iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** X **Month of publication:** October 2020

DOI: https://doi.org/10.22214/ijraset.2020.31865

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue X Oct 2020- Available at www.ijraset.com

A Study of Cybercrimes in India using Digital Forensics

Tanvi Gupta[1], Suruchi Parashar[2], Aju D[3]
[1, 2, 3]*School of Computer Science and Engineering, Vellore Institute of Technology, Vellore*

Abstract: ***Cyber crime is a criminal activity that is done using a computer device or a network. The increasing cyber crime in today's world poses a great threat to Digital Forensics as a branch of study to tackle such problems. Computer forensics is the process that applies computer science and technology to collect and analyze evidence which is crucial and admissible to cyber investigations. Network forensics is used to find out attackers' behaviours and trace them by collecting and analyzing log and status information. A digital forensic investigation is an inquiry into the unfamiliar or questionable activities in the Cyber space. Digital forensics is the science of identifying, extracting, analyzing and presenting the digital evidence that has been stored in the digital devices. Various digital tools and techniques are being used to achieve this.***
The paper aims to deal with a cased named 'Sony.sambandh.com case', one of the first cyber crime convictions in 2013.The case revolves around how cyber crimes are increasing and cannot be solved using normal investigation. This paper deals with different tools for analysing and comparing the evidence and generating results Various work has been carried out in the domain of cyber crime and digital forensics to deal with cybercrimes. It also aims to gather and study various evidences and generate various reports that gives much deeper insights into the case. The various Indian laws pertaining to the case has also been discussed.
Keywords: Digital Forensics, Cybercrime, Indian Laws, Evidence, Forensic tools

I. INTRODUCTION

Cyber crime is a criminal activity that is done using a computer device or a network. The increasing cyber crime in today's world poses a great threat to Digital Forensics as a branch of study to tackle such problems. Computer forensics is the process that applies computer science and technology to collect and analyze evidence which is crucial and admissible to cyber investigations. Network forensics is used to find out attackers' behaviours and trace them by collecting and analyzing log and status information. A digital forensic investigation is an inquiry into the unfamiliar or questionable activities in the Cyber space. Digital forensics is the science of identifying, extracting, analyzing and presenting the digital evidence that has been stored in the digital devices. Various digital tools and techniques are being used to achieve this.

The paper aims to deal with a cased named 'Sony.sambandh.com case', one of the first cyber crime convictions in 2013.The case revolves around how cyber crimes are increasing and cannot be solved using normal investigation. This paper deals with different tools for analysing and comparing the evidence and generating results Various work has been carried out in the domain of cyber crime and digital forensics to deal with cybercrimes. It also aims to gather and study various evidences and generate various reports that gives much deeper insights into the case. The various Indian laws pertaining to the case has also been discussed.

II. LITERATURE SURVEY

This paper deals with temporal sequence of cyber-victimization and traditional victimization. The popularity and perceived popularity as possible antecedents and consequences of cyber-identity thefts and traditional victimization. The sampling of proof comprised 665 early adolescents (356 boys, 309 girls) aged 11.63 (*SD* = 0.84) at Time 1. Data were collected using self- and peer reports. To test for the temporal sequence a cross-lagged panel design was used. Traditional rates of cyber identity theft, popularity and perceived popularity were moderately stable for both boys and girls.[1]

Cyber-Identity Theft was neither stable during a one-year period, nor could it be predicted by traditional victimization, popularity or perceived popularity. Instead, Identity Theft fostered popularity in girls. Thus, the paper describes how the rates of identity theft on a cyber domain keeps increasing and how it is threatening everyone. The fraudulency and the fear of identity theft is growing as people are now getting exposed to the malware and spoofing attacks.

Researchers, in this paper, came across a finding that criminal identity theft can create a myriad of headaches for the victim after the fact [2].

Though a less common form of fraud, a thief could get caught for a traffic violation or a misdemeanour and sign the citation with your name. Then you get stuck paying those annoying fees and fines. If a thief uses your name when getting arrested for a crime, you could end up with a criminal record, which could affect your ability to get a job or buy/rent property. Another case is when the thief commits a crime using your identity, and then a warrant is issued for your arrest. But instead of looking for the criminal, they are looking for you—you could have a warrant out for your arrest and not even know it! The type of information taken during a breach can vary widely depending on what personal info the company has stored, and what the perpetrator is able to access. Sometimes, the types of info stolen can also depend on the purpose of the breach, which could vary from making a political statement to a hacker simply "showing off". Perpetrators that are committing breaches for financial gain generally target personal information that can be resold on the dark web and be used for identity fraud, focusing on info like full names, email addresses, passwords, Social Security number, date of birth and driver's license number to name a few.

In this paper, there were 21 cases of Hacking of computer systems wherein 18 persons were arrested in 2003. Of the total 21 Hacking cases, the cases relating to Loss/Damage of computer resource/utility under Sec 66 of the IT Act were to the tune of 62 percent 13 cases and that related to Hacking under Section 66 of IT Act were 38 percent.[3]

During 2003, a total of 411 cases were registered under IPC Sections as compared to 738 such cases during 2002 thereby reporting a significant decline of 44 percent in 2003 over2002. Andhra Pradesh reported more than half of such cases (218 out of 411) (53 percent). Of the 411 cases registered under IPC, majority of the crimes fall under 3 categories. Criminal Breach of Trust- Fraud, Forgery, Identity Theft and Counterfeiting. Though, these offences fall under the traditional IPC crimes, the cases had the cyber tones Where in computer, Internet or its related aspects were present in the crime and hence they were categorized as Cyber Crimes under IPC.

During 2003, the number of cases under Cyber Crimes relating to Counterfeiting of currency/Stamps stood at 53 wherein 118 persons were arrested during 2003. Of the 47,478 cases reported under Cheating, the Cyber Forgery 89 accounted for 0.2 per cent. Of the total Criminal Breach of Trust cases 13,432, the Cyber frauds 269 accounted for 2 percent.IT professionals need good definitions of cybercrime in order to know when (and what) to report to police, but law enforcement agencies must have statutory definitions of specific crimes in order to charge a criminal with an offense. The first step in specifically defining individual cybercrimes is to sort all the acts that can be considered cybercrimes into organized categories.

This paper talks about the rise and proliferation of newly developed technologies have started to operate many cybercrimes in recent years. Cybercrime has become great threats to mankind. Protection against cybercrime is a vital part for the social, cultural and security aspect of a country. The Government of India has enacted IT Act, 2000 to deal with cybercrimes. The Act further revised the IPC, 1860, the IEA (Indian Evidence Act), 1872, the Bankers Books Evidence Act 1891 and the Reserve Bank of India Act, 1934.[4] Any part of the world cyber crime could originate passing national boundaries over the internet creating both technical and legal complexities of investigating and prosecuting these crimes. The international harmonizing efforts, coordination and co-operation among various nations are required to take action towards cyber crimes. Our main purpose of writing this paper is to spread the content of cyber crime among the common people. At the end of this paper "A brief study on Cyber Crime and Cyber Laws of India" we want to say cyber crimes can never be acknowledged.

According to a new report, no crime is growing faster in the US and India than cybercrime, and it is increasing in size, sophistication, and cost.The "Official 2019 Annual Cybercrime Report," is based on research conducted by Cybersecurity Ventures and sponsored by Herjavec Group , It predicts that cybercrime will cost companies across the world $6 trillion annually by 2021, increasing from $3 trillion in 2015.[5] On the defensive side, the report predicts more than $1 trillion will be spent globally on cybersecurity between 2017 and 2021. It also will require 3.4 million workers by 2021, up from 1 million in 2014. That growth will keep the cybersecurity unemployment rate hovering near 0%, according to the report.

