Digital Forensic and Systems Investigation Analysis

Sanja Mutong'wa Michael, Thomas Gisemba Onsarigo, Nyauncho Josiah

1Catholic University of Eastern Africa, Dept of Computer Science, P.O.Box 1031, Kitale
2MOI University, Lecturer - School of Arts and Social Sciences, P.O.Box 8346, Eldoret
3The Catholic University of Eastern Africa, Lecturer - School of Commerce, P.O.Box 132-30100, Eldoret

ABSTRACT

Computer forensics is used to bring to justice, those responsible for conducting attacks on computer systems throughout the world. Different users apply computer forensic systems, models, and terminology in very different ways. They often make incompatible assumptions and reach different conclusions about the validity and accuracy of the methods they use to log, audit, and present forensic data. The objectives of the study identifies various types of insecurities on systems; cyber-crimes and their impacts over organization, it examines possible causes and hence establishes the need for forensics evidence. The major forms of insecurity on systems worldwide is Cyber-attacks, cybercrimes, cracking, snooping, operation denial and data theft hacking .In this Judges plays a gatekeeper role in determining what scientific evidence and how it is admissible in their courtrooms .Our research presents several forensic systems and discusses situations in which we produce valid and accurate conclusions and also situations in which accuracy is suspect. Finally, the we presents some recommendations about how computer scientists, forensic practitioners, lawyers, teachers, judges and engineers could build implement forensics that take into account appropriate legal details and lead to scientifically valid forensic analysis.

Keywords: Cyber Attacks, Digital Forensics (DF), Cyber-crimes and Potential Economic Impact

1. INTRODUCTION

Digital Forensics is the art of discovering, retrieval of information about a crime in such a way to make it admissible to the court. Digital Forensics (DF) has grown from a relatively obscure tradecraft to an important part of many investigations, (Patrick D. Gallagher, June 2010). DF tools are now used on a daily basis by examiners and analysts within local, state and Federal law enforcement; within the military and other world government organizations .In today’s world of advancing technologies, more and more information is being generated, stored and distributed by electronic means. There are a huge number of cyber threats and their behavior is difficult to early understanding hence difficult to restrict in the early phases of the cyber-attacks, (Patrick D. Gallagher, June 2010).

According to Nance, Hay, & Bishop (2009) the digital forensics community involves an examination of technical issues such as network forensics, evidence modeling, and mobile devices rather than social aspects such as the understanding of digital evidence. Cyber-attacks may have some motivation behind it or may be processed unknowingly .This requires many agencies to increase the use of digital evidence gathering as a frequent or standard tool in their fight against cartels (Cohen. F. 2008). In the current era of online processing, Cyber security and online threats exploit the increased complexity and connectivity of critical infrastructure systems hence placing the global’s security, economy and public safety.

The objectives of the study identifies various types of insecurities on systems; cyber-crimes and their impacts over organization, it examines possible causes, the need for forensics evidence and integrated security solutions. The major forms of insecurity on systems worldwide is Cyber-attacks, cyber-crimes, cracking, snooping, operation denial and data theft hacking .Forensics refers to the application of scientific evidence in courts of law. Judges play a gatekeeper role in determining what scientific evidence is and how it is admissible in their courtrooms (Cohen, 2008, 2010; Jones)

1.1 WHY COMPUTER FORENSICS?

Forensics is the application of investigative and analytical techniques that conform to evidentiary Standards used in or appropriate for a court of law or other legal context .Chain of custody is the record of the custodial history of the evidence. Chain of evidence or authentication is the record of the collection, processing and analysis of the digital evidence. It proves that the presented evidence is unequivocally derived from the acquired digital information.
Computer forensics comes into play when a case involves issues relating to the reconstruction of computer system usage, examination of residual data, and authentication of data by technical analysis or explanation of technical features of data and computer usage, (Cohen. F. 2008). Computer Forensics requires specialized expertise that generally goes beyond normal data collection and preservation techniques available to end-users or system support personnel, (PGP Corporation, 2008).

Computer Forensics is the use of specialized techniques for the preservation, identification, extraction, authentication, examination, analysis, interpretation and documentation of digital information. Computer scientists can take steps to move computer forensics into a more rigorous position as a science by being able to make well-reasoned and concrete claims about the accuracy and validity of conclusions presented in court, (Cohen. F. 2008).

Computer Forensics requires specialized expertise that generally goes beyond normal data collection and preservation techniques available to end-users or system support personnel, (Cohen. F. 2008). Forensics may involve cryptography since it’s an authentication scheme that acts in the digital world as the equivalent of a handwritten signature on a paper document. It allows a person or organization to securely prove one’s identity to another person or organization while communicating over an unsecure communications network such as the Internet (PGP Corporation, 2008).

1.2. COMPUTER FORENSICS

Forensics is the application of investigative and analytical techniques that conform to evidentiary Standards used in or appropriate for a court of law or other legal context. Chain of custody is the record of the custodial history of the evidence. Chain of evidence or authentication is the record of the collection, processing and analysis of the digital evidence. It proves that the presented evidence is unequivocally derived from the acquired digital information, (Rogers et al., 2007).

