ABSTRACT

Information security is a growing concern for governments, companies, and people who base their day to day activities on computers. There are different motivations for security attacks, and they can originate from external sources such as hacker attacks, or employees from within the organization. One of the most important sources of evidence for a forensic investigator is the security logs that contain much of the activity happening in the computer infrastructure. High level hackers have the ability to delete this evidence after they have committed their crime. This situation can lead any investigation to a death end. Another current development affecting information technology is Cloud Computing, which is based on Virtual environments. Virtualization is a recent trend that besides a reduction in costs, and improvement in the efficiency of hardware resources use, also offers some benefits in terms of security. The purpose of this research project is to demonstrate the capabilities of well known forensic tools to recover log files after they have been deliberately erased. The forensic analysis is performed in a virtual server containing the security logs.
DEDICATION

To my lovely wife and parents for all the support they have provided during my pursuit of this graduate degree.
ACKNOWLEDGEMENTS

I would like to thank my committee chair and thesis advisor, Dr. Mario Garcia for his guidance and support throughout my graduate experience at Texas A & M University – Corpus Christi (TAMUCC). Thanks also go to my friends and colleagues and the department faculty and staff for making my time at TAMUCC a great experience. Finally, thanks to my wife for her patience and love and to my mother, father and brother for their encouragement and support.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABSTRACT</td>
<td>iii</td>
</tr>
<tr>
<td>DEDICATION</td>
<td>iv</td>
</tr>
<tr>
<td>ACKNOWLEDGEMENTS</td>
<td>v</td>
</tr>
<tr>
<td>TABLE OF CONTENTS</td>
<td>vi</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td>viii</td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td>ix</td>
</tr>
<tr>
<td>1. INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>2. NETWORK SECURITY</td>
<td>3</td>
</tr>
<tr>
<td>2.1. Defense in Depth</td>
<td>3</td>
</tr>
<tr>
<td>2.2. Security technologies: Firewalls, IDSs, NAT, Proxy Servers</td>
<td>8</td>
</tr>
<tr>
<td>2.3. Incident Response</td>
<td>13</td>
</tr>
<tr>
<td>3. DIGITAL FORENSICS</td>
<td>17</td>
</tr>
<tr>
<td>3.1. Static Acquisition</td>
<td>17</td>
</tr>
<tr>
<td>3.2. Live Acquisition</td>
<td>18</td>
</tr>
<tr>
<td>4. HACKERS &amp; OTHER THREATS</td>
<td>20</td>
</tr>
<tr>
<td>5. NETWORK FORENSICS</td>
<td>24</td>
</tr>
<tr>
<td>6. VIRTUAL INFRASTRUCTURES</td>
<td>26</td>
</tr>
<tr>
<td>7. SECURITY LOGS</td>
<td>32</td>
</tr>
<tr>
<td>8. MOTIVATION</td>
<td>38</td>
</tr>
<tr>
<td>9. EXPERIMENTS AND TEST</td>
<td>39</td>
</tr>
<tr>
<td>10. CONCLUSIONS &amp; FUTURE WORK</td>
<td>53</td>
</tr>
</tbody>
</table>
**LIST OF FIGURES**

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Defense in Depth Layers</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>Defense in Depth Pillars</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>Windows Event Viewer</td>
<td>27</td>
</tr>
<tr>
<td>4</td>
<td>Syslog Message Format</td>
<td>33</td>
</tr>
<tr>
<td>5</td>
<td>Virtual Architecture</td>
<td>35</td>
</tr>
<tr>
<td>6</td>
<td>Corporate Network Topology</td>
<td>40</td>
</tr>
<tr>
<td>7</td>
<td>Virtual Environment</td>
<td>41</td>
</tr>
<tr>
<td>8</td>
<td>Kiwi Syslog Server</td>
<td>42</td>
</tr>
<tr>
<td>9</td>
<td>Location of Kiwi Security Log Files</td>
<td>43</td>
</tr>
<tr>
<td>10</td>
<td>Cisco Pix515e Firewall Logs Configuration</td>
<td>44</td>
</tr>
<tr>
<td>11</td>
<td>NMAP Application</td>
<td>45</td>
</tr>
<tr>
<td>12</td>
<td>Data Acquisition – Virtual Machine</td>
<td>47</td>
</tr>
<tr>
<td>13</td>
<td>Deleted File on ProDiscover Application</td>
<td>48</td>
</tr>
<tr>
<td>14</td>
<td>Recovered File Using ProDiscover Application</td>
<td>49</td>
</tr>
<tr>
<td>15</td>
<td>Copies of Virtual Environments</td>
<td>50</td>
</tr>
<tr>
<td>16</td>
<td>Deleted Log Recovered by FTK Imager</td>
<td>51</td>
</tr>
</tbody>
</table>
LIST OF TABLES

Table 1 Experiment Results ........................................................................................................ 52
1. INTRODUCTION

Information security is becoming commonplace in every day’s life. Cyber security threats once a concern for the military, government agencies, and big companies, are causing distress and anxiety even to home users. New technologies such as mobile computing, the emergence of social media, and cloud computing are changing the security scenario [1]. There is no discussion about the advantages and benefits of these new tools, but at the same time new threats and vulnerabilities are discovered every day.

According to the results of the 2010 CSO Cyber Security Watch Survey, a cooperative effort of CSO Magazine, the U.S. Secret Service, Software Engineering Institute CERT® Program at Carnegie Mellon University, and Deloitte’s Center for Security &Privacy Solutions the number of cyber attacks has outpaced the number of security professionals, and is the primary cause of security breaches [1]. Another survey prepared by Fishnet Security Company among IT Security Professionals, shows that 62% believe Cloud Computing will be in the following years the second most important cause of security breaches, after mobile applications [2].

After a network has been compromised, the most important source for evidence is security logs. Log files are important tools for forensic investigators. Much of the network activity is saved either in each network appliance’s internal storage media, or in independent centralized servers used as log repository. Due the high volume of logs generated for medium and big companies, the preferred method is to configure a centralized Syslog server that collects security logs for the entire infrastructure. Another
reason for the use of a centralized log server is that networking devices such as routers, switches, and firewalls have a limited amount of memory that can be used to store the logs. This central database collect logs from all nodes in the network, and the storage capacity only depends on the size of the hard disk.

Much of the success of a cyber attack is to prevent any further investigative action from the company. It is common for network security logs to be deleted or altered covering any evidence an attack took place. This action also delays the response from system administrators and in many occasions leave the attackers free.

