International Journal For Technological Research In Engineering
Volume 1, Issue 9, May-2014 *ISSN (Online): 2347 - 4718*

CYBER TRIANGLE

Leena Patel[1] (Assistant Professor), Divya Sharma[2] (Assistant Professor)
Gandhinagar Institute of Technology
Gujarat, India.

Abstract: The use of internet and information technology has been increasing tremendously all over the world. Now-a-days CYBER SECURITY is a burning issue in the world yet so far. We have made this unique research paper based on combinational research work over three essential inter-connected cyber entities which are CYBER FORENSIC, CYBER LAWS and CYBER SECURITY along with CYBER CRIMES as a center of this triangle. Yet all papers are either mentioned only cybercrimes or cyber laws information or only cyber security concerns but here in this research paper we have covered all these three areas as a TRIANGLE to understand all aspects of computer utilizations such a way that by this research paper maximum people related to COMPUTER/IT field may get maximum information to implement cyber security along with the cyber laws and also to establish cyber awareness among people of forthcoming centuries.
Keywords: Cyber Security, Cyber Laws, Cyber awareness, Cyber Forensic, Forensic Investigation, Forensic Analysis, Forensic Tools, Malware

I. INTRODUCTION

"Cybercrime" combines the term "crime" with the root "cyber" from the word "cybernetic", from the Greek, "kubernân", which means to lead or govern. The "cyber" environment includes all forms of digital activities, regardless of whether they are conducted through networks and without borders. This extends the previous term "computer crime" to encompass crimes committed using the Internet, all digital crimes, and crimes involving telecommunications networks. This more recent terminology covers a wide variety of facets, leading to different approaches, depending on the dominant culture of the experts, making it appear either reduced or expanded, in different dimensions, dealing with emerging issues that also reflect its diversity [1].

II. LIVE SCENARIOS IN INDIA

A. Critical Infrastructure Protection in India: The Problems, Challenges and Solutions

Critical Infrastructure like Oil and Gas, Power Grids, Transportation, Satellites, etc are connected to Information and Communication Technology (ICT) these days. Recently it was revealed that Internet is full of Unprotected and Unsafe Devices, SCADA Systems and Computers. This makes the Critical Infrastructures vulnerable to various forms of Cyber Attacks. India is facing serious cyber threats and Critical Infrastructure Protection must be the top priority of Indian Government. The process of Critical Infrastructure Protection in India is still trying to tackle the sophisticated Cyber Attacks. The Cyber Security Trends and Developments in India 2013 (PDF) provided by Perry4Law and Perry4Law's Techno Legal Base (PTLB) have highlighted further Cyber Security Challenges for India. There is no second opinion that Critical Infrastructure Protection in India is needed and the sooner we ensure the same the better it would be for the National Interest of India. Acknowledging this situation, the National Cyber Security Policy of India 2013 (NCSP 2013) was drafted by Indian Government. However, the Policy lacked on many count like Privacy Protection in India. Similarly, the NCSP 2013 has also failed to "Integrate" itself with the National Security Policy of India. Recently, Huawei was accused of breaching National Security of India by Hacking Base Station Controller in Andhra Pradesh state. The DRDO has even sought Penal Provisions in National Telecom Security Policy of India for Telecom Companies Violating the Norms. The problem of embedded malware in imported Hardware and Software is still haunting India as the Imported Software and Hardware Testing for Embedded Malware was postponed till 1st April 2014 by India. With India being recognized as Authorizing Nation under the International Common Criteria Recognition Arrangement (CCRA) this task of Hardware and Software testing may become easier in India [3].

B. Cyber Security Must Be an International Issue

Cyber Security has been for long considered to be a National Policy matter. However, the recent E-Surveillance Disclosures have forced the Governments around the world to consider Cyber Security Mandates differently. Self Defense and Privacy protection Measures have been devised to counter E-Surveillance and Illegal Eavesdropping that are increasing day by day. Even our own Technology related Trends have depicted that Information and Communication Technology (ICT) related Legal Issues must be redressed at National and International Levels. The Cyber Law Trends and Developments of India 2013 (PDF), Cyber Security Trends and Developments in India 2013 (PDF) and Cyber Forensics Trends and Developments in India 2013 (PDF) reiterate this Regulatory need at both Indian and International Levels. India is facing lack of Legal Cooperation from E-Mail Service providers of U.S. This force India to formulate a dedicated E-Mail Policy so that dependence upon G-Mail, Yahoo, Hotmail, etc can be reduced for Governmental functions. In fact, these E-Mail Services are actually Abetting and Encouraging commission of Cyber Crimes in India and other parts of the World. Indian Government also faced helplessness when the Foreign

Companies like Google, Facebook, etc not only failed to comply with Indian Laws but even the U.S. Blocked India's MLAT Attempt to make Google, Facebook, etc Comply with Indian Laws. India negotiated this aspect with U.S. and finally an Indo-American Alert, Watch and Warn Network for Real Time Information Sharing in Cyber Crime Cases was constituted. Though its efficacy is still to be seen yet this is a good step in the right direction.

