Digital Forensic Science in Indian Ecommerce Environment

Dr Padmalatha N A
Assistant Professor, Dayananda Sagar University
Hosur Main Road, Kudlu Gate
Bangalore- 560 068
E-mail: drpadmalatha-socm@dsu.edu.in

ABSTRACT:
In today's environment crimes are becoming more digitised and more sophisticated. This sophistication of crime leads not only users but also companies to lose some important data. Protecting the data and users requires a strong forensic techniques and knowledge of the investigation process. In Indian scenarios, frauds are predominant in domains such as financial services and real estate and infrastructure.

Even though there is a rise in cybercrime activities, most of the times forensic investigation tools were not used. One of the main reasons for the same is the business criticality of the application. Because of which, the system can neither be slowed down nor shut down. This leads to further increase in cyber-attacks to the storage, network and applications of business systems.

As per research conducted by previous researchers, India has the internet user base of 450 million. Approximately 15% of the users have a digital experience of more than three years. This makes fraud detection in Indian ecommerce industry all the more relevant.

The research is not intended to provide a complete view of all factors to be considered for forensic tool selection. But it has taken some areas which seems to be important for the choice of the tools. The present study makes a comparison of the select tools based on platform, capability, reporting, and tool support. Among the forensic tools available in the market, the researcher indicates that CAINE and SIFT can be considered important. CAINE forensic platform provides all the forensic tools that are required in the investigation process like preservation, collection, examination and analysis. SIFT provides tools for in-depth investigations for file systems, memory and network investigations.

Keywords:
Forensic tool, E-Commerce fraud, Digital Forensic Process
Article Received: 18 October 2020, Revised: 3 November 2020, Accepted: 24 December 2020

Introduction

With core industry verticals in India such as manufacturing and construction aligning their businesses with an IT driven approach, Information and Communication Technology (ICT) adoption is bound to increase in the coming years. With the widespread use of ICT, organizations in India need to establish with sufficient forensic capabilities to support investigation of criminal activities within and outside organizations. The application of forensic tools varies with the domains. These tools were widely use in courts to accept or deny certain hypotheses. In business, forensics may be involved during internal corporate investigations or intrusion investigation.

Traditional frauds that are tackled in the organizations are diversion of goods, theft, bribery, etc. whereas emerging frauds are social media fraud, e-business fraud, crypto-currency fraud, etc. Even though many organizations have certain mechanisms to tackle these frauds, some of these areas, are susceptible to more problems in Indian organizations in the future.

Forensic science, which is a field of digital forensics, covers the detection of materials found in computing devices and their peripheral devices. The Companies Act, 2013, which is India's law providing a mechanism for the investigation, detection and prevention of corporate fraud. Proactive risk management, Imposing civil and criminal liabilities, Specific provisions relating to fraud prevention, etc. are some of the means by the government to prevent fraud .

Even though various laws are available across the countries for fraud prevention, there is variation in

laws and the support by industry to reduce the fraud related activities is relatively less. Analysis of various reports and data indicate that there is a shift in the type of cybercrime across the countries. For instance, Greek users concern frauds arising from social networking sites as prominent (Vlachos et al, 2010). Since most of the frauds are cyber related, the adoption of information technology tools is one of the viable solutions for managing the same. Also, the previous research has indicated that advancement in Technology and shift of business to a virtual environment are the prominent contributing reasons for increase in fraud.

This paper deals with the following findings related to cyber crimes:

- Landscape of cybercrime
- Challenges for investigation and detection
- Ecommerce Scenario
- Tools applicable for Investigation, Prevention and Detection
- Possible mechanisms of prevention of ecommerce fraud.