The field of network forensics focuses on the discovery and investigation of previous events occurred in a network environment. Usually these events are related to a security breach or misuse of the company’s assets. The purpose of the forensic investigation is to clarify the methods used by the attackers to break into the network, the tools they used to achieve their goal, the damage caused, and if sufficient traces can be found to get hold of the perpetrators and take them to a court of law.
2. NETWORK SECURITY

Network security’s goal is to protect company’s digital assets and information.

Traditional methods to secure a network environment involve preventive actions and also the detection of the attack when it is already in progress [3].

Most of the effort to protect a network goes to implement preventive measures such as a strong security policy, clear and concise procedures to help enforce the policy, personnel training, etc. One of the best strategies to achieve acceptable levels of information security is the use of Defense in Depth concept. Part of the strategy is making a good choice of the technologies that will be used to implement the security plan and protect the company from any security breach.

2.1. Defense in Depth

Given the diversity of threats a computer network is exposed, one of the best methods to secure it requires a layered approach. Defense in depth (DiD) combines several techniques and procedures to reach an acceptable degree of security. It is impossible to achieve complete protection by using a single security component [4]. DiD places information assets such as database servers, web servers, e-mail servers inside a series of concentric security barriers to restrict access to them while system administrators gain precious time to react when an attack is in progress [2].

It is important for all the defensive layers to provide mutual support and dependence to each other to be effective. The layers must be organized in such a way that an attacker
will face them one after the other in an orderly fashion, order that was previously planned by the security administrators. Any advantage would be lost if the security layers are arranged independently, because an attack could be initiated at any given point in the scheme and continue one by one until it reaches the innermost layers towards the protected information assets. [5]

Figure 1 shows the desired scheme of protection based on the defense in depth strategy locating the most important information assets under several layers of protection. Protection begins with strong security policy specifications, following with physical and perimeter protection procedures such as access control and proper configuration of Virtual Private Network connections. Firewalls and Intrusion Detection Systems can be applied to protect outer layers, but also to protect the internal network and host computers and servers. Finally the use of secure, stable and tested applications is also important because they access data and information sources directly. Antivirus and anti malware software is important in the inner most layers.
A strong defense in depth strategy is based on three key elements: People, technology, and operations [6]. IT management level plays an important role in the fight for achieving a respectable level of information security. It is important that the Chief Information Officer (CIO) and all incumbent departments in the company are committed to the mission. Part of the CIO’s job is to assign roles and responsibilities to adequate people in preparation of a security breach. Prepare for a security event is not only important for IT staff, but for all levels and departments within the company. It is usually this element the weakest link in the security schema, for this reason personnel’s training is fundamental to implement the security strategy. Included in the people side it is the physical and personnel security. The implementation of access controls to the company’s most important assets, either digital or non-digital are also important. Figure 2 depicts the Defense in Depth pillars.
Using the appropriate technology is the second key element. IT management must choose security technologies that meet the requirements of the company’s security policy. Decisions such as the type of Operating System for Servers, for desktop and laptop computers, type of web, e-mail, or file server applications, type of networking devices, the type of productivity applications, the use of mobile devices, and the use of encryption software must be made after a careful risk assessment process. There are numerous variables to take into consideration when technology equipment is acquired.

No technology is flawless and some kind of weakness can always be found. Therefore, the security of the network cannot rely on a single device or equipment. The defense in depth strategy suggests the implementation of layers of security devices to cover all
possible security aspects and to prevent a possible breach in the network. Furthermore, devices should be placed in such a way that both, the boundaries of the network, and the inner most servers and personal computers are protected. Devices for boundary protection are usually firewalls and intrusion detection systems. [6, 7]

Finally, the way how people and technology interact is the third pillar of the defense in depth strategy. The day to day operations performed to sustain the security of the company by personnel is of vital importance, and sometimes the weakest link of the schema. Some of the actions performed by security administrators are the following:

- Maintain the company’s security policy updated.
- Perform a baseline analysis of the security status of the company and update any progress or drawback of the situation.
- Perform vendor recommended practices to ensure the functionality of each element of the IT infrastructure. Such task can be: Patch and update the operating systems, update virus definitions, update access control lists, etc.
- Perform management task such as review networking logs.
- Perform periodic security assessments to determine if new vulnerabilities have arisen, or recommendations from previous security analysis have been implemented. This includes the use of vulnerability scanners, RED teams, etc.
- Perform security related drills to test incident response procedures. Some tasks include testing if backups have been obtained appropriately and they are working in case they are needed.
• Perform monitoring and responding tasks to prevent and recover from security incident respectively [6].

The successful implementation of a Defense in Depth strategy – including the three components: people, technology and operations -- depends on how closely the security policies and procedures have been followed.

2.2. Security Technologies: Firewalls, IDSs, Nat, Proxy Servers

There are several security devices that cooperate together to achieve an acceptable degree of security. As mentioned before, no single device is flawless, therefore the need to combine the functionality of such technologies.

The layered approach of the defense in depth strategy recommends the use of security devices to protect the boundaries of the network. Firewalls are usually the first line of defense in the network topology. A firewall is a software or hardware device used as a filter to prevent unwanted traffic to get into the network. Firewalls also prevent information that can be confidential to leave the boundaries of the network.

A firewall is used to prevent several types of threats. Denial of Service attacks (DoS), IP spoofing, ping of death, etc. Firewalls have evolve from simple packet filtering within routers to highly integrated security solutions including capabilities such as intrusion detection.[8] There is a number of firewall architectures that can be implemented in a network. They final solution depends on three factors: The objective of the network, the company’s ability to develop the solution, and the budget for its implementation.
There are four basic architectures: Packet filtering, screened hosts, dual-homed firewalls, and screened subnet firewalls. The most usual scenario within a company is a single connection to the external world (Internet), handled by a perimeter router. Besides connecting the network with external sites, the device can be configured to perform packet filtering based on control access lists. This implementation is simple but will add complexity to network administrators when access lists grow in size.

Screened Host firewall Systems use a second device as a proxy server behind the external router. The perimeter router filters and reduces the load for the internal proxy server, and allows it to perform a more detailed analysis of the traffic. This proxy device is usually referenced as a bastion host, and performs traffic analysis at the application layer level. This bastion host adds an additional layer of protection to the network.

Dual-homed host firewalls make use of the bastion host, but in this case it includes an additional NIC (Network Interface Card). One NIC is connected to the external unsecure network, and the second is connected to the internal network segment. In this case, the bastion host performs the packet filtering. A major drawback of this architecture is that the bastion host can become a bottle neck and represent a single point of failure. However, this approach is considered to deliver good overall protection at a reasonable cost compared to most sophisticated solutions.

