Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 1 (2024)

Cybercrime Investigator: - A Comprehensive Resource in Crime Scene Investigation and Litigation

[1]K. Prabhu Rajasekar, [2]Dr.D.Vezhaventhan

[1]Research Scholar, Saveetha University (SIMATS DEEMED UNIVERSITY), Chennai, India, School of Law, Specialization: Cyber Crime and Cyber Law, PhD Registration Number with University: 162003102, Research Period: June 2020 – May 2024,

[2]M.A.,M.Phil,PhD

Associate Professor anf Headm Department of Humanities and Social Sciencesm Sveetha Schoolof Lawm SINATS, Chennai,

Abstract:- This research paper discusses about the professionalism of a cybercrime investigator as a subject matter expert in the domain of legal investigation who is solely accountable for detecting, combating crimes. He plays a predominant role in recognizing and apprehending the cybercrimes, compiling evidence and assisting in the prosecution of the offenders. A Cybercrime detective ought to have expert technical competency in the domain of cyberspace, an insightful analysis of perpetrator deducing strategies, updated emerging e-threats, innovative technologies, and connect with the legal regulation pertaining to modus operandi. Cyber Crime Investigator should employ legally accepted techniques, devices for tracing digital footprints, analysing data, and reconstructing the series of events associated with cybercrimes. A wide range of crimes are being investigated, which includes hacking, identity fraud, online scams, malware assaults, phishing scams, and data spills. A professional investigator needs to be aware of the introspection, and it should be in a deliberate mechanism acceptable in the court of law. There is no such defined structure or a specific investigation framework for detecting, but they have to follow certain essential features like fundamental and significant concepts, legal rules and processes while investigating. Intelligence tests are notoriously an imprecise endeavour, generally executed in response to unforeseeable situations and there are still emerging events with insufficient knowledge to guide the process. Cyberespionage, e-terrorism, Social Engineering frauds, etc are booming Cyber Crimes where an investigator needs to connect the facts of the case, laws, and evidences to substantiate a case with prima facie by converting all technical evidences, audit evidences and other testimonial evidences in a forensically sound manner, acceptable in a court of law for a prosecution, verdict, remedial and getting relief measures. The detectives of cybercrime cases should implement both reactive measure as a corrective control, once a crime has already triggered and there is a intent effect , with the inputs, watchwords, or modus operandi from reactive threat as well as work on threat hunting, as a proactive approach to detect emerging threats before an incident happens implementing a deterrent control, preventing control and compensatory controls as a Forensic Scientist to invent as many controls as a protection in-depth mechanism.

Keywords*: Digital forensics, Evidence collection, cyber-crime, Forensic investigation, Investigative Forensic Journalism*

1. Introduction

Cybercrime detectives use their skill on the hardware, computer programs and cyberspace to track down and explore digital foot prints left by e-criminals. Usually they coordinate with law enforcement professionals for gathering evidence, interview the beholders, and prosecute offenders. Their profession requires professionalism

in artificial intelligence, data analytics, cybersecurity, and lawful procedures. Cybercrime detectives ought to be updated with the latest electronic gadgets and strategy for detecting, and they should also find out the mechanism adopted by e-criminals in order to efficaciously avert and discover cybercrimes. Detectives on cybercrime investigation make use of manual human intellect, open source intelligence (OSINT), vendor-paid tools along with their critical thinking and innovative skills. Their ultimate motto is to understand the facts of the case, the modus operandi of the crime execution, and the Mensrea of the crime. Based on the evidential facts, the cybercrime detective gets under way with an interview to collect preliminary data in a deep dive to consolidate all technical evidential proof that is forensically sound in a court of law. Cybercrime detectives has to relate the facts of the case, digital evidence, and law together and prepare a forensic report with a Chain of Custody, a chain of evidence, and a master copy, working copy of all witnesses with hash values to prove the confidentiality, integrity, and availability (CIA) triad.

Problem Area: Lack of tools, techniques, investigation procedure, framework, policies and skill of a cybercrime investigator as a Tech Lawyer in the Cyber Litigation.

