University of Derby
School of Computing & Mathematics

A project completed as part of the requirements for the
BSc (Hons) Computer Forensics and Security

Entitled
Insider Network Attack Investigation

By
Rachel Louise Fairbrother
rfairbrother1@hotmail.co.uk

In the years 2010 - 2014

Table of Contents
Abstract.......................................................................................................................................5
1. Introduction
1.1. Network Attack
1.2. Insider Network Attack
1.3. Aim of Project
1.4. Organisation of Project

2. Literature Review
2.1. History of Insider Network Attacks
2.1.1. Volume of Insider Network Attacks
2.1.2. Organisation of Literature Review
2.2. Insiders and the Insider threat as a whole
2.2.1. Insider Threat Overall
2.2.2. Impact of Insider Network Attacks
2.2.3. Case Studies of Insider Network Attacks
2.3. Different types of External Network Attacks
2.3.1. Back Door Attack
2.3.2. Social Engineering Attack
2.3.3. Dumpster Diving Attack
2.3.4. Denial of Service Attack
2.3.5. Tailgating
2.4. Different types of Insider Network Attacks
2.4.1. Inappropriate System Use Attack
2.4.2. Denial of Service Attack
2.4.3. Back Door Attack
2.4.4. Theft
2.4.5. Logic Bomb Attack
2.4.6. Man in the Middle Attack
2.4.7. Reasons for the number of Insider Network Attacks
2.4.8. Cross-Over of Insider and Outsider Network Attacks
List of Figures
List of Tables

Table 1 Comparison of Digital Forensic Frameworks.................................................................21

Table 2 Comparison of Network Forensic Frameworks...............................................................22

Table 3 Virtual Machine Configuration....................................................................................41

Table 4 Comparison of Network Forensic and Insider Network Forensic Framework.............43
Abstract

The increase in the number of Insider Network Attacks was focused on for this project. Due to this increase, there needs to be a way in which these Network Attacks can be investigated.

The examination of current literature to explain the problem and perceived impact of Insider Network Attacks and the Creation of a Digital Forensic Framework to investigate cases of Insider Network Attacks, together with a Comparison and Contrast of the existing Digital Forensic Frameworks against the newly designed one.

There are many Network Attacks that occur from both Inside or Outside of the network, it can be seen that there are no frameworks available specifically for the investigation of Insider Network Attacks. During the course of the project the research was gathered using qualitative methods and secondary sources (Greetham, 2009). The Framework created consists of all of the primary elements necessary for an investigation to meet the digital and network forensic guidelines, as well as extra components necessary for the distinction between External and Internal Network Attacks.

A Digital Forensic Framework was created for the investigation of Insider Network Attacks; this framework meets the second objective.
1. Introduction

Network Attacks can be carried out from either Inside or Outside of the network, the most common form of network attack is from an external perpetrator. The following information will look at the research that has already been carried out for Insider Network Attacks by the most trusted individuals within the organisation. This means that no matter how much network security is put in place on the outside, the people who attack the network are the ones that have the authority to change passwords and have access to the most crucial information that if released could destroy the company’s reputation and functionality.

Insider Network Attacks pose a huge risk to the integrity and reputation of organisations all around the world, it is these types of attack that need to be investigated in order to highlight the risk that is involved if an attack of this type is allowed to be executed. Currently there is a lot of research into network security and network attacks from an external point of view, in order to develop a Digital Forensic Framework for network attacks that originate from inside the organisation, there needs to be an understanding about the different types of network attack which can be carried out by the trusted individuals within an organisation. This is due to the need to provide Digital Forensic Investigators with a procedure to follow when it comes to investigating cases of Insider Network Attacks. Ross provides an invaluable article “Defending the Corporate Crown Jewels from the Dangers that Lurk Within” (Ortega, 2007,
p. 54) this article explains the dangers of Insider Network Attacks to the organisation’s reputation, as well as their ability to conform to confidentiality standards within the Information Technology Industry (Ortega, 2007).

The different systems and processes that can be used when undertaking Internal Network Attacks, can be seen to have authentication already rolled in, this makes attacks easy to carry out. A good example of a protocol that verifies the user’s passwords and checks the encryption level on organisational network is Kerberos (Trost, 2009). The many different protocols and standards that are incorporated into a network security system help to protect against external attacks, however the high level employees will already know the encryption details that are used within the company.

Insider Network Attacks can happen from any part of the network, however the main focus when it comes to network security is protecting the network from outsiders, unauthorised users who should never gain access to the network. The reality is that a lot more damage can be done to the company as a whole from an authorised user or disgruntled employee who knows the network and is already authenticated on the network, this situation requires more research. Garfinkel states that

“Cybersecurity can be viewed solely as an insider problem. What is needed, say advocates, are systems that prevent authorised users from acting improperly.” (Garfinkel, 2012, p. 29).

This view is not necessarily an accurate one as an organisation cannot function if the entire network is locked down; the employees need access to the data in order to carry out their day to day jobs. The problem comes when that trust of not having the network completely locked down is exploited and then the company’s image is damaged and needs to be rebuilt if that is even possible.

Insider Network Attacks can be put into two different categories according to Nong, these two categories are: “User Error” and “Abuse or Misuse” (Nong, 2008, p. 21).

The reason for developing a Digital Forensics Framework for the investigation of Insider Network Attacks is that there are many different Forensic Frameworks for the investigation of Digital Forensics in general and therefore one that focuses on a specific area of Digital Forensic Investigations would provide investigators with more guidance. Chirillo (2001) provides useful ideas that must go into the creation of a Digital Forensic Framework, these

Insider Network Attacks are becoming more apparent so it seems, however there is evidence that Insider Network Attacks have been a problem affecting organisations although these cases do not get reported as often in order to protect the reputation of the affected organisation.

1.1. Network Attack

A network attack is a malicious activity carried out by an external party to an organisation’s network infrastructure (Symantec, 2013). The purpose of a network attack is usually to deprive the organisation of their network resources or prevent the use of the network as a whole.

1.2. Insider Network Attack

Insider Network Attacks are malicious activities that are carried out by a current or previous employee. An Insider Network Attack can sometimes have the same purpose of a Network Attack by an external party to the organisation. However Insider Network Attacks need to use the network system, or inside knowledge of it, in order to carry out their attack and gather the information they wish.

As the number of networks continues to grow around the world, so does the number of network attacks that are happening every day. Given this it would seem that more research would need to be undertaken into the number of these network attacks which appear to be originating from an external entity, however from the details that are uncovered about the number of External Network Attacks reported, it can be seen that of these attacks Perry (2006) states that “80% of network attacks are instigated by authorised users and not by an external hacker.” (Perry, 2006, p. 11)

This statement shows that the real problem is in understanding the ways in which the Insider Network Attacks are being conducted, as a way to develop a full process for investigating these specific types of attack.

Another problem with the number of Insider Network Attacks that are occurring is to do with the varying way in which these attacks are carried out, with most Insider Attacks being carried out in a different way. A Digital Forensic Framework needs to be produced with the ability to be able to provide the Investigators with steps necessary to investigate all types of Insider Network Attacks.
1.3 Aim of Project
To study the different types of Insider Network Attack and formulate a detailed framework to be used to investigate incidents of this type.

The objectives of this project are:

1. Examine current literature to explain the problem and perceived impact of Insider Network Attacks.
2. Create a Digital Forensic Framework on how to investigate cases of Insider Network Attacks.
3. Compare and Contrast the existing Digital Forensic Frameworks against the newly designed one.

1.4 Organisation of Project
Chapter 2 introduces the ideas about Insider Network Attacks and the dangers that they pose to the organisation’s network infrastructures.

Chapter 3 explains the Proposed Digital Forensic Framework to be created for the Investigation of Insider Network Attacks.

Chapter 4 shows the strengths and weaknesses of the existing Digital Forensic Framework as well as the Proposed Digital Forensic Framework.
2 Literature Review

2.1 History of Insider Network Attacks

History shows that the very first computer crime which was committed was actually done so by an Insider, this fact in itself shows just how dangerous crimes committed by Internal Members of an organisation are (Contos, 2007). Insider Attacks have been around since the 1800s, they still pose the same amount of risk to an organisation as they did in the 1800s and there has been no way to prevent the occurrence of these attacks using technology and security policies (Contos, 2007).

2.1.1 Volume of Insider Network Attacks

An InfoWorlds article in 2010 provides information from a number of crime surveys in order to show the number of Insider Network Attacks that are currently being conducted. The aforementioned article provides actual figures about the reason research needs to be focused into Insider Network Attacks. This can be shown as follows

“Many sources have long cited an estimate that insiders are responsible for 80 percent of malicious attacks.” (Grimes, 2010, p. 2).

Insider Network Attacks account for a large number of the reported Network Attacks currently occurring within society. The above statement can be seen to be verified by a number of sources and surveys which are carried out, including the 2013 Information Security Breaches Survey (PwC, 2013). However there are a lot of common ideas surrounding the quantity and effect of Insider Attacks on organisation’s network security and their reputation, which when looked into further can be seen to not be entirely true. The idea that the number of Insider...
Attacks far outweigh the number of attacks carried out by External Attackers can be seen to not be the entire story (Schultz, 2002). However this discrepancy in the number of Insider Network Attacks when compared against the number of External Network Attacks, comes from the fact that organisations are less inclined to report an incident of an Insider Network Attack which means that the statistics available for the number of Insider and External Network Attacks are not always valid.

People need to be aware of the risks that insiders pose to the security of the network as well as the way in which to deal with the different types of attack. There needs to be information about the crossover of the type of Network Attacks that are conducted by Insider and Outsiders.

With the increasing number of Insider Network Attacks occurring there is a need for a definitive Digital Forensic Framework to be created. This is to ensure that there is a standard for all future digital forensic investigations. Before a Digital Forensic Framework can be designed for Insider Network Attacks, a comparison of the current research in this area needs to be carried out.

Conflicting evidence and comments in the literature available about the rate and effect of Insider Network Attacks causes a problem as to the truth. There are quite a few sources that claim the Insider Attacks occupy a greater rate of the overall numbers of the Network Attacks that are effecting organisations all over the world (McCormac, et al., 2012). There is one author Schultz (2002) who states that Insider Attacks do not account for any more of the Network Attacks than the External Attackers. It is for this reason that due to the amount of current literature that expresses the view and figures from Crime Surveys that the Insider Attacks have a higher proportion of the overall amount of attackers that attack the world’s organisational networks, that a framework is required.

2.1.2 Organisation of Literature Review

The review below of the current literature is organized in the following way;

- Information about Insiders.
- Details of the type of attacks that can be carried out by Insiders within the organization.
- Current Digital Forensic Frameworks which can be used to investigate Network Attacks.
2.2 Insiders and the Insider threat as a whole

An Insider can be anyone who is given authorised access and credentials to an organisation’s network systems.

There are many different definitions and ideas about who can turn out to be a malicious insider, as well as the reasons why they are choosing to attack the networks of the organisation they are employed by.

Skoudis & Liston (2005) provides a complete account about the people who can threaten the organisations they work for, including the reasons why they choose to attack the very organisations that they work for or provide services to. Skoudis & Liston (2005) says that the threat from an insider can come from an employee who is not happy with the way in which the organisation treats them. As well as from employees who do not realise that their activities on the network could cause harm to the data which is protected within. Insider threats can easily and more frequently occur from the current employees within an organisation. (Skoudis & Liston, 2005).

There are many different classifications of Insiders, depending on the reasons and motives behind the execution of the Insider Network Attack. The first and possibly one of the most frequent classifications of Insiders is the Disgruntled Employee. This is due to the fact that they already have the access necessary in order to carry out the Insider Network Attack. This type of Insider is the one who is possibly not pleased about the way they are treated (Skoudis & Liston, 2005). A Clueless Employee is the second most frequent classification responsible for Insider Network Attacks, although the attacks from these Insiders are not necessarily intentionally executed. Customers can attack their own suppliers as a way to correct the prices that they are being charged in order to make their payments fairer in their eyes (Skoudis & Liston, 2005). The most dangerous classification of Insider is the Contractor, these employees are given the access right necessary for their jobs; however these access rights are not always revoked once the contract has ended. (Skoudis & Liston, 2005).
The lack of knowledge of certain employees causes problems, with those employees then accidently making the data held within the organisation vulnerable. This lack of knowledge is often due to the lack of education about the importance of security within the organisation’s network systems. PwC (2013) show that from their research into the reasons surrounding the number of data breaches that occur every year,

“36% of the worst security breaches in the year were caused by inadvertent human error (and a further 10% by deliberate misuse of systems by staff).” (PwC, 2013, p. 2),

This figure shows the importance of user education. Organisations of varying sizes do not pay as much attention as is necessary to the importance of creating and implementing security policies, to protect the organisation from external and internal forces. Without education and information about the security policies that are in place and the importance of sticking to the regulations and security procedures that are discussed in the policy, employees will continue to place the systems at risk. This may be by purely unintentional actions which cause security lapses. (PwC, 2013).

