evidence. Such a voluntary statement leading to the discovery of incriminating electronic data or material content will not amount to self-incrimination under Article-20(3) of the constitution of India.

The opinion of Certifying Authority under Chapter-VII ITA in relation to the digital signature is relevant for the purpose of forensic evidence within the scope of amended Sections-47A, 81A, 85A, B&C, 90A IEA and Article-9(2) of the Model Law, 1996. Section 65A IEA assures evidential weight to forensic evidence, while Section-65B read with Article-9(1) of the Model Law, 1996 admissibility to e-records in evidence.

By reversing the imaging[48] process onto another Central Processing Unit (CPU) of similar configuration, an exact image of the contents of the original disk can be obtained forensically.

In Doe vs. U.S[49], the U.S. Court has laid down the 'triple test' towards assuring evidentiary value to the digital or forensic evidence, which include -

(i) Functional reliability of the system;

(ii) Testimony of the computer operator or system administrator, or programmer; and

(iii) Authenticity, integrity and non-repudiation of digital or forensic e-data.

The trustworthiness of forensic evidence lies in its authenticity, integrity, reliability and accuracy. If the integrity of evidentiary electronic

---

[46] (200) 1 Crimes 176 SC

[47] 1999 Cr .L.J. 4294: (1999) AIR SC 3381.

[48] Imaging refers to the taking of a complete virtual image of the hard disk inclusive of the hidden and deleted electronic data.

[49] 805 F. Supp. 1513, 1517 (D. Hawaii, 1992.

data is lost with the alteration or damage, it renders the forensic evidence inadmissible in evidence. The digital signature assures authenticity and reliability to e-record. In the U.S. vs. Allen[50], the court ruled that mere raising doubt regarding the possibility of tampering electronic document is insufficient to render forensic evidence inadmissible. The digital certificate[51]affords to provide solution against uncertainties authenticity and integrity to electronic record. Section-35 IEA lays down the procedures for the issue of digital certificate by the Certifying Authority.

The printout of logs of the Internet Relay Chat (IRC) room is held to be authentic forensic evidence in U.S. vs. Tank[52]. The U.S Courts have laid down the procedures and validity of seizure of computer hardware[53], seizure of computer equipment[54], seizure of computer program[55] and seizure of computer terminals[56]. The digital detectives need to obtain customers' accounts i.e. perpetrators from the Internet Service Provider (ISP)[57] together with their subscription details which forms the good circumstantial evidence.

Computer-stored electronic records are admissible in evidence if they are created in the course of e-business transactions or generated by the computer without human interference. The digital evidence retrieved from the computer system, network system or database qualifies as primary evidence as held by the Supreme Court of India in Prithvi Chand vs. State of Himachal Pradesh[58]. Justice M.K. Sharma in Yahoo, Inc vs.

---

[50] 106 F. 3d. 695, 700 (6th Cir. 1997.

[51] Section-2(1) (p) defines the digital certificate as "authentication of any electronic by a subscriber by means of an electronic method or procedure in accordance with provisions under section-3.

[52] 200 F. 3d. 627, 630-31 (9th Cir. 200.

[53] U.S. vs. Hay, 231 F. 3d. 630, 634 (9th Cir. 2000.

[54] U.S. vs. Campos, 221 F. 3d. 1143, 1147 (10th Cir. 2000).

[55] U.S. vs. Upham 168 F. 3d. (1st Cir. 1999(.

[56] U.S. vs. Henson, 848 F. 2d. 1374 (6th Cir. 1988.

[57] Failure of ISP to preserve and retain electronic data in a required format under Section-67C ITA.

[58] AIR 1989 SC 7002: (1989) 1 SCJ 325.

Akash Arora[59] held that the use of electronic record is recognized in evidence. Electronic record or electronic file contains electronic impulses which can be stored in the system, remote server or any other storage media. Ambient data forms the best forensic evidence in virtual crimes like; cyber homicide, stock scams, financial frauds and others.

Hackers resort to website forgery by pocket sniffing to identify packets with the help of 'File Transfer Protocol' (FTP) requests. The spoofing incident of the website of the Labour Party the United Kingdom has occurred in 1996[60].

Mute Evidence as Best Evidence Rule

Forensic evidence must fulfil the 'best evidence rule' or real evidence rule and to withstand the test of scrutiny in the court of law.

The computer generated electronic data like; the system log or syslog files, proxy server logs and date & time stamps constitute the best evidence or real evidence because they truly reflect the original status of electronic data. such of those electronic data can be forensically recovered from the virtual crime scene. They exist in the mirror cache beyond the knowledge of the user of the system or the perpetrator[61]. Application programs generating the word processed electronic document, database file or picture display of the last modification made, fulfils the best evidence rule. Since the printable database is similarly categorised as e-record, it is held to be the best evidence in Derby & Co. vs. Weldon[62]. In R vs. Sipby[63], the U.K court held that an e-record generated by the computer automation without human intervention is considered as the 'best evidence'. In the instant case, the court of appeal ruled that the printout generated by the hotel computer showing the details of telephone calls made by its occupants and the calls recorded

---

[59] Suit No. 2469/1998 II AP Delhi 229 78 (1999) DLT 288, decided on January 19, 1999.

[60] http://www.proptel.org,uk,labourparty.

[61] http://www.cybersearch.org, visited on 02.06.2004.

[62] (1991) 1 WLT 73.

[63] (1990) 1 91 Cr. App. R. 186 CA.

automatically by the computer is a valid forensic evidence. The accused charged for an offence of smuggling of narcotic drugs into the United Kingdom has made calls to his accomplice in France from the hotel.

It is essential that integrity of saved e-files must be ensured. Since the user of electronic data has control over e-data and its processing, he cannot add, modify or delete originality of the content. Electronic records generated in the normal course of business activity forms the best evidence as held in the U.S. vs. Catabran[64]. In the U.S. vs. Glasser[65], the U.S. Supreme Court held that the party opposing the admissibility of computer printout should prove the type of better security required to prevent tampering of electronic data stored in the computer chip. Onus of proof lies on the party contesting the admission of the computer printout. The process of obtaining the bit-stream backup imaging or sector-by-sector copying involves the true replication of original e-data stored in the system. The evidence generated by the server logs through their audit function also constitute the best evidence provided that it is generated without human intervention, free from contamination and malfunction of the system.

Conclusion

It is the foremost task of the digital detectives and forensic specialists to identify, retrieve and process the evidentiary electronic data. It is equally essential to analyse the digital forensics copiously which comprises of computer forensics, network forensics, router forensics, SIMM forensics, web forensics, e-mail forensics and software forensics in the evaluation of forensic evidence[66].

---

[64] 836 F. 2d. 453,457 (9th Cir. 1988.

[65] 773 F. 2d. 1553 (11th Cir. 1985

[66] I discussed the digital forensics in greater detail in my Article published in the High Court Law Journal.