According to R. B. Vaughn, personal communication, (July 22, 2010). Computer Forensics is the use of specialized techniques for the preservation, identification, extraction, authentication, examination, analysis, interpretation and documentation of digital information, (Rogers et al., 2007). This research considers the computer forensics to be a more rigorous position as a science by being able to make well-reasoned and concrete claims about the accuracy and validity of conclusions presented in court.

According to Rogers et al., (2007). It’s true that Computer forensics comes into play when a case involves issues relating to the reconstruction of computer system usage, examination of residual data, authentication of data by technical analysis or explanation of technical features of data and computer usage. It requires specialized expertise that generally goes beyond normal data collection and preservation techniques available to end-users or system support personnel, (Rogers et al., 2007).

1.3 DIGITAL INVESTIGATIONS AND CYBERCRIME ARE STILL NEW

Research show that judges’ perceptions about digital evidence has not been previously accomplished because the digital forensics research field has been, in large part, ill defined. Research reveals the digital evidence domain still lacks a universally accepted definition, foundational research, and a substantial body of literature (Rogers et al., 2007; Van Buskirk & Liu, 2006). Although computer forensics has been an area of active investigative practice by law enforcement (LE) for over 15 years, the use of digital evidence in court is still not widespread (Marsico, 2004; Rogers et al., 2007; Van Buskirk & Liu, 2006).

Digital investigations are still not routinely taught in most police academies (Carlton, 2006; Rogers et al., 2007); law schools and judicial colleges are just starting to emphasize digital evidence (Ball, 2008; Rogers et al., 2007, Van Buskirk & Liu); the formal study of computer forensics, digital investigations, and cybercrime remains a relatively new academic discipline (Carlton); and the under capacity of most agencies to examine all computers that could be seized results in an underuse of digital evidence (Rogers et al., 2007).

1.4 INTERNET AS A SOURCE TO CYBERCRIME

A number of companies worldwide have had to turn over e-mail in response to a civil lawsuit or regulatory investigation (Manes, 2007). Indeed, electronic discovery (e-discovery) is one of the fastest growing sub disciplines of computer forensics and is rapidly becoming the most costly part of civil litigation, thou rare in Kenya and other developing countries. Current era is too fast to utilize the time factor to improve the performance factor hence it is only possible due the use of Internet, (Mack, 2008). Internet being the collection of millions of
imposed upon conviction, (U.S. Courts 2008). Other
crimes or commanding it and for which punishment is
committed or omitted in violation of a law forbidding
the use of Internet. The cyber-crime being an act
directed related to the use of computers, specifically
illegal trespass into the computer system or database of
another, manipulation or theft of stored or on-line data,
or sabotage of equipment and data (U.S. Courts 2008).

1.5 THREATS ON-LINE

1.5.1 HACKERS AND TYPES OF HATS

Hackers: According to Michael M, Wasilwa and
Muneria (2014), Hackers are those individuals who
write programs or manipulate technologies to gain
unauthorized access to computers and networks or
diverge data or direct computers and networks to
unauthorized access. Sometimes malicious Active
Content delivered through web pages can reveal credit
card nos, mobile phone numbers, user names,
passwords and another information.

Our study reveals that majority of computer
users or everyone appreciates the use of Internet but
there is another side of the coin that is cyber-crime by
the use of Internet. The cyber-crime being an act
committed or omitted in violation of a law forbidding
or commanding it and for which punishment is
imposed upon conviction, (U.S. Courts 2008). Other
words represents the cyber-crime as Criminal activity
directly related to the use of computers, specifically
illegal trespass into the computer system or database of
another, manipulation or theft of stored or on-line data,
or sabotage of equipment and data (U.S. Courts 2008).

White Hats: According to (Martha A. Walker, 2011). White hats is the name used for security experts. While
they often use the same tools and techniques as the
black hats, they do so in order to foil the bad guys.
That is, they use those tools for ethical hacking and
computer forensics. Ethical hacking is the process of
using security tools to test and improve security (rather
than to break it!). Computer forensics is the process of
collecting evidence needed to identify and convict
computer criminals.

Black Hats: The “black hats” are the bad guys. These
are the people who create and send viruses and worms,
Blue Hat is process control “thinking about thinking”.
This is the hat worn by people chairing or facilitating
the session. Blue Hat may be used at the beginning of
the session to set the agenda or the sequence for using
the “hats” and at the end of the session when seeking a
summary and next steps. Blue Hat focuses on
questioning, fishing and shooting and provides the
structure for use of other hats and other

Green Hat stands for energy and creativity. According
to Martha A. Walker, (2011). This is where you generate
new, innovative ideas and develop creative solutions to
a problem. It is freewheeling way of thinking in which
there is little criticism of ideas, and “movement” is
made using provocation to move “forward with an idea
or from an idea. Seeking alternative solutions. Green
Hat thinking must involve shaping the idea for the user
or “buyer”.