As discussed in this paper, digital forensics plays a significant role in the criminal justice system as we continue to incorporate a range of technologies into our everyday lives. Evidence of all types of crime are increasingly found in digital devices that either the perpetrator or the victim used. As a result of this potential evidence which did not exist in the past, investigators of conventional crimes increasingly need to consider any digital evidence that may be available. In addition, Security professionals routinely use such tools to analyze network intrusions not to convict the attacker but to understand how the perpetrator gained access and to plug the hole. Data recovery firms rely on similar tools to resurrect files from drives that have been inadvertently reformatted or damaged.[6]

The recent advances made in the field of information technological all around the world has made people very tech savvy. People have indulged in over use of the technology and have become highly dependent over it.With such advancements and overuse of the technologies there has been observed a high increase in the number of crimes committed in the internet by people as it is considered

the safest medium of committing a crime due to everything being virtual and there being no personal interaction of the criminal with the victim. Criminals spread viruses which in turn crash other people's computers, steal identities of others and one such incident was the sonysambandh case.[7]

One of the greatest hurdles in the field of Cyber Crime is the absence of comprehensive law throughout the World. Further the immense growth types of attacks and cyber crimes make the situation more complicated. Though a beginning has been made by the enactment of I.T. Act and amendments made to it provide more powers but still problems associated with cyber crimes continue. In this scenario there is a need of understanding Cyber attacks and their Technical specifications by Police/Intelligence Departments and Judges.[8]

In this paper, the authors have tried to focus on basic concepts of cybercrime, cyber laws and some legal issues related to it.Cyber crimes are easy to commit and hard to detect, due to increase in use of computers and internet it is very easy for criminals to commit a crime by using IT resources. Since most of Indian population is not aware about legal issues related with IT, it is very easy for perpetrators to get into their systems and steal their personal information. They also included some of the cybercrime cases in India for better understanding. It is necessary to gear up the efforts to prevent cybercrimes as technology and its related issues are increasing India.[9]

With the coming of the new innovations and the progression in the method of correspondences, the Internet has become another type of life. It is perhaps the quickest method of correspondence and has spread its limbs, covering all potential shades of humankind. Yet, as the platitude goes, "each great side has an awful side as well". The equivalent is valid with PCs, the Internet innovation. The approach of the PC has been an aid to understudies, attorneys, money managers, educators, specialists, scientists and furthermore not to overlook the hoodlums. Today we adventure into the virtual universe of the internet where our security doesn't exist by any means. What you share, in accordance with some basic honesty, can be abused against you.Crimes are not any more restricted to the physical space alone however have gone into the virtual the internet as well. The weapons which are utilized to perpetrate these violations are profoundly refined and as the lawbreakers are consistently out in front of the law masters as they themselves concur, distinguishing these crooks and forestalling their wrongdoings is probably the best test before them.[10]

Change is the essence of life. What seems impeccable and indestructible today might not remain the same tomorrow. Internet, being a global phenomenon is bound to attract many crimes. India has taken a key step in curbing Cyber Crimes by the enactment of the Information Technology Act and by giving exclusive powers to the police and other authorities to tackle such crimes. Similar efforts have been made by various countries to fight this menace by enacting national legislations but in the long run, they may not prove to be as beneficial as desired. An effort is still wanted to formulate an international law on the use of Internet to curb this imminent danger of Cyber Crimes and to achieve a crime free Cyber Space. Prevention they say is the best cure. Cyber laws aim to prevent cyber crimes through the use of penal provisions. A great deal however needs to be done before Cyber laws can stand a fair chance to influence the modern.Michael L. Rustad and Thomas H. Koenig propose a new tort of negligent enablement which will hold software vendors accountable for defective products and services that pave the way for third party cybercriminals who exploit known vulnerabilities. At present, the software industry has externalized the costs of making code safe for its intended environment of use onto its end users through one-sided mass market agreements. The proposed negligent enablement tort fills the void left by the failure of contract law to give meaningful remedies for the unacceptably high levels of risk of computer intrusions due to defective software. The public policy rationale for imposing secondary tort liability on software publishers who aid and abet cybercriminals is to reduce the rate of cybercrime. The proposed negligent enablement tort draws upon well established principles of the Uniform Commercial Code (UCC) Article 2 warranties, premises liability, and negligence-based product liability to construct a modified duty of care to produce safe software suitable for its environment of use. This Article examines the elements of duty, breach, causation, and damages for the proposed negligent enablement tort as well as defenses, procedure, and possible policy-based objections. [11]

Cyber-crime, once the domain of disaffected genius teenagers as portrayed in the movies "War Games" and "Hackers," has grown into a mature and sophisticated threat to the open nature of the Internet. "Cyber-criminals," like their non-virtual traditional criminal counterparts, seek opportunity and are attracted to vacuums in law enforcement. The news media is filled with reports of debilitating denial of service attacks, defaced websites, and new computer viruses worming their way through the nation's computers. However, there are countless other cyber-crimes that are not made public due to private industry's reluctance to publicize its vulnerability and the government's concern for security.' Along with the phenomenal growth of the Internet has come the growth of cyber-crime opportunities. As a result of rapid adoption of the Internet globally, computer crimes include not only hacking and cracking, but now also include extortion, child pornography, money laundering, fraud, software pirating, and corporate espionage, to name a few.

Law enforcement officials have been frustrated by the inability of legislators to keep cyber-crime legislation ahead of the fast-moving technological curve. At the same time, legislators face the need to balance the competing interests between individual rights, such as privacy and free speech, and the need to protect the integrity of the world's public and private networks. Further complicating cyber-crime enforcement is the area of legal jurisdiction. Like pollution control legislation, one country cannot by itself effectively enact laws that comprehensively address the problem of Internet crimes without cooperation from other nations.[12] While the major international organizations, like the Organisation for Economic Co-operation and Development (OECD) and the G-8, are seriously discussing cooperative schemes, many countries do not share the urgency to combat cyber-crime for many reasons, including different values concerning piracy and espionage or the need to address more pressing social problems. These countries, inadvertently or not, present the cyber-criminal with a safe haven to operate. Never before has it been so easy to commit a crime in one jurisdiction while hiding behind the jurisdiction of another.[13]

Online services provide extensive individual and socio-economic benefits to modern society. Online banking has introduced a convenient yet inexpensive and effective way of remotely handling financial transactions, e-commerce has increased product availability while decreasing trading costs and online social networks have deepened personal relationships worldwide. Reviewing the economic growth literature, Cardona et al. show in that information and communication technology increased labor productivity in the EU by at least 31% (33% in the US) since 1995. Brynjolfsson emphasizes the magnitude of the consumer surplus generated by online services, which provides additional social welfare not reflected in the traditional statistics.

To avoid precarious situations, many Internet users remain hesitant to use online services. Such reluctance leads many to miss out on the social and economic benefits provided by an Internet-connected world. Anderson et al. agree that the majority of cybercrime costs are indirect opportunity costs, created by users avoiding online services. Understanding how these costs are formed is a main prerequisite to craft appropriate responses for dealing with a global cybercrime problem. Work on the social effects of cybercrime is still rare, as most studies focus on the criminals' motives and attacks, or propose technical, organizational, and regulatory measures to prevent cybercrime. To fill this gap, we synthesize work from information systems (IS) research and criminology.