Proposed Solution: Tech lawyers ought to be technically educated with forensic skills, intelligence, technologically and legally sound as a subject matter expert. Therefore, all the educational institutions for cybercrime courses have to frame a practical-oriented new education policy to create proficient tech lawyers and produce skilled resources, who should be proficient in manual research, trained in open source intelligence for cost-effectiveness and work with open source AI/ML model skills like Chat GPT for building an effective approach to handle Cyber Crime cases.

Research question

What are the skills as a Cyber Crime Investigator is the need of the hour to be developed to handle effective cyber investigation, litigation in building a substantial evidence?

2. Research objectives

i. What sort of competencies are required as a Cyber Crime investigator in order to handle cybercrime cases?
i. What are the prospective research directions and management consequences in the area of cybercrime and examination techniques for handling the current requirement?
ii. How can a Nation build skilled Cyber Crime Investigator to meet the market need?
iii. How could have been the challenges associated with handling Cyber Crime Cases for a successful prosecution and conviction?
iv. What are the cyber security issues in the Cyber Space universally where there no UNCITRAL model of laws and policies implemented to regulate cybercrime from investigators view?
v. How to evaluate the competencies required for a skilful cybercrime detective in a nation to determine the future paths by continuous research in the area of cybercrime detective techniques?
vi. How to implement legal measures against cybercriminals by the investigator?
vii. How a nation needs to build a mechanism or framework in investigation techniques with good infrastructure in LEA, Judiciary in collecting electronic devices evidences suing tools and techniques for detecting the cybercrime?
viii. How to research the difficulties in detecting, prosecuting, and preventing cybercrime that causes potential impact on intellectual property infringements, Financial Thefts and other damages?
ix. How a nation needs to lay-out various controls as a layer of defense, defense in depth mechanism to control cybercrime by an investigator?

3. Cybercrime in The Current Era

Cybercrime is a perpetrator action that involves an electronic data processor, cyberspace, and other gadgets example like electronic device could be employed as an object to assault another device, such as through hacking, SQL injection, distributed denial-of-service attacks, etc. or as a tool to further real-world-based crimes such as violations of intellectual property rights, child pornography, financial frauds, etc for financial gain. Cybercrime probing involves tracking down the perpetrators of the digital crime and acquiring knowledge about their true

objectives by detecting, assessing, and retrieving cardinal cyber forensic evidence from the attacked network, which might be the cyberspace or a local area network. Information system experts who are conversant with not just software programs, application software, and operating systems but also cyber forensic skills, digital security and laws knowledge are required for investigating cybercrimes. They ought to be competent to figure out how these components interact in order to acquire a complete view of what happened, why it occurred, when it occurred, who committed it, and how people can safeguard themselves from future cyber-attacks.

Categories of Cybercrime

Cybercrime investigation falls under three main categories: property, individual and government. The types of strategy used and the challenges vary contingent on the category.

Property: it is identical to the actual occurrence where by the delinquent possess details of a person's bank account and plastic money. The cyberpunk pilfers an individual's account details for monetary benefits, making online purchases, fraudulently getting their accounting details. They make use of malevolent application program for gaining access to websites possessing confidential details. Crimes against property refers the occurrence of the online offence against property by making use of the information system and electronic gadgets.

.**Individual**:

This category of cybercrime involves on individual's by distributing malicious or illegal information online. This can include cyberstalking, distributing pornography and trafficking. These crimes include cyber harassment and stalking, distribution of child pornography, credit card fraud, human trafficking, spoofing, identity theft, and online libel or slander.

Government: This is the least common cybercrime but the most serious offense if the crime is committed against the government it is treated as an attack on Nation's sovereignty.it is also termed as cyber terrorism, which includes cybernetic war, digital terrorism, warez and so on. They hack the databases of the government and defense forces for terrorism purpose.

Lack Of Skills For A Cybercrime Cases And Its Potential Impact

1. Lack of technical, technological skills causes an investigator to delay in understanding the background of the case, deriving the modus operandi, Mensrea in the case, etc

2. Without knowing digital devices and methodologies, it will be impossible to substantiate a case, which will disprove Primafacie.

3. Skills in networking with Law enforcement agencies and processes will lead to failure in filing a PC and converting it to a FIR.

4. Lack of legal provisions will lead to failure in connecting evidence to the facts of the case, which will jeopardize the prosecution and lead to failure in conviction.