Yellow Hat is a deliberate search for the positive
(optimistic viewpoint) through exploration and
speculation defining the benefits of the decision and
the value in it. Yellow Hat thinking is constructive
blending “curiosity, pleasure, greed, and the desire to
make things happen” (91) enhancing the proposal by
generating alternative ideas “based on experience,
available information, logical deduction, hints, trends,

Triggering is what relates a type of code to a real bomb. When setting up a bomb you would like to have
some time to run away before it explodes. This could
be done by setting a timer or by sending a radio signal
to the bomb when you’re out of danger. The same
principle applies to a logic bomb. You may plant a slag code somewhere in the financial system and tell it to “explode” 6 months from the current date. If you’re still an employee at this time you can add another 6 months to the counter, but if you’ve been fired the destructive payload will be unleashed. Here is a list of possible triggers that exist. This list is not exhaustive, but the most common triggers are listed here: Specific date/time: The payload will be executed when the system clock is equal or higher than the specified date/time.

1.5.2 PASSWORD CRACKING

Password crackers are among the most common and elementary tools in the hacker toolkit. These have been around for some time and are fairly effective at “guessing” most users’ passwords, at least in part because most users do a very poor job of selecting secure passwords. The first step to password cracking is often simple guesswork, Wolfe 2001).

While passwords may deter many users, the investigator should be able to recover these files. Password cracking programs can be used to gain access to password protected files. There are few passwords that cannot be cracked. Most people use weak passwords which makes recovering these files fairly easy with the right software. The evidence sought after may be encrypted. It is usually infeasible to try to crack encryption unless weak encryption is used. It is highly unlikely that strong encryption can be broken but it may be possible to find the encrypted files on other parts of the drive (Wolfe 2001).

This research reveals that an investigator is better off leaving these files alone or else convincing the suspect to decrypt them. If the private keys cannot be obtained, there may be a trace of the encrypted file residing on the drive from before it was encrypted. This is made easy by social engineering. Hackers know that most users select simple passwords that are easy to remember.

1.5.3 MALICIOUS CODE

According to Eduardo Gelbstein and Ahmad Kamal (2014) “Malicious code” is an umbrella term for any computer software designed to make computers perform unwanted actions. Two best known forms of malicious code are viruses and worms. (Viruses use software in the affected machine to replicate. Worms are self-replicating). Various forms of malicious code include:

Macros written for Microsoft Office applications (file extension .vbs). This was used in the Melissa virus (.Executable files (file extension .exe). A recent virus was hidden in a digital picture file (file extension .jpeg). This technique is called steganography.

Trojan Horse software which performs legitimate functions but which includes within it malicious code Forms of malicious code have been in existence since early computer applications, in this case designed and introduced by expert programmers. Examples of such code include: Logic bomb, Back door or unauthorized, Super-user rights, fraudulent transactions. The following case provides a sufficient example the legal rights involved in computer forensics. In the winter of 1999, during contract negotiations, a Northwest Airlines flight attendant hosted a message board on his personal website; among the messages were anonymous messages by Northwest employees urging co-workers to participate in sick-outs, which is illegal by U.S. federal labor laws. That season over 300 flights were cancelled.

Northwest Airlines subsequently obtained permission from a federal judge to search union office computers and employee personal computers, in order to obtain the identities of the anonymous posters (Caloyannides 2001). Note that the employer was granted the right to view not only the office computer, but the personal ones as well. The question on the table is how can that be possible? One may argue that the constitution prohibits such actions and that the accused should have had some form of legal protection against such an intensive search.

1.6 SAVE GUARD OUTSIDE ATTACKS USING FIREWALLS

This research considers the firewall as one of the best remedy to save guard outside attacks on Mobile money transfer transaction. Firewall is a combination of hardware and software that sits between the internet and internal network of an organization to protect the network from outside attack. Rapid growth of cybercrime takes the interest of researchers in the world of digital forensic. Digital forensic is a science to help the investigator in order to identify & analyze the evidence which are collected from the computers or the networking devices. As far as the digital forensic is concern it works with the multi-relation classification, (Xue-Gang Hu el at., 2005, Rogers, m.k. And k. Seigfried, (2004).

Most of the time it seems to be that the investigation has to perform with huge data set. When data is large there is a need to narrow the search for the criminal. It is a major problem before us Rogers, m.k. And k. Seigfried, (2004). Firewalls can examine the
data entering or leaving from the network and can filter the data according to certain rules, thus, protects the network from an attack. This research considers four main types of Packet filter firewalls i.e Packet filter firewall, Circuit level firewall, Application gateway firewall, Screened host firewall and Cryptography.

1.7 FACT-FINDER.
According to Cohen, F. (2008) the fact-finder is the person or body responsible for listening to testimony and reviewing evidence to determine the facts of the case. In a jury trial, the jury is the fact-finder; in a bench trial, the judge is the fact-finder (U.S. Legal, 2010). According to Jones A(2009) assessing the impact of losses , the insecurity cause and make recommendations to the organizations globally. It can harm an organization’s ability to innovate and to gain and maintain customers. The attacks, those that are processed knowingly can be considered as the cyber-crime and they have serious impacts over the society in the form of economical disrupt, psychological disorder, threat to National defense, Cohen, F. (2008) . Restriction of cyber-crimes is dependent on proper analysis of their behavior and understanding of their impacts over various levels of society.