The paper devises a model that explains the impact of cybercrime on the avoidance of online services by showing how cybercrime creates perceived risk and how this risk makes users hesitant to use online services. We test our model with a secondary analysis of the 2012 Eurobarometer Cyber Security Report (CSR), a representative pan-European survey on the public perception of cybercrime. We use structural equation modeling to test seven hypotheses for three important online services, namely: online banking, online shopping and online social networking.[14]

This paper examines a predominantly Australian sample of computer crime offenders involved in fraud and/or unauthorized access. This paper focuses on the extent to which offenders are involved in organised crime, the nature of the relationship between co-offending, initiation and knowledge transmission, and how the online environment facilitates organised crime and co-offending. This qualitative analysis draws from interviews with self-identified offenders, law enforcement officers who investigate these offenses, and court documents, providing a unique understanding of organised crime involving computer systems. Due to the hidden nature of the population who engage in offending involving computer systems, it is often unclear to what extent such activities are attributable to organised crime syndicates, sole operators, or other groups. Felson states that criminologists, along with the mainstream media, tend to overstate the extent that commonplace crimes are organised. However, research evidence indicates that computer crime offenders do work and collaborate together to some extent, both on- and offline. Jordan and Taylor suggest that the hacker community is characterised by a fluid, informal and loosely structured membership, with a high 26 turnover. The computer crimes that are considered in this paper are those that compromise data and financial security. These offences affect the public greatly, including the direct cost of victimisation, emotional harm, and associated costs, such as banks passing on losses through higher fees.[15]

Many computer crimes are not reported to authorities, and of the small percentage of computer crimes that are reported, less than 20 per cent are likely to result in criminal charges. Whilst underreporting and under-prosecution may be typical of most crime types, computer crimes are notoriously difficult to bring to prosecution, with problems including inadequate legislation, lack of evidence, and jurisdictional difficulties. Data security – the defending of PC frameworks and the trustworthiness, privacy, and accessibility of the information they contain – has for some time been perceived as a basic public strategy issue. Its significance is developing as the combination of PCs into an ever increasing number of parts of current life proceeds. What's more, cyberattacks, or breaks of data security, give off an impression of being expanding in recurrence, furthermore, few are eager to overlook the likelihood that the seriousness of future assaults could be a lot more noteworthy than what has been seen to date. Examinations concerning the stock value effect of digital assaults show that recognized target firms endure misfortunes of 1%-5% in the days after an assault. For the

normal New York Stock Exchange company, value drops of these extents convert into investor misfortunes of between $50 million and $200 million. [16]

A few PC security counseling firms produce appraisals of aggregate overall misfortunes inferable from infection and worm assaults and to antagonistic advanced acts in general. The 2003 misfortune gauges by these organizations run from $13 billion (worms and infections just) to $226 billion (for all types of clear assaults). The unwavering quality of these gauges is frequently tested; the basic system is essentially recounted.

The protection business' reaction to rising impression of digital danger has been twofold. At first, most organizations barred, and keep on barring, digital assaults rom standard business protection inclusion. After this underlying avoidance, a few safety net providers at that point started selling particular digital danger arrangements. Development of the market has been moderate; coming up short on the exact information to develop actuarial tables, guarantors can't to value hazard with the level of certainty they appreciate in conventional protection lines. Appraisals of the macroeconomic expenses of digital assaults are theoretical. As long as any digital assault is restricted in degree and brief almost certainly, macroeconomic results will be little. In any case, the capacity to recoup rapidly is significant, since the time span PCs are influenced is a significant determinant of the expenses. It might be nearly as significant for firms to deliver their capacities to re-establish tasks as to protect themselves from possible assaults.

BBC NEWS:Losses from online banking fraud rose by 48% in 2014 compared with 2013 as consumers increasingly conducted their financial affairs on the internet. The rise is due to increased use of computer malware and con-artists tricking consumers out of personal details. Business Standard: With the increase in banking on mobile phones and the internet, financial frauds in the system have also seen an uptick, says a survey on financial frauds in the financial sector by Assocham and PwC.

Worldly post: Assocham-Mahindra SSG study has delivered a report expressing the number of digital wrongdoings in India may twofold to 3 lakhs in 2015. India currently being the most loved and simple to focus for cybercriminals, generally programmers, different pernicious clients could present genuine monetary and public security challenges. India has been inclined for all the fraud, spamming, phishing and different sorts of extortion, as there is an upswing use of Smart telephones and tablets for internet banking and other money related exchanges lately.[17]

In this research paper the authors have introduced the concept of frauds related to credit cards and their various types. The authors have explained various techniques available for a fraud detection system such as Support Vector Machine (SVM), Artificial Neural Networks (ANN), Bayesian Network, K- Nearest Neighbour (KNN), Hidden Markov Model, Fuzzy Logic Based System and Decision Trees.[18] An extensive review is done on the existing and proposed models for credit card fraud detection and has done a comparative study on these techniques on the basis of quantitative measurements such as accuracy, detection rate and false alarm rate. This research paper concludes by explaining the drawbacks of existing models and provides a better solution in order to overcome them. From the comparative analysis of the various credit card fraud detection techniques in this research paper it is clear that Artificial Neural Networks performs best. But the drawbacks of Artificial Neural Networks is that they are very expensive to train and can be easily over trained. In order to minimize their expense the authors suggest that there is a need to create a hybrid of neural networks with some optimisation technique. Optimisation techniques that could be successfully paired with Neural Network are Genetic Algorithm, Artificial Immune System, Case Based Reasoning and any other similar optimisation technique. Genetic Algorithm helps by selecting the optimised weight of the edges in the neural network. This research paper provides several views on personal safety and quality of security to payment cars and cyber- attacks. For the purposes of the analysis, the respondents were divided into categories, based on their age, level of education and occupation. The study results can help the issuers of payment cards and banks as well as clients using payment cards, especially in order to improve the prevention against fraud and the unauthorised use of payment cards.[19] Credit card fraud continues to be a significant and dynamic risk to financial institutions as a result of both new threats and the increasing regulatory interest in fraud management programs. Emerging fraud threats and solutions required to mitigate them are increasingly technically complex. To secure and maintain customers' trust, the financial institutions must prevent, detect and respond to fraud risk in an agile manner through fraud management technologies and predictive analytics. While MasterCard and Visa (chip and PIN) technology will help decrease the risk of counterfeit transactions, financial institutions must remain vigilant, as fraudsters will certainly be crafting new modes of attack.

Credit card frauds can take several forms, ranging from petty theft, where the perpetrators tend to use the credit card for smaller purchases, to greater and more sophisticated attacks, where the goal of the criminal is to alter the safety features of the bank card itself. Such cyber frauds are classified as an intentional, illegal attempt at causing an alteration and a distortion of the bank card details.It is therefore important that a new approach, for example an intelligence led approach, be considered in combating card fraud. Credit cards play a very important role in today's economy.

It becomes an unavoidable part of household, business and global activities. Although using credit cards provides enormous benefits when used carefully and responsibly,significant credit and financial damages may be caused by fraudulent activities.

Many techniques have been proposed to confront the growth in credit card fraud. However, all of these techniques have the same goal of avoiding credit card fraud; each one has its own drawbacks, advantages and characteristics.