Screened Subnet Firewalls feature at least two bastion hosts. They are located behind the filtering router and are used to build what is known as Demilitarized Zone (DMZ). This highly secure segment of the network is intended for the most important information
assets such as web servers, e-mail servers, database servers and the like. The DMZ is protected from both sides, the untrustworthy network which is connected to one of the bastion hosts, and the internal network separated by the other bastion host.

The implementation of a network firewall involves the following steps:

1. Write the security policy that describes the specific course of action for the firewall. The policy must be based on a risk analysis to determine the assets to be protected, the risks and vulnerabilities associated, and the entity in charge of managing the security of the asset. Usual targets within a network are the servers that run the basic services within the company such as, the web server, the e-mail server, FTP server, and file server. The policy precisely defines the risks, the vulnerabilities, the possible threats, the users of the service and the person in charge of the maintenance and control.

2. Design the firewall that will be used to enforce the security policy. The firewall solution should be based on all the information gathered in the previous step. A decision must be made for acquiring either a hardware or software device.

3. Implement the firewall either by installing a hardware appliance, or configuring a software mechanism.

4. Test the functionality of the firewall to ensure proper performance.

5. Update the access control rules of the firewall. This is necessary specially if the network has changed, or new services are provided.[9]
It is important to follow these guidelines from step one for any major change in the topology of the network or if new services are added or removed.

Intrusion detection systems (IDSs) are considered another essential component of the layered schema proposed by the defense in depth strategy. An IDS is configured to detect any misuse or attack to the protected network or device. When a security incident happens, an alarm is activated and system administrators are made aware of the incident. The notification can be an e-mail, text message, or the activation of security mechanism to stop the security breach and start the investigation process.

Like firewalls, IDSs exist as software or hardware devices. There are two types of IDSs, Host based and Network based. Host based IDS’ primarily goal is to protect a single computer or server containing sensitive information. A software agent is installed in the target device to monitor all activity such as file updates, software installation, logs, etc. Host-based IDSs record attributes of critical files, including its location, size, and modification date. If a variation in the stored information is identified, or a file is created or deleted, the agent sends an alert to the administrator to notify the occurrence.

Host-based IDSs are especially useful to audit log information in servers or computers. Based on the changes found on the logs, the agent can decide if a security breach has occurred. Agents can be installed into several computers in the network and be monitored from a centralized console. All information is sent to the management computer from where it is decided if a particular alert is valid or not. Well configured
host-based IDS tend to present low incidence of false positive alarms; on the other hand they are not well suited for large companies given the high number of computers. [8, 9]

Alike host-based IDSs, network based IDS are not set to monitor a single device, but a whole network segment. All traffic passing through a network segment is examined for certain patterns. This type of IDS has two components, sensors installed in a segment of the network, and management software used to display the information gathered by the sensors scattered around the network. The management system is also used for configuration purposes.

The network sensors use both, the packet’s headers from all traffic intercepted and the contents (payload) of the data packet to determine if a specific attack signature is encountered. If a packet or sequence of packets matches a known signature or pattern, an alert is sent to the management console for further analysis.

Both types of Intrusion Detection Systems can use either anomaly-based detection, or signature-based detection. Anomaly-based IDS, also known as heuristic or behavior-based detection, works building statistical information about the considered “normal” behavior of the user of the system. This data is collected, and stored into a database to establish a baseline usage pattern. Data about users can include: specific time the user logs in and out of the network, the usual locations accessed, the files used, etc. The agents periodically check the current usage of the network resources and compare this information with the baseline stored. If a substantial difference is found, an alarm is executed.
The advantage of anomaly based IDS is that even unknown threats can be detected when their behavior sets them apart from the well known traffic in the network. One of the drawbacks of this approach is that user behavior is not always predictable and can change depending of some circumstances. False positives are common due this reason. Furthermore, this type of IDS needs huge amounts of data collected and a “training” period before it can perform at an acceptable level. Signature-based detection works in a similar way than an antivirus software. Signatures are well known attack patterns that are configured and periodically updated. The IDS compares the traffic with these signatures. If a packet matches a signature an alert is sent to the system administrators. The performance of this type of IDS is more deterministic, either the traffic matches with the signature or not. Even though most IDSs allow the network administrators to create new signatures, they basically rely on the updates posted by the vendor. Another disadvantage is the lack of response when a new attack not included in the signatures database occurs.

2.3. Incident Response

An intrusion into a network can be divided into three phases: The first one happens before the intrusion, and it is when information about the structure of the network is gathered. The second phase occurs when the attacker has gain access and privileges on the system and is exploiting the vulnerability found. In the third phase the intruder erases traces of the attack. [10]
Incident Response is part of a contingency plan in case a security breach occurs in the network. Disaster recovery and business continuity are the other components of the contingency plan. The goal of this plan is to design and implement the procedures for the company to prepare for, react to, and recover from security incidents affecting the information assets. [8]

The Incident Response Plan (IRP) must be based on a security policy covering the following steps:

- **Preparation.** The Company must be equipped for the occurrence of any security incident by allocating the available resources for the protection of the information assets in the network. All tasks that must be performed have to be clearly stated on the policy including, the individuals who need to participate. Training the personnel involved in the contingency plan, install all the security software and hardware, apply patches and updates for applications and operating systems, and other preventive tasks are included in the preparation phase. It is important to enable the option of logging all the activity taking place in the network.

- **Detection.** Even when the preparation phase has been carefully performed, it is a fact that a security incident will occur, either small or catastrophic. For this reason, the implementation of incident recognition tools is of essential importance. The sooner a security breach is detected, the better the chance to avoid major damages. If a hacking attack is detected in the early stages, the like
hood that the information assets or a Denial of Service are compromised is low. It is important to perform a backup of the compromised system as soon as possible since the moment of detection. This will prevent any further loss of information and in some cases also save the state of the system so a forensic analysis can be performed in later phases of the investigation. It is important to obtain some information in the detection phase such as the location and number of systems affected for the attack, the level of privileges gained by the attacker, what technique was used for the attack, what was the vulnerability that was exploited, how many people was affected, and who knows about the incident. A report including the previous items needs to be submitted to the CIO for further analysis. Intrusion Detection Systems play a key role in this phase.