2. LITERATURE REVIEW

2.1 GATEWAY FIREWALL
Gateway Firewall operates at application layer of the OSI Model. It uses strong user authentication to verify identity of a host attempting to connect to the network using application layer protocols such as FTP (File transfer Protocol). In contrast to packet filter firewall, it filters the requests rather than packets entering/leaving the network. It can block any outgoing HTTP (Hyper Text transfer Protocol) or FTP requests. It can prevent employees (in the Mpesa, banking centers of a company inside a firewall from downloading potentially dangerous programs from the outside. In other words, this type of firewall is used to control connections thus employees of a company can be restricted from connecting to certain web sites.

This research considers the following Figure: 5 Firewall, proxy server and DMZ (Demilitarized Zone).When a high proportion of individuals in a country feel powerless to prevent political outcomes unfavorable to them, cynicism may become widespread and lead to a decline in support for the political system. Another view presents the decrease in political trust as a more contingent reaction to the performance of incumbent political leaders. In short, a loss of political support simply reflects dissatisfaction with the authorities holding power at a given point in time (Citrin 1974; Citrin and Green 1986). More recent work has also emphasized the importance of political performance on support for democratic regimes, especially in new democracies. Mishler and Rose (2001) show that transitional governments can generate system support by responding effectively to public priorities and by protecting the newly acquired freedoms.

2.2 CHAIN OF CUSTODY
According to Ashish.G.Florent. K and Natarajan,(2009), When a piece of evidence is to be presented in a court, the chain of custody of the evidence must be established to guarantee that it has not been tampered with. The process makes two assumptions that do not hold by default in the virtual world. The first is that the evidence was not altered from the time it was created to the time it was collected. In a world where data is rapidly combined to produce new content, it is likely that the data found during an investigation will have already undergone editing operations before it was collected as evidence. The second assumption is that a piece of evidence was created by a single individual. A virtual object is much more likely to have multiple co-author.

2.3 SECURITY ISSUES OVER THE INTERNET
According to Jon(2011) Security issues over the internet as a hindrance to mobile money transfer since majority of the attacks against web servers are through network firewalls and through the http (hypertext transfer protocol Some of the most commonly used hacking techniques include denial of service, leakage, cross-site scripting, SQL (structured query language) injection and disclosure (Jon, 2011).

Security is the biggest factor slowing down the growth of ecommerce worldwide issue of computer and data security is the biggest hurdle in the growth of mobile money transfer. Web servers also face this security threat. Programs that run on a server have the potential to damage databases, abnormally terminate server software or make changes in the information placed there. A number of international organizations have been formed to share information and combat security threats to computers and computer networks (Jon. P,2011).
2.4 VOLUME OF DIGITAL EVIDENCE

According to U.S. Legal, (2010). Evidence refers to information that can be introduced at trial to help judges and juries make a decision in criminal and civil legal cases. The court has to balance the probative value of the evidence (i.e., whether the information has relevance to the case and can help prove or disprove a fact or question in dispute) against the potential prejudicial nature of the evidence (i.e., whether the information will unfairly influence the judge or jury) (Cohen, 2008, 2010; Kerr, 2009; U.S. Legal, 2010).

Managing the growing volume of digital evidence is even more daunting in civil litigation. With the pervasive use of e-mail in the corporate world, computer forensics has long been considered one of the most important processes in civil cases (Bensen, 2004). The growing popularity of mobile devices such as cell phones, PDAs, and digital cameras has made them so ubiquitous that such devices are found at nearly every arrest and crime scene. Increasingly, according to (Losavio, Wilson, & El maghraby, 2006; Mislan, Casey, & Kessler, 2010) these devices contain information related to criminal activity. This research reveals that digital devices are widely used by all segments of the population; are the source of a growing amount of evidence; and employ processing, storage, and communication technologies that are not fully understood by most users (Leroux, 2004; Losavio et al.; Van Buskirk & Liu, 2006).

2.5 HACKER BREAK MODEMS TO ACCESS

2.5.1 Telephone modems

According to David M. Nico (2011) circuit breakers have historically been controlled by devices connected to telephone modems so that technicians can dial in. It is not difficult to find those numbers; hackers invented programs to dial up all phone numbers within an exchange and make note of the ones to which modems respond. Modems in substations often have a unique message in their dial-up response that reveals their function. Coupled with weak means of authentication (such as well-known passwords or no passwords at all), an attacker can use these modems to break into a substation’s network for telephone modem. From there it may be possible to change device configurations so that a danger condition that would otherwise open a circuit breaker to protect equipment gets ignore.

Data communications between the control station and substations use specialized protocols that themselves may have vulnerabilities. If an intruder succeeds in launching a man-in-the-middle attack, that individual can insert a message into an exchange (or corrupt an existing message) that causes one or both of the computers at either end to fail. An attacker can also try just injecting a properly formatted message that is out of context—a digital non sequitur that crashes the machine.