The threats of Cyber Crimes and Cyber Security attacks are alarming these days. As more and more Critical Infrastructure is connected to ICT, a need has been felt to protect Critical ICT Infrastructures (PDF) all over the World. In a typical Cyber Attack by an Enemy State, the Critical Infrastructure is the first choice. Estonia witnessed this truth in the past. Further, in cases of Cyber Warfare, Cyber Espionage and Cyber Terrorism, Critical Infrastructure is the chief target of Cyber Attack. It is surprising that despite the seriousness of the issue we have no International Cyber Law Treaty and International Cyber Security Treaty. International Organizations and Institutions have still not taken Cyber Crimes and Cyber Security very seriously. Even Human Rights Protection in Cyberspace has not been taken by seriously by all concerned. Organizations like United Nations, North Atlantic Treaty Organization (NATO), etc have also not shown much interest in this regard in the past. Now these Organizations have taken notice of the nuisances of Cyberspace and they are gradually shifting their attentions to Cyber Crimes and Cyber Attacks. If different Countries would have different laws for these issues, it would be very difficult to truly enforce protective provisions against these menaces at National and International levels. It is high time for UN to seriously consider issues like International Cyber Law Treaty, International Cyber Security Treaty and Protection of Human Rights in Cyberspace [2].

C. Cyber Security Trends and Developments in India 2013 with cyber policies and laws

C.1 National Cyber Security Policy India

Cyber Security in India has been ignored for long. However, Indian Government realized that this is a crucial field and it needs a clear Cyber Security Policy. The National Cyber Security Policy of India 2013 (NCSP 2013) was drafted keeping this requirement in mind. It is a good Policy on many counts but it also failed to address many crucial aspects as well. For instance, the Policy has failed to protect Privacy Rights in India. Nevertheless, this is a good step in the right direction and it must be updated and improved as the time passes [4].

C.2 National Security Policy of India

National Security of India is facing many challenges these days that are mainly attributable to the use and abuse of Information and Communication Technology (ICT). A National Security Policy of India is urgently needed that must have the Cyber Security Policy as an essential element. Presently this is not the case but we hope the same would be achieved very soon by the Indian Government [4].

C.3 National Telecom Security Policy of India

There is no implementable National Telecom Security Policy of India as on date. However, it may be drafted very soon by the Indian Government. As of now the Telecom Service Providers of India are openly flouting the Laws of India. They are not following the Cyber Law Due Diligence in India. For instance, Airtel and Tata Teleservices Limited are violating Cyber Law of India in general and Internet Intermediary Rules of India in particular. These violations must be punished by Department of Telecommunication (DoT) and Telecom Regulatory Authority of India (TRAI). Even the Defense Research and Development Organization (DRDO) has communicated to the DoT that the proposed National Telecom Security Policy should have a framework to penalize Telecom Service Providers if they fail to abide by the norms [4].

C.4 Cyber Warfare Policy of India

Cyber Warfare is a concept that is not clear yet. Some believe that there is nothing like Cyber Warfare as there is no involvement of traditional military actions. Others believe that Cyber Warfare is a reality of the present time and future wars would be fought in Cyberspace. Whatever the opinion may be but it is clear that Nations have to protect their Critical ICT Infrastructures and Strategic Computers from growing Cyber Attacks. Cyber Warfare and Cyber Terrorism are issues that cannot be taken lightly by any Country. From these threats emerge the necessity of having a robust Cyber Security for Defense Forces in India. These issues are important as they strike at the very root of the Critical ICT Infrastructure Protection in India (PDF). However, India is not doing the needful in this regard. Cyber War Capabilities should be an Integral Part of Indian National Defense and Security [5]. Malware are posing significant threat to India yet there is no attention towards Cyber Security in India. For instance, we need Express Legal Provisions and Specified Policies to deal with issues like Denial of Service (DOS), Distributed Denial of Services (DDOS), Bots, Botnets, Trojans, Backdoors, Viruses and Worms, Sniffers, SQL Injections, Buffer Overflows Exploits, etc. Although India has formulated the National Cyber Security Policy of India 2013 (NCSP 2013) yet it is deficient on many counts. For instance, it has no Coordination with the National Security Policy of India. Similarly, the NCSP 2013 has "Failed to Protect" the Privacy Rights in India (PDF). The Privacy Rights in India in the Information Age (PDF) have not at all been covered by the NCSP 2013. Similarly, there is no E-Surveillance Policy of India (PDF) framed by Indian Government so far. Obviously, we have no Cyber Warfare Policy of India as well. Even the Cyber Law of India is weak and ineffective and deserves to be repealed. The biggest hurdle before curbing Cyber Warfare Threats at the International Level is Lack of Harmonization in this regard. Till now we have no "Internationally Acceptable Definition" of Cyber Warfare. Further, we have no Universally Acceptable Cyber Crimes Treaty as well. There is also no International Cyber Security Treaty. India is not a part of any International Treaty or Conventions regarding Cyber Crimes,

Cyber Security, etc. We cannot have a Cyber Warfare Policy in India till we have a Cyber Crimes Policy in India, Cyber Security Policy in India, cyber Terrorism Policy in India and other similar Policies. Indian Government must urgently work in this crucial direction as it is the most urgent need of the hour [5].