- **Containment.**- The technique used to stop the attack depends on the individual situation. In some cases is necessary to shut down the system to prevent further loss of information, but in some cases the system has to be left on to prevent loss of evidence. Some other measures to be considered are: disable any user account used for the attack, change or update access lists on the routers, replace a compromised appliance from the network, and so forth.

- **Eradication.**- This step is especially important in cases where a virus or malicious code is the cause of the security incident. Execute the antivirus software will remove the infection and it may also be necessary to format the hard drives and recover information from the backups.
• Recovery.- As soon as the threat has been eliminated the recovery process can be started. Performing a full formatting and configuration of the compromised systems is the best way to ensure no traces of the problem are being carried over, but this is usually time consuming prolonging the time the systems are inoperable. It is important to change all passwords, because there is no way to know which one was compromised.

• Follow up.- This step is sometimes overlooked and forgotten because at this point all the compromised systems are already in working condition and people are back into their routine tasks. However, this is the phase where the incident gets analyzed, and recorded for future reference. An analysis if the causes of the incident can lead to a overhauling of the preventive measures and to take the corrective actions to remove the vulnerabilities exploited. The incident can be also used as training material for personnel. This phase is very important for the forensic point of view, because this is the time when the case will be prepared for court if the company decided to take further action and all the evidence collected during the security incident has to be prepared for submission to the legal department or law enforcement officers. [9, 11]
3. DIGITAL FORENSICS

Traditionally forensic analysis has been performed statically, this means, over previously acquired data [12]. In terms of network forensics, static analysis is performed over log files from the different network security devices such as firewall, IDS, proxy server, NAT server, etc.[13,14] The amount of data collected is generally huge and the analysis is performed by the security analyst [12]. In [15] a method is proposed to integrate and then correlate logs from various sources in order to determine interesting and uninteresting events. A better approach for log analysis is proposed by [16]. They intend to identify data packets based on the content of the payload and correlate them recognizing individual sessions.

Live acquisition is becoming the preferred acquisition method in forensic investigations either for computer or network cases. Some evidence is only visible when the system is running, and it will be lost if it is shut down. Especially for network forensics, research efforts are going toward live analysis techniques given the volatile nature of network traffic [14].

3.1. Static Acquisition

Static data acquisition is the traditional way forensic investigations take place. Usually the target computer is turned off and the content of the storage devices is copied to another media similar in shape and capacity. A bit by bit copy us the best approach to guarantee that even hidden portions of data are copied from the original disk.
The next phase of the investigation is to load the captured data in a forensic workstation usually located in a forensic laboratory. Specialized software such as Encase or ProDiscover is used for this purpose. [17]

3.2. Live Acquisition

Volatile data is that data obtained from a live machine and can provide essential information about the logged on user and their running or current actions.

It might be possible for the investigators to obtain from main memory: Command history, services/driver information, passwords, data associated with user applications such as word documents, system date and time, logged on user and their authentication credentials, clipboard contents etc.

From the network state it may be possible to capture the state of a malicious connection with its associated IP address, providing further leads for an investigator. From running processes in addition to any user data it may be possible to capture process options, e.g. Hacking tools run from the command line may show the command line options used together with IP addresses. Malicious processes such as anti-forensics tools may be identified and acquired, thus allowing later forensic analysis which may assist the examiner during the traditional postmortem examination of the system.

In addition to the potential risk of losing evidence, in certain situations powering off a system is not feasible. Turning off mission-critical servers could cause loss of business productivity. Acquisition of the whole drive (in the order of Terabytes or Petabytes) may
not be feasible so selective data acquisition must be considered. Powering down the system means the loss of potential network evidence such as traffic session data. Old systems may not restart.

Therefore to prevent the loss of potential valuable evidence; passwords used for encryption, indications of anti-forensic techniques, and memory resident malware, live analysis is becoming increasingly important and can be most revealing as to what the logged on user is actively engaged in. [17]
4. HACKERS & OTHER THREATS

Security breaches tend to make big headlines in the news when the attack has been perpetrated by an external hacker. The reality shows that the big majority of security breaches that occurred have been performed from within the company’s network. It is usually an angry employee that has access to the information assets of the company that executes this type of attacks. The motivation for the attack can be financial gain, prevent legitimate authorized users from accessing network, or industrial espionage, but there are common elements found in cyber attacks such as the use of malicious code to corrupt or damage data, the illegal use of user accounts and privileges.

When an external attack occurs it is usually performed by using a predefined plan. In some cases the hacker has criminal intentions and the motivation is to cause losses and damage the assets and reputation of the company attacked. Possible motives can also include greed, terrorism, politics, racism and criminal payoffs. Criminal hackers need to posses outstanding skills on network design. They need to know the methods that would allow them to avoid all types of security devices and procedures such as Intrusion Detection Systems (IDSs), firewalls, routers. They also need to have a strong set of hacking tools that will allow them to exploit the security breaches. Some of these hacking tools are freely available for download from the internet.

Some external threats originate from inexperienced attackers who use cracking or scripted tools readily available on the Internet, to perform a network attack. One of the most used set of tools is Back Track. This is a Linux special distribution containing a
collection of tools used for penetration testing and forensics. Some utilities include:
Scanning tools, password crackers, vulnerability identifiers, radio network analysis, etc.

Most hacking tools can also be used by system administrators for testing and learning purposes. In some cases external attacks are aimed to cause distress to services such as web sites offered to the public by companies. The internal network and services can also be the target of cyber attacks. To gain access to internal locations, hackers can use modems or attempt to authenticate into the systems by brute force password cracks.

Internal attacks originate from dissatisfied employees who have access and some kind of privileges to the system. They usually try to hide their attack by deleting the security logs or any possible trace that could be used as evidence against them.

There are a number of different attacks lunched by hackers to attempt to access a network. The initial step in hacking a corporate network is foot printing. The purpose of foot printing is to create a map of the network to determine the type of operating systems, applications and ranges of IP address that are being utilized. The process is also useful to identify open ports that can be used to break into the system. Port scanning is used by the hacker to collect information about the network services available on a target network. Hackers also try to collect information about applications installed on the host and unprotected resources and services.

Password hacking programs and Trojan horses are used to obtain access to systems. It is usually a security weakness that is exploited by the attacker in order to gain access to a system or the network. After access is obtained, the intruder is able to modify or delete
data and add, modify or remove network resources. Another common type of attack is unauthorized privilege escalation. Privilege escalation occurs when an intruder attempts to obtain a higher level of access such as administrative privileges to gain control of the network system. Other common tools used by hackers are backdoors. These programs are installed to maintain an access door open for future attacks. [8]

Some of the more common types of network attacks are listed:

- IP address spoofing occurs when attackers change their source IP address to make it appear as though the packet originated from another IP address. Using this technique the attacker can pretend he is a trusted entity on the network and can access locations containing confidential information.

- An eavesdropping attack occurs when an attacker monitors and analyzes network traffic, the traffic then is interpreted and any non-encrypted data is available for interpretation. Sniffer applications are used by hackers to capture traffic in transit. Many applications send passwords over the network on plain text, this is an opportunity for hacker to obtain this information.

- Password attacks are intended to obtain the password for a system. A common approach is the brute force attack which tries all possible combinations until the correct password is found. Once the attacker obtains a password, he can gain access to classified network locations as authorized users and access information.

- A man-in-the-middle (MITM) attack occurs when a hacker monitors, captures and controls all the traffic being exchanged between two parties communicating.
The attacker has to impersonate both the receiver and sender making them believe each one is communicating with the other.

- A Denial of Service (DoS) attack is intended to prevent legitimate users from accessing services on the network. DoS attacks are usually initiated by sending invalid data to applications until a server hangs up or crashes. Some DoS attacks initiate the offensive from multiple computers against a single network or system. This type of attack is known as a distributed denial of service (DDoS) attack. It is usually very difficult for network administrators to defend against DDoS attacks. The main reason is that trying to block all the attacking computers can also result in blocking authorized users. [8]
5. NETWORK FORENSICS

A formal definition of the term Network Forensics follows: "The use of scientifically proved techniques to collect, fuse, identify, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities” [3].

Purpose, collection and nature are the three characteristics used to classify network forensic systems. According to the purpose of the investigation they can be: ‘General Network Forensics’ when the objective is to enhance the security of a particular network. In these cases there is no requirement to follow any legal principle, because the evidence will not be used for court. ‘Strict Network Forensics’ occurs when it is necessary to get evidence satisfying the legal principles. Collection of Traffic: ‘Catch-it-as-you-can’ systems where all the packets passing through a particular traffic point are captured and analysis is done requiring large amounts of storage and ‘Stop-look-and-listen’ systems where each packet is analyzed in memory and certain information is saved for future analysis requiring a faster processor. Nature: The network forensic system may be an appliance with hardware and preinstalled software or exclusively software. [18]
A key concept with forensic investigations is the chain of custody. When evidence is acquired, all procedures and actions performed by the investigator must be chronologically recorded into a log. This record of events is a testimony that any evidence described has not been tampered and can be admitted in a court of law. The evidence has to be in custody by a trusted person at all times from the initial location where the incident occurred until it is used as evidence in court. The chain of custody document needs to clearly state the procedures followed to acquire the evidence, identify any individual that had contact with the evidence, and also any location the evidence was taken to. [17]
6. VIRTUAL INFRASTRUCTURES

It was in the 60’s when virtualization was introduced by IBM as a means to share the resources of the supercomputers of that time to run various separate processes. Alike these early stages, today’s virtualization can be run almost in any computer, even in most mobile devices [21].

Advances in computer’s processing power and storage capabilities are supporting the development of a new model for IT infrastructures [22]. Although the concept of virtualization is not new, its popularity and incorporation into industry is still in early stages. A virtual environment gives the ability to run numerous isolated servers on a single physical device. Different Operating Systems (guests) run over a host Operating System. Physical devices such as hard drive, memory, processor, video card, NIC card, and controllers are emulated and presented to each guest OS as if it was the only one running over the actual hardware. Probably one of the most important features of virtualization is the isolation it offers to the servers running simultaneously on the same hardware platform [23]. This capability makes it possible to turn on or off any of the virtual machines without affecting the others. Figure 3 shows the architecture of virtualization.
Some of the characteristics of virtual environments are the following:

- Optimization of hardware usage. Several underutilized servers can be consolidated delivering better performance using less physical resources.

- Fast and easy server deployment. A virtual server represents a small set of files in the host machine. These files can be saved and deployed when needed at a later time. Therefore, new servers can be set up with no additional hardware or software configuration. The required time to have the servers in working is greatly reduced either for production servers or test environments.
• Lower Total Cost of Ownership (TCO). - Several factors help reduce costs: postponed acquisition of new servers, reduced datacenter footprint, reduction in maintenance costs, reduction in cooling, cabling, rack, and ventilation costs, lower disaster recovery costs, and reduced deployment costs.

• Enhanced Availability and Business Continuity. - Virtual servers are easy to backup, and deploy. Whenever a new server needs to be installed, the time required to complete the task is reduced. The fact that several servers are working on a single host computer (server), introduces a single point of failure for the whole set of servers. However, replication procedures are used to overcome this difficulty.

• There are also some disadvantages related to the implementation of virtual environments such as performance degradation. If the load under which the host server is working is too heavy, some components will see their performance affected. Processor, memory, storage and networking capabilities will suffer.

There are two types of virtual machines: Process virtual machines and system virtual machines. The purpose of a process virtual machine is to execute a single process. It is created and terminated when the process is created and terminated respectively. The virtualizing software is called runtime software and usually runs at an API level, on top of the Operating System configuration. This type of virtual machine is rarely recognized as a virtual machine.[23] The software for a system virtual machine is called Virtual Machine Monitor (VMM) and works in a middle layer between the host OS and the guest OS[23].
There are several types of system Virtual Machines: Classical virtual machines place the VMM directly in top of the hardware running in privileged mode in contrast to the rest of the guest systems. Hosted virtual machines use the host’s operating system to deploy the VMM. The VMM is installed just like any other application. VMware is an example of this type of virtual machine. Whole-System virtual machine is used when host and guest OSs do not share the same Instruction Set Architecture (ISA). In this case, OS and applications are virtualized.

Cloud computing is one of the new computing paradigms that can be highly benefitted from the use of virtual infrastructures. While it is not mandatory to virtualize the hardware support of a cloud, it would be the natural development for this type of infrastructure. All the advantages mentioned early would provide a cloud with the flexibility and availability to deploy any kind of solutions with high degree of reliability.

In terms of security, virtual environments represent an improvement in terms of availability, but the impact on integrity and confidentiality are less favorable [24]. Confidentiality can be threatened by a misuse of the VMM since it has access to the internal state of any virtual machine. Multiples copies and deployments of some virtual servers also can affect confidentiality. Integrity can also be affected if the VMM is used to change the state of a particular virtual machine. As mentioned before, availability will be benefited due the easy procedures to deploy a server in case it is needed.

Some security problems might arise if the host operating system is compromised. Either host or guest operating systems should be updated and patched. DiD concepts should be
applied to protect the servers. Another threat could arise if the VMM (also called Hypervisor) is compromised. VMMs usually have the highest level of privilege on the use of the hardware resources. Administrators must ensure the implementation of the virtual environment complies with the security policy of the company [21].

VMs can be used as forensic tool or as evidence. Forensic investigator can use VMs to analyze acquired data. Although it might not be forensically sound to proceed this way, the procedure can be used as an alternative way of analysis. This method is faster than the traditional procedure. After the investigator found some evidence he can use traditional forensic techniques to replicate the findings and ensure the acceptability of the evidence in court.

An interesting approach is described in [25]. Virtual Machine Introspection (VMI) can be used when a VM’s security is compromised. The security analyst uses a parallel VM (in the same host), or the Virtual Machine Monitor (VMM) to “look inside” the attacked VM. The VMM has complete access to the memory section of any VM running upon it, and can be used to take snapshots of the memory status of any VM currently running. It is still not possible to perform a reliable “live” acquisition using this method, that is, the VM has to be stopped to take a picture of memory. Taking the memory dump while the VM is running might result in inconsistent data, which in turn, would not be forensically sound. New capabilities can be added to the VMM to make possible a forensic analysis while a VM is running.
The inclusion of such features into the VMM arises several questions. Since it runs with
high privilege level, if the VMM is compromised it could be more dangerous for the
VMs integrity. VMM can also have the possibility to insert or get data from a running
VM. An administrator might get data to perform a forensic analysis. On the other hand it
could be helpful to insert new data or codes to a compromised VM in order to trick the
attacker changing the environment. The intruder might get confused and discontinue the
attack. Finally, an interesting perspective is to determine if it is useful to permit VMs to
determine if any intervention is in place from the VMM. Running processes in the VM
would detect that they are being monitored.
7. SECURITY LOGS

A log is a record of all or some of the activity generated within a network or a computer device such as a firewall, IDS, router, server, or personal computer. An event occurring in a particular system generates an entry in the security log. This information is used for troubleshooting purposes, for auditing, for monitoring, for performance improvement, but especially for security reason. One of the fundamental sources of evidence when the security of a system has been compromised is the security log files.

Each entry recorded in the logs can include several fields, but the essential pieces of the network traffic information are: Date, time, source IP address, destination IP address, protocol, source port number, and destination Port number. There are three basic types of logs: Security appliance and software logs, operating system logs, and application logs.

Security devices and software installed across the network are the primarily source of logs for networked environments. Some network-based and host-based devices include: Antimalware software such as antivirus programs, Intrusion Detection Systems, remote access software, web proxies, authentication servers, firewalls, and routers. Operating system logs from servers and workstation capture lots of security related events. Some of the most common items recorded are system events and audit records. System events include information such as when the computer was turned on, turned off, restarted, when updates were installed. Audit records capture user related information such as successful and failed logons, file access, changes in accounts and their privileges. In
both cases the system administrator is allowed to specify the type and amount of logs that are going to be recorded.

Application logs document the activity generated by the software run by the company. Either Commercial of the Shelf (COTS) or custom-developed applications include the capability to track most transactions and operations performed by the users. Some applications use their own logging procedures, whereas other use the operating system’s logging capabilities. The type of information logged ranges from client data request and server responses, to an account of the transactions performed during a determined period of time. Most applications also log significant actions such as when the application was started or terminated, or when major configuration changes were made. Figure 4 shows log manager from Windows Operating Systems.

Figure 4 Windows Event Viewer
The increase in the number of computer devices, networking scenarios, and security threats has had an impact in the amount and diversification of logs. A management method for computer security logs and log correlation are areas gaining attention from researchers and considered to be of critical importance in the development of network security. It is not enough to generate and store security logs. A proactive approach requires performing routine evaluations of the information captured.

Part of a log management plan is the analysis of the security logs. There are many benefits for this to be done. The ability to spot attacks in progress, operational issues with the network, policy contraventions, or deceptive behaviors from internal employees or external sources are some of them. Logs will provide valuable data that can be used to solve the situations mentioned above. [19] Log correlation is the process of combining security logs from different sources such as networking appliances, servers, or intrusion detection systems in a way that is easier for systems administrators to analyze the information gathered. Log analysis has been traditionally performed using intensive manual procedures with high dependence on the skills, knowledge and experience of the investigators. The complexity of the network environments and the ever increasing amount of security logs makes the analysis procedure overwhelming, especially when each technology uses a different log format. [10] Each different format has to be interpreted and integrated into a regular representation in order to make the information useful. Templates are used to convert log data from one form to another. Furthermore, if the network infrastructure changes or new devices are installed in most cases the
Syslog is a layered protocol developed in 1980 with the purpose of having a means of generate and manage events within a system. These events can be for information, troubleshooting or security purposes. It is defined by the Request For Comment 5424 (RFC 5424). Syslog has become the de facto standard for logging. One of the most important fields of a syslog message is priority (PRI). The priority of a syslog is based on two values: Facility and Severity. Facility ranges from 0 to 23 and represents event messages such as kernel messages (0), user-level messages (1), security/authorization messages (4, 10), log audit (14), or local use 7 (23). Severity is in the range of 0 to 7 with the following values: Emergency (0), Alert (1), Critical (2), Error (3), Warning (4), Notice (5), Informational (6), and debug (7). The priority number is calculated multiplying facility by 8 and adding the value for severity. Figure 5 shows the format of a syslog message.

![Figure 5 Syslog Message Format](image)

One of the biggest disadvantages of the syslog protocol is security. Some of the factors that undermine the syslog protocol security are the following:
• Syslog sends its information in clear text which can be easily captured by an attacker with the use of a sniffer. To avoid this situation, syslog messages can be sent using a separate or secondary network or by encrypting the traffic flowing to the syslog server.

• Syslog uses UDP for its exchange of data. UDP protocol is unreliable by definition. There is no guarantee the packets will reach the syslog server. Packet can also be easily spoofed by an attacker and modified before they reach the syslog server. The use of the TCP protocol can mitigate this threat.

• Centralized logging easy to manage by system administrators, but it is also a single point of failure if attackers gain access to the server. If the central syslog server is compromised, an attacker can delete all the syslog messages to clean up his trail and prevent further investigation. The server must be hardened by system administrators to try to minimize vulnerabilities.

Another effort to homogenize the logging process is the Common Event Expression (CEE) project. The purpose of CEE is to develop a universal format for event representation, communication, and interpretation. Log syntax and logging representation are also addressed within the scope of this project. CEE also complies with security regulation such as COBIT, ISO27001, HIPAA, FISMA, ITIL, GLBA, and others. Besides the main goal of standardize logging procedures, CEE also accomplishes an improvement in monitoring techniques, improve in code reuse for log analysis applications, and liberates companies from product dependence.
The use of log information for investigations needs to be done carefully. It is important to verify the reliability and validity of the source of the data. It is not uncommon for hackers to modify or erase entries in the log files that could be used as evidence in a future investigation. Storage and transport mechanisms should also be carefully designed in order to preserve the integrity and confidentiality of the log information. [19]
8. MOTIVATION

Having the ability to retrieve and make use of security logs after a security breach is of fundamental importance for network and system administrators. In many cases the evidence of intrusion and proof of the damage caused to the information assets is in the security logs. Dates and times of intrusion, the techniques and methods used to break into the network, and sometimes the location of the attacker are recorded in the security logs. Logs can also be useful in determining inappropriate usage of computer assets within the company or indications of some kind of fraud. Audit or application logs can be used to verify the previous. In cases where the investigation will develop into a criminal case and law enforcement agencies are going to participate it is even more important to guarantee the reliability of security logs as evidence. Log management techniques are necessary for this purpose. The aim of this research project is to develop a forensic procedure for the recovery of any type of log that has been deleted, or removed from a centralized server. The procedure will allow corporate investigators or law enforcement agents to use the recovered evidence and use it to pursue an investigation or to build a trial case if necessary.
9. EXPERIMENTS AND TESTS

The purpose of the experiments is to demonstrate the use of forensic tools to recover log files after they have been deleted from the centralized syslog virtual server. In order to confirm the results, two forensic tools were used to perform the experiments. The following steps were performed:

1. Set up the network environment
2. Centralize log collection
3. Simulate an attack
4. Acquire forensic evidence
5. Recover deleted files
6. Report findings

An enterprise network infrastructure was configured for the forensic procedure to be conducted. The following items were used to build the testing scenario:

- Cisco PIX 515e Firewall (1)
- Cisco Router 2600 (1)
- Cisco Fast Ethernet switch 3500 (2)
- Windows Vista Client computer (1)
- Windows Web server 2003 (1)
- Windows 2003 Virtual syslog server (1)
- Microsoft Virtual PC 6.0.156.0
• Solarwinds Kiwi Syslog Server version 9.1.0
• NMAP Zenmap 5.35DC1
• Technology Pathways ProDiscover version 6.5.0.0
• Aces Data Forensic Toolkit v 1.81.6 and FTK Imager

Figure 6 depicts the infrastructure used.

![Corporate Network Topology](image)

**Figure 6 Corporate Network Topology**

The network configuration followed the structure of a screened subnet DMZ combined with a screened host topology (both mentioned above). With this type of topology three different zones were created. The external segment or Internet connection which is considered the insecure zone, the internal network containing the employees’ computers, laptops, printers, and finally the 3rd segment called the Demilitarized Zone or (DMZ)
which contains the most important servers and information assets. The DMZ typically contains an e-mail server, a web server, file server and it is protected from both two other segments by the firewall. The router connected between the firewall and the Internet is intended to perform a previous screening of the traffic coming from the internet.

The device performing the syslog function was a Windows 2003 Server. It was installed using Microsoft Virtual PC 2007 using as host platform a computer with Windows Vista Home Premium. Figure 7 shows the virtual environment. Unix-like operating systems have a native controller for the syslog operations. This functionality is built-in and it has to be enabled by system administrator to start receiving syslog messages from any device configured to generate logs. Although Windows operating systems have their own logging engine, they don’t have the ability to receive logging events from external sources. 3rd party software can be installed to convert the server into a Syslog Server.

Figure 7 Virtual Environment
Kiwi Syslogd Server is the most popular syslog server for Windows operating systems. Some important features of Kiwi Syslogd Server are the following:

- It offers a GUI for easy management.
- It uses both TCP and UDP ports.
- It displays messages in real time.
- It features automatic log-file archiving based on a custom schedule.
- It shows statistics including graphics.
- It features e-mail notification for certain events and if the log file size exceeds a certain limit.

Figure 8 shows a screen shot of Kiwi Syslog Server

![Kiwi Syslog Service Manager](image)
The Kiwi Syslog Server was installed and configured as follows:

The Kiwi Syslog Daemon version 9.1.0 was downloaded and installed. After the installation was complete several configurations were performed: the amount of logs generated and stored, the destination folder for the log files, and the alarm to notify the system administrator before the server stops working because of insufficient disk space. This option is useful for Cisco PIX Firewalls that use TCP syslogs. If the hard drive on the syslog server is full, the Cisco PIX Firewall will stop processing traffic causing a denial of service issue. All logs are saved by default to the following text file:

C:\Program Files\Syslogd\Logs\SyslogCatchAll.txt. Figure 9 shows the location of the log files from Kiwi syslogs server.

![Figure 9 Location of Kiwi Security Log Files](image)

It is possible to choose other file formats for the log files. To view a graphical summary of syslog statistics, a bar representation can be generated with the number of messages received during a time interval. There is also a Syslog Statistics option containing
History, Severity, Top 20 Hosts, and Counters. The Severity tab lists a summary of messages by priority level. The Top 20 Hosts tab identifies hosts with high log activity. It is important to note that a large number of messages from a particular host can be an indication of a problem on that device. The Counters tab reports the traffic and error statistics for the syslog server.

Most Cisco devices use the syslog protocol to manage system logs and alerts, which is enabled by default, but unlike PCs and servers, Cisco devices don’t provide large internal storage space for the logs. Since the size of the buffer is just a few kilobytes, only the most recent messages are logged. Furthermore, when the device reboots all syslog messages are lost. For this reason once the firewall, router and switches were configured and the infrastructure was up and running, all logging activity was directed to the central syslog server. The basic configuration command simply indicates the IP address of the server that will be used as syslog server. Figure 10 shows the basic configuration performed in the Cisco PIX515e Firewall.

```
Firewall-PIX(config)# logging host 192.168.10.30
Firewall-PIX(config)# logging facility 21
Firewall-PIX(config)# logging trap 7
Firewall-PIX(config)# logging on
Firewall-PIX(config)# exit
Firewall-PIX# show logging
Syslog logging: enabled
Facility: 21
Timestamp logging: enabled
Standby logging: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: disabled
Trap logging: level debugging, 6 messages logged
Logging to inside 192.168.10.30
History logging: disabled
Device ID: disabled
Firewall-PIX#
```

**Figure 10 Cisco Pix515e Firewall Logs Configuration**
Before configuring the Cisco devices to send syslog messages, they all were configured with the right date, time, and time zone. Syslog data would be useless for any future investigation if it would show the wrong date and time. Since it is a networked environment that is being configured, it is important to have all devices time synchronized using Network Time Protocol (NTP). Using NTP is intended for a correct and synchronized system clock on all devices within the network. Setting the devices with the accurate time is helpful for event correlation.

Having the entire network infrastructure configured, the Cisco Devices, the Virtual Server containing the Syslog Server, the Windows Vista Client Computer was used to perform a network scan. NMAP Zenmap was the application used to perform this task. As mentioned above, reconnaissance is the first step in a network intrusion. This activity was detected and logged by the Firewall and all event messages were immediately sent to the centralized syslog server. The Kiwi application stored the data in the location previously configured. Figure 11 shows NMAP application in action.

![Figure 11 NMAP Application](image-url)
The security logs were received and stored by the virtual syslog server. Since no Intrusion Detection System was installed as part of the infrastructure, there is no indication an attack was in progress. For the purposes of this research project, the attack procedure continued with the last step in the sequence of an intrusion in the network. The attacker gained access to the centralized syslog server and deleted the security logs generated.

The deletion of the security logs was performed in two different ways. For the first experiment the log files were deleted from the local machine, as if the attacker had physical access to the server. For the second experiment, the deletion operation was performed remotely with the attacker accessing the syslog server from a computer in the same network (internal network). For the local deletion it is assumed the attacker is an employee with some knowledge and access to the server. When the log file used by the Kiwi Server is deleted, it is immediately replaced by a new empty file with the same name. Without forensic evidence systems administrators don’t have enough material to carry on an investigation. For this reason a forensic procedure is started.

The first step in the forensic procedure is acquiring a snapshot of the target server. Since the compromised server is virtualized, the best way to acquire evidence is to copy the entire files containing the configuration of the virtual machine and the virtual hard disk. Figure 12 shows the files captured.
The next step was to restore the files captured into a forensic workstation. This computer included Windows Virtual PC 2007 as well. The purpose of capturing a copy of the virtual server is to allow the original instance to keep performing its intended task. The acquisition task in this type of cases is of essential importance because the investigator has only one opportunity to get evidence. The dynamic nature of a syslog server would destroy any evidence while it is running.

Once the captured evidence of the virtual syslog server was configured in the forensic workstation, the forensic application Technology Pathways ProDiscover was installed, and the following steps were taken to recover the deleted file:

- A new project was started providing case number, case name and description.
- The evidence disk was added to the case.
- Using Content View option the folder containing the deleted log file was located.
ProDiscover displayed the contents of the folder.

The deleted log file was selected to be recovered from the work area. This is shown in figure 13.

**Figure 13 Deleted File on ProDiscover Application**

The contents of the selected file are showed by ProDiscover at the bottom of the main window.

To recover the file a Save as option was selected from a context menu copying the file to a selected location in the hard drive.

Finally from that location, the recovered log file was moved to a safer location. Figure 14 shows how the recovered file was saved to a selected location.
The forensic process for this experiment was not conducted following the strict forensic method mentioned in previous chapters. The purpose of the research activity was to demonstrate the feasibility to recover deleted log files in virtual environments. The forensic analysis can be repeated several times using for every time a clean copy of the acquired files.

To confirm the results obtained with ProDiscover, a second recovery experiment was performed using another forensic application. Forensic Toolkit Imager (FTK Imager)
was used. Since evidence had already been acquired and replicated. A copy of the virtual environment was restored in the forensic workstation. Figure 15 shows the different virtual environments acquired.

![Table showing virtual environment copies](image)

**Figure 15 Copies of Virtual Environments**

The same procedure was conducted using FTK Imager.

- The evidence disk was added to the case.
- Using the evidence tree view, the folder containing the deleted log file was located.
- FTK Imager displayed the contents of the folder.
- The deleted log file was selected to be recovered from the work area.
- The contents of the selected file are showed by FTK Imager at the bottom of the main window.
- To recover the file a Save as option was selected from a context menu copying the file to a selected location in the hard drive.
- Finally from that location, the recovered log file was moved to a safer location.

Figure 16 shows the log file recovered by FTK Imager.

![FTK Imager Interface](image)

**Figure 16 Deleted Log Recovered by FTK Imager**

Four experiments were conducted using both forensic tools. Each application was tested once for each type of deletion. A local deletion and a remote deletion were performed. The following table summarizes the results:
Both tools were able to recover the log files deleted locally on the server; however FTK Imager was also able to recover log files that were initially deleted remotely. ProDiscover was not able to recover log files deleted remotely.
10. CONCLUSIONS & FUTURE WORK

This research shows the importance of security logs as a source of evidence for forensic investigations. Much of the activity happening in the computer infrastructure is recorded in this log files. After a computer network has been compromised, the attacker usually deletes security logs to prevent investigators to obtain evidence and investigate the event. Hackers have the ability to delete this evidence after they have committed their crime leading any investigation to a death end. The research project demonstrates the feasibility of using forensic tools for the recovery of security log files after they have been deliberately erased. The forensic analysis was performed in a virtual server containing the security logs. The deletion of the log files was performed in two ways. Local deletion, assuming the attacker had physical access to the server, and remote deletion which was performed over the network from a computer in the same local area network. Two forensic applications were used to confirm the results. Each tool was tested with each type of deletion. Results showed that both applications were used to recover the deleted files when the deletion was local. FTK was the only one that could recover the log files deleted remotely. The results of this investigation can be improved by testing the performance of other forensic tools. Furthermore, the analysis can be also applied to different operating systems such as Linux or Mac which were not tested for this thesis project. Also the source and complexity of the attacks can be also adjusted to obtain more comprehensive results.
REFERENCES


networked environments.” Internet:


VITA

Name: Jose J. Escobar

Address: 5445 South Alameda Street Apt 19G Corpus Christi, TX 78412

Email Address: jescobaru@gmail.com

Education: B.S., Computer Science, UAGRM at Santa Cruz - Bolivia, 2001
M.Sc., Computer Science, Texas A&M University – Corpus Christi, 2010