2.5.2 Hacking Electrical Power Industry

Attackers can also use clever methods that exploit the economics of the power industry. Because of deregulation, competing utilities share responsibility for grid operation. Power is generated, transmitted and distributed under contracts obtained in online auctions. These markets operate at multiple timescales one market might trade energy for immediate delivery and another for tomorrow’s needs, (David M. Nico 2011). Normally the electrical control station must have up-to-the-second information about what is going on at every step of the process for technicians to make smart decisions about what to do next. Hackers with access to thousands of ordinary computers—a so-called botnet—could direct these machines to send messages that interrupt the flow of ordinary network traffic. Such a denial-of-service attack would mean that control operators would be making decisions based on old information—something akin to driving a car using the information you had 10 seconds ago, (David M. Nico2011).

According to David M. Nico (2011) transmission substation or Electricity coming out of generating stations comes at very high voltages the better to avoid losses from electrical resistance en route. Transmission substations are the first step in bringing this voltage down. Many older stations have dial-up modems so that technicians can dial in and perform maintenance. At the Generating station electricity going into the main power grid must alternate and enters perfectly aligned with the rhythm of the rest of the grid. An attacker might send instructions to a generator that throws its output off by a half-step, the electrical equivalent of throwing your car into reverse while heading down the highway at 50 miles per hour. The generator—like your car’s transmission will end up a smoking heap.

At distribution Substation normally before electricity goes into homes or businesses, these substations might combine power coming in from a few different power stations and send it out on dozens or hundreds ofaller lines. Newer stations might be equipped with wire-less communications equipment either radio signals or Wi-Fi.
A hackers who hides just outside a station’s walls could intercept traffic and mimic legitimate instructions. Hackers can use these devices to access and change critical settings. A utility’s business unit must have a constant flow of real-time information from its operations unit to make smart trades. (And vice versa: operations need to know how much power they need to produce to fulfill the business unit’s orders.) Here the vulnerability lies. An enterprising hacker might break into the business network, ferret out user names and passwords, and use these stolen identities to access the operations network. The cyber attacker then sends an engineer at the power plant a forged e-mail that tricks the engineer into fetching and opening the booby-trapped manual. Just by going online to download an updated software manual, the unwitting engineer opens his power plant’s gates to the Trojan horse, (David M. Nico 2011).

2.6 DIGITAL EVIDENCE

Digital information is all information in digital form and can be divided into the content itself (of a text document, a drawing or photo, a database, etc.), and the information about this content, the so called metadata (filenames, pathnames, the date and time that a document has been created or edited or an e-mail has been sent, received or opened, the creator/sender of a document or e-mail etc. It is often not possible to handle digital information without acquiring knowledge of at least some of this metadata.

Digital evidence is all digital information that may be used as evidence in a case. The gathering of the digital information may be carried out by confiscation of the storage media (data carrier), the tapping or monitoring of network traffic or, the making of digital copies (forensic images, file copies, etc.), of the data held. Although hard copy print outs of digital information are not digital evidence in the strict sense of this definition, it is considered a starting point for applying digital evidence gathering in the future.

According to Casey, (2011) In the U.S., computing devices such as laptop and desktop computers, mobile telephones, PDAs, and portable music players are nearly ubiquitous. Since the turn of the century, these devices have become increasingly the target, record keeper, and/or instrument of all types of illegal activities and, therefore, the source of a growing amount of evidence in criminal and civil court proceedings. The Federal Bureau of Investigation (FBI), for example, reports that nearly 80% of their cases involve some form of digital evidence, and the number is even higher for the U.S. Secret Service (Rogers et al., 2007). While the FBI, Secret Service, and other federal agencies respond to this growing need with well-trained and well-funded cybercrime units, the response at the local level is comparatively slight because most local law enforcement agencies in the U.S. have one investigator assigned to computer crimes (NIJ, 2007; Scarborough et al., 2009).

2.7 APPLICATION OF DIGITAL SIGNATURES

Digital signatures can be used for many types of documents where traditional pen-and-ink signatures were used in the past. However, the mere existence of a digital signature is not adequate assurance that a document is what it appears to be. Moreover, government and enterprise settings often need to impose additional constraints on their signature workflows, such as restricting user choices and document behavior during and after signing. An encryption (or decryption) procedure typically consists of a general method and an encryption key. The general method, under control of the key, enciphers a message M to obtain the enciphered form of the message, called the cipher text C. Everyone can use the same general method; the security of a given procedure will rest on the security of the key.

This research reveals an encryption algorithm then means revealing the key. If electronic mail systems are to replace the existing paper mail system for business transactions, "signing" an electronic message must be possible. The recipient of a signed message has proof that the message originated from the sender. This quality is stronger than mere authentication (where the recipient can verify that the message came from the sender); the recipient can convince a "judge" that the signer sent the message. To do so, he must convince the judge that he did not forge the signed message himself! In an authentication problem the recipient does not worry about this possibility, since he only wants to satisfy himself that the message came from the sender.