C.5 E-Surveillance Policy of India Is Needed

India has no E-Surveillance Policy and Legal Framework. This is despite the fact that many Indian projects are so e-surveillance oriented that they cannot pass the scrutiny provisions of Indian Constitution. India has launched Projects like Aadhar, National Intelligence Grid (NATGRID), Crime and Criminal Tracking Network and Systems (CCTNS), National Counter Terrorism Centre (NCTC), Central Monitoring System (CMS), Centre for Communication Security Research and Monitoring (CCSRM), Internet Spy System Network And Traffic Analysis System (NETRA) of India, etc. None of them are governed by any Legal Framework and none of them are under Parliamentary Scrutiny. If this was not enough the sole Cyber Law of India (Information Technology Act 2000) was amended through the Information Technology Amendment Act 2008. The IT Act 2008 made the Cyber Law of India an "unregulated and unaccountable" piece of E-Surveillance Legislation. It is now wide open to misuses by Indian Government and its Agencies. Further, the IT Act 2008 also violated various provisions of Indian Constitution and hence is "Unconstitutional" as well [6].

D. What can be the solution internationally?

Answer is: International Cyber Security Treaty Is Required!

The dependence and reliance upon Internet and Information and Communication Technology (ICT) had grown tremendously in the year 2013. This had also given rise to many Techno Legal Issues that are almost common in all the Countries. These issues have been aptly covered by the Cyber Law Trends and Developments of India 2013 (PDF), Cyber Security Trends and Developments in India 2013 (PDF) and Cyber Forensics Trends and Developments in India 2013 (PDF) provided by Perry4Law and Perry4Law's Techno Legal Base (PTLB). Cyber Security has become a Very Crucial Policy Issue world over. Even India has realized that it must deal with Cyber Security on a priority basis. The National Cyber Security Policy of India 2013 (NCSP 2013) was drafted by Indian Government [7]. However, it failed to cater many Techno Legal aspects and it was also not "Integrated" with the National Security Policy of India. Nevertheless a "Good Beginning" has been made by Indian Government and these efforts must further be improved and strengthened in the year 2014. However, this is a National Cyber Security Perspective of India and it is essentially different from International Cyber Security Perspective. This is so because Cyber Security must be an International Issue (PDF) to be "Effective and Useful". Just like India, United States has also formulated the U.S. International Strategy for Cyberspace that is much wider than mere Cyber Security Policy. However, these efforts of Countries like India and United States are "Piecemeal Actions" and there is an urgent need to have "International Harmonization" regarding Cyber Security Cooperation at the Global Level.

This means that an International Cyber Security Treaty is required to be formulated so that Nations across the world can harmonize their Domestic and National Laws accordingly. Presently, there is a "Complete Chaos" in this field as different Countries are applying different Laws in "Similar Situations". This is also giving rise to Conflict of Laws in Cyberspace that is making the International Cyber Security Norms and Regulations more "Complicated and Redundant". It is surprising that despite the seriousness of the issue we have no International Cyber Law Treaty and International Cyber Security Treaty. International Organizations and Institutions have still not taken Cyber Crimes and Cyber Security very seriously. Even Human Rights Protection in Cyberspace has not been taken by seriously by all concerned. Organizations like United Nations, North Atlantic Treaty Organization (NATO), etc have also not shown much interest in this regard in the past. Now these Organizations have taken notice of the nuisances of Cyberspace and they are gradually shifting their attentions to Cyber Crimes and Cyber Attacks. If different Countries would have different laws for these issues, it would be very difficult to truly enforce protective provisions against these menaces at National and International levels. It is high time for UN to seriously consider issues like International Cyber Law Treaty, International Cyber Security Treaty and Protection of Human Rights in Cyberspace [7].

III. FORENSIC INVESTIGATION

A. General Steps in a Forensic Investigation

The three main steps to a forensic investigation are the acquisition of the evidence, the authentication of the recovered evidence, and the analysis of the evidence [8][9]. Although each forensic investigator may add their own steps in the forensics process, these three steps (acquisition, authentication, and analysis) are essential to any forensic investigation. Acquiring evidence in a computer forensics investigation primarily involves gaining the contents of the suspect's hard drive. But other aspects may be involved in the acquisition of evidence. Photographs of the computer screen and the entire computer system in its installed configuration may yield useful information to the investigator. In addition, some forensic investigators believe in gathering evidence before shutting down the suspect's computer; this is a source of arguments within the forensics community - whether to shut down the computer immediately and preserve the exact state that it was found, or to gather evidence before shutting down in order to gain any volatile data that might be destroyed on shutdown (like the running processes on the computer) [8][10]. Ideally, the forensic analysis is not done directly on the suspect's computer but on a copy instead. This is done to prevent tampering and alteration of the suspect's data on the hard drive. The contents of the hard drive are copied on one or more hard drives that the investigator will use to conduct the

investigation. These copies, or images, are obtained by coping bit by bit from the suspect's hard drive to another hard drive or disk. The hard drive containing the image of the suspect's hard drive obtained in this manner is called a bit-stream backup. The reason why hard drives must be copied bit by bit is because doing so ensures that all the contents of the hard drive will be copied to the other. Otherwise, unallocated data (such as deleted files), swap space, bad sectors, and slack space will not be copied. A goldmine of evidence may be potentially held in these unusual spaces on the hard drive [8][11].