2.2.1 Insider Threat Overall

The insider threat problem as a whole poses a huge risk to the credibility and capability of the organisation that is affected (Theoharidou, et al., 2005). There are many systems and mechanisms which can be put into place in order to prevent, or certainly make it harder for, external parties to attack the network, but when it comes to preventing or protecting against your own employees using the resources at their disposal to damage the integrity of the organisation, this is much harder to stop. You cannot simply prevent your employee’s access to the network system as a whole.

“There is no “silver bullet” for stopping insider threats” (Cappelli, et al., 2012, p. 3). This statement expresses just how hard it is to prevent Insider Attacks from happening against your system. It can also be seen by Cappelli et. al. (2012) that the highest priority for prevention of Insider Network Attacks is the continual review of the access controls and user accounts to ensure that all accounts are necessary and relate to an active employee.

Insider Network Attacks do not necessarily require great technical skill this is shown below:

“Martin Jordan, who heads up the cyber response team for KPMG, demonstrated an attack using weaponised PDF document. The attack was
created in just two days by an intern, who was a geography graduate with little computer knowledge, using free, easily available software.” (Ashford, n.d.)

Cyber-Ark (2011) took the view that from 2011 onwards there would be an increase in the risks presented by external attackers which would outweigh the risks of the Insider attacking their own organisation. Although this source disagrees with the many that state the Insider threat will still continue to pose a huge risk to the organisation as a whole as well as their reputation.

The following four sources all show that insiders are committing an increasing number of attacks, Furnell (2004) states that 80% of the threat of Network Attacks are emanating from an internal entity within the organisation. Skoudis and Liston (2005) explain that the external Network Attackers do account for a majority of the overall Network Attack figures, however Skoudis and Liston (2005) also explain that a large number of the attacks do indeed occur from an internal entity. Ortega (2007) explains that instead of focusing on network security from an external point, the new way of looking at network security is on the home front within their own organisation. Kerner (2013) as one of the newest view points within the debate about the Insider Threat as a whole, shows that 54% of people within the survey state that it is more difficult at present to build defences against Insiders than in previous years. The above points of view show that there are far more sources that state that the number of Insider Network Attackers are increasing and will continue to do so as there are no technical solutions that come off the shelf, which will prevent employees attacking the organisation.

2.2.2 Impact of Insider Network Attacks
The impact of Insider Attacks being conducted on an organisation’s network system is not just applicable to the data that has been made vulnerable, but the extensive damage that the reports of this attack could have on the reputation of the organisation.

Ortega (2007) explains that there are more serious threats and risks to company’s welfare through internal attacks, than ones that are externally motivated.

As technology grows and expands, so does the risk and effect that being attacked by one of your own employees has on the organisation. When it comes to the decision about which organisation a customer will buy its services from, it is not likely to be the organisation that
has reported incidents of an employee within the organisation of leaking customer’s sensitive information.

Oltisik (2013) is able to sum up the reasons why Insider Network Attacks have such an effect, this is due to the fact that unlike dealing with an external attack, where technical security measures can be put into place, guarding against insider attacks is not the same, because there are no technical measures that can be put into place.

Perry (2006) shows that the cost of Insider Network Attacks on an organisation far outweighs the costs when compared to the cost of viruses. It can be seen that Insider Attacks cost millions more than the cost of dealing with a virus that hits an organisation.

2.2.3 Case Studies of Insider Network Attacks

In order to demonstrate the varying degrees on Insider Networks Attacks that are affecting organisations network infrastructures over previous years, the following case studies show just a few cases of Insider Network Attacks:

In 2012 The Swiss Intelligence Agency, experienced the loss of classified information due to a system administrator being able to walk out with the sensitive information. The systems administrator in question had unlimited access rights which meant that the sensitive information held within the network infrastructure was at the users fingertips and no access rights were needed for the administrator to carry out the attack (Lemos, 2012)

Another Case Study of an Insider Network Attacks is the recent attack on a Supermarket where the employee’s personal information was stolen by another employee within the organisation. The information was then published on an internet site. (Davey, 2014)
2.3 Different types of External Network Attacks

There is a huge amount of literature available about the different types of Network Attacks that are and can be carried out by external entities; some of the different types of Network Attacks are explained below:

2.3.1 Back Door Attack
A Back door attack is an external network attack that is based around the creation of an external point of access to the network. This type of attack would not need to be carried out by an internal member of the organisation as they already have access to the network using their normal work credentials. Back door attacks are conducted by the attacker getting access to the organisation’s Network Infrastructure, through the creation of an Administrator account into the firewall, so that they have all of the access rights to be able to launch the attack of their choosing (Cole, et al., 2009).

2.3.2 Social Engineering Attack
Social engineering could be carried out by an Insider within the organisation. An IT technician for the organisation could easily extract the hard drive and sell the information or hold the company to ransom if they were disgruntled. However this type of attack is usually carried out by an External entity, this is due to the fact that External entities do not have all of the required information necessary to commit their chosen network attack. So they need to use social pressures as a way in which to get the preliminary information (Cole, et al., 2009). There are several different versions of a Social Engineering attack, the main one being a Phishing attacks. This type of attack is where the Attacker creates duplicate web pages of organisations in the hope that Users will click on this web page and enter in their Username and Passwords for the website, which means that the Attacker now has access to the User’s account for that organisation. The Attacker can also send emails to the Users requesting that they enter their personal details into the fake web site (Joshi, 2008).

2.3.3 Dumpster Diving Attack
Dumpster Diving has to be considered as an entirely external attack on an organisation as an Insider within an organisation would have access to the information without needing to look for what was being discarded from the organisation. The only time in which this attack would be needed to be conducted by an internal member of the organisation is if the least privilege access control system was put into place. If this was the case then a disgruntled insider would not have access to the most vulnerable information, which in the wrong hands could do the most damage or be able to hold the CEO’s of the company to ransom. With all of the literature
that is available about the different types of network attack that have been known to have been conducted from most probably an external source the problem with the descriptions, example and explanations of these types of attacks is that they are explained from an external point of view, which plays down the actual risk that the Internal members of staff can pose to an organisation. (Cole, et al., 2009).

Dumpster Diving Attacks are conducted with little or no technical expertise; as the attacker needs to get the required information about the Network Infrastructure, in order for them to be able to attack the network (Long & Mitnick, 2008).

2.3.4 Denial of Service Attack
The Denial of Service attacks are usually committed from an external entity, this attack occurs by taking up all of the resources that are available within the network, so that there are no resources available for any of the authorised users of the network (Cole, et al., 2009).

For this type of attack, the attacker would send request after request to the servers on the chosen network. This increase in the number of requests would mean that there would be no resources left available on the servers to handle the legitimate requests from authorised members of the organisation.

During a Denial of Service Attack, the messages sent to the servers are using the TCP protocol, whereby the SYN flag informs the server of the need to reserve a portion of the resources until an ACK flag is sent to inform the server that all of the information has been transferred successfully (Joshi, 2008).

The Denial of Service Network Attack can be explained using the following scenario:

The attacker is seen as Fred. The User and the Server are used to explain the process of a Denial of Service Attack.

The User would send a message to the Server with a SYN flag; this then means that resources will be set aside until the User has transferred the data. Once the data is transferred the User sends a message with an ACK flag which means that the Server can then reallocate the resources. Fred can then send streams of messages with an SYN flag meaning that the Server will allocate resources for each message sent. Due to the limited resources each server has, if enough of these messages are sent by Fred, without sending the ACK message to reallocate the resources the server will become overloaded. When the User wants to send a SYN message and then the data, there will be no resources left, thereby preventing the authorised
user of the Network from accessing the resources available on the server. This whole sequence of events creates a Denial of Service Attack (Joshi, 2008).

The above example is a TCP SYN flood type of a denial of service attack (Nong, 2008).

2.3.5 Tailgating

Tailgating is an attack upon an unsuspecting organisation by blending in with their other employees when they leave the organisation for a break, by the time they go back in they believe that you belong within the company, organisations do not necessarily make checks on the employees that walk back into the building once they have gotten through the alarmed doors, although the organisation needs to be sure that the employees are aware that not everyone who appears to be a part of the organisation is not necessarily true. They should also be sure that when everyone re-enters the building that they use their own security passes (Long & Mitnick, 2008).

2.4 Different types of Insider Network Attacks

It is recognised that the most published types of network attack are those that are carried out by external attackers, with criminal motives. However this does not mean that these attacks
cannot be carried out by an Insider within an organisation. For Insiders half the work is done as they already have their own credentials and the trust of the organisation's management.

When it comes to seeing the difference between the types of network attack that are carried out by the Insiders in comparison to the attack carried out by external parties, the main characteristic is in the amount of knowledge of the system that is needed to carry out the attacks.

2.4.1 Inappropriate System Use Attack
The main attack that can be easily conducted on an organisation’s network by an Insider is "Inappropriate System Use" (Cole, et al., 2009, p. 13). This is due to the fact that they can use the organisation’s resources with the credentials that they have been given and instead of carrying out the work that is required for the organisation, they are conducting their own personal activities, by downloading their own information on works time, which in turn could slow the network down for the other legitimate users.

2.4.2 Denial of Service Attack
A Denial of Service Attack which is carried out by downloading huge files in order to max out the amount of storage space is an attack that could be carried by a disgruntled insider in an organisation. There would be little or no need for technical knowledge, except for the amount of space available on the server and therefore the amount of files or size of files that would need to be downloaded. (Cole, et al., 2009). A user would download as many files as necessary from the network in order to keep the server busy and prevent the server from accepting anymore TCP packets or requests from the other members of staff within the organisation. This continual download would prevent the legitimate business of the employees from being carried out.

2.4.3 Back Door Attack
A Back Door Attack could be carried out by an Insider as a way for them to have access to the network infrastructure from a remote connection. This would be done by creating a door within the security and firewalls within the organisation’s network. Once this is created the user would be able to log into the network through a remote connection with his own credentials and launch any number of pieces of software, for example a worm which will slowly destroy the network, therefore reducing if not stopping the productivity of the organisation (Blackwell, 2012).
2.4.4 Theft
The most basic attack which an Insider could conduct is the theft of sensitive information, if an organisation allows the use of USB memory sticks, then an employee can connect the USB and copy over or simply take all of the files that are on the network drives. This information could then be deleted meaning that the organisation would have to rely on the use of the backups or the information could be given to a competitor. (Long & Mitnick, 2008)

2.4.5 Logic Bomb Attack
The Logic Bomb is a very dangerous example of Insider Network Attacks, they are committed by insiders due to the privileged access they have and that is required in the planting of this Logic Bomb (Lewis, 2013).

This type of Insider Network Attack can be conducted, by a disgruntled system administrator who is not happy with the way the organisation is treating them. The Logic Bomb is a line of code which can be programmed to attack whenever the disgruntled insiders decide. The Logic Bomb is launched on the Network Infrastructure for example one of the organisation’s server systems, once it has been launched there will be a condition set in the line of code that once the condition is met the Logic Bomb will, for example, delete the files that exist on the server system. The idea of the Logic Bomb being able to have a condition set means that the disgruntled insider can be nowhere near the computer system when the Logic Bomb activates (Lewis, 2013).

2.4.6 Man in the Middle Attack
Man in the Middle attacks have many different connotations which can be used depending on the information that is necessary for the attack to be successful and the type of Network Infrastructure, the different types of Man in the Middle attacks are “Eavesdropping”, “Ettercap sniffing” and “KeyLoggers” (Nong, 2008, p. 16).