2.7.1 PUBLIC KEY INFRASTRUCTURE

PDF’s digital signature capabilities are designed for compatibility with all the standards associated with mainstream public key infrastructures (PKI) deployed in enterprise and government settings. A PKI is the set of people, policies, procedures, hardware, and software used in creating, distributing, managing, and revoking, and using the digital IDs that contain the public/private key pairs used when signing a PDF. In the context of PDF signature workflows, “PKI” generally refers to the digital ID issuers, users, administrators, and any hardware or software used in
those workflows. PDF viewers that implement and conform to the PDF language specification are able to interact with all of these components in a seamless and robust way.

2.7.2 FIREWALLS PROTECTION

A firewall protects only the perimeter of its environment against attacks from Outsiders who want to execute code or access data on the machines in the protected environment. Firewalls cannot protect from internal threats (through disgruntled employees). Firewalls cannot protect against malware imported via laptop, PDA, or portable storage device infected outside the network, then attached and used internally. Firewalls can be held responsible for any security breach in if they are the only Means to control the entire network perimeter.

If a host in the inside network has a connection to the outside network through a modem, the whole of the inside network is exposed to the outside network through the modem and the host. A firewall cannot be responsible for any attack. Firewalls cannot protect data after they have left them. A firewall is often a single point of failure for a network. A more layered approach like a screening router, followed by a proxy firewall, followed by a personal firewall may be more helpful. Firewalls must be frequently configured and updated to take into account the Changes in the internal and external environment and based on the review of the firewall activity reports that may indicate intrusion attempts.

2.8 WORLDWIDE THREAT OF CRIME AND TERRORISM

2.8.1 CRIMINAL VIOLENCE IN LATIN AMERICAN COUNTRIES

The issue of the impact of criminal violence on political support in Latin America has been completely neglected until very recently. In the last decade, some works focusing exclusively on Central America started to address this issue. Orlando Pérez (2004) analyzes how democratic legitimacy is affected by public insecurity in El Salvador and Guatemala. While much more sophisticated on the methodological front, the work of José Miguel Cruz (2003) still begs the question of the generalizability of his conclusions. Cruz demonstrates that criminality and violence have a negative impact on regime legitimacy in three Central American countries (Nicaragua, Guatemala, and El Salvador).

Criminal violence is more widespread in these three countries (especially El Salvador and Guatemala) than in most other Latin American countries. This paper will try to assess if the findings of Cruz are also valid in other countries in Latin America, where criminal violence has also increased considerably but still remains at much lower levels. Another recent contribution explores how violence affects support for political institutions in Latin America (Richard and Booth 2008).

But the authors focus on political violence and political terror, thereby ignoring the more timely preoccupation with criminal violence. The present paper intends to fill the gaps identified in the previous works, in order to gain a broader understanding of the impact of criminal violence on political support in Latin American countries. I contend that crime-related variables may be essential for understanding system support in Latin America, where criminal violence has increased exponentially since the return to democratic rule. Victimization and high perception of violence may lead to a decrease in support for the political system for three main reasons. First, Latin American citizens exposed to criminal violence may become disenchanted with a political system that is unable to respond efficiently in one of their main areas of concern (public security). Second, they may grow dissatisfied with a judicial system that fails to punish those responsible for the increasing levels of violence. Third, direct or indirect exposure to criminal violence may have a negative impact on interpersonal trust which in turn negatively affects system support.

2.8.2 REDUCE WORLDWIDE THREAT OF CRIME AND TERRORISM

With the worldwide threat of crime and terrorism increasing daily, the demand for high quality, fully networked video surveillance systems is also growing rapidly. Users are demanding new capabilities and greater efficiency from their security systems. Samsung Techwin is committed to its goal of producing high performance products that introduce features and capabilities able to push the boundaries of what can be achieved. We are redefining what you should expect from a total security solution.

Samsung Integrated Security Solution brings cutting-edge security equipment and advanced systems together into one centrally managed, fully integrated solution. Designed to deliver an optimized security solution for a host of applications, including critical infrastructure, national defense, urban security and Intelligent Traffic Systems (ITS); Samsung Techwin’s solution is the result of Samsung’s technical evolution.
and innovation with the goal to create a safer, more convenient world.

It is commonly thought that elections help to secure the positive legitimacy of the political order, leading citizens who may vehemently disagree with the current course of public policy to accept the government’s right to rule, to comply voluntarily with duly enacted laws, and to channel their disagreements toward the next election. The Supreme Court’s constitutional election law jurisprudence seems motivated, at least in part, by a desire to ensure that American elections perform this function.

As yet, however, the Court’s legitimacy-minded interventions have been predicated on judicial surmise about the relationship between election law and positive legitimacy. Recent research by political scientists has cast doubt on some of the Court’s suppositions, while also suggesting that features of the electoral process which the Court has treated as inconsequential may have significance for empirical legitimacy.

It will not be long before this body of work is regularly cited in legal briefs. That will put pressure on the courts either to clarify the sense in which the exigencies of empirical legitimacy inform the substance of (and limitations upon) constitutional political rights, or else to abandon the notion that citizens’ legitimacy-related beliefs or behaviors have doctrinal relevance. In recognition of the moment at hand, I seek in this paper to clarify why a reasonable judge might want to make constitutional election law responsive to social science findings about positive legitimacy; to summarize the relevant empirical findings to date; and to outline a path forward for the courts.