The authentication of the evidence is the process of ensuring that the evidence has not been altered during the acquisition process. In other words, authentication shows that the no changes to the evidence occurred during the course of the investigation. Any changes to the evidence will render the evidence inadmissible in a court. Investigators authenticate the hard drive evidence by generating a checksum of the contents of the hard drive. This checksum is like an electronic fingerprint in that it is almost impossible for two hard drives with different data to have the same checksum. By showing that the checksums of the seized hard drive and the image are identical, the investigators can show that they analyzed an unaltered copy of the original hard drive.

The algorithms most commonly used to generate these checksums are MD5 and SHA. Some tools to generate checksums use a combination of algorithms such as CRC (cyclic redundancy check) with MD5 in order to ensure a higher quality of authentication [8][12]. Of course, the investigator must make sure that the hard drive or disk used to hold the copy is completely free of any data so that the evidence will not be tainted. The commonly used forensics tools for the imaging of hard drives are Safe back and Encase, which also performs many other forensics functions. There are also disk-wiping tools to clean the image hard drive. The last and most time-consuming step in a forensics investigation is the analysis of the evidence. It is in the analysis phase that evidence of wrongdoing is uncovered the investigator.

Because of the differences between Windows-based operating systems and UNIX, I will discuss the analysis of the data on these two systems in separate sections. In general, forensic investigators rely on special forensics tools to analyze the huge amounts of data on the hard drive (the size of hard drives continues to get larger and larger). These range from a hex editor (a text editor that views the data in hexadecimal format) to full-blown forensic toolkits like Encase. It is important that the chain of custody is maintained throughout the investigation. The chain documents everything that happens to the evidence: who handled it, where and how it was handled, and how it was stored. It preserves the integrity of the evidence. Even if the suspect was guilty, if the chain is not maintained, a lawyer can argue that the chain of custody was not properly established, casting doubt on the damning evidence acquired during the forensic analysis phase [8].

IV. AN INVESTIGATION INTO COMPUTER FORENSIC TOOLS

Cyber-criminals associate themselves with one of or all of these crimes by making it their jobs to find vulnerabilities in operating systems, applications or services that run on a computer connected to the internet [13][14]. Once a vulnerability is discovered and exploited, the criminal is able to view or store sensitive information on some form of storage media. The storage medium can either be local, i.e. hard-drives or removable, i.e. floppy disks, zip drives, memory sticks or CDs. Once the crime is committed, prosecution becomes extremely difficult since the crime venue could easily be in different cities and countries and involve unsuspecting third parties. At this point, a computer forensic specialist (CFS) is tasked to investigate the digital crime scene by impartially scrutinizing a number of digital sources that are either involved or thought to be involved in the crime, and ultimately produce a single document reflecting a summary of the contents of the digital source. Like any other forensic science, CFSs make use of a number of specialized software tools and hardware devices to carry out investigations. These investigations follow a strict methodology to maintain the credibility and integrity of all storage devices involved. The general methodology is to [13] [15]:

- **PROTECT** the subject computer system during the forensic examination from any possible alteration, damage, data corruption or virus infection.
- **DISCOVER** all files on the subject system which includes existing normal files, deleted yet remaining files, hidden files, password-protected files and encrypted files.
- **RECOVER** as much as possible, files that are discovered to be dele ted.
- **REVEAL** to the extent possible, the contents of hidden files as well as temporary files used by both the application programs and the operating system.
- **ACCESS** the contents of protected or hidden files if possible and legally appropriate.
- **ANALYZE** all relevant data found in special areas of the disk. The concept of special areas of a disk is explained later in section 3.
- **PRINT** out an overall analysis of the subject computer system. This analysis includes a listing of all relevant files and discovered file data. The print-out also provides an overview of the system layout, file structures and data authorship information. Any attempts to hide, delete, protect or encrypt information will also be revealed through the print-out.
- **PROVIDE EXPERT CONSULTATION** and/or testimony as required. This testimony would typically be required to prove the points of a case in a court of law [13].

Some of the forensic software tools that CFSs use during their investigations are as below:

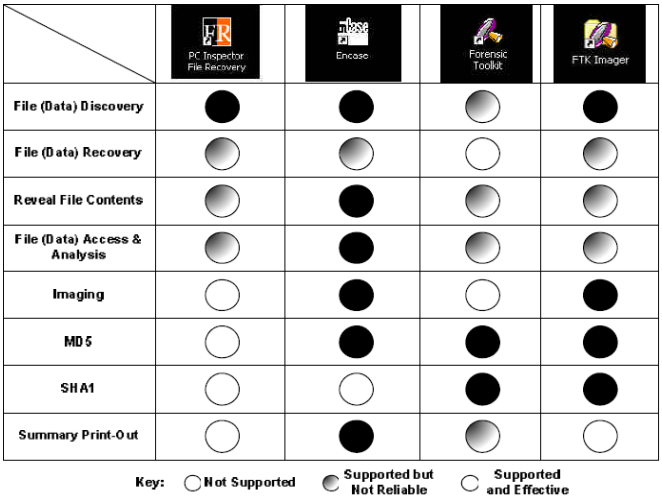

Fig. 1. Some forensic tools and highlights their effectiveness at achieving the requirements of the investigation methodology.

A. PC Inspector File Recovery

PC Inspector File Recovery is a freely available forensic tool. This tool serves two main purposes. Firstly, to reveal the contents of all storage media attached to the computer system and, secondly, to recover any deleted data from the media. As suggested in figure 1, this tool is very effective at detecting all files resident on a storage device. That is, all the file categories mentioned within the discovery step of the investigation methodology. All unreferenced files are associated with a condition. This condition can either be "good" or "poor" [13].