In this research paper, after investigating difficulties of credit card fraud detection, the author seeks to review the state of the art in credit card fraud detection techniques, datasets and evaluation criteria. The advantages and disadvantages of fraud detection methods are enumerated and compared in this research paper by the author.[20]

The main contributions of this research paper are:i) The absence of a complete and detailed credit card fraud detection survey is an important issue, which is addressed by analyzing the state of the art in credit card fraud detection.ii) The state of the art fraud detection techniques are described and classified from different aspects of supervised/unsupervised and numerical/categorical data consistent.iii) In credit card fraud research each author has used its own dataset. There is no standard dataset or benchmark to evaluate detection methods. iv) The authors of this research paper have attempted to gather different datasets investigated by researchers, categorize them into real and synthetic groups and extract the common attributes that affect the quality of detection. In this research paper, the credit card fraud detection techniques are classified in two general categories: fraud analysis (misuse detection) and user behavior analysis (anomaly detection). The first group of techniques deals with supervised classification tasks at transaction level. In these methods, transactions are labeled as fraudulent or normal based on previous historical data.The second approach deals with unsupervised methodologies which are based on account behavior. In this method a transaction is detected fraudulent if it is in contrast with the user‟s normal behavior.[20]

This research paper presents, compares and analyzes the recently published findings in credit card fraud detection. The authors have defined common terms in credit card fraud and highlighted key statistics and figures in this field. Depending on the type of fraud faced by banks or credit card companies, various measures can be adopted and implemented. The authors have proposed certain methods in this research paper which are likely to have beneficial attributes in terms of cost savings and time efficiency. The significance of the application of the techniques reviewed in this research paper is in the minimization of credit card fraud. Yet it is observed that there are still ethical issues when genuine credit card customers are misclassified as fraudulent.[21] This research paper has also reviewed recent findings in the credit card field. This paper has identified the different types of fraud, such as bankruptcy fraud, counterfeit fraud, theft fraud, application fraud and behavioral fraud, and discussed measures to detect them. Such measures have included pairwise matching, decision trees, clustering techniques, neural networks, and genetic algorithms. In the upcoming research work the authors will build scoring models to predict fraudulent behavior, taking into account the fields of behavior that relate to the different types of credit card fraud identified in this research paper, and to evaluate the associated ethical implications.

III.INVESTIGATION PROCEDURE AND RESULTS

A. Analysis

Tools used for Analysis

1) FTK Imager

All the three evidences which were claimed to be the most precise and obvious for claiming and accusing Arif Azim

a) Phone numbers which were been called from Arif's SIM have been collected for the investigation.

b) The Criminal's lawyer claimed that the accused was unconscious and his images were been captured from the society CCTV camera when he came back from party the night before the burglary.

c) The accused's laptop had the list of his victims and the people whom he used for his big shot burglary fraud. The Laptop turned out to be the most important witness of all where the victim could not deny about the judgements made.

Accumulately, the image was made to be clear about the evidences.


Drive/Image Verify Results

Name	#7-10-10-2020.E01
Sector count	30302208
MD5 Hash	
Computed hash	319c3e1749d88b6ebd09fb0bb738c329
Stored verification hash	319c3e1749d88b6ebd09fb0bb738c329
Report Hash	319c3e1749d88b6ebd09fb0bb738c329
Verify result	Match
SHA1 Hash	
Computed hash	47f2c08d6c83f5e54ac15331b0d22055ae80e51e
Stored verification hash	47f2c08d6c83f5e54ac15331b0d22055ae80e51e
Report Hash	47f2c08d6c83f5e54ac15331b0d22055ae80e51e
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Figure 1: FTK Image for Arif Azim's case

2) *Autopsy:* The image which constituted the evidences was tested against Autopsy Forensics Tool, where the results were obvious and helpful. The suspected user contents were the images and call logs of the Accused. Autopsy report had 7 distinct domains of tests and investigation.

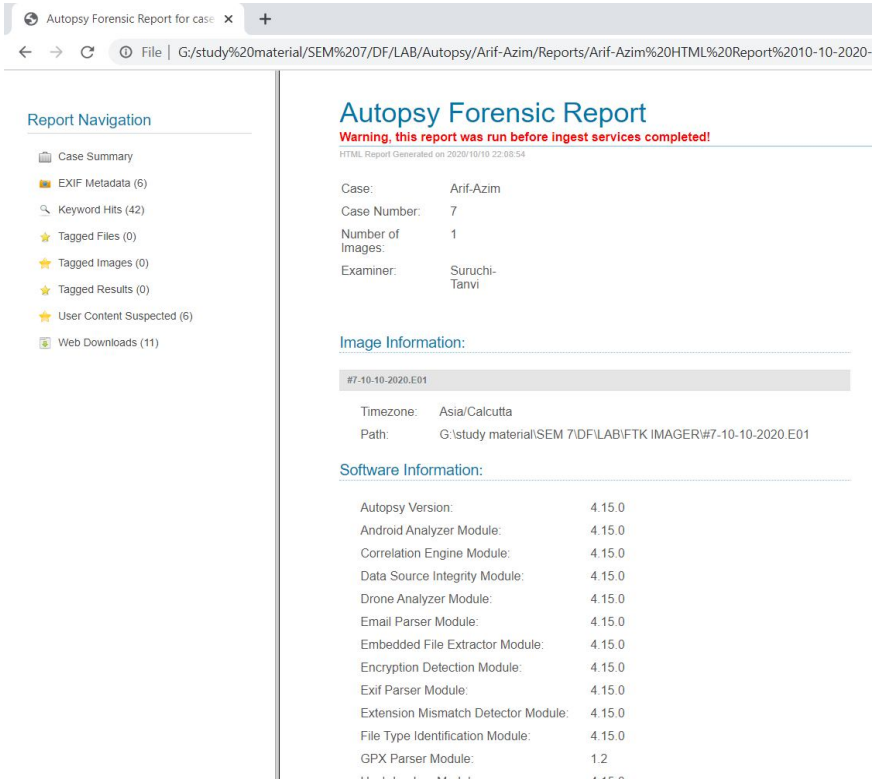


Figure 2: Autopsy Cumulative Report

3) *EXIF Metadata:* Exif Info is a tool that allows you to upload a file, and will show you the (normally hidden) metadata that is embedded in that file. The tool focuses on displaying the metadata from Exif images (i.e. .jpeg files), but can extract the metadata from almost every common media format including images, movies, audio files, Microsoft Word documents, Adobe PDFs, and many more.

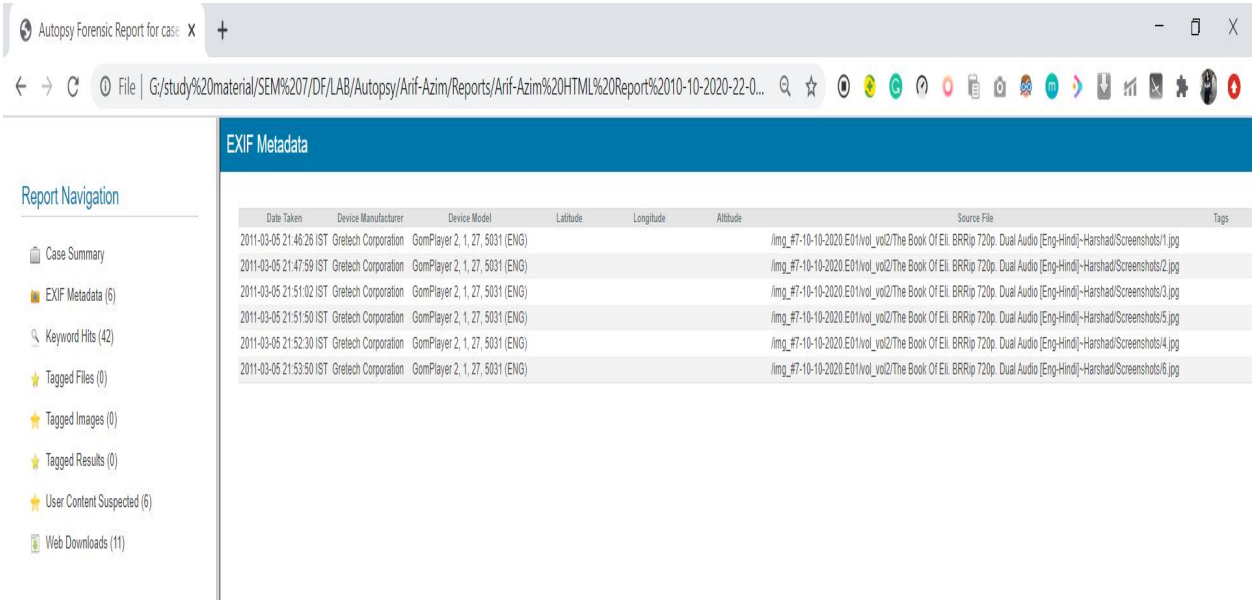


Figure 3: EXIF Metadata

4) *Keyword Hits:* The evidence clearly showed the suspicious entries which were in the hit list. The Keywords which are mostly used in the entry of Cyber crime cases.