5. Lack of forensic science knowledge will lead to all evidence being rejected in court.

6. There should be proper preventive controls, Detective Controls, Deterrent Controls, Compensatory Controls along with Corrective Controls like Technical Corrective Control, Administrative Corrective Control, Remedial Corrective Controls. This will have a checks and balances on the ongoing cyber crime and evade the bad actors from the Cyber Space.

7. Since Cyber Crimes are borderless there are lots of Jurisdictional Challenges. An expert cyber crime investigator apart from Forensics on the lawful aspects have to understand connecting Global Law enforcement Agencies, Global Judiciary and Global laws like Comparative laws, Transnational Laws, Antitrust, Competition laws, International Arbitration and other national, international laws.

8. Most of the times the crime perpetrators are remote and unknown. As a detective one has to invent author talents like psychology to judgementally figure out, perform examination with results to prove the evidence factually.

9. In many situations there is a possibility for the non-availability of tools, techniques, where a detective has to figure-out on work-arounds to get the evidence. Primary evidences like Direct Evidence / Oral evidence, Material evidence, Document evidence could not be gathered easily in a Cyber Crime cases. At that point time they have to rely on a circumstantial evidence which needs to be linked with other primary evidences to factually prove the case.

10. When the evidences gathered are unable to be factually proven as a Primary evidence then connect with the fact of the case to prove the Primafacie.

Investigating A Cyber Crime

Mastering the art of being a cybercrime investigator is a difficult task, mainly because of its dynamic nature. The investigators have to make use of a wide variety of approaches for the investigation. Cybercrime detection is a procedural method of investigating, examining, and retrieving the investigated data for cyber forensics of a crime. The two general categories of cybernetic investigations are digital forensics and open-source intelligence. The detectives must determine the gadgets to be used and predict how efficiently these tools and methods will work out. The investigative discipline of cyber forensics can provide evidential analysis to support a proactive or reactive cyber-attack. Forensic investigators ought to be trained to safely protect and examine data found on connected devices and in cyberspace, often identifying the root cause of the incident and the type of evidence recognized. Investigative tools are programs and gadgets used by investigators for collecting and analysing evidence. In this day and age, investigative gadgets generally refer to programs and other technologies. Corporate investigators make use of investigative gadgets to streamline and simplify the methods of investigations. Investigators use different methods of examination in different circumstances. These methodologies include (in no particular order) fair testing, recognizing and classifying, modelling, pattern seeking, and researching.

1. The tasks performed by cybercrime investigators include: A cybercrime investigator works at the intersection of electronic information security and criminal law. The work of a cybercrime investigator starts with evidence gathering from electronic systems that can be used in the prosecution of internet-based, or cyberspace-based, offenses. Cybercrime detectives primarily focus on social responsibility, preferably they would like to have propitious outcomes. They also tend to have high qualities like honesty, sincerity, impartiality, receptiveness, curiosity, creativity and insightfulness.

2. The investigative mindset can be broken down into five principles:

i. Understanding the source of the material

ii. Planning and preparation

iii. Examination

iv. Recording and collation.

v. Evaluation.

3. **Investigation Tools:** Investigative tools are software, tools, techniques and devices that investigators use to gather and analyse evidence. Corporate detectives prefer to use forensic toolkit for streamlining and simplifying their inquiry. if the investigations are handled efficiently and effectively then reaching the end result can be made swiftly, which in turn helps the organization to take precise and constructive curative action.

4. Data crunching leads to different phases from different perspectives, and finally, along with all the evidence, it identifies the perpetrators. For executing a cybercrime investigation, the investigators should possess certain specialized, updated skills, and well-organized tools and techniques. The IT Act, 2000 has come up with

certain provisions of the Criminal Procedure Code and the Evidence Act, to meet the need for cybercrime investigation, certain new ordinances have been enforced by IIS.

5. Who can investigate: Section 78 of the IT Act 2000 states that the authoritative power to detect cybercrime criminals involves a process of events. The investigator identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques. According to crpc,1973 police officer not below the rank of inspector has the right to investigate any crime.

4. Cybercrime Investigation Techniques

To solve a case, an investigation agency should have the proper technique to find the culprit. While keeping this under consideration, cybercrime investigation agencies have formed the following procedure:

1. Response and reservation**:** After getting a scam complaint, the first and foremost task of cyber investigators is to reach and reserve the digital devices involved in the crime. It is necessary to do so because there is a possibility of mishandling or loss of information.