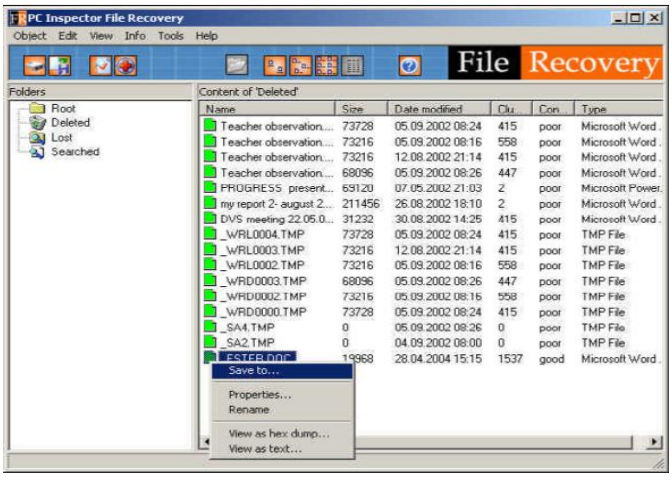

Figure.2 File recovery using PC Inspector File Recovery.

One of the appealing aspects about this tool is its simple interface which makes it useful to a CFS as well as the ordinary computer user. The tool is also very reliable in terms of discovering all the contents from storage media. However, PC Inspector File Recovery is generally not reliable in terms of data recovery [13].

B. Encase®

Encase [13][16] is a commercial forensic tool developed by Guidance Software. It was introduced to the forensics market in 1998. Encase's functionalities include disk imaging, data verification and data analysis. An important feature is the recovery of data through the inspection of unallocated spaces. We must remember that these unallocated spaces could contain information relevant to an investigation. A CFS using Encase would typically begin an investigation by seizing and imaging the storage device to be investigated. Encase refers to the resulting image file as an "Evidence File". The Evidence File is a bit-stream image of the storage device. The software then verifies the integrity of the image file and the original storage media using the MD5 hash function. In order for the investigation to proceed, the imaged file is mounted by the tool to eliminate the need to restore the seized storage device [13] [16]. The tool offers a cluster-by-cluster view of all files detected on the storage media. Vital information such as last access, time created, and last modifications of a file are all provided by this tool. Figure 3 illustrates how files are viewed with the Encase software tool. The first column, "File Name", gives the names of some of the files being previewed within the tool. The "Description" column then gives the corresponding status of each file [13].

C. Forensic Tool Kit

Forensic Tool Kit is a commercial forensics tool developed by Access Data [20]. This tool allows the CFS to view all files on the chosen storage device. A function of this tool includes immediate generation of hash values for files that are viewed within an investigation. From figure 1, it is clear that the most effective functionalities offered by this tool are the hashing functions. From the user- interface, it is apparent that the tool's developers intend the tool to be as simple and interactive as possible. Unlike the above mentioned forensic tools, Forensic Tool Kit does not support data recovery. Since the data discovery functionality of the tool is not effective, data analysis and recovery are both affected. In light of all this, it is important to mention that all investigations were conducted on a trial version of Forensic Tool Kit. Therefore, it is our view that the full version does incorporate more effective and comprehensive functionality [13].

D. FTK Imager

FTK Imager is a commercial tool offered by Access Data [20]. Its main function is to view and to image storage devices. Data recovery can be attained in most instances as a result of the tool's ability to effectively preview these storage devices. It is worth noting that the tool's effectiveness at data recovery depends largely on the time when the file was actually deleted. The tool is also able to generate either MD5 or SHA hash values of all visible and accessible files. In particular, the MD5 hash value is generated and presented to

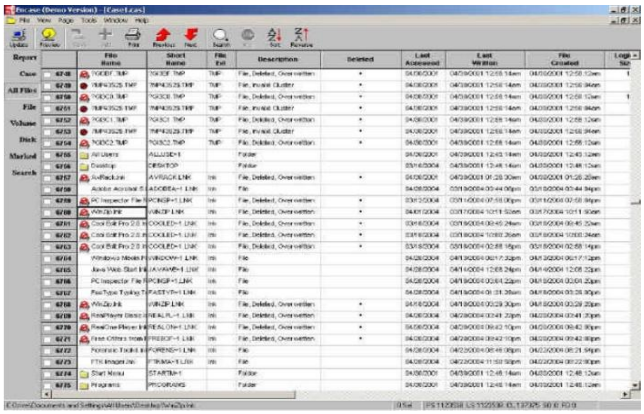

Figure.3 Data discovery view with Encase.

the investigator as part of the completed process notification to guarantee the integrity of the original files. Figure 4 illustrates a successful completion for the imaging of a floppy disk using FTK Imager. The integrity of the storage media is guaranteed through the generation of the MD5 hash value. FTK Imager is a commercial tool offered by Access Data [20]. Its main function is to view and to image storage devices. Data recovery can be attained in most instances as a result of the tool's ability to effectively preview these storage devices. It is worth noting that the tool's effectiveness at data recovery depends largely on the time when the file was actually deleted. The tool is also able to generate either MD5 or SHA hash values of all visible and accessible files. In particular, the MD5 hash value is generated and presented to the investigator as part of the completed process notification to guarantee the integrity of the original files. Figure 4 illustrates a successful completion for the imaging of a floppy disk using FTK Imager. The integrity of the storage media is guaranteed through the generation of the MD5 hash value [13]. It is very important that computer forensic specialist (CFSs) is able to stay ahead of cyber-criminals through the use of forensic tools that allow them to reliably carry out their tasks within an investigation. We believe that if the suggested improvements to these tools are further researched, prosecutions of cyber-crimes will definitely increase [13].