Objectives of the Study

In many forensic crimes, the procedure for conducting forensics is not standardised. A lot of researches have attempted to provide guidelines, but does not provide appropriate activities with the phases of investigation. Hence this research makes a systematic procedure for

- To find the phase and activities along the phase of digital forensic process
- To examine the various tools used for forensic investigation
- To assess the tools based on the select parameters

Methodology

Research methodology adopted for the study is in-depth analysis of the previous research with an appropriate framework. This methodology was adopted to answer the following research questions:

- The forensic tool currently known by most of the organizations
- The rationale behind the selection of software tools
- General software selectin issues and policy from the firm's perspective
- Technical selection criteria with reference to forensic software tools
- Management selection criteria with reference to forensic software tools

The forensic tools used for the study is based on the criteria as shown in Fig 1.0

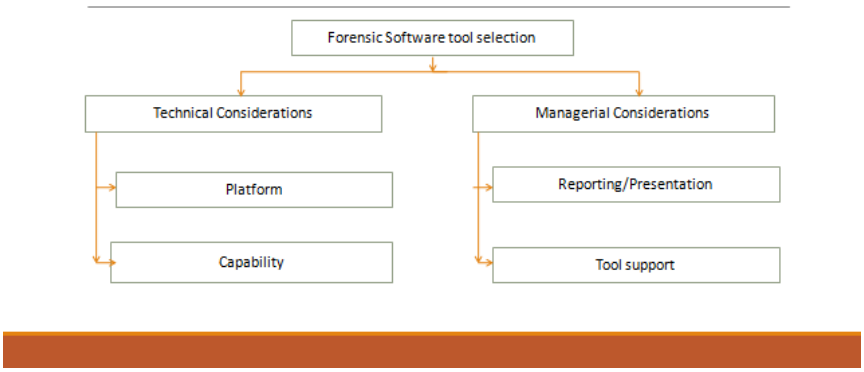

Fig 1.0: Research framework

Landscape of cybercrime:

The continuous growth of cybercrime and the involvement of various criminal group and the

revenue generated by them is a serious threat to Public sector as well as any Private Sector organizations. Some of the prominent frauds are corporate espionage, money laundering, intellectual property fraud, frauds arising from regulatory non-compliance, etc. Government of India is spending a significant amount of money on forensic investigating tools and detection tools. Factors contributing to frauds are Lack of an efficient internal control/ Compliance System, Inadequate due diligence on employees/ third party associates, Unrealistic targets or goals linked to monetary compensation. As per Deloitte reports (2014), bribery, theft of funds, Non- compliance to regulatory requirement are the frauds commonly found in many organizations.

Even though there is a rise in cybercrime activities, most of the times forensic investigation tools were not used. One of the main reasons for the same is the business criticality of the application. Because of which, the system can neither be slowed down nor shut down. This leads to further increase in cyber-attacks to the network and applications of business systems.

The reports of Corruption Perceptions Index, 2018, has ranked India in 78th position out of 180 countries. Bribery or greasing the wheel and corruption is not uncommon in India. Companies Act, 2013 ensures corporate governance through channels such as auditors, cost Accountants, Serious Fraud Investigation Office (SFIO) and National Financial Regulatory Authority (NFRA).

Two types of crimes are discussed below:

Computer based crimes- Cyberbullying, Cyberstalking, Spamming or cyberterrorism are some of the examples to Cyber based crime. Here, forensic experts will analyse computing device and hard disks.

Computer Targeted Crime- Here, the forensic experts will analyse memory, operating system and network. .

ISO/IEC (International organization for Standardization/ Electro technical Commission) 27043:2015 provides a general overview of all the incident investigation principles and processes.

- Setting up a governance for investigation management
- Security related incident management
- Digital evidence handling
- Managing the storage security
- Choosing the appropriate investigation and detection method
- Conduction of the investigation
- Interpreting the outcome

Based on the above standard , the key components of digital forensic model can be designed as shown in figure 2.0. The activities related to the digital forensic model are:

Preparation: Identifying the type of forensics from the indicators. .E.g.: network forensics, media forensics, etc. Preparing appropriate tools, techniques, search warrants, and monitoring authorization and management support. Having an appropriate strategy for the appropriate technology usage in question.

Interaction: Involves preservation which includes storing the state of evidence. Collecting the information involves record the physical scene and duplicate digital evidence using standardised and formal method.

Reconstruction: Includes examination which is in-depth systematic search of evidence relating to the suspected crime. Determine significance, reconstruct fragments of data and draw conclusions based on evidence found.

Presentation: Provides the explanation of conclusion.

Finally, forensic model concludes with returning the property to the appropriate owner.