A Man in the Middle attack is conducted by the attacker having the skills to be able to put themselves within the line of communication between two legitimate users on the Network. This means that one user could send an encrypted message to another user using an Asymmetric Encryption system, during the transmission of the message the attacker can change the content of the message and send the edited version to the legitimate user, without either users noticing that anything untoward has happened during message transmission. This process is carried out due to the attacker substituting their public key with the one of the receiver of the message, which provides the attacker with the key to be able to decrypt the intercepted message (Cole, et al., 2009).
2.4.7 Reasons for the number of Insider Network Attacks

Oltsik (2013) stated that in 2008 there was the view that the Insider attack posed the greatest risk of all to network security and this was stated to be the case as

“insiders tend to know what they want, where it is, and how to get it” (Oltsik, 2013)

The results of many surveys into the risk organisations believe they are susceptible to based on their current network set up, show that quite a lot of organisations are realising that the Insider threat is growing and their security policies and procedures used to protect against external attackers will have little or no effect, when it comes to preventing Insiders intentionally or unintentionally attacking the organisation.

There is a large amount of disagreement over the number of Insider Network Attacks that are occurring; this is due to the classification of certain types of attack. An attack which is set up by an External entity, but carried out by a person with legitimate access within the organisation, would not be considered to have been an Insider Network Attack.

The attacks with an inside element are due to the fact that they all have the access necessary for these attacks to be undertaken, the easy way of preventing these attacks would be to limit the access levels of the employees. This is however impractical as within every organisation there needs to be trust in order to prevent the increase in the number of disgruntled employees and therefore repeat the cycle of the ever increasing Insider Network Attacks.

Perry (2006) states that 80% of the attacks occurring within organisation’s Network Infrastructure are as a result of Insiders and not as it is seen within the media, carried out by external hackers.

2.4.8 Cross-Over of Insider and Outsider Network Attacks

There are many different instances of attacks which are conducted by both an Insider and a person on the Outside of the organisation. This is due to the fact that for an Outsider it is easier for them to take advantage of a disgruntled employee and get all of the information necessary to carry out an attack on the organisation in half the time.

Lee (2012) explains the dangers of disgruntled employees teaming up with an Outsider. The disgruntled employees have all of the access controls, or if they do not have the access controls necessary for themselves, then they would be able to borrow the credentials of
another employee which would also act as a way to cover the tracks of the attacker (Lee, 2012).

2.5 Digital Forensic Investigations

The information gathered about the different types of External and Internal Network Attacks will be used in order to see where these types of attacks fit into the existing Digital and Network Forensic Frameworks.

The section will discuss the literature that is available about the best ways in which to investigate cases of externally initiated network attacks. As well as the frameworks created for
externally initiated attacks which can be applied to an attack from an Insider within an organisation will also be discussed.

Pilli (2010) provides the details necessary when it comes to looking at creating Digital Forensic Frameworks for Insider Network attacks. The real reason and situation of Network forensics compared with general Computer forensics investigations is shown

"In computer forensics, investigator and the hacker being investigated are at two different levels with investigator at an advantage. In network forensics, network investigator and the attacker are at the same skill level. The hacker uses a set of tools to launch the attack and the network forensic specialist uses similar tools to investigate the attack." (Pilli, et al., 2010, p. 15)

The above realisation shows the need for research and detailed processes to be created for investigating all types of Network Forensics in order to be sure that the network investigators have the same upper hand that can be seen from the computer forensic investigators.

For every forensic investigation there are the basic steps which must be followed at all times in order to prevent the case from being kicked out of court. Most of the processes and frameworks that exist for dealing with cases of Network Attacks or attacks on other services employed by organisations, only look at how to investigate and uncover the evidence that is left behind after an external attacker has taken advantage of the vulnerabilities that exist within the organisations network structure.

The current literature that is available about the different types of Digital Forensic Framework shows a theme about how to forensically analyse cases of external breach within organisations. These frameworks show the different processes needed to discover the source of the breach within the varying services and media that is used.

Bosworth & Kaybay (2002) shows that the use of the term framework can be a confusing one, much like the way in which the people who commit the attacks are portrayed. Bosworth & Kaybay (2002) displays that the term frameworks and models are easily interchanged. Bosworth & Kaybay (2002) provides information about how to go about securing computers and networks that can be used within the organisations, however the information which is included on the different types of Denial of Service attacks shows crucial information about how these attacks can be carried out (Bosworth & Kaybay, 2002).
2.5.1 Types of Digital Forensic Frameworks

There are quite a varied amount of frameworks available for investigating cases of Network Attacks; these include frameworks for investigating when different services used within the organisations get attacked.

The majority of frameworks that currently exist from research into the ways in which Network Attacks occur, are done using external case studies as a base to form the framework. On the other hand the frameworks that are available for dealing with Network Attacks from an internal point of view look at predicting and detecting the attacks, there are not Digital Forensic Frameworks that look at how to investigate once an Insider Network Attack has been carried out. Schultz (2002) provides a valuable article about the ways in which Insider Attacks can be best predicted by using the research that was available to assess the reasons why Insiders attack their own organisations. This article and framework was created as Schultz (2002) stated that

“The need for better prediction and detection of insider attacks is great given the magnitude of the insider threat” (Schultz, 2002, p. 531).

2.5.2 Evaluation of Existing Digital Forensic Frameworks

There are many Digital Forensic Frameworks which can be used for the investigation of different types of cybercrime. Each of these Frameworks have their own strengths and weaknesses, these are discussed below.

The Integrated Framework is made up of the following four phases: “Evidence Source Identification and Preservation, Collection, Examination and Analysis, Reporting and Presentation” (Martini & Choo, 2012, pp. 74-75).

This framework is built for the investigations within the Digital Forensics field; all of the phases included in the framework are the required elements that would mean that any cases investigated using this framework would be able to be presented in front of a court of law. The Integrated Framework also incorporates the most important element when it comes to the investigation of any type of Cybercrime which is the Preservation phase. Before any investigative methods can take place in the evidence that is collected, the evidence itself must be copied in a forensically sound manner to ensure that there are no changes made to the actual evidence during the Examination and Analysis Phase.
McKemmish’s Digital Forensic Framework consists of four phases which are as follows: “Identification of Digital Evidence, Preservation of Digital Evidence, Analysis of Digital Evidence, Presentation of Digital Evidence” (McKemmish, 1999, pp. 1-2)

The McKemmish Framework can be seen as one of the early Digital Forensic Frameworks which was created. The following frameworks that were created are based on the McKemmish Digital Forensic Framework, this framework is based specifically on the Digital Crime Scene side of an Investigation.

The first phase of this framework explains the importance of gathering information about all of the details to do with the location of the evidence in question in the varying investigations. The inclusion of a phase about the preservation of the evidence that is collected is of great importance in a Digital Forensics Framework. This phase acts as an important addition to the base four steps.

The Digital Forensic Framework produced by NIST consisted of four phases which are encapsulated in every Digital Forensic Framework, these phases are: “Collection, Examination, Analysis and Reporting” (Kent, et al., 2006, p. 1)

The NIST Framework can be seen to contain the main components that are necessary for a Digital Forensic Investigation to be forensically sound according to the guidelines issued by the Association of Chief of Police Officers (Williams, 2011).

The Investigative Process Model consists of the following phases: “Incident Alerts or Accusation, Assessment of Worth, Incident/Crime Scene Protocols, Identification or Seizure, Preservation, Recovery, Harvesting, Reduction, Organization and Search, Analysis, Reporting, Persuasion and Testimony” (Freiling & Schwittay, 2007).

The Collection, Examination, Analysis and Reporting phases are broken down into the specific steps which occur during each of these phases which provide the Investigator with the tools and steps needed to correctly gather and examine the evidence.

This framework expands upon the initial phases that are necessary within the guidelines issued for the course of Digital Forensic Investigations, and has the advantages of having phases which expand to the best ways in which the investigator can explain the opinions that were reached during the Digital Forensic Investigation report.
### 2.5.3 Comparison of Digital Forensic Frameworks

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Evidence Source Identification and Preservation</td>
<td>Identification of Digital Evidence</td>
<td>Incident Alerts or Accusation</td>
<td>Identification</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Assessment of Worth</td>
<td>Preparation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Incident/Crime Scene Protocols</td>
<td>Approach Strategy</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Identification or Seizure</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collection</td>
<td>Collection</td>
<td>Collection</td>
<td>Collection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Examination and Analysis</td>
<td>Examination</td>
<td>Recovery Harvesting Reduction Organization and Search</td>
<td>Examination</td>
<td>Examination</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Analysis of Digital Evidence</td>
<td>Analysis</td>
<td>Analysis</td>
<td>Analysis</td>
<td></td>
</tr>
<tr>
<td>Reporting and Presentation</td>
<td>Presentation of Digital Evidence</td>
<td>Reporting</td>
<td>Reporting</td>
<td>Presentation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Persuasion and Testimony</td>
<td></td>
<td>Returning Evidence</td>
<td></td>
</tr>
</tbody>
</table>

**Table 1 Comparison of Digital Forensic Frameworks**

Within the above six Digital Forensic Frameworks there are many similarities, the main phases that are included in every Digital Forensic Framework are: Preservation, Collection, Evidence, Analysis and Reporting.

These phases incorporate all of the necessary components of a cybercrime investigation.
2.5.4 Network Forensic Frameworks

The field of Digital Forensics is too broad for the specialised investigation of Network and Insider Network Attacks, for these kinds of investigations there are Network Forensic Investigators. Pilli (2010) states that the definition of Network Forensics and the kinds of evidence that Network Forensics deals with is:

“The concept of network forensics deals with the data found across a network connection mostly ingress and egress traffic from one host to another.” (Pilli, et al., 2010, p. 1)

The Network Forensics field requires investigative methodologies in order to have a standard way for all Network Forensic Investigators to investigate every case of Network Attack cybercrime.

Since the separation of Network Forensic from the Digital Forensics field there are multiple methodologies that can be adopted depending on the Network Forensics Investigators preference, Pilli (2010) posed a Generic Framework for the Investigation of Network Attacks which can be used for every type of Network Attack. This methodology incorporates the guidelines from the Association of Chief Police Officers which is that all examination of data must be carried out on a copy of the data only, in order for the test to be repeated if necessary (Williams, 2011).

2.5.5 Evaluation of Network Forensic Frameworks

The “Network Forensic Investigative Methodology (Oscar)” (Davidoff & Ham, 2013, p. 17), is a framework which can be used to investigate cases of Insider Network Attacks.

General Process of Network Forensics is created to include the following five phases: “Capture, Copy, Transfer, Analysis, Investigation, Presentation” (Ren & Jin, 2005, p. 5).

This framework is the first for the field of Network Forensics, and the Network Forensics Investigators. The phases included in this framework are the basic steps for a Network Forensic Investigator to follow for the Investigation to run smoothly. This framework due to the nature of the phases included could be used for any Cybercrime, not just Network Attacks as the name of the framework indicates.

All of the phases included in this framework are in accordance with the guidelines given by the Association of Chief Police Officers, which ensures that all of the evidence collected and examined using this Forensic Process should be forensically sound (Williams, 2011).
On the other hand with this Process it starts at the collection of the evidence and there are no preceding phases about the crime scene or the identification of the evidence. This limitation means that this process would only be helpful to a Network Forensic Investigator once all of the evidence had been collected and the examination was about to begin.

Network Forensics Investigative Methodology includes five phases which are: “Obtain Information, Strategize, Collect Evidence, Analyse, Report” (Davidoff & Ham, 2013, p. 17) this is known as OSCAR.

The Network Forensic Investigative Methodology includes phases which are required in order to complete a full Network Forensic Investigation on a network infrastructure, each phase provides the Network Forensic Investigator with steps about the sort of questions that need to be asked and the various components of the Network Infrastructure that need to be looked into in order to ensure that no evidence is missed.

A phase where the evidence is collected is needed in every single Digital Forensic Framework as well as every forensic framework; the processes that need to be followed during this phase will change depending on the area that the framework applies to. This is one of the most important phases in the entire framework that will be included. Without the collection framework there would be no case as there would be nothing to show.

The incorporation of multiple review phases may be one to be considered as this OSCAR framework appears to incorporate many of the important elements for an Investigation Framework but does lack the inclusion of a Review Phase, which would remind the forensic investigators that evidence may have been overlooked during the analysis stage (Davidoff & Ham, 2013).