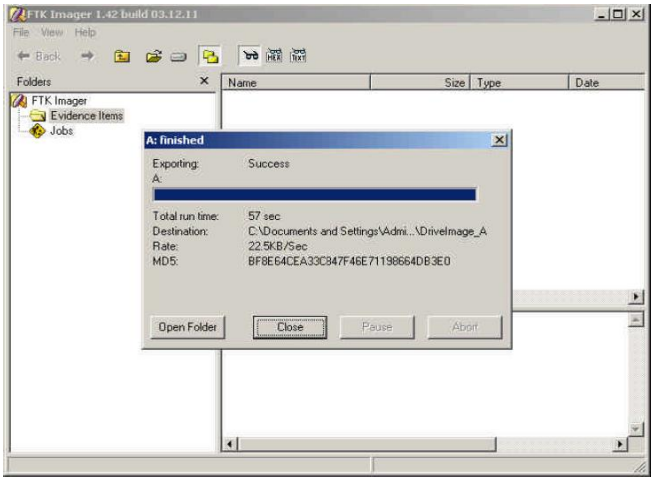

Figure.4 Storage device imaging with FTK Imager.

V. SMARTER, SHADIER, STEALTHIER MALWARE

A. Malware Evolves In 2013

Reflecting on the security and threat landscape of 2013, one trend that stands out is the growing ability of malware authors to camouflage their attacks. Widespread dissemination of advanced botnet and exploit kit source code allows more malware authors to create innovative and diverse new attacks. Cybercriminals have started to leverage online marketing as a way to promote and sell their services on the black market. In 2012, the Blackhole exploit kit broke new ground. But in 2013, Blackhole was replaced by several new exploit kits that grew out of it, borrowing some of its code. The resulting botnets are responsible for a sharp increase in ransomware attacks, with Cryptolocker being the prime malice. Modern malware is all about stealth. Advanced persistent threats (APTs), one of the most vicious examples of a stealth threat, precisely target individuals, businesses, governments and their data. APTs are a sophisticated weapon to carry out targeted missions in cyber space. Data leaks—including espionage and exposure of corporate data—was a primary theme this past year. APT attacks in 2013 were well-planned and well-funded; carried out by highly-motivated, technologically advanced, and skilled adversaries. Even after successfully accomplishing the mission, the APT continues to live on to gather additional information. Defending against the stealthy and persistent nature of APTs is a complex undertaking, and requires a coordinated approach on the systems as well as the network level [17]. Businesses and governments rightfully concerned about privacy and protecting sensitive data now have to be more aware of troublesome security issues that could be found in critical infrastructure systems. As we fly in airplanes, draw cash from a nearby ATM, or rely on a steady supply of electricity and water, we can no longer assume the security of these systems. Incidents of attacks on these critical network infrastructure and control systems demonstrate vulnerabilities in the essential infrastructure of our society. Systems including the smart grid infrastructure could become more of a focus for cybercriminals in the coming year. The growing popularity of the "Internet of Things" (e.g., mobile devices, applications, social networks, and interconnected gadgets and devices) makes the threat landscape a moving target. New threats arise with emerging technologies like near field communications (NFC) being integrated into mobile platforms. Innovative uses of GPS services to connect our digital and physical lives present new opportunities for cybercriminals to compromise our security and privacy. Such systems could yield attacks that have a very personal impact on each of us. In 2014 we need to start watching not just the evolution of existing attacks, but new types emerging that we haven't previously dealt with [17].

B. Botnet Grow In Size And Stealth

In the past 12 months, botnets have become more widespread, resilient and camouflaged—and they seem to be finding some dangerous new targets. Botnet source code has traditionally been tightly protected by its owners. Even when

cybercriminals choose to retire from running botnets, they can often sell their code at high prices. But in recent years, working botnet source code has been leaked. This allows imitators to create their own new botnets, and then evolve them to behave in ways the original coders never imagined [17].

C. Botnets Are More Resilient

Botnets are now integrating multiple backup forms of command and control. For example, if a botnet-infected client such as Gameover can't connect to addresses of other infected machines on the network, it runs built-in "domain generation" algorithms. If these algorithms discover even one of the new centralized command and control C&C servers that have been established, the client can restore its active role on the botnet [17].