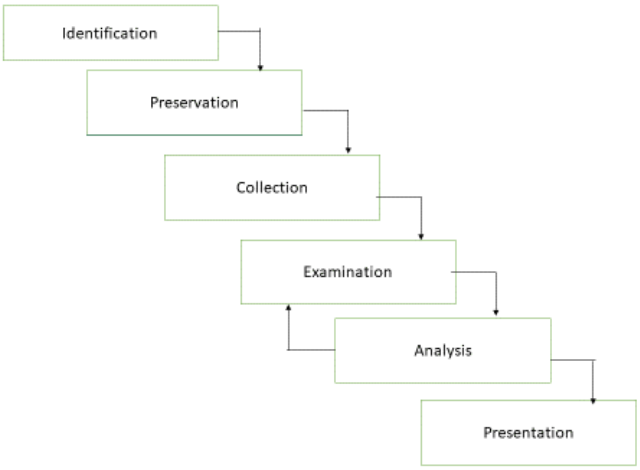

Fig 2.0 Key Components of Digital Forensic Model

Investigation categories

Depending in the type of digital device used, the investigation is divided into the following major categories: Computer forensics; Network forensics; Mobile device forensics.

Computer Forensics: Is a branch of digital forensic science pertaining to evidence found in computers and digital storage media.

Network Forensics: Is the branch of digital forensics that is characterised by capture, documenting, and analysing of activities, that takes place on a network for the purpose of identifying imposition and subjecting them to investigation

Mobile Device Forensics: Is the branch of digital forensics that is characterized by capturing of evidence from a mobile device.

Challenges of investigation and detection

The challenges of fault investigation and detection involves finding the people involved in playing a pivotal role. Even though every employee takes an important role, external auditors need to be responsible for fraud detection. Chief Security Officer plays a vital role since they know the organization's operations, weak links, etc. Having a strong regulatory mechanism is important at the operational and tactical level. Unavailability of resources to manage data on a daily basis, Lack of awareness of using appropriate tool in fraud risk monitoring, High cost of skilled resources and software, Lack of knowledge amongst decision/ Policy makers on the use of data analytics, Non availability of data, Poor quality of data are the major challenges for fraud investigation.

Ecommerce Environment

Electronic Commerce (E-Commerce) has made a vital presence in rural and urban India. The increasing awareness for acceptance of internet is shown in Table 1.0. The Indian E-Commerce industry is currently valued at approximately INR224bilion and is growing at the rate of 50-55 Per cent annually. It is expected to be INR 504 billion large in the next ten years. Currently travel related booking, online retail of consumer goods, etc. forms the largest share of e-Commerce industry. Potential for the E-Commerce in India is high because of the increasing Internet population of India.

	2012	**2017**	**2022**
Digital champions	<1million	10—20 million	50-60 million
Digital Live	5-10 million	50-60 million	100-130 million
Digital explorers	10-15 million	80 million+	130-150 million

Digital Beginners	50 million+	Approx. 200 million+	500 million+

Table 1: Number of people who have crossed the digital phases
Source: Secondary Research, PWC analysis

Even though Government of India launched various initiatives like Udaan, Umang, Start-up India Portal, etc. and allocated Rs. 8000 crores to BharatNet Project to provide broadband services to 150,000 Gram panchayats. (www. Ibef.org), some of the key fraud risks that deter the organization from doing business online are:

Leakage and Data loss of confidential company information: Fraudulent transactions through usage of stolen or hacked credit/debit card information and liabilities, Lack of adequate security at payment gateways, Risks related to fictitious invoicing, Lack of delivery of goods after payment, Risks related to fictitious invoicing, etc.,

Site Replicating: Fraudsters replicates the original website with an aim to gather information such as credit card details, bank account passwords, which is sent unknowingly by gullible customers

Credit Card Chargeback: Chargeback refers to a scenario when the refuses to honor the payment on credit card. The customer's bank then refuses to make the payment and the revenue of the merchant is held up until the dispute is resolved.

Sale of Spurious / Counterfeit goods: Fraudsters may sell fake/duplicate products at significantly cheaper price, causing loss of revenue to the original merchant/manufacturer.