2.8.3 INTERNATIONAL SECURITY ATTACKS

Modern military of most of the countries depends heavily on advanced computers. Information Warfare, including network attack, exploitation, and defense, isn’t a new national security challenge, but since 9/11 it has gained some additional importance. It can easily spread malware, causing networks to crash and spread misinformation. Since the emphasis is more on non-information warfare, information warfare is definitely ripe for exploration. The Internet has 90 percent junk and 10 percent good security systems . When intruders find systems that are easy to break into, they simply hack into the system. Terrorists and criminals use information technology to plan and execute their criminal activities. The increase in international interaction and the widespread usage of IT has facilitated the growth of crime and terrorism. Because of the advanced communication technology people need not be in one country to organize such crime. Hence terrorists and criminals can find security loopholes in the system and can function from unusual locales instead of their country of residence.

Most of such crimes have been originating in developing countries. The widespread corruption in these countries fuel these security hacks. The internet has helped fund such crimes by means of fraudulent bank transactions, money transfer etc. Greater encryption technology is helping these criminal activities.

2.8.4 INTERNATIONAL LAWS AND LEGAL BODIES

European Council Cyber-Crime Convention: Establishes international task force overseeing Internet security functions for standardized international technology laws. Attempts to improve effectiveness of international investigations into breaches of technology law. Well received by intellectual property rights advocates due to emphasis on copyright infringement prosecution!

Lacks realistic provisions for enforcement. The issue of political support has attracted considerable scholarly attention, especially since the beginning of the Third Wave of democratization, which brought about many fragile democracies in which political legitimacy has wavered (Inglehart, 2003).

Political support has been defined as the way in which a person evaluative orient toward the political system i.e. political institutions and the values undergirding the regime- through his attitudes or his behaviors (Easton 1975). Easton’s original conceptualization of political support was very broad. Easton identified three objects of political support: the political community, the regime, and the authorities (Easton 1965). Since the publication of this seminal work, the issue of regime support –i.e. support for political institutions and regime values- and support for politica authorities has received considerable scholarly attention. Support for the performance of political authorities is associated with specific support, while the concept of diffuse support is associated with the citizens’ attitudes toward the political system (i.e. political institutions). In this paper, I will focus on
diffuse support or system support, even if I will control for the possibility of a positive correlation between specific support and diffuse support, as this is a hypothesis that has been advanced in the literature. Political support is very closely linked to the concept of political legitimacy and trust in government institutions. Political trust refers to the evaluation of the performance of the political institutions according to normative expectations (Miller 1974b). The mainstream explanation of political support at the individual level is the performance of government. Some scholars focus on the political performance of the governmental authorities. Miller (1974a, 1974b) focuses on structural problems of the political system that can have a negative impact on political support. He argues that sustained discontent may crystallize when members of a given social group in a divided society are continuously unable to influence the political sphere through voting or other means.

2.8.5 SOLUTION BY FBI TO CRACK DOWN CYBERCRIME

Digital evidence is one of the evidence to facilitate FBI in cracking down cybercrime. Digital evidence comes from a variety of sources including computing devices (e.g., desktop and laptop computers, digital cameras, music players, personal digital assistants (PDAs), and cellular telephones); network servers (e.g., supporting applications such as Web sites, electronic mail (e-mail), and social networks); and network hardware (e.g., routers found in businesses, homes, and the backbone of the Internet) (Brown, 2010; Casey, 2011; NIJ, 2007).

According to Dominic Rushe,( 2011), Cyber crime as outlined by FBI includes three types, first organized crime groups focuses on Cybercrime. However, this category appears limited to those crimes that target the financial services sector. While the second category includes the theft of intellectual property and other activities that may be considered cybercrimes, this category is more roughly aligned with state sponsored espionage.

The distinction between cybercrime and other cyber-based malicious acts such as terrorism or state sponsored espionage is the actor’s motivation. Information of evidentiary value may be found on digital media such as compact discs (CDs), digital versatile discs (DVDs), floppy disks, thumb drives, hard drives, and memory expansion cards found in digital cameras and mobile phones (Brown; Casey; NIJ).

Cyber criminals can exhibit a wide range of self-interests, deriving profit, notoriety, and/or gratification from activities such as hacking, cyber stalking, and online child pornography. As one FBI agent specializing in cybercrime has reported stated, “Hacking into a company, whether it’s to put information on the web for everyone to see or if you’re going to make money, is still hacking, it’s still a crime.” As such, the FBI’s conceptualization of cybercrime surrounds the activities primarily financial of organized crime groups, FBI considers these malicious activities under the umbrella of cybercrime.

The FBI may prioritize investigation of criminal organizations engaging in cybercrime over lone actors. While there is a clear distinction that organized crime groups are motivated by profit and terrorists are motivated by ideologies, the motivation of state sponsored cyber threat actors may be more difficult to categorize and determine. This may be in part because different state sponsored actors may have different motivations, as is implied by the FBI description of the range of state sponsored cyber threats.