D. Botnets Delivering More Dangerous Ransomware

As users grow more resistant to fake alerts and antivirus scams, more botnets are delivering ransomware instead. Now, users are faced with an absolute demand to pay exorbitant sums in order to restore access to their own data. Perhaps the most dangerous and widespread current example is Cryptolocker. This ransomware adds itself to the list of Windows programs that run at startup, tracks down an infected server, uploads a small ID file from your computer, retrieves a public key from that server (which stores a matching private key), and then encrypts all the data and image files it can find on your computer. Once your data has been encrypted by the bad guys, the only way to retrieve it is with the private key stored on their server—for which you have to pay the criminals (which we do not recommend) [19]. While Cryptolocker is sometimes delivered through email spam, it often arrives through botnets that have already infected you. In those cases, the bots are simply responding to an upgrade command that allows the crooks to update, replace, or add to the malware they've already dropped onto your PC—and you won't know until it's too late [20].

E. Android Malware: Mutating and Getting Smarter

Android malware continues to grow and evolve, following paths first blazed by Windows. But there is progress to report in securing the platform. Since we first detected Android malware in August 2010, we have recorded well over 300 malware families. And we have seen the Android malware ecosystem follow in many of the paths first established years ago by Windows malware [17].

F. Sophisticated At Avoiding Detection And Removal

Recently, we have seen great innovation in how Android malware seeks to avoid and counter detection methods. Ginmaster is a case in point. First discovered in China in August 2011, this Trojanized program is injected into many legitimate apps that are also distributed through third-party markets. In 2012, Ginmaster began resisting detection by obfuscating class names, encrypting URLs and C&C instructions, and moving towards the polymorphism techniques that have become commonplace in Windows malware. In 2013, Ginmaster's developers implemented far more complex and subtle obfuscation and encryption, making this malware harder to detect or reverse engineer [21]. Meanwhile, with each quarter since early 2012, we have seen a steady growth in detections of Ginmaster, reaching more than 4,700 samples between February and April 2013 [17].

G. New Android Botnets

Recently, reports surfaced of a large-scale botnet controlling Android devices in much the same way botnets have controlled PCs. This botnet, which Sophos detects as Andr/GGSmart-A, thus far seems limited to China. It uses centralized command and control to instruct all of the mobile devices it has infected; for example, to send premium SMS messages that will be charged to the device owner. Unlike typical Android attacks, it can change and control premium SMS numbers, content, and even affiliate schemes across its entire large network. This makes it better organized, and potentially more dangerous, than much of the Android malware we've seen before [22].

H. Securing Android

We're pleased that Google has taken some significant steps to further secure the Android platform in recent months. First, Android 4.3 eliminates automatic app downloads that existed in previous versions. Second, Google has tightened its Developer's Agreement, especially as it relates to potentially unwanted apps (PUAs), which aren't unmistakably malware but tend to behave in ways far more intrusive than most users desire. Google has identified several app and ad framework behaviors that will no longer be permitted. For example, developers can no longer place third-party advertising and links on the home screen, change the browser home page, or use the system notification area for purposes unrelated to their useful functionality [23]. The creators of malware, exploit kits and botnets became smarter and more aggressive in 2013. They identified new forms of attack, new ways to repurpose older approaches, new targets, and new techniques for hiding their activities [17].

VI. CONCLUSION

Defending against the new attacks requires us all to get smarter. Whether you're an IT professional, entrepreneur, or individual user, chances are you're getting smarter about security too. You are (or should be) making sure all your systems are protected, whatever conventional or mobile platform they're running on. Stay up to date with patches, because most attacks are aimed at old vulnerabilities. And do the security basics right (like using strong passwords, and training your users to evade social engineering). The battle for IT security won't end any time soon. But if you stay focused, apply best practices, judiciously use security technology, and get the right help, you can keep your organization safe. This research paper will lead all IT professionals to think more about the latest malwares to be developed such a way that all three entities will maintain the

balance between CRIMES and COMPUTER. Cybercrimes are happened when cyber laws are not efficient to remove them and cyber security and cyber forensic are not properly working with establishment technically by legislation but cyber security can be established when enough cybercrime, cyber laws and cyber forensic awareness are there among cyber users gradually. Cyber Crimes ever form perimeter for the three essential components cyber laws, cyber forensic and cyber security to be in runny mode. We wish good fortune for forthcoming generations.

This research work will provide enough sufficient information for awareness all over India to be implemented technically. ***Cyber Triangle of CYBER FORENSIC, CYBER SECURITY and CYBER LAWS rotating circular on the perimeter of CYBER CRIMES is concluded!!*** Security is no longer a "nice to have," but a must-have. The following model concludes the basic situation along with the reality existing a TRIANGLE OF CYBER!!

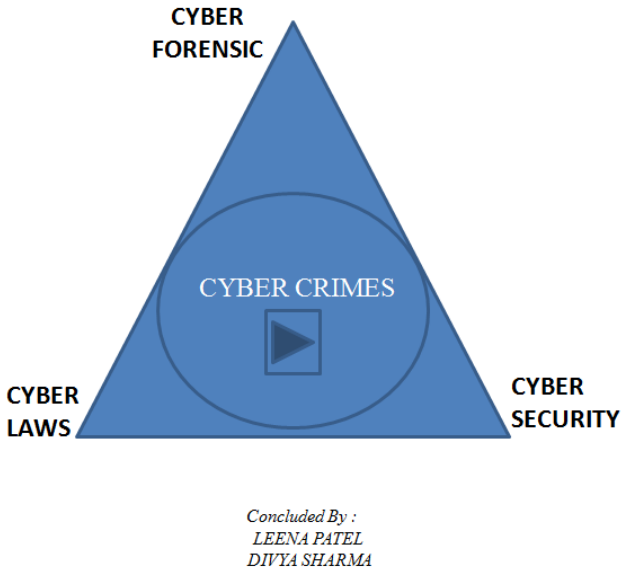

Figure. 5 Cyber Crimes

REFERENCES

[1] Yougal Joshi, Anand Singh. A Study on Cyber Crime and Security Scenario in INDIA, International Journal of Engineering and Management Research, Volume-3, Issue-3, June 2013. ISSN No.: 2250-0758 Pages: 13-18 at www.ijemr.net