Tools applicable for Investigation, Prevention and Detection

Information Technology plays an important role in fraud investigation and detection. While investigation tools inquire into or study in order to ascertain facts or information, the detection tools discover or find by careful search, examination or probing. At present companies are putting in place basic processes and controls to improve operational efficiency and risk mitigation.

Fraud Investigation Tool

Following processes are monitored using the appropriate tools:

E-mail and external communication: Automatic notifications to designated stakeholders when an event is triggered. It helps to reduce the response time required to contain the fraud risk.

Cross Departmental integration of data: Most ERP systems have business intelligence modules that can be configured depending on the type of business and data inputs available, to generate deeper inquiry. Enabling cross departmental integration of data from systems such as between HR, Payroll administration and finance will minimise the issues related to fraud.

Data Leakage Prevention Software: Having appropriate policy guidelines that, the emails going outside certain domains, only if a copy is marked to a particular email id.

Times and Physical access control: Access control on devices (employee owned and office owned) containing confidential office data by having appropriate security. In case the device is stolen, software tools can remotely wipe data to ensure that unauthorised people will not get the data.

Logging and monitoring an audit trial of activities: Perception of detection tools such as audio visual monitoring which is believed to increase the awareness among employees.

Detection Mechanisms:

Information technology tools can be used to identify the frauds such as Theft of inventory, Asset misappropriation, Bribery and Corruption, Supply Chain fraud, Cybercrime, Mergers and acquisitions fraud, Financial Statement fraud, Ecommerce fraud, counter freighting, Capital Markets fraud etc. Among the various control such statutory audit, whistle-blower hotline, audit controls, IT controls, etc. are prominent modes of control.

Logging and maintaining an audit trail activities: Maintaining a log maintenance and a multidisciplinary team develops a log policy. Logs should be routinely reviewed to discover the patterns.

Whistle Blower Hotline: Anonymity of whistle-blower and confidentiality of information need to be maintained.

Digital Forensic Tools

In the following section, a discussion on data forensic tool which can be used under a variety of situations are discussed:

a. Hard Drive Forensic Tools

Autopsy: Is a graphical user based open source digital forensic program to analyse hard drives and smart phones effectively. It is used by thousands of users worldwide to investigate what actually happened in the computer.

Encrypted Disk Detector: Can be useful to check encrypted physical drives. The tool supports TrueCrypt[1], PGP[2], BitLocker[3], SafeBoot encrypted volumes.

b. Network Forensic Tools

Wireshark: Is a network capture and analyser tool to see what's happening in your network. Wireshark will be handy to investigate network related incident.

Network Miner: Is an interesting forensic analyser for Windows, Linux & MAC OS X to detect OS, hostname, sessions and open ports through packet sniffing.

c. Memory Forensic tools

Magnet RAM Capture: It is used to capture the physical memory of a computer and analyse artifacts in memory. We can export captured memory data in raw format and easily upload into leading analysis tool.

Nmap (Network Mapper): Is one of the most popular networks and security auditing tool. It is one of the open source tool.

RAM Capturer: Is a free tool to dump the data from computer's volatile memory. It is compatible with Window's operating system. Memory dumps may contain encrypted volume's password and login credentials for webmails and social network services.

Bulk Extractor: The tool ignores the file system structure, so it is faster than other available similar kinds of tools. It is basically used by intelligence and law enforcement agencies in solving cybercrimes.

d. Web Page Forensic Tool

FAW(Forensic Acquisition of Websites)- is to acquire web pages for forensic investigation which has the following features: Capture the entire or partial page; Capture all types of image; Capture HTML

source code of the web page and integrate with Wireshark

HashMyFiles: This forensic tool assists to calculate the MD5[4] and SHA1[5] hashes. It works on almost latest windows.

e. USB Drives Forensic Tool

USB Write Blocker: USB Write blocker has the capability to view the USB drivers without making any changes to the content.

f. Multimedia Forensic Tool :
NFI Defraser: NFI Defraser forensic tool helps to look at the evidence from the multimedia files.

g. Meta Information Forensic Tool :
ExifTool: Has the capability to do manipulation on metadata information.

h. Browser History Forensic Tool:
This tool helps to capture and view the browser history.