Figure 4: Keyword Hits

a) *Tagged Files:* In information systems, a tag is a keyword or term assigned to a piece of information (such as an Internet bookmark, digital image, database record, or computer file). This kind of metadata helps describe an item and allows it to be found again by browsing or searching. There are not leads for the tagged files in the evidence image.

b) *Tagged Images:* We have not found any tagged images. No highlights were mentioned. There are not leads for the tagged images in the evidence image.

c) *Tagged Results:* There are not leads for the tagged results in the evidence image.

d) *User Content Suspected:* The content in the Drive's image, there were some files and images which had been transferred and deleted from the USB drive just before the burglary occurred. These files had subsequent evidences for the footage of the actual scene. The Accused had already found all the evidences and stored and them for creating fake replicas. The evidences were further tried to destroyed and shifted. The Digital forensics report has proved that the evidences were renamed and forged in the name of different .mp4 videos. The evidences were shifted to different drives which was a clear record of fear and containment.

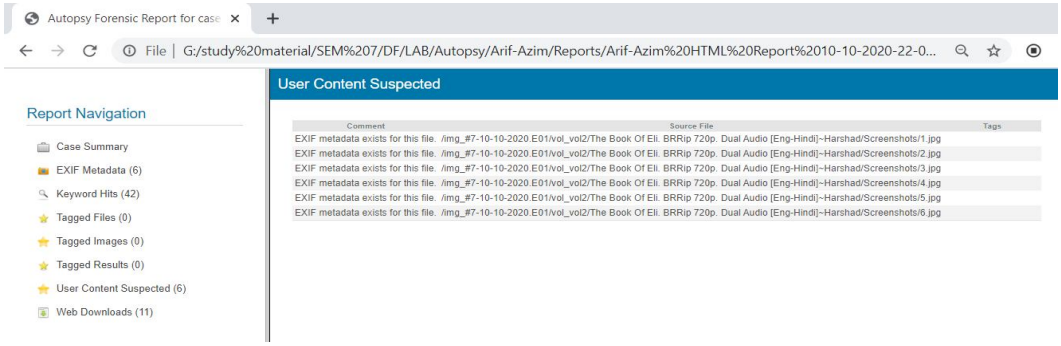


Figure 5: User Content Suspected

e) *Web Downloads:* The Accused had downloaded some random images from web and replaced them with his images of the Society CCTV footage. The Images were not tagged and were of degraded pixel quality.

Figure 6: Illustration of Image Processing done to retrieve Evidence from CCTV footage of Arif

Figure 7: Illustration of Processing done to retrieve Evidence from CCTV footage of Arif's car

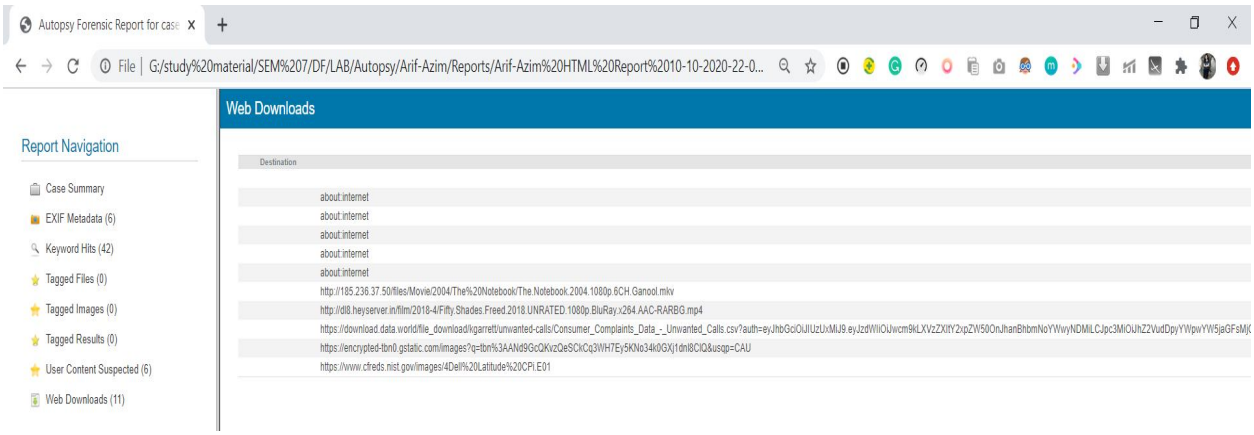


Figure 8: Web downloads

The evidence of phone call logs had been captured. The following is the header evidence of the same.