2.8.6 ACCEPTABILITY OF DIGITAL EVIDENCE

To make informed and proper decisions about the acceptability of digital evidence sources and expert testimony, judges and other judicial panels must be knowledgeable in a variety of information and communication technology (ICT) areas (Gary.C.Kessler 2010). The knowledge is on personal experiences involving the use of computers, Telephony and networks such as the Internet (Cohen, 2010).

This research recommends that judges must be able to balance the imperatives of a thorough examination with the needs of a speedy trial (Casey, 2009). Very few people are not consciously aware about the impact that digital devices and the large volume of data stored in digital repositories have on everyday operations. Consider automated operations and functions within computer controlled buildings, utility company facilities, and telecommunication carrier networks; data gathered by security systems, closed-circuit television, surveillance cameras, and automobiles; and online activities such as e-mail, online payment systems, and social networks all the above causes complication digital evidence,(Gary.C.Kessler 2010).
3. RECOMMENDATION

There is need for consistent training of the Police in Cyber Crime Prevention and Forensic science for cyber-crime policy and control. Development of national community education and training targeted at school children and senior communities.

Establishment of a centralized national reporting Centre such as the IC (Internet Computer Crime Complaints Centre) in the US which is managed by the FBI which is online crime reporting Centre and clearing house for cyber-crime. The IC plays a pivotal role in detecting and reporting the identity of cyber criminals and proving information to victims of cyber-crime.

Deployment of Biometrics and device fingerprinting supported by secure gateways and quality encryption. This strategy will assist in overcoming the anonymity of a good deal of internet activity and provide enhanced security. There is urgent need to develop a single national database to gather and compile cybercrime data. The National Assembly should consider enacting a legislation that encourages incident reporting while reducing the risks associated with reporting and provide policies that provide stronger sentences for those found guilty of committing a cybercrime. There is need to establish a partnership amongst the academic, law enforcement to educate the society on when and how to report cyber-crime incidents and cyber-crime prevention. Every organization should increase investment in information security to reduce the level of victimization to cybercrime.

4. CONCLUSION

This research put its eye not only on the understanding of the cyber-crimes but also explains the impacts over the different levels of the society. This will help to the world community to secure all the online information critical organizations which are not safe due to such cyber-crimes. The understanding of the behavior of cyber criminals and impacts of cyber-crimes on society will help to find out the sufficient means to overcome the situation.

The way to overcome these crimes can broadly be classified into three categories: Cyber Laws (referred as Cyber laws), Education and Policy making. All the above ways to handle cyber-crimes either are having very less significant work or having nothing in many of the countries. This lack of work requires to improve the existing work or to set new paradigms for controlling the cyber-attacks.

REFERENCES


APPENDIX I

DEFINITIONS OF TERMS

Computer Forensics is the use of specialized techniques on a computer system for the preservation, identification, extraction, authentication, examination, analysis, interpretation and documentation of digital information.

Digital information is all information in digital form and can be divided into the content itself (of a text document, a drawing or photo, a database, etc.), and the information about this content, the so called metadata (filenames, pathnames, the date and time that a document has been created or edited or an e-mail has been sent, received or opened, the creator/ sender of a document or e-mail.

Digital evidence is all digital information that may be used as evidence in a case. The gathering of the digital information may be carried out by confiscation of the
storage media (data carrier), the tapping or monitoring of network traffic c, or the making of digital copies (forensic images, file copies, etc), of the data held.

**Forensics** is the application of investigative and analytical techniques that conform to evidentiary Standards used in or appropriate for a court of law or other legal context.

**Chain of custody** is the record of the custodial history of the evidence.

**Chain of evidence** or authentication is the record of the collection, processing and analysis of the digital evidence. It proves that the presented evidence is unequivocally derived from the acquired digital information.

**Characteristics of Information:** It has three characteristics: It is based on substances such as ; it can be recorded and retrieved and it has value. It can exist in many forms, e.g. written, printed, spoken, electronically stored, physically transmitted or transmitted in electronic form.

**A Data carrier:** is any device that contains or transports digital information and includes a physical hard drive, a floppy disk, Personal Digital Assistants (PDAs), Universal Serial Bus devices (USBs), a SIM-card from a cell phone, a flash memory stick/card, a network and a server, etc.

**Hash value** is a mathematical algorithm produced against digital information (a file, a physical disk, a logical disk) thereby creating a digital fingerprint for that information. It is by purpose a one-way algorithm and thus it is not possible to change digital evidence, without changing the corresponding hash values. In other words, if the hash value of a file has (not) changed, the file itself has (not) changed.

**Forensic image** (sometimes called a forensic copy) is an exact bit-by-bit copy of a data carrier including slack, unallocated space and unused space. There are forensic tools available for making these images. Most tools produce information, like a hash value, to ensure the integrity of the image.

**Computer Forensics** is the use of specialized techniques for the preservation, identification, extraction, authentication, examination, analysis, interpretation and documentation of digital information.