The report phase is needed within every forensic framework; this is because there is a need to be able to present the investigative results in a format that can be used in a court of law.


This framework was created in 2010 and focuses on the methods required for the investigation of Network Attacks undertaken by Network Forensic Investigators, this framework includes many phases that are not seen in the Digital Forensic Frameworks.
“Preparation and Authorization” (Pilli, et al., 2010, p. 4) phase ensures that the organisation has all of the necessary security measures in place to for an investigation to take place, as there needs to be evidence of the Network Attack. With the breakdown of the phases within this framework; the Network Forensic Investigator has an easy to follow process which includes steps before the collection of evidence, which are necessary in order to plan out the investigation appropriately.

2.5.6 Comparison of Network Forensic Frameworks

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Preparation and Authorization</td>
<td>Strateitize</td>
<td></td>
</tr>
<tr>
<td>Detection of Incident/Crime</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident Response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collection of Network Traces</td>
<td>Collect Evidence</td>
<td>Capture</td>
</tr>
<tr>
<td>Protection and Preservation</td>
<td>Copy</td>
<td>Transfer</td>
</tr>
<tr>
<td>Examination</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analysis</td>
<td>Analyse</td>
<td>Analysis</td>
</tr>
<tr>
<td>Investigation and Attribution</td>
<td>Investigation</td>
<td></td>
</tr>
<tr>
<td>Presentation and Review</td>
<td>Report</td>
<td>Presentation</td>
</tr>
</tbody>
</table>

*Table 2 Comparison of Network Forensic Frameworks*

Within the above three Network Forensic Frameworks that are used to investigation Network Attacks, there are three key phases of Investigation that can be seen within all three Network Forensic Frameworks. These are Collection or Capture of Evidence, Analysis of the evidence that was collected and Presentation of the Findings that the Investigation of the Network Attack uncovered.
2.5.7 Creation of Digital Forensic Frameworks

The occurrence of Insider Network Attacks is increasing along with Network Attacks that are committed by external parties. There needs to be an appropriate way in which to investigate the number of Insider Network Attacks. This is because there is a different process when a Network Attack is committed from inside the organisation rather than from an external point of view.

Schultz (2002) shows the way in which the research and literature that is currently available can be used in order to produce a much better framework. By using the advantages of current frameworks in order to incorporate and produce a framework that meets the purposes of the author.

For Digital Forensic Frameworks there is a need for a strict process to be followed for every investigation no matter what type of digital crime is being investigated. This is in order to prevent any cases tried in the courts from being thrown out or any doubt being placed on the integrity of the evidence collected.

This fact can be seen to be confirmed by Martini and Choo who state that:

“To reduce the risk of digital (forensic) evidence being called into question in judicial proceedings, it is important to have a rigorous methodology and set of procedures for conducting forensic investigations and examinations.”

(Martini & Choo, 2012, p. 73).

The above quotation explains the importance of having a Digital Forensic Framework for investigating cases of Insider Network Attacks to be sure that the evidence collected can stand up to the scrutiny within a court of law.

2.5.8 Digital Forensic Frameworks for Insider Network Attacks

Hunker and Probst stated that "Currently, insider threat forensics appears to be highly undeveloped" (Hunker & Probst, 2011, p. 16). This statement shows that more research needs to be conducted into Insider Network Attacks, as a way to be able to forensically investigate these cases.

The work carried out by CERT explains that there would be a difficulty creating a framework for investigating all types of insider attacks on the individual organisations as there are different motivations and reasoning behind each single attack. Cappelli et al. (2012) explain
within the CERT guide to Insider Threats that there could not easily be a single method to investigate the in-depth details of each individual type of Insider Attack.

"The important thing to remember is that the patterns are different for each type of crime. There is not one single pattern for insiders threats in general." (Cappelli, et al., 2012, p. 7)

Although the literature shows that there are few definitive processes available for looking at and investigating the execution of the different types of Insider Network Attacks. However Quba (2013) does show a basic process for investigating Man in the Middle Attacks, which can be carried out from an Insider or External entity.
2.6 Summary

In this chapter the view of the current literature in the area of Network Attacks undertaken by Insiders and External parties were examined, to explain the reasons why Insider Attacks are so dangerous to an organisation.

The different types of Network Attacks both externally and internally initiated were described to show the differences and the dangers of Insider Network Attacks. There is a lot of correlation between the types of attacks that can be initiated by an External Attacker and those that are undertaken by the Insiders within the organisations.

The information gathered about the different types of Insider Network Attacks and the existing Digital and Network Forensic Frameworks that are currently being used shows that in all of the methodologies that can be followed during the course of a Digital or Network Forensic Investigation, no methodologies have been found for the Investigation of Network Attacks from an internal entity.
3 Methodology

This project was carried out using qualitative research methods (Greetham, 2009) as a way to gather informative and detailed information about the different types of Insider and External Network Attacks.

The Research was undertaken using various journal sources and books in order to get as much detailed information about the type of Insider Network Attacks that occur as possible.

The methodology used in order to design the Proposed Digital Forensic Framework, has been through the research and evaluation of the existing Digital Forensic Frameworks and Network Forensic Frameworks in order to establish the necessary components when it comes to the Investigation of Insider Network Attacks.

After conducting a review of the existing Digital Forensic Frameworks as well as the Network Forensic Frameworks, the reoccurring phases that existed in those frameworks were noted down in order to gather the most important elements which need to be included in every Digital Forensic Framework. The information gathered from this review was then used alongside the Association of Chief Police Officers Guidelines (Williams, 2011), as a way to be sure that the design of the Proposed Digital Framework includes all of the information to guide a Network Forensic Investigator about the best way in which to investigate cases of Insider Network Attacks.

The common elements of a Digital Forensic Framework will be assessed to ensure that they are incorporated into the Proposed Digital Forensic Framework for the Investigation of Insider Network Attacks.

A design of the framework is then to be developed in order to see how the chosen phases connect and what added phases may be necessary.

This design is going to consist of all of the common phases that were found within the existing Digital Forensic Frameworks, as well as the changes that are necessary for the Investigation of Insider Network Attacks. The first phase is going to be specifically for the Investigation of Insider Network Attacks as a phase about the verification of an incident within the organisation is especially important before employees’ computers are acquisitioned.
In order to test the Proposed Digital Forensic Framework an experiment will be carried out using virtual machines to simulate an Insider Network Attack, which will then be investigated using the Proposed Digital Forensic Framework.
3.1. Digital Forensic Framework Design

Digital Forensics has many different frameworks that can be used for the investigation of every single cybercrime. For the field of Digital Forensics the different types of frameworks all have a differing level of depth. With the introduction of every new framework there can be seen to be similarities as well as duplicating phases, as every framework that is created still has to adhere to the Association of Chief of Police Officers (ACPO) guidelines for Digital Forensic Investigations, the guidelines provided by the Association of Chief of Police Officers can be seen as follows:

- **Data Preservation** – When evidence is analysed the investigators must ensure that no changes are made to the data.
- **Original Data** – If the Original Data has to be examined directly the detailed and accurate records must be maintained along with valid reasons for examining the original data.
- **Audit Trail** – There needs to be a record of all processes undertaken by the investigator during the course of the investigation.
- **Chief Investigator** – The chief investigator has complete responsibility for the Investigation as a whole (Williams, 2011).

There are also four main steps which are Collection, Examination, Analysis and Report, these steps are necessary to be followed for every cybercrime investigation to be able to be tried in a court of law. These steps need to be incorporated within the creation of the Digital Forensic Framework for the Investigation of Insider Network Attacks.

Network Forensics required the introduction of even more specialised Digital Forensic Frameworks because there needed to be different steps for the collection of Network evidence and volatile data (Garfinkel, 2010).

Due to the number of different types of Insider Network Attacks, there is a need for a Digital Forensic Framework to be created to provide Network Forensic Investigators with a process to follow for all Network Forensics Investigations, where the attacks are carried out by Insiders within the organisation.

The very nature of Insider Network Attacks means that there are different ways of gathering evidence for each individual type of attack. With this information taken into consideration the proposed Digital Forensic Framework for the Investigation of Insider Network Attacks looks at investigating these Insider Network Attacks at the base level with the inclusion of Iterative Phases for those cases where once the evidence has been analysed, it can be seen that more
evidence needs to be collected, therefore the framework allows the collection phase to be repeated multiple times.

After detailed research into the area of Network Forensics, there is very little in the way of guidelines and methodologies when it comes to investigating Insider Network Attacks. There are many Network Forensics Frameworks looking at crimes from an external source, certain phases within these frameworks would still need to be used, even within an Investigation into an Insider attacking the organisation Network Infrastructure.

3.2 Proposed Digital Forensic Framework for the Investigation of Insider Network Attacks
3.2.1 Design of Proposed Framework

The blue phase above is the Incident Response Phase which will most likely be undertaken by Information Security Officers within the organisation and the rest of the phases are to be carried out by a Network Forensic Investigator.
3.3 Explanation of Proposed Digital Forensic Framework

The proposed Insider Network Attack Investigation Framework encompasses the four key phases which are required within every Forensic Investigation, no matter the source or the service. Lillard (2010) explains the importance of the inclusion of these four steps.

These four steps are “Preparation”, “Acquiring the evidence”, “Analyzing the data for the evidence” and finally “Documentation” (Lillard & Murray, 2010, pp. 10-11).
3.4 Incident Response Stage

3.4.1 Risk Assessment Phase

Once the basic information has been gathered about the organisation and the Insider Network Attack that has been undertaken further analysis can take place. A Risk assessment about the sensitive data that is vulnerable on the organisation’s network is needed because the evidence that resides on the suspects machines needs to be available for collection, however when dealing with Insider Network Attacks the suspect within the organisation may not be known.

3.5 Digital Forensic Framework Stages

3.5.1 Assessment of Insider Network Attack Status

When dealing with the Investigation of Insider Network Attacks, it is important that before any resources are used in the investigation of these attacks, the Network Forensic Investigators need to be sure that the Attack has actually been committed.

3.5.2 Information Gathering Phase

This phase provides the Network Investigators with the opportunity to gather the initial information that is necessary in order to plan out the execution of the investigation as a whole, this step is especially important in the Investigation of Insider Network Attacks because when an employee is behind the Attack on the organisation’s network, the Investigator needs to get as much information without alerting the employee to the possibility that there Attack has been discovered.

3.5.3 Documentation Phase

The Documentation Phase provides the Investigator with a way to ensure their Investigation is documented to the correct standard which is applicable in a Court of Law. This phase is an iterative phase as it will be repeated throughout the entire Insider Network Attack Investigation. Every phase within the framework after the initial Information Gathering Phase will lead to this Documentation Phase or the Documentation Phase will lead onto a particular Phase such as the Reporting Phase.

Documentation is the most fundamental part of every investigation. Documentation is important as it is necessary for an Investigator to be able to show the results of all of their steps during the Investigation, as well as being able to account for any changes that happen within the evidence that was collected and is then presented to a Court of Law. This does not change depending on the investigation of Insider Network Attacks or Externally Initiated Network Attacks.
3.5.4 Planning Phase
The investigation into the Insider Network Attack needs to be fully planned out before any investigative work is conducted.

There are many different factors that need to be considered when it comes to planning the order of the investigation as well as which pieces of evidence need to be collected first. This is because they are considered to be of the upmost importance or areas of the evidence that are the most volatile and need to be collected before any evidence is lost.

Davidoff and Ham (2013) provide a list of factors that could influence the way in which the evidence is collected. Davidoff and Ham provide the following helpful hints when it comes to the planning phase of any Network Forensic Investigation:

“Understand the goals and time frame of the investigation
List your resources, including personnel, time and equipment
Identify likely sources of evidence
For each source of evidence, estimate the value and cost of obtaining it
Prioritise your evidence acquisition
Plan the initial acquisition/analysis
Decide upon method and times of regular communication/updates
Keep in mind that after conducting your initial analysis, you may decide to go back and acquire more evidence.” (Davidoff & Ham, 2013, pp. 18-19)

The above list features all of the important considerations that need to be made while planning the investigation.

3.5.5 Collection of Evidence Phase
The collection of the evidence must be done as quickly as possible after the Insider Network Attack is discovered. This is to protect and ensure the reliability of the evidence that is collected from the computer and server systems within the organisation.