1. Browser history capture: Capture web browser history on Windows OS
2. Browser history viewer: Captures the history on modern browsers.

i. Mobile phone Forensic Tool:
Mobile phone forensic tool helps to capture evidence from mobile phone.

j. Others

- **Forensic Investigator:** If you are using Splunk, then Forensic investigator will be a very handy tool.
- **Hex Editor Neo**: is a basic hex editor that was designed to handle large files. It is used widely for loading large files and performing actions such as manual data carving, low level file editing, searching for hidden data, etc.

k. Based on the Platform

1. SIFT: (SANs Investigative Forensic Toolkit): Most popular open-source platform.
2. Dumpzilla: Popular platform when FireFox and SeaMonkey are used as browser.
3. Paladin: Most popular Linux Forensic suite
4. Coroner's Toolkit: Used when Unix-based operating systems are used.
5. CAINE (Computer Aided Investigate Environment): Is LINUX distribution software, and provides the complete forensic platform with more than eighty tools for analysis.
6. Windowscope: Analyses the Windows Kernel, drivers, DLLs, virtual and physical memory.
7. Xplico: Is an Open Source Network Forensic Analysis Tool (NFAT) widely used for extracting data from internal traffic. . Features include support for multitude of protocols and the ability to output data to a MySQL, or SQLite database, etc.

A comparison of the select popular tools is mentioned in the Table 2.0. These tools are based on the category of

Tool	Platform	Capability	Reporting/ Presentation	Tool Support
CAINE	Open Source Platform	Helps the investigator to obtain reliable data	GUI and Command Line	Provides tools such as Sleuth Kit, Autopsy, Wireshark, Photorec, etc. The

				software can operate on data storage objects.
AUTOPSY	GUI Based Program that helps to analyse hard drives and smart phones	Image details, Metadata analysis	Extensive reporting to generate in HTML, XLS file format	Used by corporate examiners, military to investigate.
SIFT	Open Source and available to Internet	Provides tools for file systems, memory and network investigations	Provides dashboards with real-time analytics	Key tool during incident response helping incident responders identify advanced threat groups.
Xplico	Free and open-source software	Handles data from probes or packet sniffer, Protocol dissector for decoding of individual protocol.	Results are presented in an easy to understand web interface. Great job in analysing and presenting information in colourful graphs and tables in a web interface.	Is installed by default in the major distributions of digital forensics.
Encrypted Disk Detector	Free program	Supports TrueCrypt, PGP, BitLocker, SafeBoot encrypted volume	Generates a screen indicating physical disks,	Useful during incident response and checks the physical drives of the system for TrueCrypt, PGP or BitLocker encrypted volumes.

Table 2.0: Comparison of popular Forensic Tools

Possible mechanisms of prevention of ecommerce fraud

Provide procedures and guidelines for transaction: Providing procedures to identify genuine websites, guidelines to conduct business.

Establish anti-fraud Policies and Procedures: Having policies and procedures for sales, online payments, shipping, sales returns, Customer detail verification, and Merchant detail verification must be included in the policies

Establishing Monitoring Mechanisms: Organization must have dedicated in-house team or third party service provider which does research on fraud and communicate the same to the organization. Having whistle blower hotlines, internal audit reviews, etc. helps to monitor the fraud effectively.

Training: Employees need to be given training to do business ethically. Training on investigating and detecting fraud is also important.

Cloud computing is gaining importance in digital economy. While most of the organizations have stringent policies for the safeguard of information, all cloud service providers must take care of these issues. To mitigate cloud computing risks, companies need to have the following guidelines

- Developing an enterprise cloud solution in coherence with the company's own policies.
- Establishing a dedicated team with the responsibility of security management.
- Deploying the use of cloud services only for approved data projections.

One of the most common problem of using the social media is that of data disclosures. This include sharing confidential information such as client information, Financial Plan, Business Plan, Private employee related matters, etc. Social media initiated frauds in certain data sensitive industries can be taken care by the following means:

- Allowing the employees use social media in the office-hours as a part of role in the company
- Establishing a general policy and guidelines about security of data related information
- Auditing Mechanism

When the employees are in the verge of leaving the company, asked to limit the interaction with the third party to prevent any misuse of information.