[2] Praveen Dalal, Perry4Law, Cyber Security Must Be An International Issue. An Exclusive Techno-Legal Corporate, IP & ICT Law Firm, New Delhi, India. http://perry4law.org/,http://perry4law.com/,http://www.ptlb.in/.

[3] Perry4Law PTLB, Critical Infrastructure Protection In India: The Problems, Challenges And Solutions. An Exclusive Techno-Legal Corporate, IP & ICT Law Firm, New Delhi, India. http://perry4lw.org/, http://perry4law .com/,http://www.ptlb.in

[4] Perry4Law PTLB, Cyber Security Trends and Developments In India 2013 An Exclusive Techno-Legal Corporate, IP & ICT Law Firm, New Delhi, India.http://perry4lw.org/,http://perry4law.com/,http://ww .ptlb.in.

[5] Perry4Law PTLB, Cyber Warfare Policy of India an Exclusive Techno-Legal Corporate, IP & ICT Law Firm, New Delhi, India. http://perry4lw.org/, http://perry 4law .com/,http://www.ptlb.in.

[6] Perry4Law PTLB, E-Surveillance Policy of India Is Needed, IP & ICT Law Firm, New Delhi, India.http://perry4lw.org/, http://perry4law .com/, http:// www.ptlb.in.

[7] Perry4Law PTLB, International Cyber SecurityTreaty Is Required, IP & ICT Law Firm, New Delhi, India. http://perry4lw.org/,http://perry4law.com/,http://www.ptlb.in.

[8] Sonia Bui, Michelle Enyeart, Jenghuei Luong, Issues in Computer Forensics, COEN 150 Dr. Holliday May 22, 2003.

[9] Kruse and Heiser, op. cit., p. 3.

[10] Digital Evidence Collecting & Handling,. March 20, 2002. [Cited May 21, 2003]. http://faculty.ncwc. Edu / toconnor/495/495lect06.htm.

[11] Kruse and Heiser, op. cit., p. 15.

[12] Ibid., p. 13.

[13] K.K. Arthur, H.S. Venter, AN INVESTIGATION INTO COMPUTER FORENSIC TOOLS, Information and Computer Security Architectures (ICSA) Research Group University of Pretoria, Department of Computer Science University of Pretoria, 0002

[14] Reinke, J, Saiedian, H. The availability of source code in relation to timely response to security vulnerabilities (ABSTRACT). Computers and Security, Vol 22, Issue 8, December 2003.

[15] Judd, R, "An Explanation of c computer Forensics".http://www.computerforensics.net/forensics.htm. [ACCESSED May 10, 2014].

[16] Casey, E et al. HANDBOOK OF Computer Crime Investigation: Forensic Tools and Technology. Academic press, 2002. pp 53-71.http://www.accessdata.com [ACCESSED May 10, 2014].

[17] Security Threat Report 2014, Smarter, Shadier, Stealthier Malware, SOPHOS, Security Threat Report 2014. http://nakedsecurity.sophos.com/2013/12/11/smarter-shadier-stealthier-security-threat-report-2014-helps-you-understand-the-enemy/

[18] An Analysis of the Zeus Peer-to-Peer Protocol, Dennis Andriesse and Herbert Bos, VU University Amsterdam, The Netherlands, Technical Report IR-CS-74, rev. May 8, 2013, http://www.few.vu.nl/~da.andriesse/papers/zeus-tech-report-2013.pdf.

[19] CryptoLocker Ransomware - See How It Works, Learn about Prevention, Cleanup and Recovery, Sophos Naked Security,http://nakedsecurity.sophos.com/2013/10/18/cryptolocker-ransomware-see-how-it-works-learn-about-prevention-cleanup-and-recovery/

[20] Destructive Malware "CryptoLocker" on the Loose - Here's What to Do, Sophos Naked Security, 12 October

2013,http://nakedsecurity.sophos.com/2013/10/12/destructive-malware-cryptolocker-on-the-loose/.
[21] GinMaster: A Case Study in Android Malware, Rowland Yu, Sophos Labs Australia, Virus Bulletin, October 2013,http://www.virusbtn.com/pdf/conference_slides/2013/Yu-VB2013.pdf.
[22] Billion Dollar Botnets, Cathal Mullaney, Symantec, presented at Virus Bulletin, October 2013, http://www.virusbtn.com/conference/vb2013/abstracts/Mullaney.xml.
[23] Google Play Developer Program Policies, https://play.google.com/about/developer-content-policy.html

AUTHOR(S) DETAILS

LEENA PATEL
Assistant Professor
Computer Engineering Department
E-mail: divine.leena@gmail.com

DIVYA SHARMA
Assistant Professor
Information Technology Department
E-mail: divya21bhardwaj@gmail.com