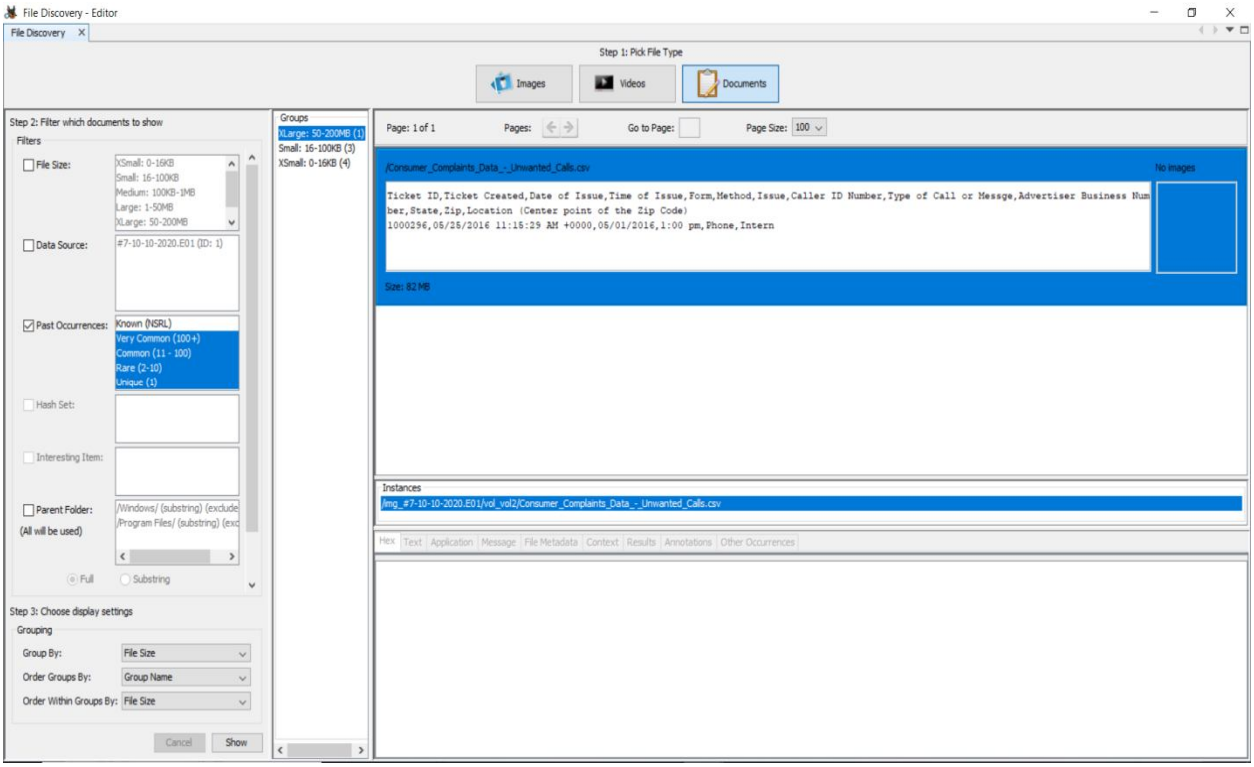


Figure 9: Phone call Header

5) *Pro Discover:* The same analysis has been made using ProDiscover tool. This tool gave the combined result and report of the case mentioned. The clusters and hidden files were mounted to a drive to be extracted. Accused's laptop had enough evidences of the Burglary. The bungalow in which he was living during the scene was sealed for investigation. His laptop was seized, and the laptop vendor was interrogated. His contact was a part of the image analyzed. The LED Television was seized and submitted to the forensic department for analysis. The images attached in the appendix shows that the TV was in good condition and was not deteriorated by the culprit.

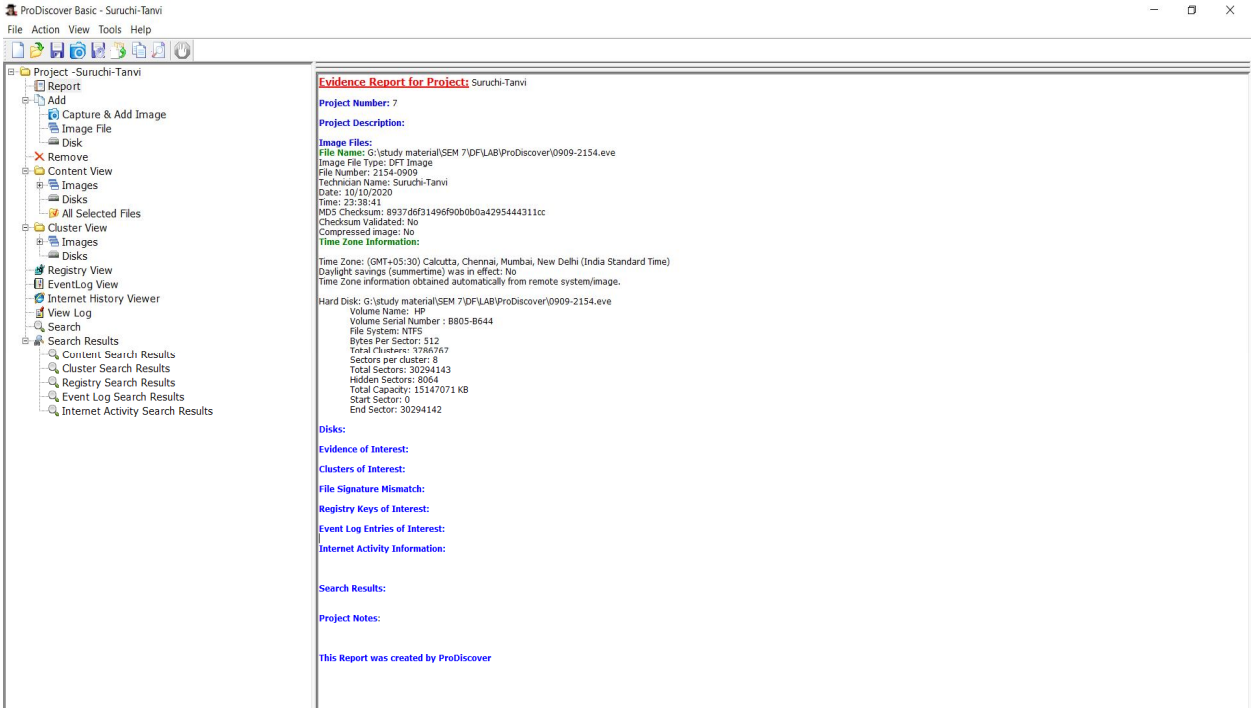


Figure 10: ProDiscover Report

B. *Statistics*

The tools used in the complete analysis showed different behavior for

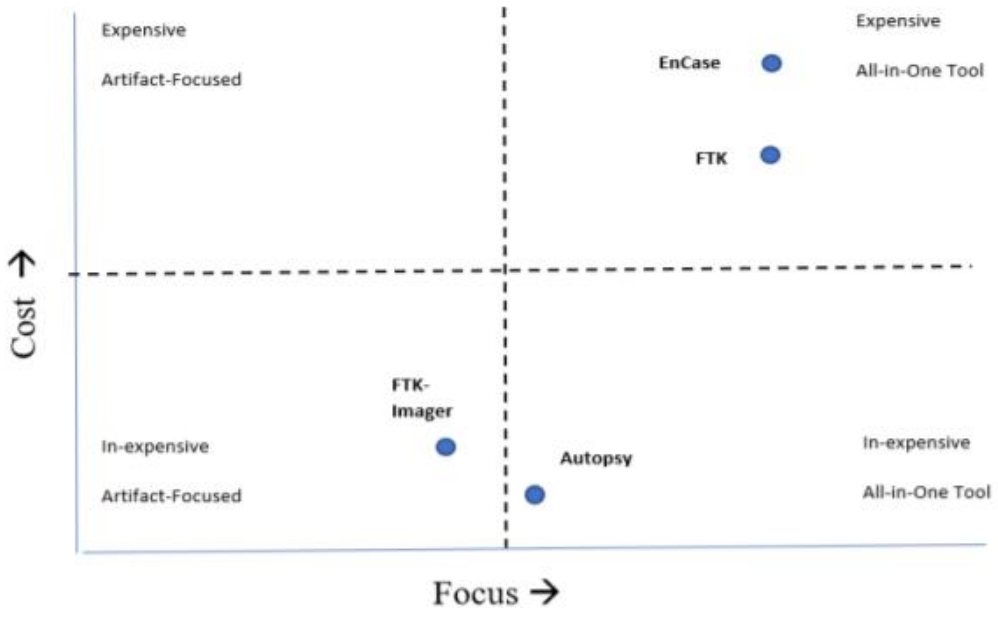


Figure 10: Cost v/s Focus

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue X Oct 2020- Available at www.ijraset.com