Discussion

Majority of the organizations use at least one tool and usage of one tool eases the way of handling the courts evidence. The usage of an integrated tool allows ease of transfer of digital evidence. Whenever you use an integrated software, the data can be shared across the applications, which makes drawing inference quite easy. However, some of the investigations require certain evidence which may require specialised tools. Whenever going for an integrated software, standard software were preferred than non-standard or custom software. . The benefit of standard software were easier to admit, capabilities of packages were well known, to mention the major few. Previous researchers indicate legal factors such as nonrepudiation, verification and repeatability to be considered for tool selection. But increasing usage of cloud computing indicates the popularity of services such as software as service (SaaS) and infrastructure as service (IaaS). This storage in virtualised environment presents some unique challenges when forensic tool selection is considered.

Scope of Further Study

The present study has limitations based on factors considered for selection. The study can be further extended to studying more factors which will be considered for selecting the appropriate forensic tool. Legal factors such as nonrepudiation, verification and repeatability can be considered for further study.

Conclusion

Forensic tool helps in accomplishing the systematic search for evidence. As users become digitally savvy, the digital forensic tools need to become more sophisticated. Hence, the outcome of the paper is to develop the phases of forensic investigation and to find the variety of tools as well as to know about select digital forensic software .One of the main outputs of this paper is the comparison of the select forensic tools. This paper attempts to improve upon existing model of digital forensic process while making a comparison with the appropriate parameters.

Bibliography

[1] Deloitte India Fraud Survey Edition 1, December 20142010, October),

[2] Azimuddin Khan and Zakir Hussain Mansuri, (2018, January-February), International Journal of Advanced Research in Computer Science, Comparative Study of Various Digital Forensic Logical acquisition tools for android smartphone's internal memory : A case study of Samsung Galaxy S5 and S6, Vol 9, No 1, pp 356-369.

[3] Dragan Ranđelović , Dragan Stojković( ), Possibilities of Autopsy Tool Use for Forensic Purposes, Journal of Criminalistics and Law, UDC: 343.983:004

[4] Kara Nance, Daniel J Ryan (2011), Legal aspects of digital Forensics, Proceedings of the 44th Hawaii International conferecnec on System Sciences-2011

[5] Mark Reith, Clint Carr, Gregg Gunsch(Fall 2002), " An Examination of Digital Forensic Models", International Journal of Digital Evidence, Volume 1, Issue 3

[6] Rory V. O'Connor(2005), Software selection: towards an understanding of Forensic software tool selection in indusrial practice, Int. J. Technology, Policy and Management , Volume 5, Number 4.

[7] Sriram Raghavan(2013, March), Digital Forensic Research : Current State of the Art, CSIT 1(!):91-114

[8] Vasileios Vlachos, Marilena Minou, Vasillis Assimakopouous and Androniki Toska(2010, October), The landscape of cyercrime in Greece, www.emeraldinsight.com.

[9] http://cybersecurity.jhigh.co.uk/digitalForensics/phasesOfInvestigation.html

[10] https://h11dfs.com/the-best-open-source-digital-forensic-tools

[11] https://www.iso.org/standard/44407.html

[12] https://linuxhint.com/sans_investigative_forensics_toolkit/

[13] ttps://geekflare.com/forensic-investigation-tools/#anchor-encrypted-disk-detector

[14] https://en.wikipedia.org/wiki/Xplico

[15] Report(2018), PwC India, propelling India towards global leadership in e-Commerce https://www.pwc.in/research-insights/2018/propelling-india-towards-global-leadership-in-e-commerce.html

[16] http://www.ibef.org

Reading Reference

[1] TrueCrypt: Is a source available utility used for o-the-fly- encryption. It can create a virtual encrypted disk within a file or encrypt a partition or the whole storage device.

[2] PGP: Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication.

[3] BitLocker: Is designed to protect data by providing encryption for entire volumes.

[4] MD5: MD5 in cryptography is a Message digest Algorithm is a cryptographic hash function producing a 128 bit hash value.

[5] SHA1: SHA-1(Secure Hash Algorithm1) is a cryptographic hash function which taken an input and produces a 160-bit hash value known as a message digest.