This is possibly the most important phase within the entire Digital Forensic Framework, because without the collection of evidence there is no case. The collection of evidence will
prove if any laws or security policies have been broken. The collection of evidence needs to be done in a forensically sound manner in order to protect the integrity of the evidence, to be admissible in a court of law.

Evidence collection is strongly linked to the documentation phase because every procedure and every system must be accessed by the Network Forensic Investigator

3.5.6 Evidence Analysis Phase
Every item of evidence that has been collected in the previous phase needs to be analysed in order to discover the true path of the Insider Network Attack. After the evidence has been analysed the investigator can now assess what areas of the organisation’s Network Infrastructure have been affected. McKemmish (1999) explains how the analysis of the evidence can be seen as the focal element of the forensic investigation.

When the evidence is being analysed this process is only done on copies of the evidence in order to continue the adherence to the ACPO guidelines for every Forensic Investigator (Williams, 2011).

3.5.7 Review of Findings Phase
The review of the entire investigation up to this point is carried out to assess the current evidence that has been collected. The Investigators will then be able to decide if there is more evidence to be gathered within the Network Infrastructure in order to find out how the Insider Network Attack happened. During this phase it needs to be decided whether or not the evidence that has been gathered and analysed would be admissible in a court of law and be able to result in the prosecution of the malicious insider.

If it is decided that there is not enough evidence, then the collection of evidence phase would be repeated in order for the forensic investigation to be produced to the correct standard.

3.5.8 Reporting Phase
This is the key phase for demonstrating the outcome of the investigation to either a court of law or the management of the organisation. For this phase the report that is produced needs to meet the guidelines set out by the courts.

The language used throughout the entire report needs to remain non-technical to ensure that the whole court can understand the motives behind the Insider Network Attacks as well as the way in which the attack was carried out within the organisation’s Network Infrastructure.
3.6 Summary

The phases of the proposed framework have been explained along with their connection to the Investigation of Insider Network Attacks. Each phase was explained with an overview of what would happen. The importance of the phases was discussed in order to explain the reasoning behind the connections of the phases as well as the ability to repeat phases at necessary stages of the investigation.
4 Low-Level Digital Forensic Framework Analysis

4.1 Explanation of the meaning of Symbols

The Input Symbol will show what information is taken from the preceding phases in order for the current phase to be able to be carried out.

The Output Symbol shows the information that comes from the analysis of the current phases and enables the Investigator to be able to carry out the next stage of the investigation.

The Phase Symbol will show which stage of the Investigation the Investigator is currently investigating.

Finally the Processes Symbol shows the different stages that will be used during the course of the investigation.

Figure 2 Explanation of Symbols
4.2 Incident Response for Insider Network Attack Investigation

4.2.1 Risk Assessment Phase

The Risk Assessment Phase is the processes that happen before an attack occurs as a way to prevent the occurrence of an attack by an Insider on the organisation’s Network Infrastructure. There are several processes that need to be followed in order to ensure that there are no vulnerabilities in the network which a disgruntled employee may be able to use to their advantage.

If an attack occurs on a Network there needs to be enough different security measures in place to ensure that there will be evidence of how the attack was able to be committed, these security measures are Incident Detection Systems and Firewalls.

A plan needs to be known within the organisations about what will happen if the organisation network is attacked, this plan includes the importance of only relevant people being informed of a Network Attack, this is especially important if the Network Attack is an Insider Network Attack. Since the very nature of Insider Network Attacks can mean that an employee who is within the organisation caused the attack, then the organisation does not want to risk informing the Attacker that they have been discovered, which could give them enough time to remove evidence of their involvement in the crime.

Once an attack has been discovered within an organisation there are certain steps that need to be taken in order to secure the evidence of the attack for the Investigation by a Forensic Investigator, these steps can be seen as follows:

- “Locate the likely machine that has been attacked;
- Take anti-contamination precautions: isolate the area close to the machine (nobody must access in the area around it or touch the machine);
- Provide access logs (firewall and servers);
• Freeze activities, whether possible - if not, try to fill a gap between those ones before the incident and after it (and keep the logs);
• In case the incident comes from inside the company, keep the logs which locate the machine.
• Determine possible data lines that can reach the machine.
• Isolate the machine from telephone lines (because data on the computer can be accessed remotely) - provide a possible password for access to the machine;
• Compile a list of users who have access to the machine; and
• Be prepared for a briefing session with the police.” (Rathmell, et al., 2002, p. 32)

These steps will help to preserve the evidence that remains within the organisation’s network infrastructure.
4.3 Digital Forensic Framework for Insider Network Attack Investigation

4.3.1 Information Gathering Phase

The first part of information gathering can be done under informal conditions in order to ascertain whether or not the attack has actually been committed.

The investigator also needs then to understand the structure of the organisation’s Network Infrastructure. This is done through the use of network maps, either being drawn up if the organisation does not already have them, or passed to the investigator if the organisation already holds a map of their Network Infrastructure.

There are a lot of differences in the types of Insider Network Attack, however due to the fact that these attacks are carried out with previous or current members of the organisation, there
is information about the behaviour as well as the current access controls which are in place which may help to narrow down the assets and the accounts of the employees who may have been responsible for the attack

With the amount of information that has to be discovered within this phase, there is a need for this phase to be broken down into several sub-phases. These sub-phases are as follows:

- Insider Network Attack
- Network Infrastructure
- Security

4.3.1.1 Insider Network Attack
This sub-phase would be where all the basic information is collected about the attack that was executed on the organisation’s network. This is due to the fact that these attacks are committed within the organisation’s own network of employees. This information is necessary as way to be sure about the number of employees within the organisation that know the attack conducted has been uncovered.

The information gathered within this sub-phase will be valuable within the Planning Phase, if it is uncovered that the entire organisation is aware of the breach in the security of the organisation’s Network Infrastructure. Then there will be a different order of evidence gathering when it comes to the Planning Phase.

The Investigator can use all of the information available to figure out which type of Insider Network Attack has been conducted on the Network Infrastructure. This information will be vital as the process of the investigation will be changed depending on the type of attack that has been carried out.

4.3.1.2 Network Infrastructure
Questions need to be asked about the Network Set-up of the organisation. The number of assets that are within the network as well as the IP addresses of every machine within the network infrastructure needs to be known, in order to discover the computer assets that were used in the execution of the Insider Network Attack. With this information the Planning Phase will be able to start with the assets that it is believed were involved in the completion of this Attack.

Anson et Al. (2012) provides a number of questions that can be asked at the start of every investigation as a way to discover what is considered to be normal usage within the organisation’s Network Infrastructure, these questions are as follows:
“Do you have employees who log in from remote locations?

Do partner organisations have access to any of your systems?

During what times do your employees normally access the network?

Do remote connections normally last for long periods of time (such as interactive user logons), short periods of times (such as automated transactions or updates), or variable amount of time?

Which systems house sensitive data, and which users should have access to these systems?

Are all of your systems located at this facility, or are you using remote data centers or cloud service providers?” (Anson, 2012, p. 7)

4.3.1.3 Security

The different types of security technologies and policies that are used within the organisation needs to be discovered to establish what information they will be able to provide the investigator in the form of logs and error reports. The Network Forensic Investigator would be able to assess the number of logs that would be available for examination using the information gathered in this sub-phase, by communication with the Information Security personnel within the organisation.

This final sub-phase requires the Investigator to discover the amount of Intrusion Detection Systems and Firewalls that are present within the organisations Network Infrastructure, after this information is discovered then this information can be used when it comes to the Planning phase.
4.3.2 Documentation Phase

The Documentation Phase requires too much information to not include sub-phases, these sub-phases are as follows:

- Chain of Custody
- Investigator Notes

4.3.2.1 Chain of Custody

When it comes to investigating the assets that may have been used during the course of the Insider Network Attack, the assets are imaged if possible to create a bit by bit copy. After this copy is made then the investigators need to create a detailed record which is known as a Chain of Custody of who has access to and analyses the evidence at any point during the investigation. This Chain of Custody is produced to be sure that if the evidence is questioned during legal proceedings, then there would be a log of all of the actions that were carried which may cause any changes within the evidence.

This sub-phase is included as it is a crucial part of evidence forensic investigation not just Digital Forensic Investigations. This is due to the fact that every forensic investigator needs to be able to account for every second of the individual pieces of evidence from the point of acquisition to the legal proceedings.
4.3.2.2 Investigator Notes

Investigator Notes are the findings of the Investigator during the course of the investigation, these notes include the location of all of the evidence that is found and the date and time that they were found.

Investigator Notes are a must within every investigation, especially those that will end up in a court of law, the investigator notes along with the chain of custody are able to provide evidence of the steps taken in order to gather and assess all of the independent pieces of evidence.
4.3.3 Planning Phase

Once the information about the Network Infrastructure within the organisation has been gathered, the investigator needs to be aware of which assets are more vulnerable to the Insider that is suspected of committing the Insider Network Attack, in order to collect and preserve the evidence present on these chosen resources first.

In order to produce a plan for the investigation, the information provided by the organisation and Information Security Personnel needs to be used completely, the volatile nature of the evidence found within Network Forensic Investigations means that the plan needs to ensure that these pieces of evidence are collected with the upmost importance.

With the inclusion and the importance of the volatile evidence that requires investigation within the Network Infrastructure, the rest of the assets then need to be prioritised to review their relevance to the Insider Network Attack that has been committed.

After the potential sources of evidence on the network have been prioritised, the investigator needs to decide which assets are required to be included within the plan. Not all assets within the Network will hold evidence about the Insider Network Attack.
4.3.4 Collection of Evidence Phase

The preceding phase highlights all of the Assets within the organisation that need to be collected in order for any evidence to be found within these chosen assets.

For each type of asset there would be processes that need to be followed, as a way to be sure that the assets within the organisation are collected in a forensically sound manner.

If all of the Assets within the organisation are local then it means that there is only one process to be followed in order to collect the evidence that may reside in the assets. This is to do with the imaging process necessary to ensure the preservation of the complete state of the computer or server at the time that they were discovered by the Network Forensic Investigator.

However if the organisation uses remote servers or cloud providers as part of their day to day business environment, then this adds an extra element into the collection of this evidence as there can be problems when it comes to getting access to the data stored within the cloud environment.

When dealing with an Insider Network Attack Investigation the way in which the evidence is collected needs to be adjusted to reduce the loss of evidence by the perpetrator of the attack. If the Insider who is suspected of committing the attack is still within the organisation or still
has access to the network infrastructure through remote connections, then steps would need to be undertaken to prevent the evidence from being removed, this would be done by temporarily restricting network access and remote connections.

If the malicious insider is unknown within the organisation, then the investigator would have to be more careful when he went about the evidence collection so as not to alert the malicious insider that the attack has been discovered. Evidence that would need to be collected is in the form of event logs, computers and possibly papers which could hold information necessary to uncover evidence during the evidence analysis phase.

The Collection of Evidence phase is split into the following sub-phases:

- Security Considerations
- Collection of Non-technical Items
- Collection of Technical Items

4.3.4.1 Security Considerations
After the Planning of the investigation has been undertaken, certain considerations need to be made as a way to ensure that all of the evidence that is collected is preserved. There are many ways when it comes to the collection of evidence that components of that evidence could be lost due to the possibility of certain procedures not being followed correctly.

4.3.4.2 Collection of Non-Technical Items
Marcella and Menendez (2010) explain the importance of investigators collecting relevant papers surrounding the area of the required computers that are to be collected, there is a need for these papers and documents to be collected as a way to prevent the problem of access when it comes to the analysis of the evidence.

4.3.4.3 Collection of Technical Items
The collection of technical items within the organisation needs to be done in a forensically sound manner in order to ensure that no evidence is lost during the collection of evidence or the transportation of the evidence from the organisation to the Network Forensic Investigators crime lab.
4.3.5 Evidence Analysis Phase

When it comes to the analysis of evidence there are many procedures and processes that need to be followed to be sure that the evidence that is found is admissible within a court of law, there is no point in an investigation taking place and evidence being found if the attacker is not prosecuted or reprimanded if the evidence found has been tainted.