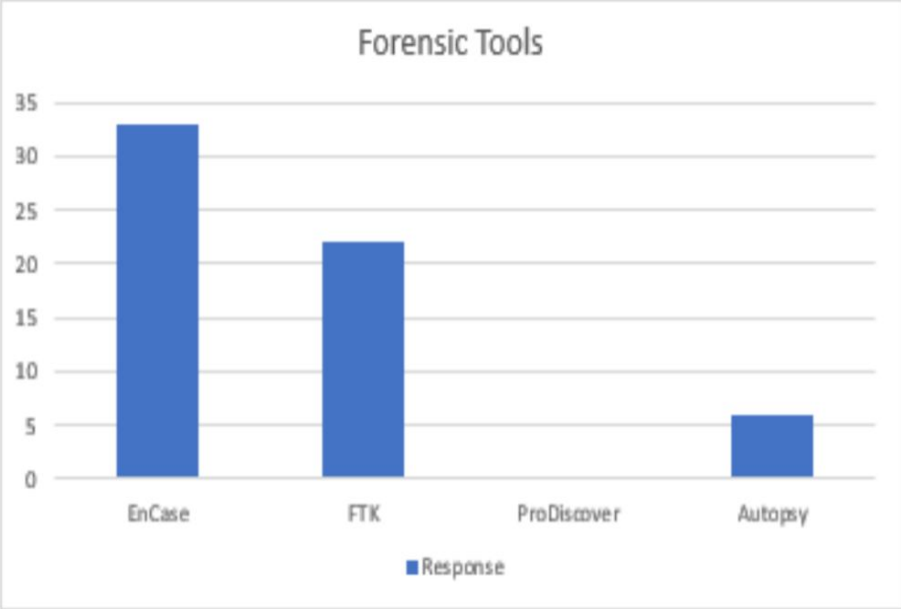


Figure 11: Response behavior of the tools used

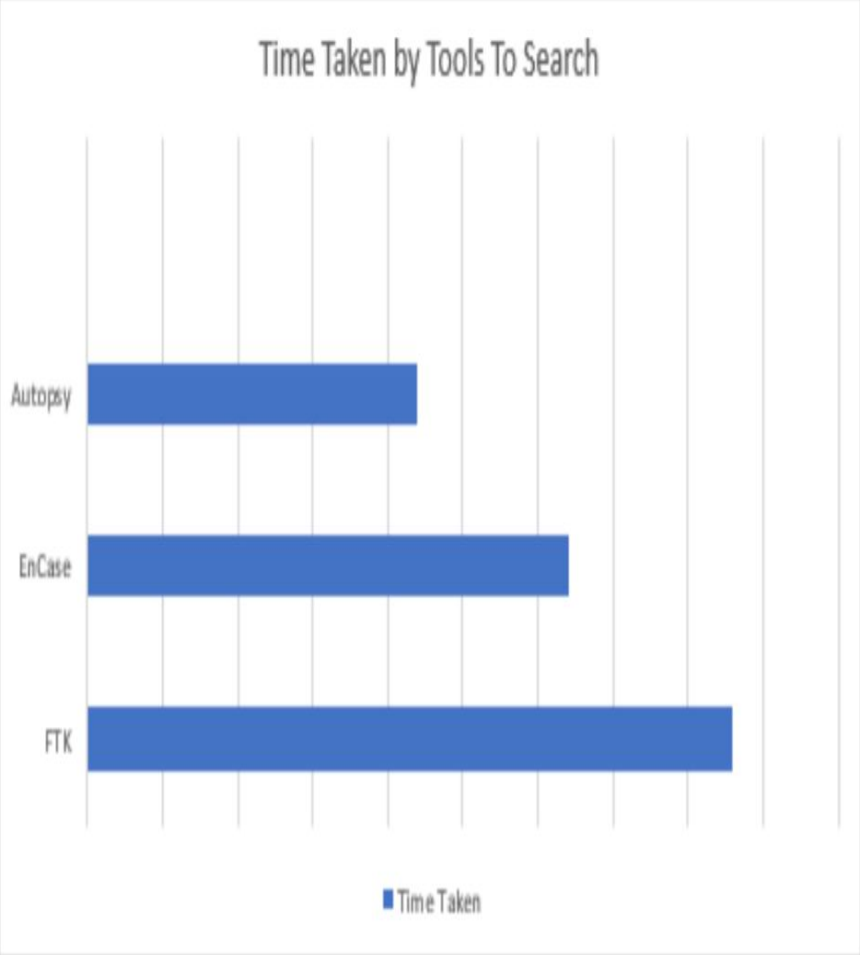


Figure 12: Time taken by the tools used

C. Comparison

Table I Comparison of three tools

Parameters	FTK Imager	Autoposy	ProDiscover Basic
Supported File System	FAT12/16 /32, NTFS, Ext2/3, ReiserFS, CDFS, UDF	NTFS/NTFS5/NTFS +EFS, FAT12/16/32, exFAT, HFS+, Ext2/3/4/BtrFS, FreeBSD Unix UFS, CD/DVD/Blue-ray UDF, ISO9600	FAT 12/16/32, NTFS, Solaris UFS, CD/DVD
Supported Disk Images	Raw DD,E01 etc.	Raw DD, E01, DIM(Active File recovery's own format)	Raw DD, eve(ProDiscov er's own format)
File Examination	Yes	Yes	Yes
Log Examination	Yes	Yes	Yes
Deleted File Indexing	No	Yes	Yes
File Indexing	Yes	Yes	Yes
Memory Dump Analysis	Yes	Yes	Yes

IV. INTERPRETATION OF THE CASE

The case 'Sony.sambandh.com' was one of the first cyber crime cases convicted in India. Three evidences were claimed in regard to this case namely, Phone numbers which were been called from Arif's SIM have been collected, his images were been captured from the society CCTV camera when he came back from party the night before the burglary.The accused's laptop had the list of his victims and the people whom he used for his big shot burglary fraud.Various techniques and tools of Digital Forensics ere used to study and analyze the evidences.

The analysis of the evidences was done on various Digital Forensics tools like the FTK Imager,Autopsy and Prodiscover.

The tools provided aple information about how the accused hid important evidences, and the reports clearly showed the sequnce of crimes with the hep of the provided support of the investigation team. The images of Srif Azim from the CCTV footage were an add on in the clear providance.

The LED TV was in good condiition according to the pictures which were extracted from the Drive of the Accused's Laptop. The main aim of the reports were to find whether the replicas made of the original evidences were shifted or not. The original evidences were destroyed and renamed in the drive several times. And the Drive was completely formatted.

The report also showed that there were user suspected files which were tagged with informal emails, which were the olf victims of this criminal. The case report also mentioned Metadata related to the web downloads which were used as replacements in the final drive, but the failed attempt cleary helped the team to extract the real images and .csv files.

The court convicted Arif Azim under Section 418, 419 and 420 of the Indian Penal Code.The court, however, felt that as the accused was a young boy of 24 years and a first-time convict, a lenient view needed to be taken. The court, therefore, released the accused on probation for one year.

V. CONCLUSION

The Cyber Crime activities in today's world is a very common activity and is of great concern. A normal guy named Arif Azim who can be anyone on a given day did a cyber fraud and theft to phish somebody else's details and use it for his own purpose. In this case, the investigation done by the prosecution and defense led to the collection of quite a few evidences which then again, are sent to the forensics. Forensic Techniques which are used to synthesize and analyze the evidence are provided. These Evidences and the Forensic Results are admitted into the court and we're looked upon by the judge to indicate the convict was guilty.

The judgment is of immense significance for the entire nation. Besides being the first conviction in a cybercrime matter, it has shown that the Indian Penal Code can be effectively applied to certain categories of cybercrimes which are not covered under the Information Technology Act 2000. Secondly, a judgment of this sort sends out a clear message to all that the law cannot be taken for a ride.