2. Information gathering**:** After acquiring the mechanism gadgets, detectives investigate further and strive to explore as much witness as they can. In this way, they can picture the crime clearly and make a path for solving it.

3. Security**:** cyberspace gadget is usually used for hacking, detectives gather all the evidence and store it in a secured place so that it can be protected and there by altering of the evidence can be avoided.

4. Data analysis**:** After collecting all the data, the agency will investigate and examine the collected facts and figures for reducing the important details from them. They do it by using specialized tools for cybercrime investigation.

5. Investigation and finding**:** Data analysis leads to suspects, who lead the investigation forward. After scrutinizing, the examination further leads to the delinquency.

6. **Investigating a Crime Scene:** Most cybercrimes are subject to various standardized detection approaches. These approaches are as follows:

a) Assessing the background of the case

b) Information gathering through interviews

c) Social Engineering and Social Networking

d) Identifying bad actor, Person of Interest artefacts

e) Manual examination through Search Engines, tools, techniques

f) Cross examination through open source, AI/ML model tools

g) Digital Forensic -Data Acquisition, Chain of custody, Master copy, Working Copy of evidence collection with hash value to reproduce the evidence in a court of law.

Cybercrime Investigator Laboratory

Crime laboratories play a pivotal role in solving all civil and criminal cases. The essential function of this lab is to deliver an unprejudiced technical suggestion on the various evidential facts and figures provided by the detecting agencies, which in turn helps the judiciary. All the evidence gathered by investigators ought to be lawful. Before preparing a forensic report, the cybercrime investigators must counterespionage the crime with respect to the act. After getting approval from LEA and an order from the judiciary, enumeration can be processed. The cybercrime investigators should make use of controlled environment information technologies like a VPN, virtual machines, and antivirus. The lab has to be free from pollution. All approved open source tools can be used, but specifications have to be provided regarding the tools and methodologies used for each purpose, and the cross verification in manual analysis has to be a true positive.

Forensic Tools For Cybercrime Investigation

Based on the methods employed and the stages, some of the major forensic tools and techniques are as follows:

1. Manual Examination and Analysis – This is just reconnaissance and collecting, available evidences through manual analysis using human intelligence and minor tools like search engines like google chrome, Mozilla firefox and other web-browser search engines with key word searches.

2. Open Source Tools and Techniques which are approved tools and techniques available openly for intelligence and analysis.

3. Vendor AI/ML Expert Systems as a Software-as-a-Service (SaaS) which are paid tools and techniques which has a faster approach but produces high false positives which needs to be evaluated through thorough examination.

Types Of Cybercrime Investigators

There are several types of cybercrime investigators, each with their own unique specialization and focus. Here are some of the common types of cybercrime investigators:

a. Law Enforcement Cybercrime Investigators

b. Corporate Cybercrime Investigators

c. Computer forensic investigators

d. Cybersecurity Investigators

e. Cyber Threat Intelligence Investigators

Stages Of Evidence Collection In Cybercrime Investigation

1. Systematic approach of collecting evidence by conducting interview to collect preliminary information with all synergy of questions framing with 5W and 1H (Why, When, What, Where, Who, How). Human intelligence through reconnaissance, manual research, interviews, and interrogations using various interview techniques like the Wicklander Zuwalski interview method, the PEACE interview method, and the RAID interview technique, which are close to their purpose.
2. Perform analytical approach to derive the cause of action or fact of the case by studying the fact of the case, modus operandi, mens rea, at the first level from data trends and patterns. An analytical approach for identifying the trends and patterns of a crime after data aggregation, data engineering, and data correlations, provided statistical tools and techniques.
3. Perform Risk Management Framework and Integrated Auditing Approach for further collection of audit evidence that proves the Mens Rea, Potential Impact, Damage, Loss, Financial Theft, Loss, Issue, Problem, Root Cause of the Issue, and solution with respect to GRC.
4. Historical Approach of evidence collection where they use appropriate vendor SaaS-based AI/ML-driven tools to collect as much evidence as possible in digital footprints and eDiscovery in a faster, more complete way. Use of open-source tools and techniques to cross-verify, eliminating false positives, True negatives, and false negatives and capture only true positives. Technical intelligence has two parts like one is Open source intelligence as manual research in cyberspace and the second one is Cyber threat intelligence using open-source tools or vendor AI/ML model tools. Cross examination of manual research from open source intelligence, open source tool output, and vendor tool output needs to be performed for hunting true positives. Applying the analytic approach again to eliminate false positives (wrongly accepted) and false negatives (wrongly rejected) and focus on true positives (rightly accepted) and true negatives (rightly rejected) through a cross-examination for maintaining the cross-over error rate.
5. With all the evidence gathered, filing for law enforcement actions like police complaint, file FIR, and confirm the crime after Law enforcement interrogation proving Primafacie and take legal action to next level of filing a charge sheet for court prosecution and conviction.

6. Prepare a detailed cybercrime report in a forensic investigative journalism approach to have all fraud investigations, digital forensics, technical intelligence, and case briefs to be narrated.
7. Evidence gathered have to be in the form of a master copy and a working copy having a hash value generated from where the evidence was gathered with timestamp showing CIA Triad of Cyber Security.
8. Chain of Custody with information on the person who collected evidence, timestamp, geolocation, and status of evidence before, during, and after collecting, chain of evidence for tracking the order in which evidence is acquired.
9. All evidences should be in line with Indian Evidence Act, Section 65B to be forensically and legally sound.
10. Risk Management Framework in a Monte Corlo approach measures both qualitatively with scenario-based questions, answers and qualitatively with risk calculation applying formulas to study risk assessment in a cybercrime case to indicate as a Key Risk Identifier (KRI) and measure Key Performance Indicator (KPI) by maintaining a periodic audit and building a risk register. Information technology auditing is the process of identifying risks. Hence, forensic auditing is an important step for risk mitigation. They need to follow an integrated auditing process that comprises technical audits, process audits, operational audits, functional audits, discovery audits, and other special audits, and perform reliability testing. In a qualitative approach, set up a risk appetite, risk capacity, and risk tolerance level. Based on that, the risk is measured using formulas to decide whether it is accepted, transferred, or mitigated.

Required Skills For A Cybercrime Investigator

1. The cybercrime investigator should have a thorough understanding of business operations, functions and understand the facts of the case thoroughly.
2. In cybercrime, there is mostly intellectual property damage and financial loss for the financial benefit of the bad actors. A cybercrime investigator should have a thorough understanding of banking and fintech transactions.
3. Information technology infrastructure, landscape configuration and functionality in a technology, business data functioning inside applications, integration of various applications, data flow, and data structure in a database knowledge is a must.
4. A cybercrime investigator should possess expert data analytics knowledge to study the current trends, patterns and future impacts of cybercrime.
5. A cybercrime investigator should have updated knowledge in different fields such as data science, artificial intelligence, and machine learning, as well as expert systems skills for measuring key risk indicators and key performance indicators.
6. Good understanding of information technology and sound technical skills in various tools, techniques, open source, other alternatives, and manual methods
7. Good knowledge of all Legal Provisions from National Laws, International Laws, UNCITRAL model of laws, the TRIPS agreement, conventions, treaties, transnational laws, comparative laws, antitrust laws, competition laws, international arbitration, trade laws, IT Acts, IP Laws, and data protection laws
8. Forensics Science knowledge like Fingerprints, Biometrics, Hand Geometry, Voice, Audio, Video, Iris, Retina, Multimedia Forensics, Chip of Forensics, Cloud Forensics, Application Forensics, IoT Forensics, Database Forensics, and Other Digital Forensics and the various tools for collecting evidence is also vital.
9. Good understanding of various functions of all Law enforcement agencies, National and International Law enforcement agencies, the judiciary, the UN Functions is required. Also, to build Person of Contacts network, approaching methods, and building a mechanism to report, track, and execute an issue from end to end until resolving is required for an investigator.
10. Good understanding of all psychological factors affecting an individual, society, organization, and government is mandatory, as is the ability to work in a multi-jurisdictional or cross-jurisdictional environment.
11. Forensics Investigative journalism writing skills with data, narrative writing skills with multimedia skills in presenting with data analytics having visualization in all documents in a triangular way of writing with Bottom line up front (BLUF) method.

12. Good understanding of all cyber litigation processes, expert witness requirements, and processes.
13. Cybersecurity skills to analyse corrective controls, preventive controls, deterrent controls and, compensatory controls.
14. Thorough understanding of industrial regulations like governance, risk, compliance, integrated auditing, reliability testing, and data protection impact assessments.
15. Knowledge in threat intelligence is a reactive investigation that works as a detection system after an incident has been triggered.
16. Knowledge in threat hunting to covert reactive inputs to a proactive investigation that acts as a preventive and deterrent control based on the Threat Modelling Framework with the watchwords of use cases, modus operandi, current ongoing cybercrimes and social engineering fraud threat feeds to be automated into threat hunting.
17. Threat Research acts as a corrective control with technical corrective control in applying security controls, bugs, fixes, patches in applications, infrastructure, cloud, databases, networks, hardware, software. Administrative corrective control in reviewing governance, risks, compliance, and performing forensic auditing. Remedial corrective control, which works like a deterrent control; and compensatory controls.
18. Internal investigations inside an industry are mostly about theft, pilferage, and process of non-compliance by employees in supply chain risk management, manufacturing logistics, data warehouses, and transportation, under the roof and out on the roads, as part of business operations or within a organization or Nation by insider threats called espionage.
19. External investigations are mostly related to fraud via social media, messaging channel platforms, the surface web, deep web, dark web, blogs, forums, fake websites, phishing emails, vishing, cross site requests, cross site content forgery, etc performed by external agent sabotage.

Duties And Responsibilities Of Tech Lawyers And Cybercrime Investigators

The duties and responsibilities of a cybercrime investigator are not static in nature; they vary depending upon the organization for which they are working and the nature of the digital threats they investigate. Here are some of the common duties and responsibilities of a cybercrime investigator:

- Conducting investigations
- Conducting forensic analysis
- Developing investigative strategies
- Working with law enforcement agencies
- Testifying in court
- Providing training and education
- Staying up-to-date with the latest technologies and techniques

Forensics Report Writing

In a cybercrime investigation, which has sequence of activities like threat hunting, threat intelligence, and threat research which must be done simultaneously with gathering audit evidence. Forensics report writing should be in the form of investigative forensic journalism with a synergy of questions in 5W and 1H with data, conclusive writing, visualization, and presentation discussing both hard news and soft news in the forensics report, connecting the facts of the case with law and evidence. A typical digital forensics investigation report for a cybercrime case would have the following:

1. Fact of the case with argumentative data, narrative in active voice, and the facts placed in a sequential order with facts, law, and evidence connected and illustrated.

2. Modus Operandi (Tactics, Techniques, and Procedures) to be traceable from the facts of the case. The source of origin, channel of attack, and workflow of attack are to be illustrated in the modus operandi.

3. Parties to the case—victim and person of interest—and the victim's complaint proof are to be given clearly in the cybercrime investigation report.

4. Mens Rea (Guilty Intention, Potential Damage, Loss, Financial Theft, Breach, Infringement, etc.) and Cause of Action should be derivable from the facts of the case.

5. Primafacie has to be in the form of a substantial evidence beyond reasonable doubt connecting the circumstantial evidence and factually proving as a primary evidence is essential in Cyber Crime Investigation report, arranging all screen shots arranged in sequential order and refer in the Cybercrime Report wherever necessary.

6. Remediation connecting fact, law and evidence to specify the Relief and Punishment, to be illustrated in the conclusion, recommendation and suggestion.

5. Conclusion

Investigations today may look very different than they did 10 years ago, but good investigators learn how to adapt. By employing high-level investigative techniques and innovative investigative tools, they can perform more efficient and effective investigations and protect the society from cybercrimes. Cybercrime is a massive threat to any country. It has the threatening potential to trigger national unrest, financial crisis, the shutdown of services, etc. In 2022 alone India witnessed a whopping number of 13.91 lakhs registered cybercrimes. These cybercrimes adversely affect the lives of thousands of innocent individuals, companies, and governments. Also, several cyber-attack cases go unreported due to a lack of awareness or infrastructure. Thus, a Cyber Crime Investigator has to play a multi-facet role “Jack of All Trades master none rather than mastering one” need to understand business, Technology, possess technical skills and convert all technical screen shots, logs, traces in a forensic sound manner with a Forensic Investigation report in a Law enforcement and judiciary understandable, acceptable terms which is acceptable in a court of law. It has been observed that due to lack of knowledge and advancements, cyber wings in India are struggling while combating with cybercrimes, this paper presented some issue which should be focused on while dealing with computers crimes and evidences, which will help the investigating authority to upgrade against present scenario. Legal profession is an integrated profession of multiple skills and that too, as a Cybercrime investigator, the required skill should be above the par with lots of learning, innovations and critical thinking skills to mould as a perfect Cyber Law expert in the current trend. University to design Law degree in a CBCS pattern for a Cybercrime Lawyer with required skills and syllabus to meet the needs. Cross functional training post LLB for a year to be in the Government Forensic Laboratory, Courts, Law enforcement agencies as a compulsory one-year internship program. Good Technologies and infrastructure in a Government particularly in LEA and Judiciary which helps to implement strong corrective controls like Technical corrective control, Administrative corrective control, Remedial corrective control and also implement on compensatory controls, deterrent controls there by tracking the cause of action easily.

References

[1] Crime in India 2015 Statistics. – National Crime Record Bureau (NCRB)
[2] Cybercrime – a growing challenge for government. - July 2014
[3] Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations
[4] H. Marshall Jarrett Director, EOUSA. Michael W. Bailie Director, OLE
[5] ACPO computer evidences and guidelines. (www.acpo.police.uk)
[6] Baggili et al, 2007 Ibrahim M. Baggili, Richard Mislan, Marcus Rogers, “Mobile Phone Forensics Tool Testing: A Database Driven Approach”, International Journal of Digital Evidence Fall 2007, Vol. 6, Issue 2 [7]. Jansen, Ayers, 2006 Wayne Jansen, Rick Ayers, “Forensic Software Tools for Cell Phone Subscriber Identity Modules”, Conference on Digital Forensics, Security and Law, 2006

[7] Marcella, Albert, 2008 Marcella Jr., Albert J., "Cyber Forensics: A Field Manual for Collecting, Examining and Preserving Evidence of Computer Crimes". 2008. Taylor & Francis Group, LLC. Auerbach Publications. pp. 27-48 pp.77-85 pp.87. 118 International Journal of Computer Science, Systems Engineering and Information Technology
[8] https://www.infosecawareness.in/cyber-laws-of-india
[9] https://www.pandasecurity.com/en/mediacenter/panda-security/types-of-cybercrime/
[10] https://cybersecurityguide.org/careers/cyber-crime-investigator/
[11] https://www.business-standard.com/article/technology/the-face-of-indian-cyber-law-in-2013-113123000441_1.html
[12] https://www.statista.com/statistics/309435/india-cyber-crime-it-act/
[13] https://economictimes.indiatimes.com/wealth/personal-finance-news/cyber-criminals-stole-rs-1-2-trillion-from-indians-in-2019 survey/articleshow/75093578.cms#:~:text=Rs%20131.2%20million%20is%20the,the%20global%20average%20being%2067%25
[14] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1599067
[15] Rogers, 2006 Rogers, M. (2006), "DCSA: A Practical Approach to Digital Crime Scene Analysis". West Lafayette, Purdue University
[16] Akazue, M. I., Ojugo, A. A., Yoro, R. E., Malasowe, B. O., & Nwankwo, O. (2022). Empirical evidence of phishing menace among undergraduate smartphone users in selected universities in Nigeria. Indonesian Journal of Electrical Engineering and Computer Science (IJEECS), 28(3), 1756-1765.
[17] Arshad, H., Jantan, A. B., & Abiodun, O. I. (2018). Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence. Journal of Information Processing Systems, 14(2).
[18] Bhatele, K. R. R., Mishra, D. D., Bhatt, H., & Das, K. (2020). The Fundamentals of Digital Forensics and Cyber Law. In Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications (pp. 64-81). IGI Global.
[19] Fernandes, R., Colaco, R. M., Shetty, S., & Moorthy, R. (2020, July). A new era of digital forensics in the form of cloud forensics: a review. In 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 422-427). IEEE.
[20] Greer, B. (2017). The growth of cybercrime in the United States. Growth