The Evidence Analysis Phase is split into the following sub-phases:

- Preliminary Analysis
- Technical Analysis

4.3.5.1 Preliminary Analysis

Once the evidence has been collected initial analysis needs to be carried out in order to see if there are any reasons or hidden elements to the evidence that would prevent low level analysis from being carried out, with the use of various digital forensic examination tools.

4.3.5.2 Technical Analysis

After the initial analysis of the evidence has been carried out, then the evidence needs to be viewed and analysed in a detailed way using accepted digital forensic tools, such as Encase and Forensic Toolkit.
4.3.6 Review of Findings Phase

- Findings to be reviewed
- Review of Findings Phase
- Decision of Next Stage
- Look over all of the evidence
- Ensure the Investigation Timeline is complete

Figure 9 Review of Findings Phase
The evidence that has been analysed to produce the findings needs to be reviewed. This allows the investigators to look back over the investigation up to this point to decide if there is any more evidence to be found, which was missed or if the findings so far show that there is another area of investigation that is necessary. A timeline is to be produced in order to show how the attack took place and the timescale for the attack. With this in mind the investigators need to ensure that the evidence that has been discovered at this point is the whole story of how the attack took place. If on the other hand the evidence that has been collected and analysed does not yet show how the attack was conducted then the Investigator needs to go back to the collection of evidence phase in order to discover what areas of the network extra evidence could be found. The use of Event Logs within the Windows Operating Systems need to be analysed in order to discover if there are any anomalies that could point to evidence of an Insider trying to hide their attack.

4.3.7 Reporting Phase

*Findings*

- Findings need to be ordered
- Opinions formulated

*Figure 10 Reporting Phase*
During the reporting phase the Network Forensic Investigator needs to look through the findings that were produced throughout the investigation as a whole. This needs to be done to ensure that the findings are shown in a way that clearly shows the course of the attack and how it took place.

The opinions of the investigator need to be clearly defined within the report in order for the management within the organisation or a court of law to be able to understand what the evidence uncovered throughout the investigation shows, or what the investigator believes that the evidence shows.

5 Evaluation of Proposed Digital Forensic Framework

The proposed framework has been built around the fundamental elements required for every digital forensic investigation. These elements also include the requirements given by the Association of Chief Police Officers, which is an added element that will ensure that if those rules are obeyed then the evidence that is gathered will have been collected in a forensically sound manner.

The design of the proposed framework covers all of the key elements that would be needed in order to investigate an Insider Network Attack in order to be sure that the investigators could get the investigation from an organisation to a court of law.

The design of the proposed Digital Forensic Framework for the Investigation of Insider Network Attacks incorporates many of the ideas, which exist in the existing Digital Forensic and Network Forensic Frameworks. The main consideration that was kept in mind during the entire design phase of this framework is the fact that this framework needed to be able to be used to investigate the many different types of Insider Network Attacks.
Since every Insider Network Attack is different, there needs to be an element of flexibility within the proposed framework as certain Insider Network Attacks may require different phases to be included.

5.1 Experiment Using Proposed Digital Forensic Framework

In order to create the experiment two Virtual Machines were created, one with a set-up which included a 20GB hard drive, which is the hard drive size necessary for the Ubuntu 12.04 Operating System. While the other Virtual Machine was created with a set-up which included a 20GB hard drive, which was suitable for the Kali Linux Operating System.

The two operating systems were set up with a Host-Only network connection to ensure that the attack completed was only carried out on the Target Virtual Machine.

The Target Machine has an IP: 192.168.197.129 and

The Attacker Machine has an IP: 192.168.197.131

<table>
<thead>
<tr>
<th></th>
<th>Target Machine</th>
<th>Attacker Machine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Ubuntu 12.04</td>
<td>Kali Linux</td>
</tr>
<tr>
<td>Hard Drive</td>
<td>20 GB</td>
<td>20 GB</td>
</tr>
<tr>
<td>Memory</td>
<td>1 GB</td>
<td>1 GB</td>
</tr>
<tr>
<td>Network Connection</td>
<td>Host-Only</td>
<td>Host-Only</td>
</tr>
<tr>
<td>IP Address</td>
<td>192.168.197.129</td>
<td>192.168.197.131</td>
</tr>
</tbody>
</table>

Table 3 Virtual Machine Configuration

Of the two Virtual Machines one acted as the Attacker and the second the Target.

The Insider Network Attack was executed on the Target Machine using the tools provided within Kali Linux and Armitage.

An Investigation of the Insider Network Attack was carried out using the Proposed Digital Forensic Framework for the Investigation of Insider Network Attacks.

Documentation has been produced, documenting all of the processes used in order to both collect and analyse the evidence. During the course of this investigation snapshots were taken as a way for an analysis to be completed of the evidence and times in which the attacks were attempted against the target machine. Since there was only one investigator during the course of this Investigation there is no chain of custody until the evidence and the analysis is handed over.

The Assessment of Insider Network Attack Status was carried out using information about the machine used during the execution of the attack, which in this case is a local machine within
the network domain. Error logs show that attempted attacks were made on the target machine by a machine on the local network.

Information Gathering was carried out using information provided by the network administrators at the organisation. The network consists of local machines.

The plan of the evidence collection was carried out taking into account the fact that the machine which had been used to unleash attacks against the Target machine needs to be locked down before evidence of the attempted breaches in security can be removed. Also the machine which was targeted and raised the alert needs to be imaged in order to prevent the loss of any information.

Collection of Evidence was carried out following the aforementioned plan. In order to collect and preserve the integrity of the targeted machine, a clone was made. The passwords that were used on the targeted machine were collected by asking the employee for the passwords.

Evidence Analysis is conducted once the computers have been collected and imaged according to Digital Forensic Protocols. The targeted machine was able to be analysed as the password that was necessary could be collected from the employee. The targeted computer is analysed first where the error logs show repeated attempted attacks. Within the error logs was the IP address of the computer responsible for the attempted attacks, this means that the computer with this IP needs to be collected if it was not already done during the initial planning phase. This IP address is 192.168.197.131, the error log that was found can be seen below:
Once the IP address was found within the error logs of the targeted computer, the correct attacker machine could be investigated to find the network attacking tools present within the operating system installed on this machine.

A Review of Findings was undertaken in order to complete an Investigation and Evidence log and timeline to be attached to the final digital forensic report. Within this Investigation the evidence found in the error log in the target machine as well as the capture and clone of the machine responsible for the attempted attacks, shows that all of the evidence that is necessary for the organisation to take action against the party responsible for the attacks.

The Reporting of the details of the attack and the investigation incorporates the documentation created during the investigation as well as the report produced from the chosen Digital Forensic tool used to analyse the evidence found during the course of the investigation. The report that is created during the course of the investigation enables the test organisation to be able to discover the party responsible for the attack.

The experiment showed that the planning phase is necessary as this allows the evidence to be collected in the correct order, as well as ensuring that the information collected about the network infrastructure is correctly assessed in the plan.

Figure 11 Error Log from Targeted Virtual Machines
When it comes to collecting the evidence, there needs to be processes about the ways in which to gather passwords of systems that are used during the course of the Insider Network Attack.

During the course of the Evidence Analysis phase the sub-phases of Initial and Technical analysis, provide the investigator with the processes and information necessary to ensure that no evidence is lost.

5.2 Strengths of Proposed Digital Forensic Framework
The list of questions which need to be considered at the beginning of the Investigation has the ability to be customised for each different Insider Network Attack, so that the correct information is collected and the evidence is looked for in the correct level of priority.

The analysis phase of the Insider Network Forensic Investigation Framework allows the Investigators to be encouraged to repeatedly review the information and the evidence that has been gathered at regular intervals to ensure that the Investigation of the Insider Network Attack is completed in a forensically sound manner.

Following the experiment of the Proposed Digital Forensic Framework, the breakdown of the phases and sub-phases makes the Investigation easier to follow.

5.3 Limitations of Proposed Digital Forensic Framework
Since for Digital Forensic Frameworks to be used within the investigation of cybercrimes, they need to be approved, this would need to be done for the Proposed Digital Forensic Framework to be accepted within the Digital Forensic community.

The limitation of this project is that the Proposed Digital Forensic Framework for the Investigation of Insider Network Attacks is only theoretical and would need to be tested against a test investigation to see if the Framework incorporates all of the Frameworks necessary.

The differing nature of Insider Network Attacks makes the construction of the Proposed Framework more difficult, as the differing Insider Network Attacks all have differing processes to be carried out.

With the lack of existing frameworks specifically for the Investigation of Insider Network Attacks, there is limited research into the necessary components which are needed for a complete Investigation of Insider Network Attacks.
The Proposed Digital Forensic Framework for the Investigation of Insider Network Attacks does not contain any main phases specifically to do with the Preservation of the evidence that will be collected during the course of the investigation.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Assessment of Insider Network Attack Status</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Obtain Information</td>
<td>Information Gathering Phase</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Strategize</td>
<td>Planning Phase</td>
<td></td>
</tr>
<tr>
<td>Preparation and Authorization</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detection of Incident/Crime</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident Response</td>
<td>Collect Evidence</td>
<td>Capture</td>
<td>Collection of Evidence Phase</td>
</tr>
<tr>
<td>Collection of Network Traces</td>
<td>Collect Evidence</td>
<td>Capture</td>
<td>Collection of Evidence Phase</td>
</tr>
<tr>
<td>Protection and Preservation</td>
<td>Copy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preservation</td>
<td>Copy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protection and Preservation</td>
<td>Copy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Examination</td>
<td>Examine</td>
<td>Analysis</td>
<td>Evidence Analysis Phase</td>
</tr>
<tr>
<td>Analysis</td>
<td>Examine</td>
<td>Analysis</td>
<td>Evidence Analysis Phase</td>
</tr>
<tr>
<td>Investigation and Attribution</td>
<td>Investigation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Investigation and Attribution</td>
<td>Investigation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Presentation and Review</td>
<td>Report</td>
<td>Presentation</td>
<td>Review of Findings Phase</td>
</tr>
<tr>
<td>Presentation and Review</td>
<td>Report</td>
<td>Presentation</td>
<td>Review of Findings Phase</td>
</tr>
<tr>
<td>Reporting Phase</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5.4 Comparison of Network Forensic and Proposed Framework

*Table 4 Comparison of Network Forensic and Insider Network Forensic Framework*

6 Conclusion

There are many different Network Attacks which when looked at more closely fit into the category of both Insider and External Network Attacker.

Following the research included in this project it can be seen that the network attacks that are committed by Insider and External Entities are very similar when looked at side by side. There are many types of Network Attacks which are conducted by External forces, however
when looked at further these types of attack can also be carried out by Disgruntled Insiders and most of the time they can be carried out more easily by the Insiders.

The aim of this project was to develop a Digital Forensic Framework which has been created and analysed, for use during the Investigation of cases of the Insider Network Attacks that were defined within the Literature Review.

The analysis of the Proposed Digital Forensic Framework shows that in order for the Framework to be fully proven, the framework would need to undergo complete testing against multiple detailed test cases as a way for the Investigation method to be confirmed as a valid method of Investigation against the different Insider Network Attacks. This is due to the fact that the experiment testing the Proposed Digital Forensic Framework was only on a small scale.

The Proposed Digital Forensic Framework incorporates all of the strengths of the previous Digital Forensic Frameworks and Network Forensic Frameworks. This is done as a way for this newly created framework to have all of the proven phases that are necessary within the Investigation of both Network Attacks and cybercrimes. The added phases are for the differences of investigating internal cybercrimes.

Throughout the course of the project when it came to finding information about the processes necessary to investigate Insider Network Attacks it was difficult as there is not as much information available.

Creating the experiment to test the way in which the Proposed Digital Forensic Framework would be used was difficult as the simulated Insider Network Attack did not work in the expected way. However it did show that even when an attack is not successful there is still evidence of the attempted attacks to be found within the error logs within the system.

By ensuring that the framework flowed in the correct way and all of the phases and sub-phases were connected in the most accurate manner, no evidence is missed when the Digital Forensic Framework is utilised.

6.1 Future Research

More research into the area of Insider Network Attacks and the process that is necessary to investigate Insider Network Attacks, would be necessary for the review and redraft of the Digital Forensic Framework which has been created within this project for the Investigation of Insider Network Attacks.
Once the Proposed Digital Forensic Framework for the Investigation of Insider Network Attack, is followed against test cases as a way to ensure the reliability and validity of the Digital Forensic Framework, this Framework could become an approved methodology for the Investigation of Insider Network Attacks.

References


**Bibliography**


Upper Saddle River: Prentice Hall.


Appendix One – Ethical Approval Form

**Request for ethical approval for students on taught programmes**

Please complete this form and return it to your supervisor as advised in your module handbook. Feedback on your application will be via your supervisor or co-ordinator.

<table>
<thead>
<tr>
<th>Your Name:</th>
<th>Rachel Fairbrother</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student ID:</td>
<td>100157602</td>
</tr>
<tr>
<td>Unimail address:</td>
<td><a href="mailto:R.Fairbrother2@unimail.derby.ac.uk">R.Fairbrother2@unimail.derby.ac.uk</a></td>
</tr>
<tr>
<td>Other contact information</td>
<td>Personal Email: <a href="mailto:rayfairbrother92@gmail.com">rayfairbrother92@gmail.com</a></td>
</tr>
<tr>
<td>Programme name and code</td>
<td>Computer Forensic Investigation (F490)</td>
</tr>
<tr>
<td>Module name and code</td>
<td>Independent Studies (6CC995)</td>
</tr>
<tr>
<td>Name of supervisor</td>
<td>Dr Olga Angelopoulou</td>
</tr>
<tr>
<td>Name of co-ordinator</td>
<td>Jianjun Zhang</td>
</tr>
<tr>
<td>Title of proposed research study</td>
<td>Insiders Network Attack Investigation</td>
</tr>
</tbody>
</table>

**Supervisor Comments**

<table>
<thead>
<tr>
<th>Are the ethical implications of the proposed research adequately described in this application?</th>
<th>Yes ☑</th>
<th>No ☑</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does the overall study have low, moderate or high risk in terms of ethical implications?</td>
<td>Low ☑</td>
<td>Moderate ☑</td>
</tr>
<tr>
<td>High ☑</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the study method describe a process of research that is ethically sound?</td>
<td>Yes ☑</td>
<td>No ☑</td>
</tr>
</tbody>
</table>

**Signatures**

100157602  Insider Network Attack Investigation  Page | 91
The information supplied is, to the best of my knowledge and belief, accurate. I clearly understand my obligations and the rights of the participants. I agree to act at all times in accordance with University of Derby Policy and Code of Practice on Research Ethics:
http://www.derby.ac.uk/research/ethics-and-governance/research-ethics-and-governance

<table>
<thead>
<tr>
<th>Signature of applicant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of submission by applicant</td>
</tr>
<tr>
<td><strong>Signature of supervisor</strong></td>
</tr>
<tr>
<td>Date of signature by supervisor</td>
</tr>
</tbody>
</table>

For Committee Use
Reference Number (Subject area initials/year/ID number)
……………………

Date received .................. Date approved ............... Signed .........................

Comments
1. What is the aim of your study? What are the objectives for your study?

Aim:
To study the different types of Insider Network Attack to formulate a detailed framework to be used to investigate incidents of this type.

Objectives:
Examine current literature to explain the problem and perceived impact of Insider Network Attacks.
Create a Digital Forensic Framework on how to investigate cases of Insider Network Attacks.
Compare and Contrast the existing Digital Forensic Frameworks against the newly designed one.

2. Explain the rationale for this study (refer to relevant research literature in your response).

Network attacks can be carried out from either Inside or Outside of the network, the most common form of network attacks is from an external perpetrator. The following information will look at the research that has already been carried out for Insider Network Attacks by the most trusted individuals within the organisation. This means that no matter how much network security is put in place on the outside, the people who attack the network are the ones that have the authority to change passwords and have access to the most crucial information that if released could destroy the company.

Insider Network Attacks pose a huge risk to the integrity and reputation of organisations all around the world, it is these types of attack that need to be investigated in order to highlight the risk that is involved if an attack of this type is allowed to be executed. Currently there is a lot of research into network security and network attacks from an external point of view, in order to develop a Digital Forensic Framework for network attacks that originate from inside the organisation, there needs to be an understanding about the different types of network attack which can be carried out by the trusted individuals within an organisation. This is due to the need to provide Digital Forensic Investigators with a procedure to follow when it comes to investigating the cases of Insider Network Attacks. Ross provides an invaluable article “Defending the Corporate Crown Jewels from the Dangers that Lurk Within” this article explains the dangers of
Insider Network Attacks to the organisation’s reputation, as well as their ability to conform to confidentiality standards within the Information Technology Industry (Ross. O, 2007).

The different systems and processes that can be used when undertaking Internal Network Attacks, can be seen to have authentication already rolled in, this makes attacks easy to carry out. A protocol that verifies the user’s passwords and checks the encryption level on organisational network is Kerberos (Trost. R, 2009). The many different protocols and standards that are incorporated into a network security system help to protect against external attacks, however the high level employees will already know the encryption details that are used within the company.

Internal Network Attacks can happen from any part of the network, however the main focus when it comes to network security is protecting the network from outsiders, unauthorised users who should never gain access to the network. The reality is that a lot more damage can be done to the company as a whole from an authorised user or disgruntled employee who knows the network and is already authenticated on the network, this situation requires more research. Garfinkel states that “Cybersecurity can be viewed solely as an insider problem. What is needed, say advocates, are systems that prevent authorised users from acting improperly.” (Garfinkel. S. L, 2012, p29). This view is not necessarily an accurate one as an organisation cannot function if all of the network is locked down, the employees need access to the data in order to carry out their day to day jobs. The problem comes when that trust of not having the network completely locked down is exploited and then the company’s image is damaged and needs to be rebuilt.

Internal Network Attacks can be put into two different categories according to Nong, these two categories are User Error and Abuse or Misuse (Nong. Y, 2008).

The reason for developing a digital forensics framework for the investigation of Insider Network Attacks is that there are many different forensic frameworks for the investigation of digital forensics in general and therefore one that focuses on a specific area of Digital Forensic Investigations would provide investigators with more guidance. Chirillo provides useful ideas that must go into the creation of a Digital Forensic Framework, these can be found in his book “Hack Attacks Denied: A Complete Guide to Network Lockdown” (Chirillo. J, 2001).
References


3. Provide an outline of study design and methods.

Introduce the idea of Insider Network Attacks. This will introduce the topic of Insider Network Attack Investigation and explain the current thinking on the state of Insider Network Attacks within the information technology industry.

Examine the current literature and define any key terms. This chapter will look at the current research into the different types of Insider Network Attacks including the precautions that can be taken in order to prevent the occurrence of Insider Network Attacks.

The end of the literature review will explain where my research and ideas fit into the current knowledge and process involved to prevent network attacks from inside the organisations network.

Research the different types of Network Security Attacks occurring from an insider perspective.

Look at case studies, journals, conference proceedings, legal documents and books. This research will follow the descriptive research method so that the different types of Insider Network Attacks can be explained and expanded upon.

Research into the existing Digital Forensic Frameworks. This will include what a Digital Forensic Framework is and see what needs to be done in order to produce such a model.

Assess what needs to be changed to investigate cases of Insider Network Attacks. The research that is carried out about the current Digital Forensic Frameworks will be evaluated to come up with a list of protocols that need to be included in a Digital Forensic Framework to be used to provide a structure to investigate cases where Insider Network Attacks have occurred.

Create a Digital Forensic Framework on how to investigate cases of Insider Network Attacks. The Digital Forensic Framework that is created will incorporate all of the protocols that were assessed in the above section, to have a real impact in investigations.

Evaluate the newly designed Digital Forensic Framework. This step of the study will
follow the Evaluative Research method so that the new Digital Forensic Framework can be assessed against all of the existing Digital Forensic Frameworks to determine whether or not this framework will provide guidance about the procedure to follow when investigating cases of Insider Network Attacks.

4. Research Ethics

PROPOSALS INVOLVING HUMAN PARTICIPANTS MUST ADDRESS QUESTIONS 5 - 11.

Does the proposed study entail ethical considerations  No (please delete as appropriate) If you are unsure please seek advice before submitting this form.

If ‘No’ provide a statement below to support this position.

The proposed study does not entail ethical considerations as the research will be carried out using secondary sources and there will be no involvement of human participants. The research methods that have been chosen will look at secondary sources and evaluating what has been done before.

If ‘Yes’ move on to Question 5.

5. Please provide a detailed description of the study sample, covering selection, sample profile, recruitment and if appropriate, inclusion and exclusion criteria.

6. Are payments or rewards/incentives going to be made to the participants? Yes  
No  

If so, please give details below.
7. Please indicate how you intend to address each of the following ethical considerations in your study. If you consider that they do not relate to your study please say so.

Guidance to completing this section of the form is provided at the end of the document.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>Consent</td>
</tr>
<tr>
<td>b.</td>
<td>Deception</td>
</tr>
<tr>
<td>c.</td>
<td>Debriefing</td>
</tr>
<tr>
<td>d.</td>
<td>Withdrawal from the investigation</td>
</tr>
<tr>
<td>e.</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>f.</td>
<td>Protection of participants</td>
</tr>
<tr>
<td>g.</td>
<td>Observation research</td>
</tr>
<tr>
<td>h.</td>
<td>Giving advice</td>
</tr>
<tr>
<td>i.</td>
<td>Research undertaken in public places</td>
</tr>
<tr>
<td>j.</td>
<td>Data protection</td>
</tr>
<tr>
<td>k.</td>
<td>Animal Rights</td>
</tr>
<tr>
<td>l.</td>
<td>Environmental protection</td>
</tr>
</tbody>
</table>

8. Are there any further ethical implications arising from your proposed research? Yes ☐ No ☐

If your answer was no, please explain why.

9. Have / do you intend to request ethical approval from any other body/organisation? Yes ☐ No ☐

If ‘Yes’ – please give details

10. What resources will you require? (e.g. psychometric scales, IT equipment, specialised software, access to specialist facilities, such as microbiological containment laboratories).

11. What study materials will you use? (Please give full details here of validated scales, bespoke questionnaires, interview schedules, focus group schedules etc and attach all materials to the application)

Which of the following have you appended to this application?
- Focus group questions
- Self-completion questionnaire
- Other debriefing material
- Information sheet about your research study
- Other (please describe)

- Psychometric scales
- Interview questions
- Covering letter for participants
- Informed consent forms for participants

PLEASE SUBMIT THIS APPLICATION WITH ALL APPROPRIATE DOCUMENTATION
Advice on completing the ethical considerations aspects of a programme of research

Consent

Informed consent must be obtained for all participants before they take part in your project. The form should clearly state what they will be doing, drawing attention to anything they could conceivably object to subsequently. It should be in language that the person signing it will understand. It should also state that they can withdraw from the study at any time and the measures you are taking to ensure the confidentiality of data. If children are recruited from schools you will require the permission, depending on the school, of the head teacher, and of parents. Children over 14 years should also sign an individual consent form themselves. If conducting research on children you will normally also require Criminal Records Bureau clearance. You will need to check with the school if they require you to obtain one of these. It is usually necessary if working alone with children, however, some schools may request you have CRB clearance for any type of research you want to conduct within the school. Research to be carried out in any institution (prison, hospital, etc.) will require permission from the appropriate authority.

Covert or Deceptive Research

Research involving any form of deception can be particularly problematical, and you should provide a full explanation of why a covert or deceptive approach is necessary, why there are no acceptable alternative approaches not involving deception, and the scientific justification for deception.

Debriefing

Debriefing is a process of reflection once the research intervention is complete, for example at the end of an interview session. How will participants be debriefed (written or spoken feedback)? If they will not be debriefed, give reasons. Please attach the written debrief or transcript for the oral debrief. This can be particularly important if covert or deceptive research methods are used.

Withdrawal from investigation

Participants should be told explicitly that they are free to leave the study at any time without jeopardy. It is important that you clarify exactly how and when this will be explained to participants. Participants also have the right to withdraw their data in retrospect, after you have received it. You will need to clarify how they will do this and at what point they will not be able to withdraw (i.e. after the data has been analysed and disseminated).

Protection of participants

Are the participants at risk of physical, psychological or emotional harm greater than encountered ordinary life? If yes, describe the nature of the risk and steps taken to minimise it.
Observational research

If observational research is to be conducted without prior consent, please describe the situations in which observations will take place and say how local cultural values and privacy of individuals and/or institutions will be taken into account.

Giving advice

Students should not put themselves in a position of authority from which to provide advice and should in all cases refer participants to suitably qualified and appropriate professionals.
Research in public places

You should pay particular attention to the implications of research undertaken in public places. The impact on the social environment will be a key issue. You must observe the laws of obscenity and public decency. You should also have due regard to religious and cultural sensitivities.

Confidentiality/Data Protection

You must comply with the Data Protection Act and the University’s Good Scientific Practice [link]. This means:

- It is very important that the Participant Information Sheet includes information on what the research is for, who will conduct the research, how the personal information will be used, who will have access to the information and how long the information will be kept for. This is known as a ‘fair processing statement.’
- You must not do anything with the personal information you collect over and above that for which you have consent.
- You can only make audio or visual recordings of participants with their consent (this should be stated on the Participant Information sheet)
- Identifiable personal information should only be conveyed to others within the framework of the act and with the participant’s permission.
- You must store data securely. Consent forms and data should be stored separately and securely.
- You should only collect data that is relevant to the study being undertaken.
- Data may be kept indefinitely providing its sole use is for research purposes and meets the following conditions:
  - The data is not being used to take decisions in respect of any living individual.
  - The data is not being used in any which is, or is likely to, cause damage and/or distress to any living individual.
- You should always protect a participant’s anonymity unless they have given their permission to be identified (if they do so, this should be stated on the Informed Consent Form).
- All data should be returned to participants or destroyed if consent is not given after the fact, or if a participant withdraws.

Animal rights.

Research which might involve the study of animals at the University is not likely to involve intrusive or invasive procedures. However, you should avoid animal suffering of any kind and should ensure that proper animal husbandry practices are followed. You should show respect for animals as fellow sentient beings.

Environmental protection

The negative impacts of your research on the natural environment and animal welfare, must be minimised and must be compliant to current legislation. Your research should...
appropriately weigh longer-term research benefit against short-term environmental harm needed to achieve research goals.
### Appendix Two – Gantt Chart

<table>
<thead>
<tr>
<th>Task Mode</th>
<th>Task Name</th>
<th>Duration</th>
<th>Start Date</th>
<th>Finish Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>Ethical Approval Form</td>
<td>30 days</td>
<td>Mon 23/09/13</td>
<td>Fri 01/11/13</td>
</tr>
<tr>
<td>✓</td>
<td>Project approval with supervisor</td>
<td>11 days</td>
<td>Wed 16/10/13</td>
<td>Wed 30/10/13</td>
</tr>
<tr>
<td>✓</td>
<td>Submit Ethical Approval Form</td>
<td>1 day</td>
<td>Wed 30/10/13</td>
<td>Wed 30/10/13</td>
</tr>
<tr>
<td>✓</td>
<td>Literature Review</td>
<td>69 days</td>
<td>Fri 01/11/13</td>
<td>Wed 05/02/14</td>
</tr>
<tr>
<td>✓</td>
<td>Research Insider Network Attacks</td>
<td>48 days</td>
<td>Fri 01/11/13</td>
<td>Tue 07/01/14</td>
</tr>
<tr>
<td>✓</td>
<td>Write Literature Review Draft</td>
<td>11 days</td>
<td>Wed 08/01/14</td>
<td>Wed 22/01/14</td>
</tr>
<tr>
<td>✓</td>
<td>Literature Review (Review)</td>
<td>9 days</td>
<td>Fri 24/01/14</td>
<td>Wed 05/02/14</td>
</tr>
<tr>
<td>✓</td>
<td>Framework Design</td>
<td>30 days</td>
<td>Thu 06/02/14</td>
<td>Wed 19/03/14</td>
</tr>
<tr>
<td>✓</td>
<td>Draw up table of components of framework</td>
<td>3 days</td>
<td>Thu 06/02/14</td>
<td>Mon 10/02/14</td>
</tr>
<tr>
<td>✓</td>
<td>Model Framework Design</td>
<td>3 days</td>
<td>Tue 11/02/14</td>
<td>Thu 13/02/14</td>
</tr>
<tr>
<td>✓</td>
<td>Framework Explanation</td>
<td>3 days</td>
<td>Fri 14/02/14</td>
<td>Tue 18/02/14</td>
</tr>
<tr>
<td>✓</td>
<td>Evaluation Planning</td>
<td>2 days</td>
<td>Thu 06/02/14</td>
<td>Fri 07/02/14</td>
</tr>
<tr>
<td>✓</td>
<td>Evaluation</td>
<td>17 days</td>
<td>Thu 20/03/14</td>
<td>Fri 11/04/14</td>
</tr>
<tr>
<td>✓</td>
<td>Conclusion</td>
<td>3 days</td>
<td>Thu 20/03/14</td>
<td>Mon 24/03/14</td>
</tr>
<tr>
<td>✓</td>
<td>Abstract</td>
<td>3 days</td>
<td>Tue 25/03/14</td>
<td>Thu 27/03/14</td>
</tr>
<tr>
<td>✓</td>
<td>Proof Reading of Dissertation</td>
<td>12 days</td>
<td>Wed 26/03/14</td>
<td>Thu 10/04/14</td>
</tr>
<tr>
<td>✓</td>
<td>Submit Independent Study</td>
<td>1 day</td>
<td>Fri 11/04/14</td>
<td>Fri 11/04/14</td>
</tr>
</tbody>
</table>
Appendix Three – Record of Supervisor Meetings

09/10/13: Discussion of Initial Project Idea

Rachel Fairbrother
Mon 09/10/2013 13:15
Sent Item

To: Olga Angelopoulou <o.angelopoulou@derby.ac.uk>

Hi Olga,

That would be great, I will make sure to have a copy of my plan with me.

Many Thanks,
Rachel

Olga Angelopoulou <o.angelopoulou@derby.ac.uk>
Mon 09/10/2013 11:48

Hi Rachel,

Wednesday at 10:30 then. Could you please also bring a copy of the plan with you?

Regards,

Dr Olga Angelopoulou
Lecturer, Programme leader MSc Computer Forensic Investigation University of Derby Faculty of Business, Computing and Law School of Computing and Mathematics
ES10
Tel. 01332591827

16/10/13: Discuss Ethical Approval Form

Rachel Fairbrother
Mon 16/10/2013 14:04
Sent Item

To: Olga Angelopoulou <o.angelopoulou@derby.ac.uk>

Hi Olga,

That would be great, thank you.

Many Thanks,
Rachel

Olga Angelopoulou <o.angelopoulou@derby.ac.uk>
Mon 16/10/2013 13:07

Hi Rachel,

I could meet you at 11:30 on Wednesday.

Regards,

Dr Olga Angelopoulou
Lecturer, Programme leader MSc Computer Forensic Investigation University of Derby Faculty of Business, Computing and Law School of Computing and Mathematics
ES10
Tel. 01332591827

23/10/13: Email Communication about ethical approval form

Rachel Fairbrother
Insider Network Attack Investigation
Rachel Fairbrother

Wed 30/10/2013 11:09
Sent Items

To: Olga Angelopoulou <o.angelopoulou@derby.ac.uk>
Hi Olga,

I have had a look at several examples of project aims, including the one outlined on your proposal and I am still unsure how to develop my aim further.

Any advice you could give me would be greatly appreciated.

Many thanks
Rachel

Olga Angelopoulou <o.angelopoulou@derby.ac.uk>

Wed 30/10/2013 12:49

Hi Rachel,

Please work on the aim of your project, as this is outlined on my proposal. Other than that your proposal is good.

Regards,

---------------------------------------------
Dr Olga Angelopoulou
Lecturer, Programme Leader MSc Computer Forensic Investigation
University of Derby
Faculty of Business, Computing and Law
School of Computing and Mathematics
ES10
Tel: 01332591827

Olga Angelopoulou <o.angelopoulou@derby.ac.uk>

Wed 30/10/2013 14:52

Hi Rachel,

The aim is not to critically assess existing frameworks, but to study insider attacks and develop a framework for their investigation. Whether existing frameworks are incapable to accommodate the investigation of insider attacks or not is something you will assess as part of your M. Review.

Regards,

Dr Olga Angelopoulou
Programme leader MSc Computer Forensic Investigation
University of Derby
Faculty of Business, Computing and Law
School of Computing and Mathematics
ES10
Tel: 01332591827

Rachel Fairbrother

Wed 30/10/2013 14:50
Sent Items

To: Olga Angelopoulou <o.angelopoulou@derby.ac.uk>
Hi Olga,

Since my last email I have been reconsidering my aim as follows,

"To critically assess the existing Digital Forensic Frameworks while discussing the different types of Insider Network Attacks therefore formulating a common framework for investigating incidents of this type."

Is this way better, if not could you please advise me on where I am going wrong?

Many Thanks
Rachel

30/10/13: Signed and Submitted Ethical Approval From

Rachel Fairbrother Insider Network Attack Investigation
06/11/13: Discussion about structure of first three chapters of the independent study

Olga Angelopoulou <o.angelopoulou@derby.ac.uk>

Hi Rachel,

Wednesday at 11:30

Regards,

Dr Olga Angelopoulou
Lecturer, Programme leader MSc Computer Forensic Investigation
University of Derby
Faculty of Business, Computing and Law
School of Computing and Mathematics
ES10
Tel. 01332591827

http://about.me/oangelopoulou

Rachel Fairbrother
Mon 04/11/2013 13:26
Sent Items

To: o.angelopoulou@derby.ac.uk

Hi Olga,

Would it be possible to have a meeting this week?

Many Thanks
Rachel

20/11/13: Project Plan Created and printed for feedback
Hi Olga,

That would be great thanks.

Many Thanks
Rachel

Hi Rachel,

Tomorrow at 15:30 then?

Regards,

Dr Olga Angelopoulou
Lecturer, Programme leader MSc Computer Forensic Investigation
University of Derby
Faculty of Business, Computing and Law
School of Computing and Mathematics
ES10
Tel. 01332591827
22/01/14: Discussion and review of work that has been completed. Completion of first draft of the literature review set along with an idea for the first draft of the framework design.

Rachel Fairbrother

Insider Network Attack Investigation
Olga Angelopoulou <o.angelopoulou@derby.ac.uk>

Mon 20/01/2014 13:13

Hi Rachel,

I could see you on Wednesday at 13:00

Regards,

Dr Olga Angelopoulou
Lecturer, Programme Leader MSc Computer Forensic Investigation
University of Derby
Faculty of Business, Computing and Law
School of Computing and Mathematics
ED10
Tel. 01332591827

http://about.me/oangelopoulou

Rachel Fairbrother
Fri 17/01/2014 15:15
Sent 15:15

To: olga.angelopoulou@derby.ac.uk

Hi Olga,

Would it be possible for me to have a meeting with you next week?

Many Thanks
Rachel Fairbrother

10/02/14: Discussion and review of work that has been completed. Complete first draft of Literature Review reviewed.
06/03/14: Discussion and review of the work that has been completed up until this point, information about the extra information that needs to be included in the Dissertation Project.
Hi Rachel,

we can have a meeting on Thursday at 10:30.

Best regards,

Dr Olga Angelopoulou
Lecturer, Programme leader MSc Computer Forensic Investigation
University of Derby
Faculty of Business, Computing and Law
School of Computing and Mathematics
Tel: 01332591827
http://about.me/angelopoulou

Hi Olga,

I wondered if you would be able to take a look at the work that I have done so far on my dissertation as a whole.

Would it be possible to have a meeting with you this Thursday 6th March in order to discuss the attached work?

Many Thanks
Rachel Fairbrother

24/03/14: Discussion of draft dissertation, discussed the use of an experiment to better evaluate the Digital Forensic Framework.

Hi Olga,

I can meet tomorrow 25th March at 14:00

Many Thanks
Rachel

Hi Rachel,

It was a mistake from my side. I teach on Monday mornings. I only realised you asked me to meet on Monday, while on my calendar I had booked you in for last Thursday and I thought you just didn't show up.

We can rearrange for Tuesday at 14:00 or Thursday at 11:00.

Best regards,
Olga

Dr Olga Angelopoulou
Lecturer, Programme leader MSc Computer Forensic Investigation
University of Derby
Faculty of Business, Computing and Law
School of Computing and Mathematics
Tel: 01332591827
Appendix Four – Low Level Digital Forensic Framework Design