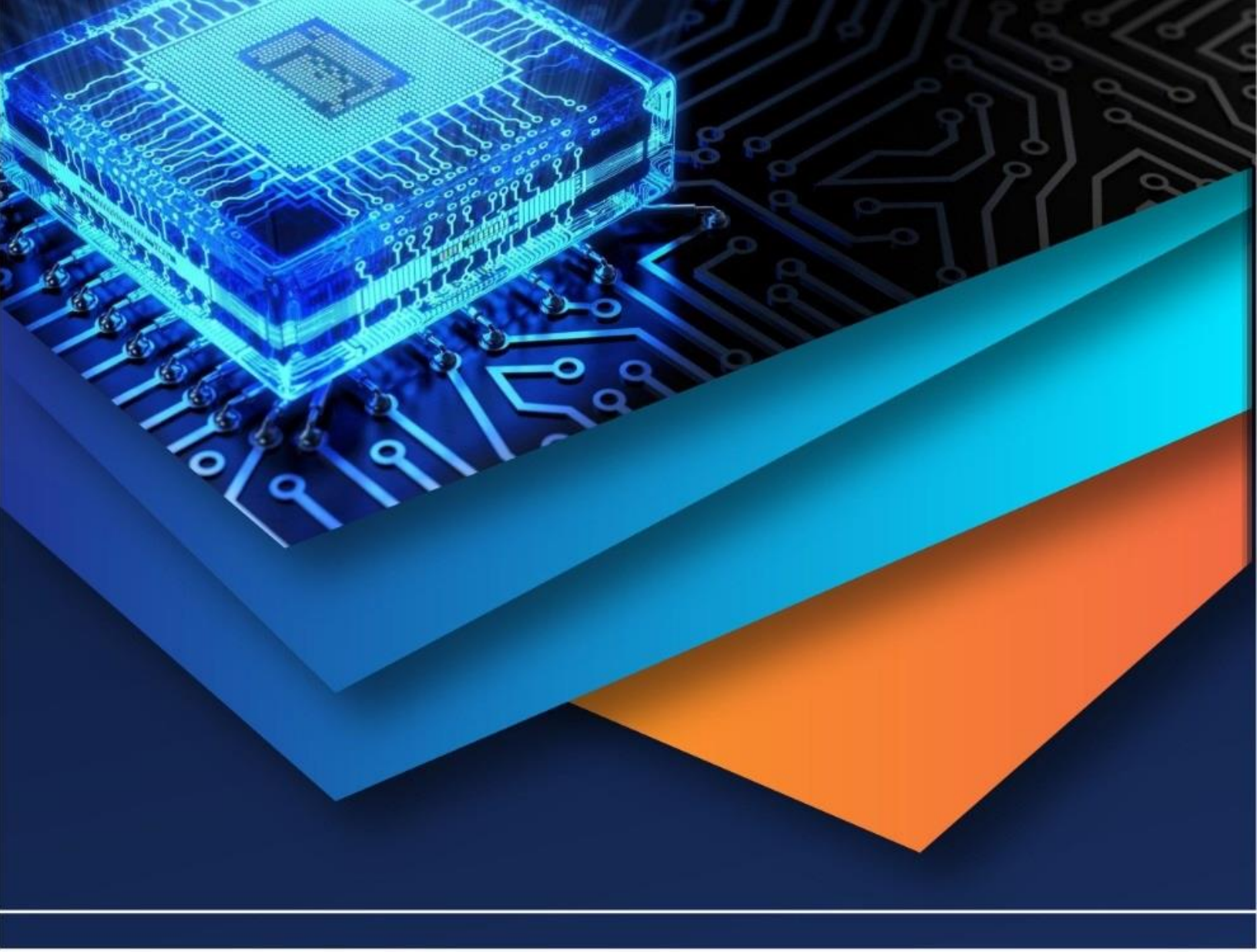
The Importance of Digital Forensics nowadays in the modern world has risen to such importance that, with the advanced technology we can date backwards, find damaged data and kindle down things which weren't imaginable a few years back. The quickness in which the case was solved using Digital Forensics also shows how important it is to have the knowledge and the System of Digital Forensics as an aid in the current system. Thus, Digital Forensics, which are used in various fields is quite important in Judicial System and Investigation with which we can get to the cherry very quickly comparing them to other orthodox methods.

VI. ACKNOWLEDGMENT

We would like to express our sincere gratitude to Professor Aju D. for his valuable guidance and suggestions through the process. His knowledge on the various tools of Digital Forensics is commendable that proved to be very helpful for deeper understanding of the evidences and the case.

REFERENCES

[1] Roberts, L. D., Indermaur, D., &Spiranovic, C. (2013). Fear of cyber-identity theft and related fraudulent activity. Psychiatry, Psychology and Law, 20(3), 315-328.
[2] Kashyap, N., Malali, H. R. K., & Gururaj, H. L. (2020). Cyber Attacks and Security—A Critical Survey. In Soft Computing: Theories and Applications (pp. 895-904). Springer, Singapore.
[3] Singh, T. (2007). Cyber law & information technology. District & Sessions Judge, Delhi.
[4] Sarmah, A., Sarmah, R., & Baruah, A. J. (2017). A brief study on cyber crime and cyber laws of India. International Research Journal of Engineering and Technology (IRJET), 4(6), 1633-1640.
[5] Franke, K., & Srihari, S. N. (2008, August). Computational forensics: An overview. In International Workshop on Computational Forensics (pp. 1-10). Springer, Berlin, Heidelberg.
[6] Krishnan, S. (2019). Role and Impact of Digital Forensics in Cyber Crime Investigations. INROADS-An International Journal of Jaipur National University, 8(1and2), 64-75.
[7] Bahuguna, S., Raizada, T., &Wadje, A. Crimes in Cyberspace: Indian Scenario. IITM Journal of Information Technology, 69.
[8] Goel, A., Vasishtha, A., & Gupta, M. (2012). In-depth Analysis of an Indian IT Act Related to Unauthorized Access. International Journal of Computer Applications, 58(7).
[9] Thakare, S. P., Shivratriwar, N. M., & Sarda, S. N. A Review on Information Technology and Cyber Laws. International Journal of Engineering and Applied Sciences, 2(5).
[10] Dhupdale, V. Y. Cyber Crime and Challenges Ahead.
[11] Rustad, M. L., & Koenig, T. H. (2005). The tort of negligent enablement of cybercrime. Berkeley Tech. LJ, 20, 1553.
[12] Sindhu, K. K., &Meshram, B. B. (2012). Digital forensics and cyber crime datamining.
[13] Sinrod, E. J., & Reilly, W. P. (2000). Cyber-crimes: A practical approach to the application of federal computer crime laws. Santa Clara Computer & High Tech. LJ, 16, 177.
[14] Riek, M., Bohme, R., & Moore, T. (2015). Measuring the influence of perceived cybercrime risk on online service avoidance. IEEE Transactions on Dependable and Secure Computing, 13(2), 261-273.
[15] Hutchings, A. (2014). Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. Crime, Law and Social Change, 62(1), 1-20.
[16] Cashell, B., Jackson, W. D., Jickling, M., &Webel, B. (2004). The economic impact of cyber-attacks. Congressional research service documents, CRS RL32331 (Washington DC), 2.
[17] More, D. M. M., &Nalawade, M. P. J. D. K. (2015). Online banking and cyber-attacks: the current scenario. International Journal of Advanced Research in Computer Science and Software Engineering Research Paper.
[18] Jain, Y., NamrataTiwari, S., & Jain, S. (2019). A comparative analysis of various credit card fraud detection techniques. Int J Recent Technol Eng, 7(5S2), 402-407.
[19] Korauš, A., Dobrovič, J., Rajnoha, R., &Brezina, I. (2017). The safety risks related to bank cards and cyber attacks. Journal of security and sustainability issues.
[20] Zojaji, Z., Atani, R. E., &Monadjemi, A. H. (2016). A survey of credit card fraud detection techniques: data and technique oriented perspective. arXiv preprint arXiv:1611.06439.
[21] Delamaire, L., Abdou, H., & Pointon, J. (2009). Credit card fraud and detection techniques: a review. Banks and Bank systems, 4(2), 57-68.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY