Edith Cowan University

Research Online

Theses : Honours Theses

2010

Remote access forensics for VNC and RDP on Windows platform

Paresh Kerai
Edith Cowan University

Follow this and additional works at: https://ro.ecu.edu.au/theses_hons

Part of the Computer Sciences Commons

Recommended Citation

Kerai, P. (2010). *Remote access forensics for VNC and RDP on Windows platform*. Edith Cowan University. https://ro.ecu.edu.au/theses_hons/8

This Thesis is posted at Research Online.
https://ro.ecu.edu.au/theses_hons/8

Edith Cowan University

Copyright Warning

You may print or download ONE copy of this document for the purpose of your own research or study.

The University does not authorize you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site.

You are reminded of the following:

- Copyright owners are entitled to take legal action against persons who infringe their copyright.
- A reproduction of material that is protected by copyright may be a copyright infringement.
- A court may impose penalties and award damages in relation to offences and infringements relating to copyright material. Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.

REMOTE ACCESS FORENSICS FOR VNC AND RDP ON WINDOWS PLATFORM

By

Paresh Kerai

This thesis is presented in fulfilment of the requirements for the degree of Bachelor of Computer Science Honours

Faculty of Computing, Health and Science

School of Computer and Security Science

Edith Cowan University

Perth, Western Australia

November 2010

Supervisor: Professor Craig Valli

USE OF THESIS

The Use of Thesis statement is not included in this version of the thesis.

DECLARATION

I certify that this thesis does not, to the best of my knowledge and belief:

1) Incorporate without acknowledgement any material previously submitted for a degree or diploma in any institution of higher education;
2) Contain any material previously published or written by another person except where due reference is made in text; or
3) Contain any defamatory material.

Signed: keraiparesh Date: 26/11/2011

Paresh Lalji Kerai

ACKNOWLEDGEMENT

I would like to take this opportunity to thank my dissertation supervisor Professor Craig Valli for his continuous and unlimited help and support. He has always been there to guide me with the research and with layout of this thesis.

I would also like to express my gratitude towards the School of Computer and Security Science lecturers who assisted me with advice and guiding with this thesis during research meetings conducted weekly.

I am grateful for all the financial support and help received from my Dad Mr Lalji Patel. I would also like to express many thanks to my family for the motivation and support that I received during my Honours year.

ABSTRACT

There has been a greater implementation of remote access technologies in recent years. Many organisations are adapting remote technologies such as Virtual Network Computing (VNC) and remote desktop (RDP) applications as customer support application. They use these applications to remotely configure computers and solve computer and network issues of the client on spot. Therefore, the system administrator or the desktop technician does not have to sit on the client computer physically to solve a computer issue.

This increase in adaptation of remote applications is of interest to forensic investigators; this is because illegal activities can be performed over the connection. The research will investigate whether remote protocols and applications do produce and leave valuable artefacts behind on Windows systems. The research aim to determine and retrieve any artefacts left behind remote protocols and applications in a forensic manner. Particular remote applications are selected to perform the research on and initial analysis will be performed on the applications to evaluate the potential forensic artefacts present on the computer system. The research will focus on Windows XP service packs 1, 2 & 3 for analysis of the remote applications and find out what artefacts if any are left behind these systems.

Table of Contents

List of Figures

List of Tables

GLOSSARY

Computer Forensics – this is the process or application of specialised annalistic and investigative techniques to find and identify, extract, examine, document and preserve information from computer system or network so that it may serve as evidence in court of law (Russell, 2006).

Denial of Service attack (DoS) – Denial of service attack is an attack by hacker or malicious program on a computer network that is designed to prevent legitimate users of the service from gaining access to the network (Rita, 2003).

DES – Data Encryption Standard (DES) is block cipher encryption algorithm that encrypts data in blocks of 64 bits each (Kahate, 2003).

Encryption – this is a process of converting readable data or information into cipher or unreadable form (Whitman & Mattord, 2005).

Firewall – A firewall is a software application or hardware device that protects the computer network from internet intrusions. Firewall also controls traffic between two or more computer networks for security reasons (Mayur, Thomas, & Thomas von der, 2002).

Hacker – this is a person who writes malicious programs and also performs malicious activity on any computer network, whether it be accessing database without permission or cracking passwords of networks or users (Basta & Halton, 2008).

Internet – this is a worldwide network that has many different networks that connect many computer systems and users to interact with each other, by sending and receiving emails, logon to remote computers and also browse web site databases (Nguyen, 2004).

Man-in-middle attack – This type of attack is where the hacker intercepts data transmission between the source and the destination of the communication transmission. Therefore the attacker can read, modify, and insert messages between the communications, without the person knowing (Sud & Edelman, 2004).

OSI Model – The Open System Interconnection (OSI) model is the base for the entire communications that takes place between the network devices and computers. The model consists of seven layers of communication (Ciccarelli & Faulkner, 2004).

Remote Desktop Protocol (RDP) – RDP is a protocol in presentation layer that allows a Windows based terminal or other Windows client to communicate with a Windows XP professional computer system (MicrosoftSupport, 2007).

Remote Frame Buffer (RBF) – which is a simple protocol used by the system for remote access to graphical user interface (Tristan, Quentin, Kenneth, & Andy, 1998).

Secure Shell Layer (SSL) – SSL is a protection layer that is between the TCP/IP protocol and application layer. SSL adds security features to the stream such as authentication of the server, authentication of the client, data confidentiality and data integrity (Garfinkel & Spafford, 2002) .

Security Vulnerability – security vulnerability is flaws or exploits that can be attacked by hackers or malicious programs to gain access to the system or even corrupt the system or networks.

TCP/IP – The Transmission Control Protocol and Internet Protocol is a connection oriented and end to end dependable protocols. These are set of protocols, the primary communication for all internet traffic ("About TCP/IP," 1995).

Virtual Network Computing (VNC) – VNC and enables users to remotely access centralised resources and computer systems from various devices (Wannous, Member, IEEE, & Nakano, 2010).

Virtual Private Network – A VPN is a secure tunnel from the user’s computer to the end user’s access point or organisations wireless device, where the user log’s in to the network using the username and password set on the network (Ciampa, 2005).

Windows Registry – Windows registry is a hierarchical database of configuration values of hardware and software configuration information stored in proprietary file format (Steel, 2006) (Casey, 2002). The registry contains five hives and under each hive is the list of keys and all the keys contain multiple values pairs and sub keys (Steel, 2006)

1.0 INTRODUCTION

1.1 Background of Study

Mobile computing is becoming a more common practise, which means the ability to remotely connect to networks is growing too (LaRose, 2010). To accomplish this, the right combination of equipment, protocols and applications are required.

The ability to access files, information and data from your work computer over the internet from home is useful and productive for many organisations and there are, several remote access technologies that are available to enable this (Mike, 2007). Ideally, you can access the entire working environment over the network from wherever you are outside the office; this eliminates the need for synchronising files between the computers and laptops (Mike, 2007).

The current remote desktop software available does have some downsides. Firstly that the current remote access technologies does not allow for total control of a remote computer, and secondly that the computing experience will be slower than it would be if the person was seated next to the computer (Mike, 2007).

The increasing use of remote connectivity applications such as virtual networking communication (VNC) introduces threats to organisations and governments as illegal activities can be performed remotely on a system or network. Computer forensics analysis of these protocols and supporting applications may provide valuable collateral evidence to investigators.

Computer forensics is the procedure that involves " extraction, preservation, identification, documentation and interpretation of computer data" (Kruse & Heiser, 2002). The information and data obtained from the computer system is then analysed for use as evidence in civil, criminal or administrative cases in a court of law (Nelson, Phillips, & Steuart, 2010).

Possible artefacts and information that can be found from remote access include: the internet protocol (IP) address of the server or of the client the computer connected to, the password used for the connection between the two machines, connection times from the log and also the settings used on the remote applications by the user.

The scope of this research is to examine the virtual network computing applications and remote desktop protocols on Windows XP system and to track any artefacts left behind by the application for forensic purposes. There are several remote applications computer users can install in order to use remote access services. Remote access servers, such as virtual private network (VPN) and modem servers can also be used to access the network remotely. However for the purpose of this research, the following applications: Microsoft RDP, Real VNC, Ultra VNC, Tight VNC and Team Viewer will be used. Forensic analysis will be applied to analyse the VNC and RDP applications for any residual artefacts left behind. Since the remote access applications mentioned above are freeware, it is possible for any user to download and use them for remote connectivity. The report will focus primarily on the analysis of the Windows registry and the file system on Windows XP.

1.2 Purpose of Study

This research will contribute to the body of knowledge for digital forensics and, in particular, remote access forensics. As previously explained the research will test the operating and file systems to find any artefacts left by remote access to a remote network. The outcome of this research will aid police and law agencies in fighting computer related crime. It will also help professional security analysts to perform forensic analysis for organisations.

The outcome of the analysis will state whether a computer had been connected to an outside network and if so, what type of information sent to the network can be identified. Hence this evidence should help law enforcement agencies fight cyber crime.

1.3 Research Questions

The study is designed to answer the following questions;

1) Does the use of remote access protocols on a Windows platform PC produce artefacts?

    1.1. If remote access protocols produce any artefacts on a Windows platform PC, then what types of artefacts are produced?

2) Can a forensic process be developed for the extraction of remote access protocol artefacts from a device using VNC and RDP clients and servers?

2.0 LITERATURE REVIEW

2.1 Remote Access

Remote access is used to allow users to view and fully interact with information or data from one computer to another. Remote access simply uses a RemoteFrameBuffer (RFB) protocol over a TCP/IP connection. Many organisations and individuals use this protocol to monitor and troubleshoot remote computers and systems.

Remote access can be exploited by criminals and internet fraudsters to perform illegal activities and commit crime over the internet. Hackers and criminals can use this technology to perform crime from a remote location, this makes it harder to trace the crime as hackers are not using their computers to perform the acts, instead they use a remote computer that does not belong to them (Remote PC Access, 2009).

In September 2010 Watchguard technologies did a survey on *IT security manager priorities for 2011*, and found that 48 percent of IT security managers will focus more on stipulation of remote access security as their top priority in 2011 (Watchguard, 2010). The survey highlighted the need for secure remote access for the organisation employees as top security priority (Watchguard, 2010).

Hackers target small organisations that have less security measures in place to get control over the large network of the organisation. They can use a computer to perform illegal activities such as sending spam messages, which is illegal in America, or even downloading and browsing child porn images. Child pornography is illegal not only in Australia but throughout the world and consequently tough laws has been put in place to prevent it. According to the Australian Institute of Criminology in 2010, there has been a recent increase in access to, and distribution of, child pornography (Horsfall, 2010). These criminals can potentially use remote access technologies to view, spread pornography, sending pictures and videos between computers while reducing evidence in their computer.

In June 2008 the German Interior Ministry announced plans and new laws to fight cyber crime. Laws, such as those allowing police to conduct “remote searches of computer hard drives” using forensic software or rootkits, which are secretly placed on computers to monitor the traffic have been introduced (Bunyan, 2009). However the law was passed with strict conditions and such laws would only be used with cases of terrorist threats (Bunyan, 2009).

However it is problematic for the authorities and ISPs to monitor remote sessions; this is because ISPs only have the ability to track and monitor the traffic of their clients, while tracking and monitoring the service of the other party is not possible as they may be using different service providers. This creates challenge for law enforcement authorities and ISPs (Remote PC Access, 2009).

Not only hackers can gain remote access to a computer through VNC and RDP protocols, they are also able to exploit system vulnerabilities to gain administrative access to the systems remotely and install a backdoor for subsequent access to the network. This makes remote access technologies more important for organisations and governments as information or data can be exploited and misused (Remote PC Access, 2009).

2.2 Computer Forensics

Computer forensics is the process of obtaining, identifying, extracting, analysing, and documenting of computer evidence stored as data/digital/magnetically encoded information for use as evidence in civil, administrative and criminal cases. (Nelson et al., 2006); (Vacca, 2005). Forensic techniques are commonly used by many law enforcement organisations to bring criminals to justice. However, computer forensics need to be followed in a defined procedure; a handbook published by Standards Australia is currently used as a guide on how to carry and manage electronic evidence (HB171, 2003).

2.2.1 Computer Forensics Procedure

It is important to follow the procedure when performing an acquisition of the evidence in the crime scene and later following to perform the investigation in a forensically sound manner (Hannay, 2007). This is because the nature of the evidence shown to the court of law is intangible and volatile.

Basic methodology that is used to perform forensic investigation includes;

- Acquiring the evidence on the crime scene, without altering or damaging the evidence or causing minimal change to original evidence.
- Authenticating that the acquired evidence is the same as the original seized device or evidence; this can be done by chain of custody or document and obtaining photos as a proof.
- Finally analysing the acquired evidence or device without modifying or damaging it. (Kruse & Heiser, 2002).

Brown, (2006) has identified four major phases of a digital crime scene investigation these are collection, preservation, analysing and presentation, which will be explained bellow;

Collection

This is when the artefacts are considered as evidentiary value and collected. Normally these artefacts are stored in digital medium and data such as floppy drives, CD drives, hard drives, flash disks and other forms of digital media.

It is very crucial for an investigator to handle evidence in a systematic order when collecting evidence at the crime scene. If the evidence is damaged or lost then all the work done on the devices would be negligible, as the court will decline it as evidence because of inadequacies in the process (Kruse & Heiser, 2002).

The collection process is usually complex, depending on the nature of the crime scene; therefore for best practice it is necessary to collect everything possible evidence from the scene for any future reference. This is because the crime scene and any evidence left may be tampered with or cleaned (Kruse & Heiser, 2002).

Preservation

This phase focuses on preserving original artefacts that are reliable, accurate, complete and provable. The key components of this stage include cryptography hashing, checksums and documentation of the artefacts (Brown, 2006).

Chain of custody is the solution to maintain the integrity of the evidence. It is a simple process, yet the most important and effective process of documentation of the investigation of the evidence (Kruse & Heiser, 2002). Answers to the following questions need to be addressed in the chain of custody;

- Who collected the evidence?
- How and where was the evidence collected?
- Who took authority over the evidence?
- How was the evidence stored and protected in storage?
- Who took the evidence from the storage and why?

Transportation and storage is factor upon which investigators tend to concentrate less. If the devices collected as evidence are not handled gently, then they might get damaged. Static-free packaging should be used, depending on the nature of the evidence. After the evidence is transported to the forensic laboratories, storage of the evidentiary device is also crucial. The evidence could be stolen or damaged; therefore locking the original evidentiary device in a safe and secured place is advised. It is also necessary to keep it away from direct sunlight and wet areas to prevent damage to it (Kruse & Heiser, 2002).

Analysing/ Filtering

This is the stage in which the forensic investigator will perform an analysis on the seized evidence to find artefacts and filter out data which is not relevant to the case and filter in artefacts of potential evidentiary value. Typically the analysis on the evidentiary device is performed using forensic tools, applications and techniques used to recover particular artefacts on the device or recover specific data in order to support the investigation (Hannay, 2007).

Presentation

This is the final stage of the forensic investigation where the artefacts of potential evidentiary value are presented to a court of law in a variety of forms (Brown, 2006). The main focus for the investigator is to present the potential evidence to the court of law with the aim of convincing the jury, judge or other legal bodies (Hannay, 2007).

2.2.2 Computer Forensics Guidelines

In order to perform forensic on digital evidence or any related evidentiary device, investigators need to focus on the procedure and documentation needed regarding the handling of the evidentiary device (Hannay, 2007).

The HB171handbook (HB171, 2003) is a guideline for management of IT evidence showing all the steps required to handle evidence effectively, and to guarantee the use of this artefact in a court of law for prosecution. The most important step, and key to any investigation of digital evidence, is to document and record everything and to hash all the files and images to maintain their integrity.

The handbook has identified a six stage lifecycle for the management of IT evidence. Not all the stages are relevant to the research as the proposed research is not focusing on the acquisition and analysis of real evidentiary devices, (HB171, 2003).

The first stage focuses on the design for evidence. This stage identifies five objectives when designing a computer system. The objectives include: ensuring that the evidentiary device is available and useable, identifying the author of the electronic records, producing time and date of the creation and alteration of the electronic record, establishing the authenticity of the record, and establishing the reliability of the programs used for the design (HB171, 2003).

The second stage includes producing records of the evidentiary device. This is the operations stage and the objective is to establish that a particular computer program produced an accurate electronic record including the authors name and time and date created and altered (HB171, 2003).

The third stage defines the process of collection of evidence from an evidentiary device. The main objective of this stage is to find and locate all relevant potential artefacts on the device and secure the original, so that the original is not altered or modified. Collecting evidence sounds easy but it is a challenge for investigators, as they have to be always careful not alter the original electronic record (HB171, 2003).

The fourth stage is to analyse the collected evidentiary value or device for any relating artefacts as per the conviction. Analysis must be performed using a copy of the evidence making sure that the copy is the exact of the original. The investigators filter through the evidence for any data or information that relates to the case, and record the results for further analysis. Hashing of the files and documents obtained during the analysis is very important and needs to be carried out for integrity purposes (HB171, 2003).

Stage five is reporting and presenting the results of the analysis. The objective of this stage is to convince decision-makers of the validity of the results and the view deduced from the evidence (HB171, 2003).

The final stage is determining and assessing evidentiary weight. Assessment of the evidentiary weight is done in all the stages; this is done by investigators or stakeholders. However, the final assessment is performed by the judge or magistrate or any senior management personnel who make a decision after analysing the results and reports created in the previous forensic stages. Probative value and rule of evidence is used to measure the evidentiary weighting of the evidentiary device. "Proactive value is the electronic record relevant and has authorship, authenticity, correct operation and reliability been established"

(HB171, 2003). The rules of evidence state whether the evidentiary device or record have been collected and handled correctly.

All the actions and procedures followed during the investigation and analysis phases need to be documented so that the process can be repeated if required for corroboration of the results (Hannay, 2007).

2.3 OSI Layer Model

To understand how the RFB and RDP protocols work, it is important to understand the way the Open System Interconnection (OSI) model works between two network connections. The OSI model was originally developed by International Organisation for Standardisation in 1983 (Backfield & Bambenek, 2008). The objective of the model is to provide communication between the seven layers over the network. Each layer in the model performs particular functions to support other layers both above and below it (Simoneau, 2006).

The OSI model is developed in such a way that it divides all the tasks required to move information between networked computers. The model divides these tasks into seven different logical layers of communication. Each layer is self-packed responsibly, so that all the tasks are allocated to each layer and can be implemented independently. The layered approach offers advantages such as separating network functions into smaller logical pieces and also helps solve network problems through a divide-and-conquer methodology (Miller, 2001). Following are the seven layers that make up the OSI model (Cisco, 2010):

Layer 7	Application
Layer 6	Presentation
Layer 5	Session
Layer 4	Transport
Layer 3	Network
Layer 2	Data Link
Layer 1	Physical

Table 1 OSI seven layers

Application Layer

This layer provides sets of interfaces for applications to obtain access to network and interact with network services directly (Miller, 2001). The layer also provides security checking and information validation for applications and programs (Miller, 2001). File Transfer Protocol, Web browser, Hypertext Transfer Protocol (HTTP), Common Management Information Protocol (CMIP), Directory Services (DC), Virtual Terminal (VT) and email services operate at the application layer (Miller, 2001).

Presentation Layer

The primary objective is to provide a range of coding and conversion functions during network communication that are applied to application layer data (Cisco, 2010). The presentation layer makes it possible for computers on the network which have different representation to correspond. The layer also provides common communication services such as encryption, text compression, content translation, graphics formatting and cryptography for authentication and privacy of the information (Miller, 2001).

Session Layer

This layer allows two connections to hold communications between the sessions as long as the connection lasts. The session layer is responsible and handles the session setup and data exchanges between two hosts and later deletes when the session ends. The layer also allows the user to log in to a remote time-sharing system or transfer file between two computers. The session layer provides synchronisation service (Miller, 2001).

Transport Layer

The simple function of the transport layer is to accept information from the session layer then to segment the information into tiny pieces and later pass it to the network layer. The transport layer also ensures that the bits delivered to the network layer are the same as original and has not been tampered with during the process (Miller, 2001). If for some reason, an error occurs in the communication, the transport layer corrects it with set of rules. The transport layer identifies two protocols; Transport Control Protocol (TCP) which is connection oriented and User Datagram Protocol (UDP) which is connectionless.

Network Layer

The network layer basically controls the operation of routing the data and information from source host to destination host. Routers work on this layer and Internet Protocol (IP) exists in this layer. The network layer helps to control data congestion on the network and prevent bottlenecks. The layer is also responsible for assigning logical addresses to data packets (Miller, 2001).

Data Link Layer

This layer is responsible for taking the raw data transmission and transforms it to a line which appears to be free of errors for network layer. The layer completes this process by having the sender of the data break down into data frames and, later transmits the frames in sequence. The protocol in this layer packages the data into frames, each frame also contain source and destination addresses. Ethernet, ARC net and Token Ring are examples of LAN data link protocols. The layer uses Media Access Control (MAC) address to move the data and information between the network end points. The layer is also capable of encryption and is used to protect the data transmission between two network end points (Miller, 2001).

Physical Layer

This layer is mainly concerned with transmitting raw data over a communication link channel (Miller, 2001). Network Interface Cards (NIC) and the interfaces of the routers work at this level (Briscoe, 2000). The layer also specifies and defines characteristics such as voltage levels, maximum transmission distances, physical data rate and physical connectors. The layers implementations can be grouped with LAN or WAN specifications (Cisco, 2010).

2.3.1 Internet Protocol

Internet Protocol (IP) is a Network layer 3 protocol; the protocol contains addressing information that enables packets and data to be routed. The IP protocol provides the basic unit of data used for data transfer throughout the TCP/IP internet and also performs the forwarding function, where it chooses the path along which packets will be sent. Since the current version of the protocol is version 4 is usually used as IPv4. TCP/IP is the default protocol for network communications and IPv4 is used for broadcasting of packets and information over the internet (Comer, 2006). Figure below shows the format of an Internet datagram;

<table>
<tr><td>Version</td><td>Header Length</td><td>Type of Service</td><td>Total Length</td></tr>
<tr><td colspan="2">Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td>Time to Live</td><td>Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="4">Source IP Address</td></tr>
<tr><td colspan="4">Destination IP Address</td></tr>
<tr><td colspan="3">IP Options (If Any)</td><td>Padding</td></tr>
<tr><td colspan="4">DATA</td></tr>
</table>

Figure 1 IP Datagram Format

(Comer, 2006)

The table below describes briefly the attributes of the IP datagram:

Field Name	Size (bytes)	Description
Version	½ byte	Identifies the version of the IP used to generate the header.
IHL	½ byte	This states the length of the IP header in 32-bit.
TOS	1 byte	This provides the reliability and quality of service to the packets.
Total Length	2 bytes	Specifies the total length of the IP packet in bytes.
Identification	2 bytes	This is 16-bit value to identify the packet. This is used by recipient to reconstruct messages without inadvertently mixing fragments from different messages.
Flags	3/8 bytes	Used to control packet fragmentation.
Fragment offset	13 bits	Specifies the offset, and position of the overall message.
Time To Live	1 byte	States on how long the data is permitted to live on the network.
Protocol	1 byte	Indicates what type of protocol is carried on the datagram.
Header Checksum	2 bytes	Provides protection against corruption in transmission of the packet. If the header is corrupted it rejects them.
Source Address	4 bytes	32-bit IP address of the source host.
Destination Address	4 bytes	32-bit IP address of the proposed recipient of the datagram
Options	Variable	Several options can be used after the standard header of certain IP packets.
Padding	Variable	
Data	Variable	Data transmitted in the IP datagram.

Table 2 Attributes of IP datagram

(Kozierok, 2005)

2.3.2 TCP/IP Protocol

TCP is a connection-oriented protocol that offers services with error recovery, sequencing and sliding window mechanism. Because of the flexibility and reliability, TCP is the most preferred transport method for applications. A virtual connection is created by the TCP hosts with each other using the handshake process. During the handshake process the TCP hosts exchange a sequence number that is used to track the information and data as its transferred from one host to another (Chappell & Tittel, 2007). The diagram below explains the data segmentation using different headers:

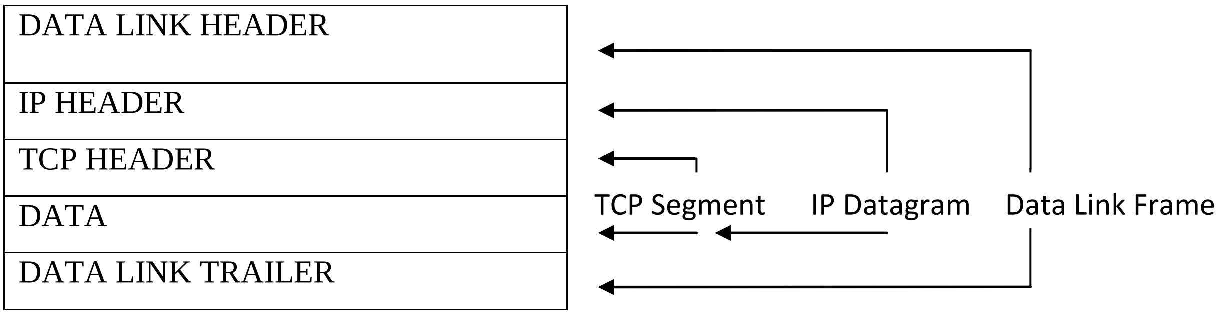


Figure 2 IP datagram segmentation

(Chappell & Tittel, 2007)

The figure shows TCP segment format:

<table>
<tr><td colspan="6">Source Port</td><td colspan="6">Destination Port</td></tr>
<tr><td colspan="12">Sequence Number</td></tr>
<tr><td colspan="12">Acknowledgement Number</td></tr>
<tr><td colspan="4">HLEN</td><td colspan="2">Reserved</td><td colspan="2">Code Bits</td><td colspan="4">Window</td></tr>
<tr><td colspan="6">Checksum</td><td colspan="6">Urgent Pointer</td></tr>
<tr><td colspan="7">IP Options (If Any)</td><td colspan="5">Padding</td></tr>
<tr><td colspan="12">DATA</td></tr>
</table>

Figure 3 TCP segment format

The segments are used to establish connections as well as to carry data and acknowledgments (Comer, 2006). Each of the segments is divided into header and data. The header, known as TCP header, carries out the expected recognition and control information.

Fields ***source port*** and ***destination ports*** contain the port numbers that identify the services running at the ends of connection. "The ***sequence*** *number* field identifies the position of the sender's byte stream of the data in the segment. The ***acknowledgement number*** identifies the number of the octet that the source expects to receive next" (Comer, 2006). The ***HLEN*** field identifies the length of the TCP header measured in 32-bit multiples. The ***option*** field varies in length and several options can be used after the standard header of certain packets segment, thus the TCP header's size varies in length. The 6-bit is used for ***reserved*** field for future use. ***Code bits*** filed is used to determine the purpose and contents of the TCP segment. In the ***Window field*** TCP software broadcasts the data it is willing to accept, when it sends a segment by stating its buffer size (Comer, 2006)

2.3.2.1Establishing a TCP Connection

Establishing a TCP connection is a three way handshake process. The figure below illustrates the process:

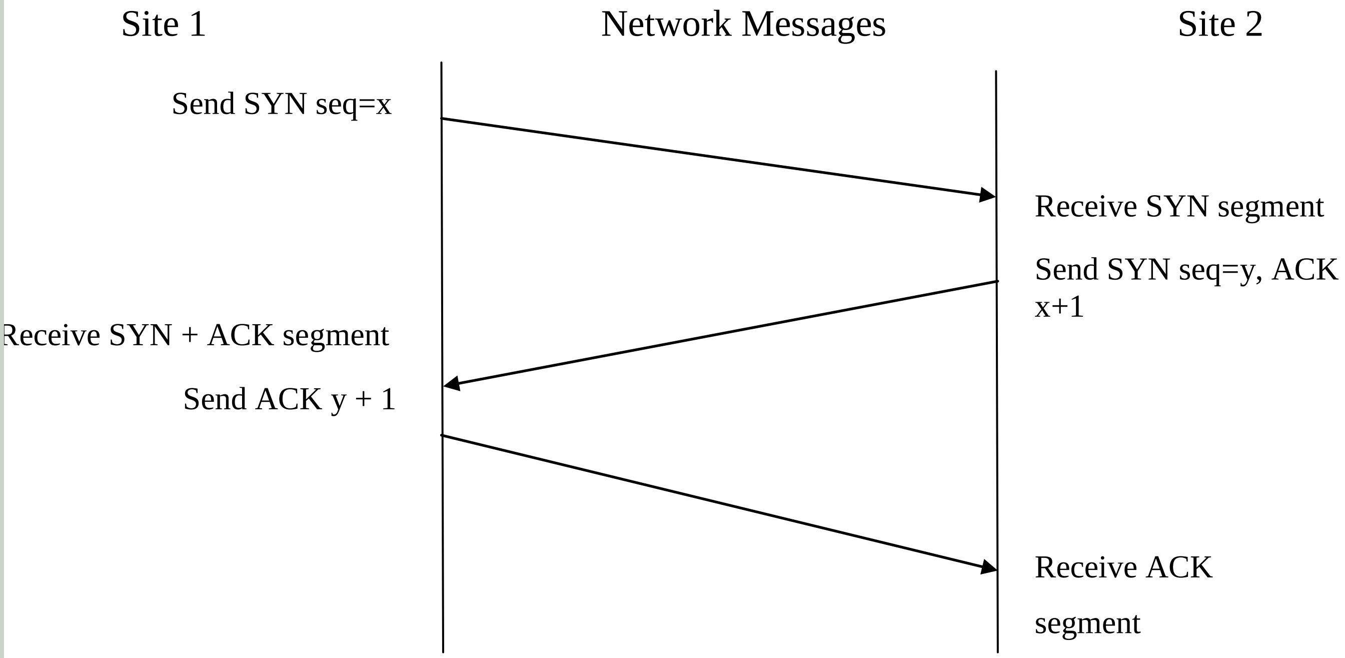


Figure 4 Establishing a TCP connection

(Comer, 2006)

The first segment of the network message, of the handshake is normally identified because of the SYN bit set it has in the code field. The second message has both the SYN and ACK segment bits set; this indicates that it acknowledges the first segment of handshake. The final segment of network message is only an acknowledgement and is formerly used to inform the destination that both sides agree the handshakes. Finally TCP connection is established between two hosts (Comer, 2006)

2.3.2.2Closing a TCP Connection

The two end points programs that use TCP to communicate with each other can close the communication using the *close* command. “Internally, TCP uses a modified three-way handshake to close the connection” (Comer, 2006). The figure below illustrates the connection:

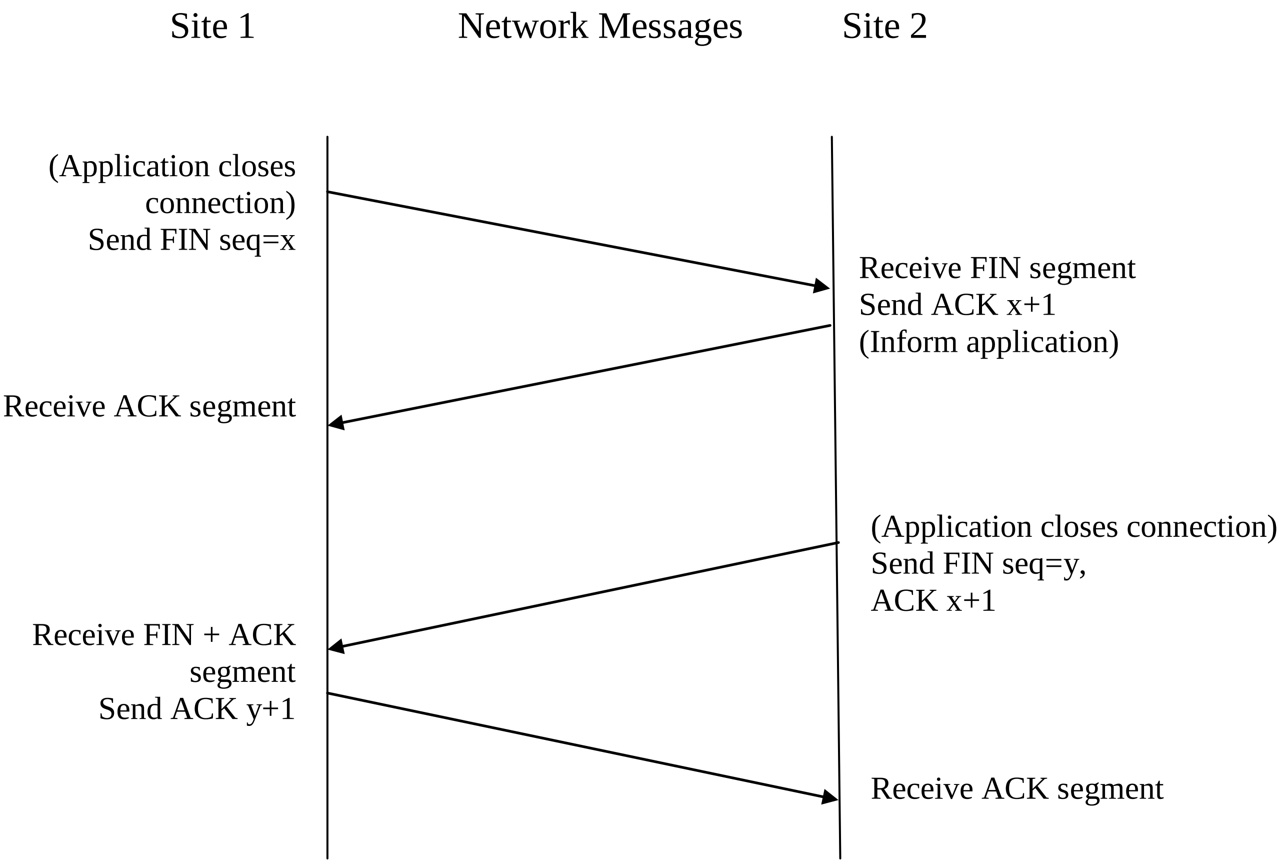


Figure 5 Closing TCP connection

(Comer, 2006)

TCP normally closes the connection from one direction and when the program has no more data packets to send Site 1 sends a FIN but set to Site 2 and waits for it to acknowledge it. The receiving site 2 acknowledges the TCP FIN segment and informs the program on other end, that no more data is available. Once the connection is closed on either direction TCP refuses to accept any more data packets (Comer, 2006).

2.4 History of Virtual Network Computing (VNC)

Virtual network computing was first developed by the Olivetti and Oracle Research Laboratory (ORL) for their telephone system, allowing the organisation of the interface of X Windows application to be displayed on a remote machine (Morris, 2001). Since a large amount of bandwidth is required for the connection, a video tile that display devices such as Pen, LCD screen and ATM connection was developed by the organisation. In January 1999, AT & T labs bought and secured Olivetti and Oracle Research Laboratory (ORL), hence making VNC a project of AT & T labs, Cambridge UK (Morris, 2001).

This technology enabled computer users to access centralised and remote resources from widely available devices (Wannous & Nakano, 2010). Virtual network computing (VNC) is a thin client technology that can be used to display and work on a remote X window, which is a graphical user interface window of another computer (Waugh, 2002).

The application has two independent versions; the client and the server, both of which run on any platform. This makes it perfect for those users who use the Windows operating system to manage Unix operating systems and vice versa (Bezroukov, 2009). The application is also useful for network and system administrators, as they would not have to attend each and every computer for troubleshooting; instead they use VNC to assign the task from one location (Bezroukov, 2009). There is also a VNC viewer written in Java, which can be accessed through a web browser.

VNC is currently moving in many directions. Olivetti and AT&T were slow to release the first VNC applications which led to several independent VNC development projects. It will be interesting to find out how VNC, as a project, will progress as original VNC developers are currently working with RealVNC (Waugh, 2002).

There are certain areas in which VNC efforts are lacking and under contention, Such areas include printing files and documents remotely and also fast and safe ways to transfer files from the viewer to the server (Waugh, 2002).

2.4.1 VNC Server

VNC server is initially configured to accept an incoming HTTP connections requested by the viewer over VNC default TCP ports 5900 to 5902 (Wannous & Nakano, 2010). VNC server and viewer negotiate the connection with a mutually understood encoding (Waugh, 2002). The server needs to be installed on the host system or machine and is currently available on Unix X window, Windows and Macintosh computer systems. The server needs to be defined, configured and installed on the host system or machine, to which the viewers have something to connect.

Communication over a VNC connection between the client and server is not completely encrypted, however the password used for the connection is encrypted by the DES or 3DES encryption standards depending on different VNC applications. This would be a concern for organisations as traffic could be intercepted and sniffed by an attacker over the network. However the PCAnywhere application has an add-on feature to version 1.0, for encrypting traffic between the connections (Green, 2004).

2.4.2 VNC Viewer

When the viewer is connected to the server, the user or administrator can connect to the remote server system and view the system. The viewer is currently available in many operating systems such as Unix X Window, Java, Windows, Macintosh 7.1 or higher and Windows CE 2.0 or later. The advantage of the viewer is that it does not require any installation and configuration like the server and can be run directly from a hard drive or any external electronic device. Interestingly the viewer can connect to the server and view any activity on the remote server without the server being controlled by the viewer. This can be used by administrators to monitor server activity remotely (Morris, 2001).

2.4.3 VNC Session Initiation

Following is the session initiation and authentication process that takes place between the viewer and the server.

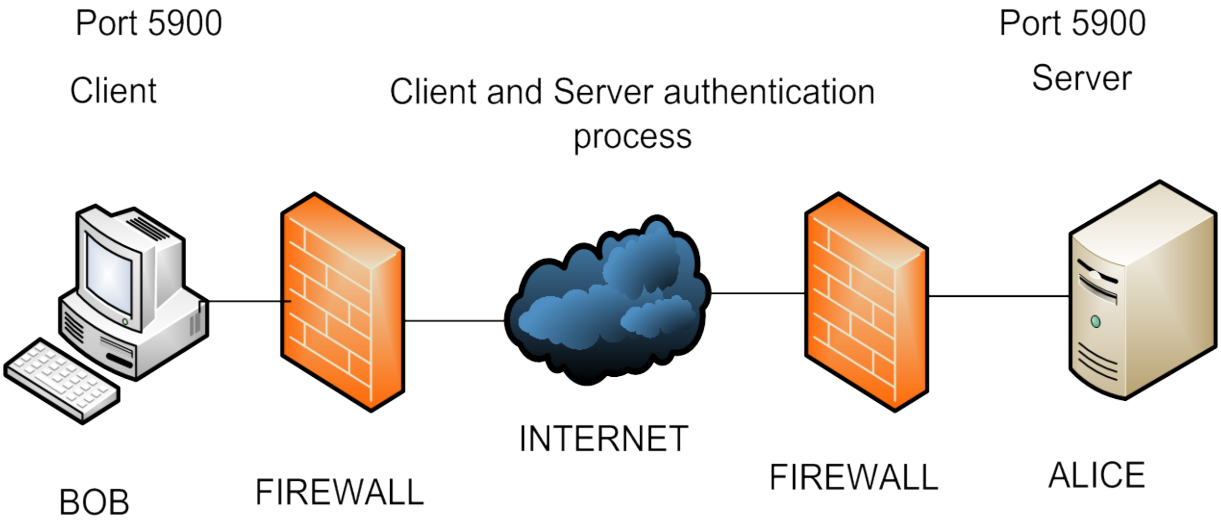


Figure 6 VNC Session Initiation process

- A Data Encryption Standard (DES) key (Luo, 2007) is used by both Bob and Alice endpoints for authentication.
- Bob connects to Alice and both exchange protocol version information.
- Alice generates a 16 byte key challenge and sends it to Bob.
- Bob then encrypts the received challenge with the DES key and sends it to Alice.
- Alice then encrypts the challenge key with DES and compares the hash with the key Bob send to her.
- If both keys match then access is granted to Bob, otherwise access is denied.

(Arce, 2001)

When the VNC connection is first established between the server and client, the former requests authentication from the client using a challenge response scheme, which this usually prompts the client to input the session password. When the authentication process is completed, the server and client negotiate pixel format, desktop size and the encoding scheme to be used for the connection. Finally after the negotiation of the display settings, the session begins (AT&T Laboratories Cambridge, 1999).

2.4.4 VNC Security Issues

It is relatively simple to compromise the security of the VNC. Largely because of the authentication mechanism it uses for connections; it requires only a one way session password with a maximum of 8 characters on TightVNC, and on the target machine the password strings are normally saved in the windows registry under `HKEY_LOCAL_MACHINE\Software\TightVNC\Server.` For RealVNC and UltraVNC the password strings is normally saved under `HKEY_LOCAL_MACHINE\Software\RealVNC\WinVNC4` and `HKEY_CURRENT_USER\Software\ORL\WinVNC` respectively.

A fixed key encrypts the VNC password using DES or 3DES encryption algorithm, enabling the attackers to gain read access to the system's registry with which they can compromise the VNC session password by brute force or using rainbow tables to crack the passwords (eTutorials.org, 2008-2010) (McNab, 2008). Commercial applications such as the password recovery bundle from Top Password Software, (TopPasswordSoftwareInc, 2010) and ElcomSoft password recovery bundle from ElcomoSoft Proactive Softwares (ElcomSoft, 2010) , can recover and brute force the protocol passwords. However there are also few freeware tools, such as VNCPassView and VNC password decoder 2.0, which can be used by anyone to crack VNC passwords (Auriemma, 2003). To recover or crack the password, it must to be no more than 8 characters. If the password is more than 8 characters long, then all the applications mentioned above fail to recover the full password.

VNC uses a challenge/response mechanism for authenticating clients over insecure channels; this mechanism helps to avoid the transmission of clear text passwords over the network (Arce, 2001). A security flaw in the design of the mechanism aids the attacker to obtain legitimate credentials from a client hence gaining unauthorised access to the server. Therefore, a legitimate attacker can eavesdrop the client/server communications and change or modify network communications. The attack is described below:

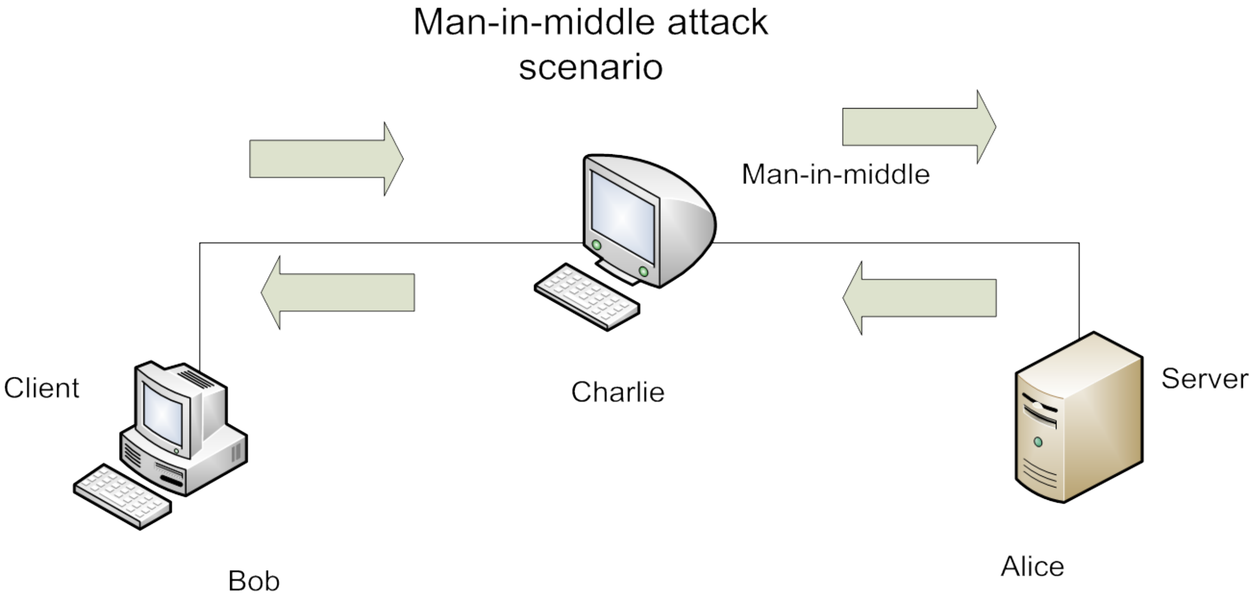


Figure 7 Man-in-middle attack scenario

- Charlie connects to Alice and both computers exchange security protocol version information.
- Alice generates a 16 byte challenge key (K1) and sends it to Charlie. Now we see that Charlie has a connection established with Alice with authentication pending.
- Charlie waits for Bob to send a connection request to Alice.
- Upon the connection request form Bob to Alice, Charlie sends a generated 16 byte challenge key (K2) to Bob.
- During this process Charlie captures the challenge and modifies the data and replaces (K2) to (K1).
- Bob receives (K1) instead of (K2) and encrypts it with DES pre shared key (KS1) and sends to Alice.
- Charlie captures the (K1S), and then sends this key to Alice in its own connection pending earlier.
- Alice receives both responses from Bob and Charlie which are equal (K1S).
- Alice then encrypts, with the DES key, the challenges (K1 and K2) and sends and compares the result form the received responses (K1C, K2C).
- For Bob the connection K2C does not match K1S and therefore access is denied.
- For Charlie the connection K1C matches to K1S and therefore access is granted to Charlie.(Arce, 2001)

VNC communication sessions can be sniffed and hijacked using Man-in-middle attacks and an ideal tool that can support this is Cain & Abel which can be downloaded from (*http:/www.oxid.it)* (McNab, 2008).

However VNC traffic and communication can be encrypted using VPN and SSH.

2.4.5 VNC Known Vulnerabilities

VNC has known vulnerabilities that can be exploited by hackers who then access the internal system. It is important to update the VNC applications for any patches or security updates on the vulnerabilities.

The table below lists serious issues that can lead to remote exploitation of VNC services.

CVE Reference	Date	Notes
CVE-2006-2450	05/07/2006	LibVNCServer 0.7.1 authentication bypass vulnerability
CVE-2006-2369	08/05/2006	RealVNC 4.1.1 authentication bypass vulnerability
CVE-2006-1652	05/04/2006	Multiple UltraVNC 1.0.1 buffer overflows
CVE-2002-2088	23/04/2002	MOSIX clump/os 5.4 blank password VNC account access
CVE-2001-0168	29/01/2001	AT&T WinVNC server 3.3.3r7 HTTP GET request buffer overflow

Table 3 VNC security vulnerabilities (McNab, 2008)

2.5 Remote Framebuffer Protocol (RFB)

VNC uses a simple protocol for remote access of a computer in graphical user interface, which is based on the remote framebuffer protocol (AT&T Laboratories Cambridge, 1999). The protocol works at the frame buffer level, hence it is applicable to all operating systems including Windows, Macintosh and Linux.

One of the strong points of the protocol is that it makes the client stateless; if the client disconnects from a given server and later reconnects to the same server, the state of the user interface is preserved. This allows the user known and identical user interface a view of the computer wherever they go (Richardson, 2009).

The RFB protocol will run over any reliable network transport such as the TCP/IP protocol (Richardson, 2009). VNC by default uses TCP ports 5900 through 5903 (for direct access using VNC viewer) and port 5800 (for HTTP access using a Java client through web browser) (McNab, 2008). As the protocol has low bandwidth requirements it is a true thin-client protocol, which can run on wide range of hardware.

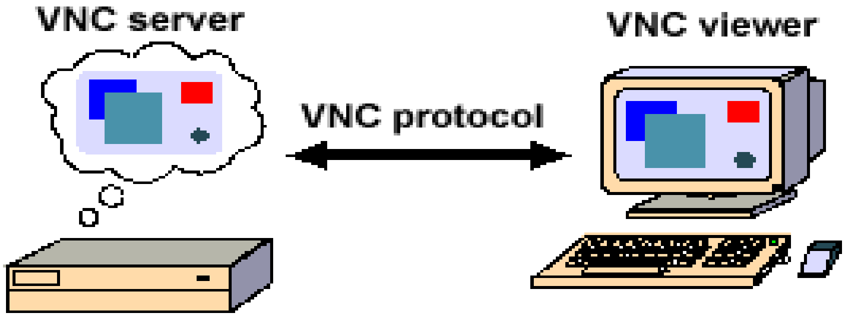


Figure 8 VNC protocol

(Richardson, 2009)

The RFB protocol has few uses other than those for which it was originally designed. One use is as a scriptable remote control; this could be used for automating tasks with applications that were not programmed with scripting in mind. Application such as rfbplaymacro can be used to control the VNC session, which takes the scripts and translates it into RFB input events (Waugh, 2002).

Another use is session playback, such as recording screens of display on a file for later display. This can be used in a demonstration for a shop or centre display (Waugh, 2002).

2.6 Remote Desktop Protocol (RDP)

Microsoft remote desktop protocol provides remote access and display over a network connection for Windows based applications that are running on server. The protocol provides access to a remote computer which is running Windows 2000 server and later versions of operating systems including Windows XP (Technet, 2000). RDP is designed to work on various types of network topologies and multiple local area network (LAN) protocols.

RDP is based on, and is an extension of, the ITU T.120 family of protocol standards. This protocol is capable of multichannel, this means that it allows separate virtual channels for carrying the encrypted communication and data from the server to the client (Technet, 2000).

The remote desktop consists of following components:

Remote desktop protocol

RDP is a protocol in presentation layer that allows a Windows based terminal or other Windows client to communicate with a Windows XP professional computer system. RDP works on any TCP/IP connection, including local area networks, wide area networks, dial-up, direct subscriber lines or even with virtual private network (VPN) (MicrosoftTechNet, 2005). The TCP/IP port 3389 is used by default by RDP.

Client software

This is software that is installed by default in the Windows XP professional system; however the CD also includes the software, which can be installed on other computer systems that are not running Windows XP professional. The client software does not require any configurations to the server, just installation, at which point a dialog box will prompt for IP address for server and password to connect to the remote computer (MicrosoftTechNet, 2005).

Remote desktop connection

This tool connects the client computer to another remote computer which is running Windows XP professional or server that has remote desktop connection enabled. As mentioned above this is installed by default in the Windows XP home and professional editions, and can be installed individually or older Windows operating systems (MicrosoftTechNet, 2005)

Remote desktop web connection

This type of connection works the same way as remote desktop connection, the only difference being the features delivered over the web through Microsoft ActiveX technology. Remote desktop web connection ActiveX can start a remote desktop session on the remote computer through being embedded on a web page, with the computer not having installed a remote desktop application (MicrosoftTechNet, 2005). However ActiveX control must be installed from a Web server with Internet Information Services (IIS) that has active web pages enabled.

In summary:

“This is how the applications work: the information from an application or service to be transmitted is passed down to the protocol stacks, sectioned, directed to the channel, encrypted, wrapped, framed, packaged on to the network protocol and finally addressed and sent over the wire to the client” (MicrosoftSupport, 2007)

2.6.1 Features of RDP

Encryption

It is very simple and easy to sniff the protocol communication, such as session passwords over the network; encrypting the traffic protects against such attacks on the network. Every version of the RDP protocol uses the RSA security encryption RC4 cipher encryption standard. RC4 is designed and used to secure all the communication and information sent from the server end to client end. The protocol also uses the Secure Shell Layer SSL to encrypt the traffic over the web sites (Technet, 2000).

In Windows 2000 server and later, the administrators have an option to choose whether to encrypt the traffic and data with either a 56 –bit or 128 – bit key.

Bandwidth Reduction Features

This helps the protocol to reduce the amount of data and information transmitted over the network. RDP uses the compression and caching bitmaps and fragments in RAM. This cache can provide significant enhancement in performance over the low-bandwidth connections.

Roaming Disconnect

This feature lets the user to restore to the state of the connection since disconnected by the user manually or if the session was disconnected to a network or client computer failure.

Clipboard Mapping

Here the users can use features such as cut, copy and paste text and graphics between the sessions.

Print Redirection

This is a useful feature for printing documents on the remote machine. Applications running with the server and client session can automatically print to a printer installed on the client machine.

Virtual Channels

"Using the Virtual Channel Architecture, new applications can be developed to add any feature that require communication and also existing application can be improved" (Technet, 2000).

Remote Control

In this the remote administrator can view and control another computer during the session. Features such as keyboard input, mouse movements and display are shared between the two computers in the session.

Network Load Balancing

RDP protocol uses Network Load Balancing (NLB) through Advanced Server and Data centre Server service. This helps clients connect to pool of servers running terminal services; this prevents one point of failure.

2.6.2 RDP Session Initiation

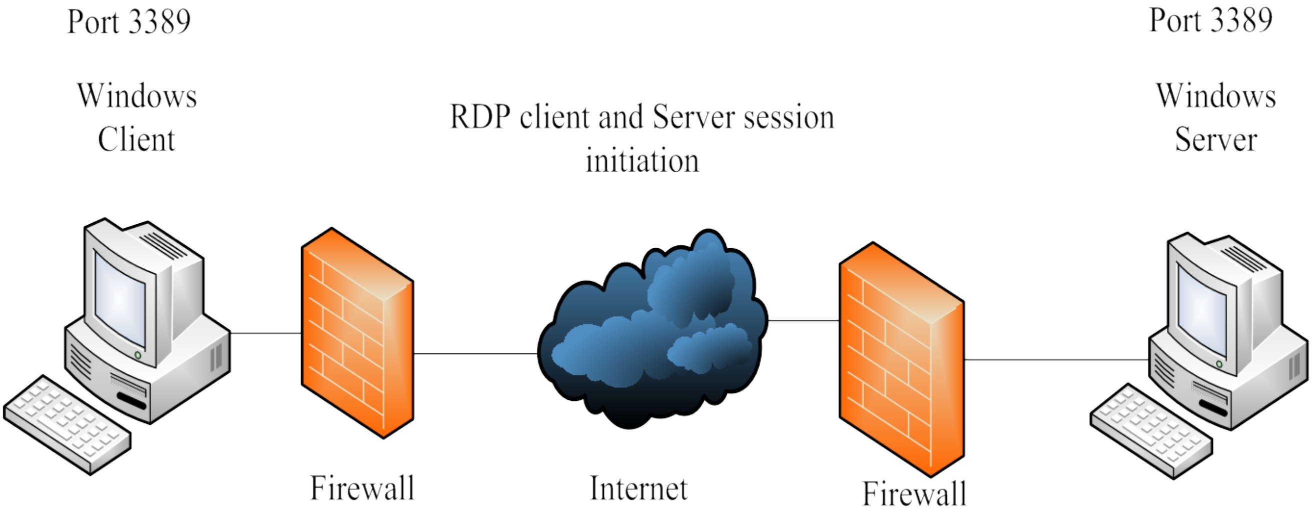


Figure 9 RDP session initiation process

- Windows client connects to Windows server and sends session connection request to Windows server.
- Windows server sends its RSA public key and random salt in clear text.
- Then Windows client sends a random salt to server, encrypted with the Windows RSA server public key.
- Windows server receives the encrypted random salt from Windows client and checks with its private key. If the hashes match then the connection is established.
- RC4-encrypted data connection is initiated.

(Longzheng, Shengsheng, & Jing-li, 2004).

2.6.3 RDP Security Issues

Man-in-middle attack using ARP poisoning – We are aware that the information sent over the network is secure and encrypted, but there is no verification of the identity of the server when setting an encryption key for the connection. This means that RDP protocol is vulnerable to Man-in-middle attack (Montoro, 2005). The attack is similar to the VNC Man-in-middle attack explained earlier under VNC security issues.

RDP Brute-Force Password Grinding – The attacker will try to locate accessible RDP servers by port scanning for TCP port 3389 and then perform an enumeration through anonymous NetBIOS sessions. This will let the attacker identify weak user accounts, those that have weak passwords and poor security settings (McNab, 2008). Tim Muller created a tool called TSGrinder that can perform an exact brute force attack on the protocol and terminal services. The tool is available at *www.hammerofgod.com/download.html*. (McNab, 2008)

2.6.4 RDP Known Vulnerabilities

There have been a number of Denial of Service (DoS) attacks and memory leak issues in the Microsoft Terminal Services for last three years (McNab, 2008). Three weaknesses have been identified that allow attackers to perform Man-in-middle attacks against RDP sessions. The weaknesses are listed in MITRE CVE as CVE-2007-2593, CVE-2005-1794 and CVE-2002-0863 (McNab, 2008). The table below identifies a serious flaw in RDP that can be exploited remotely:

CVE reference	Date	Notes
CVE-2000-1149	08/11/2000	RegAPI.DLL overflow in Windows NT 4.0 Terminal Server allows remote attackers to execute arbitrary commands via a long username.

Table 4 RDP security vulnerabilities

(McNab, 2008)

RDP communication sessions can be sniffed and hijacked using Man-in-middle attacks and a ideal tool that can support this is Cain & Abel which can be downloaded from *http:/www.oxid.it* (McNab, 2008).

3.0 RESEARCH METHODOLOGY

An accurate research methodology needs to be developed and adapted to conduct any type of research. The correct methodology will guarantee precise results and outcome for the area of research conducted and also builds a pathway for future examination on the research area. There are two types of methodology or research approaches used;

- Qualitative Research - “research that describes phenomena in words instead of numbers or measures” (Wiersma, 2000). This scientific research consists of seeking answers to a phenomenon or question, use predefined set of guidelines to answer the phenomenon, collect evidence and produce findings. “ Qualitative research is especially effective in obtaining culturally specific information about the values, opinions, behaviours, and social contexts of particular populations” (Family Health International, 2010).
- Quantitative Research – “research that describes phenomena in numbers and measures instead of words” (Wiersma, 2000). Quantitative research is about the relationships and differences between the variables. Variables such as number, time, performance, values and treatment. The relationship between the variable is achieved through descriptive and experimental methods (Hopkins, 2000).

The table below shows a comparison for the above mentioned methods:

Quantitative	Qualitative
Both are systematic	
Objective	Subjective
Deductive	Inductive
Generalisable	Non - generalisable
Numbers	Words

Table 5 Comparison of quantitative and qualitative research

(Ross, 1999)

This research will be conducted using the quantitative method as this method can be objective, deductive and has results in numerical value. There are three major types of quantitative research; descriptive, quasi-experimental and experimental. Both quasi-experimental and experimental are designed to examine cause and effect of the research (Ross, 1999).

Quasi-experimental research approach is used to conduct research for the project. This research methodology is selected because of the nature of the data collected from the acquired images needs to be tested and analysed in accordance to forensic process. After the testing and analysis, the experiment continues comparing between the test data and results between the three images of Windows XP for any variances.

The research is to focus on VNC and Microsoft RDP remote desktop applications and perform forensic analysis and extract related information using forensic tools in Windows system.

The following process will be followed in doing the analysis:

a) File System Analysis – searching a hard drive for strings of data is the most common technique used by investigators. The searching of information and data can be file based or slack based or even unallocated space searching. Each of these searching techniques will be used in the analysis of computers to look for any artefacts left behind by the remote desktop protocols. Following places will be searched for any artefacts:

    - File recovery of deleted files from file system and recycle bin.
    - Special files – such as print spool files, page file and windows shortcuts.

b) Log File Analysis – Microsoft system stores all the system logs under event logs. Event logs are broken into three areas; application logs, security logs, system logs

c) Windows Registry Analysis – an in-depth analysis will be done in the Windows registry to look for any artefacts and any connections settings left behind by the remote applications and protocols.

(Steel, 2006)

3.1 Variables Impacting Research

There are few variables that exist with potential impact on the research and the research questions mentioned earlier.

The version of the VNC and RDP applications used for the research are all latest versions, downloaded from the vendor websites, therefore they may have slight variations on the design and features when compared to the older versions. The applications are also patched and updated with the latest security patches. Therefore the analysis may differ from the old version.

The software and hardware used for the acquisition of the systems and analysis may affect the outcome, as these various tools used for analysis may impact data in different ways. To limit this impact, only one tool is used to acquire and analyse different Widows XP images using Forensic Tool Kit v 1.71 (FTK) and FTK Imager v 1.5.5.45.

A Widows system is used as the base platform for analysis. The systems may not be completely updated with the latest dated security patches, as the images are acquired within short period for analysis. The analysis on the images was done in accordance to Standards Australia *HB171: Guidelines for the management of IT evidence*.

The above mentioned are variables that may impact the proposed research. To mitigate these the research is evaluated and documented in case if they can not be controlled. However the variables are likely to impact the quality of the collected data on the images.

3.2 Theoretical and Philosophical Assumptions

There are some assumptions made during the conduct of the research and also during acquisition and analysis of the acquired images. In order to mitigate any variance in the acquisition, analysis and testing, a set of machine images will be created. It should however be noted that the acquired images are not real evidentiary devices and the machines are created as evidentiary values.

For RDP and VNC to work, router firewall needs to be configured to open the protocol ports. Therefore the user needs to open the remote protocols port for remote applications to work.

Windows firewall for XP service pack 1 does not allow any VNC remote connections as the application is not able to configure the firewall to open the ports for VNC to communicate. Therefore an assumption was made that the firewall was configured to allow VNC ports.

On Windows XP operating system firewall logging by default is not enabled, therefore an assumption is made that the firewall logging is enabled on the local network. This could help in the analysis to find incoming and outgoing connection on the network.

VNC applications do not log information on the file system unless enabled and specified by the user to do so. Therefore an assumption is made that the logging is enabled on the computer system.

On routers, mostly remote desktop ports are not open this could be because of security issue, therefore router firewall is configured to open ports of VNC and RDP for communication.

3.3 Materials

Various softwares and tools were used during the data collection, acquisition and conducting analysis on the images. The tools and software used for the research are summarised and explained below.

a) VMware application v 7.1.1 build-282343 – VMware is virtualisation software, this software will be used in the research as a base platform to install Windows XP operating systems for creating a scenario for the study. Then later the systems will be imaged for analysis and testing.
b) Windows XP operating system service packs 1, 2 & 3 – Windows XP operating system will be used for the analyses and different service packs of Windows XP will be used for testing.
c) Forensic Tool Kit (Access Data) v 1.71 - Forensic Tool Kit by (Access Data) will be used in conjunction with other monitoring tools, to analyse the different computer systems that contains Windows XP operating system.
d) RealVNC v P4.5.4, UltraVNC v 1.0.8.2, TightVNC v 2.0.2 and TeamViewer v 5.0.8232 – these are different types of VNC application that are most commonly used by many individuals and organisations for remote access of computer systems. Therefore all these different applications will be used and tested on the machines.
e) Remote Desktop Protocol (Terminal Services Client v 6.0) – RDP is a default protocol installed on the Windows XP machines. This will also be used for the analysis.
f) Abel and Cain v 4.9.35 – This is a password recovery and sniffing tool developed for Windows operating systems. The application has various features to recover passwords, such as sniffing the internet traffic, recovering wireless network passwords, recording

VOIP conversations and also cracking encrypted passwords using dictionary attacks, brute-force and cryptanalysis attacks (Cain & Abel, 2010). The tool will be used to recover and crack VNC and RDP passwords and to test the encryption of the protocols.

g) FTK Imager v 1.5.5.45 – FTK imager is a tool used to image physical and logical hard drive or any external devices as exact copy. The tool supports storage disks images in SMART’s format, dd raw data format and also EnCase format. The tool will be used to image all the three Windows XP service packs. Since it uses supports dd format it is ideal for imaging.
h) Mount Image Pro v4.01 – this is a forensic tool that allows to mount raw images files also support other file formats, as logical drive on the computer. The tool will be used to mount the images on the testing computer to find encrypted passwords or recover remote session passwords.
i) Password Recovery Tools –Tools such as Elcomsoft 2009, VNC passview v 1.02 and Password Recovery bundle 2010 v 1.30 are going to be used for cracking the session initiation password of the VNC and RDP applications.
j) Sysinternals Suite – This is a troubleshooting utilities suite developed by Microsoft. The suite includes useful tools such as portmon, process explorer, TCPView, PsLogList, PsPasswd and many more (Russinovich, 2010); such tools will help the analysis of the images to look for artefacts of the remote protocols.
k) MiTeC Windows Registry Analyser 1.5.2.0 – this tool helps to view registry files of the acquired image for analysis of the registry system of the image.

The virtual machines and images will not be real evidence seized by law enforcement, but the systems will be configured in such a way that it can be used as real seized evidence.

3.4 Research Design

The research will be conducted in two stages. Stage 1 will consist of conducting forensics analysis and testing on VMware images for any VNC and RDP artefacts on the machines. Stage 2 will consist filtering the results found in stage 1 and documenting the final results.

3.4.1 Stage 1

This is the core stage for the research, as it will help to develop this research project. This stage will consist of building VMware machines and installing images of operating systems and then conducting forensic analysis and testing on the imaged machines for any artefacts left behind by VNC and RDP protocols. Following process will be followed:

Build test environment – before starting any testing, a test environment needs to be created. The test environment will be built on VMware virtual environment and then different Microsoft XP operating systems will be installed in the VMware application. The process is outlined below:

- Create three VMware virtual machines and install three Windows XP service packs.
- Install the VNC applications. RealVNC, UltraVNC, TightVNC and TeamViewer will be used for examination and testing.
- Configure the VNC applications and remote desktop for the images, in order to make connections.
- Create legitimate connections between other computer systems, using all the VNC applications mentioned above and RDP protocol. Transfer files over the network and perform tasks between the two computers on the remote session.
- Create raw image of the computer systems.
- Three images were created of Windows XP with service pack 1, 2 and 3 respectively. All connections and configurations were made on all three images.
- Creating hash values of all the images for integrity purposes.
- Upon completion of all the configurations, connections made using the applications and creating dd raw images using FTK imager and also hashing the images; all the images are tested on the FTK tool kit that was installed on another Windows XP machine, which were used as base platform to perform the tests on the images.

Forensic examination and analysis – start to perform forensic examination and analysis on the acquired images. Windows file system, log files and windows registry will be closely examined for any artefacts left or changes made to the system after the connections.

3.4.2 Stage 2

This stage involves the process of extracting and studying all the results from stage 1 of analysis. Here the results will be studied and examined closely and then a final documentation will be created on what artefacts are left behind by the protocols.

A procedure is designed to conduct the tests and analysis on the acquired images and gather data, in order to address the research questions.

A baseline is created and established during the analysis. This baseline is normally used as a starting point of each test repetition. The baseline is required so that whenever the analysis and tests are performed, starting conditions are the same; as such impurity from earlier stages of testing is avoided.

The baseline was established by undertaking an acquisition of the Windows XP machines images as they were before any testing is done.

3.5 Analysis of Test Data

The testing on the images is carried out using forensic tool kit (FTK) application and also mount image pro tool. FTK imager is used to acquire raw images of the Windows XP three service packs. The tool acquires raw dd image, this makes the images an exact copy of the system. After all the images are been tested using the procedure mentioned above in order to acquire test data for the images. Later the images are loaded on FTK tool kit and analysed on Windows XP test machine. Both set of images are analysed and all resulted in valuable test data.

The Windows remote desktop protocol is not enabled by default on the operating system; so to make a remote connection using RDP the remote connectivity on the computer needs to be enabled. This can be done by right clicking the computer and then selecting the properties dialogue box, then clicking under remote tab for remote connection settings. By clicking enable remote desktop on the computer, this adds a rule on the firewall to open the RDP port for communication.

ADSL router does not allow any type of remote connections between the computer network and outer networks (internet). This is because the router firewall does not have the remote protocols ports open. Therefore, for someone to use the remote connectivity features either VNC or RDP, they will have to allow the application ports to communicate with internet and outside networks. This can be done through the router firewall settings under port forwarding feature. The router firewall is configured to allow the remote protocols for communications.

Upon installing the VNC applications, they automatically configure the Windows firewall settings to allow the remote connections by opening the ports. However this is not the case in Windows XP service pack 1, the applications are not able to configure the firewall of XP service pack 1, and therefore connection is not possible unless someone manually configure the firewall to open the ports. For the Windows XP service pack 2 and 3, firewall is automatically configured by VNC applications to open the ports.

TeamViewer is an application used for remote connection. It is different on how it works as compared to other VNC applications. This is because it neither uses the RFB protocol for connection nor 5900 and 5800 ports for connection and it uses HTTP port 80 for connection. It uses Advanced Encryption Standard (AES) for remote session password encryption with 128 byte string. This is very strong encryption standard as compared to DES and 3DES, used by other VNC applications.

In all Windows XP service packs, the firewall does not log any connection and network information of the computer by default. This is because firewall logging on Windows XP is not enabled; therefore no logs information can be obtained of any connections made using the VNC and RDP applications to other computers, unless firewall logging is enabled. VNC logging was enabled to retrieve the connection log information.

Also with VNC applications, the logging of the application is disabled by default, however for Team Viewer, upon installation it enables logging. Hence this will log the connections made to the application log file.

Event viewer is a component of Windows operating system and lets the users and administrators to view the event logs on the local computer. The event log service records the application, security and system events in Windows XP under event viewer. This is a critical place for administrators and forensics investigators to check for application, security and system logs for investigation purposes and also to identify and analyse the source of current system problems (Microsoft Support, 2007). Real VNC and Ultra VNC logs the connection details in the application log under event viewer on the destination computer, and not on the host or local computer. Therefore if a remote connection is initiated using Real VNC and Ultra VNC the log information of the connection is found on the destination computer, and not on the local computer. Tight VNC, Team Viewer and RDP do not log any information under event viewer. This came to a surprise as RDP is a Windows default remote protocol does not log information under event viewer.

All the VNC applications and RDP protocol stores the application and connection settings under the Windows registry. Windows registry is the core configurations database for Windows NT/ Windows 2000/ XP/ server 2003/ server 2008/ Vista and Windows 7. It stores information about the tuning parameters, device configuration, application configurations and user settings and preferences (Russinovich, 2000). The registry is divided into five different set of discrete files called *hives*. “A registry hive is a group of keys, sub keys and values in that has set of supporting files that contain backup of its data” (Microsoft support, 2008). The table below explains what each of the hives contains:

Windows PC	Settings stored
HKEY_LOCAL_MACHINE (HKLM)	Stores information about local computer, such as system memory, devices, drivers, and hardware settings.
HKEY_CLASSES_ROOT (HKCR)	Stores information used by various OLE technologies, file association and COM object registration
HKEY_CURRENT_USER (HKCU)	Stores information about the current user logged on.
HKEY_USERS (HKU)	Stores information about all the accounts on the local computer.
HKEY_CURRENT_CONFIG (HKCC)	Stores information about the current hardware profile used by the local computer.

Table 6 Windows Registry system Hives

(Microsoft support, 2008)

VNC applications store the settings under three hives, `HKEY_LOCAL_MACHINE` **(HKLM),** `HKEY_CURRENT_USER` **(HKCU)** and `HKEY_USERS` **(HKU).** The applications store information such as client IP addresses the local computer connected to, encrypted remote session passwords, desktop screen settings, graphic settings, printer settings and connection settings. The IP address stored is private IP address of the client. Server remote session password stored on the registry is vulnerable and easy to crack. During the experimentation phase the author found out that it is easy to crack the session passwords using Abel and Cain software. The software contains a feature to decrypt VNC password for up to 8 characters long. This is illustrated and shown in appendix C under figures 15, 19, 24, 29, 33, 38, 41 and 45.

All VNC applications and Team Viewer support file transfer feature, except for RDP protocol.

4.0 RESULTS

The examination of the test results shows and determines that the VNC and RDP protocols leave some artefacts behind on the windows registry and some under event viewer and log files. The results show the VNC server passwords use weak encryption standard and algorithm as it is relative easy to crack or recover the passwords using password cracking tools. Also the applications stores the private IP address of the client it connected to; this can be useful for forensic investigators as they can track the client from the private IP address. There were number of significant pieces of information identified during the experimental phase. These were:

- Connection settings of the all the VNC applications and Terminal service (RDP) settings under the Windows registry.
- Encrypted server remote session passwords in the registry.
- Private client IP addresses the local computer connected to.
- Firewall log file that showed the connections of the protocols.
- Log information in event viewer under application event.
- TeamViewer log file stored under the C:\Documents and Settings\Administrator\Application Data\TeamViewer.
- VNC applications log files located in the hard drive.

The forensic integrity of the process was maintained and established through the use of the cryptographic hashing algorithm. This shows and confirms that the contents on the imaged systems did not change during the experimental process.

4.1 Windows Registry Analysis

This shows the test results of the registry system analysis of the acquired images and shows what types of artefacts were found during the experimental phase of the research. Two applications namely: Alien registry viewer and MiTeC windows registry analyser were used side by side for the analysis of the registry files. All the registry keys were extracted and exported on a computer for analysis. The hash values were created of the files for integrity purposes. The hashes of the files are located in the Appendix A. Figures in appendix C show some registry hives snagged for reference on how and where the applications store the settings under the Windows registry.

4.1.1 Image 1 (Windows XP service pack 1).

The table below summarises the artefacts left behind by the VNC applications and RDP under the registry system of Windows XP service pack 1

VNC applications/ RDP	Artefacts left under registry system
Ultra VNC	- Under `HKEY_CURRENT_USER\Software\ORL\VNCviewer\MRU`, the application stores client private IP addresses the computer connected. - Under `HKEY_CURRENT_USER\Software\ORL\VNCviewer\History`, the application stores the connection settings for each client IP addresses.
Real VNC	- Under `HKEY_LOCAL_MACHINE\software\RealVNC\WinVNC4`, the application stores the RSA private key generated by the VNC server during the connection. - Under `HKEY_CURRENT_USER \Software\RealVNC\VNCViewer4\MRU`, the application stores the history of the client private IP addresses the computer made connections to. - Under `HKEY_LOCAL_MACHINE\software\RealVNC\WinVNC4`, the application stores the local computer VNC server session password which is encrypted. It also stores It also stores View only password and Admin password also encrypted under this value. - Under `HKEY_LOCAL_MACHINE\Software\RealVNC\VNC Address Book`, it stores the connection settings and connection password of a connection that the user saved for future quick connection.
Tight VNC	- Under `HKEY_LOCAL_MACHINE\Software\TightVNC\Server`, application stores the VNC server session password of the local computer, which is typically encrypted. The application also stores the connection settings defined by the user.

	- Under `HKEY_CURRENT_USER \Software\TightVNC\Server`, application also stores the VNC server session password of the local computer, which is typically encrypted. The application also stores the connection settings defined by the user.
Team Viewer	- Under `HKEY_CURRENT_USER \Software\TeamViewer\Version5`, the application stores the history of the client IDs, the local computer connected to. - Under `HKEY_LOCAL_MACHINE\Software\ TeamViewer\Version5`, the application stores the private and public keys of the remote connection and also other settings relating to the connection.
RDP	- Under `HKEY_CURRENT_USER \Software\Microsoft\Terminal Server Client\Default`, the application stores the history of the clients private IP addresses the local computer connected to.

Table 7 VNC applications and RDP settings stored under the registry system

4.1.2 Image 2 (Windows XP service pack 2)

The table below summarises the artefacts left behind by the VNC applications and RDP under the registry system of Windows XP service pack 2.

VNC applications/ RDP	Artefacts left under registry system
Ultra VNC	- Under `HKEY_CURRENT_USER\Software\ORL\VNCviewer\History`, the application stores client private IP addresses the computer connected. - Under `HKEY_CURRENT_USER\Software\ORL\VNCviewer\History`, the application stores the connection settings for each client IP addresses. - Under `HKEY_CURRENT_USER\Software\ORL\WinVNC`, the application stores the computer's VNC server password which is typically encrypted.
Real VNC	- Under `HKEY_LOCAL_MACHINE\software\RealVNC\WinVNC4` , the application stores the RSA private key generated by the VNC server during the connection. - Under `HKEY_CURRENT_USER \Software\RealVNC\VNCViewer4\MRU`, the application stores the history of the client private IP addresses the computer made connections to. - Under `HKEY_LOCAL_MACHINE\Software\RealVNC\WinVNC4`, the application stores the local computer VNC server session password which is encrypted. It also stores View only password and Admin password also encrypted under this value. - Under `HKEY_LOCAL_MACHINE\Software\RealVNC\VNC Address Book`, it stores the connection settings and connection password of a connection that the user saved for future quick connection.
Tight VNC	- Under

	`HKEY_LOCAL_MACHINE\Software\TightVNC\Server`, the Tight VNC application stores the VNC server session password of the local computer, which is typically encrypted. The application also stores the connection settings defined by the user. - Under `HKEY_CURRENT_USER \Software\TightVNC\Server`, application stores the VNC server session password of the local computer, which is typically encrypted. The application also stores the connection settings defined by the user.
Team Viewer	- Under `HKEY_CURRENT_USER \Software\TeamViewer\Version5`, the application stores the history of the client IDs, the local computer connected to. - Under `HKEY_LOCAL_MACHINE\Software\ TeamViewer\Version5`, the application stores the private and public keys of the remote connection and also other settings relating to the connection.
RDP	- Under `HKEY_CURRENT_USER \Software\Microsoft\Terminal Server Client\Default`, the application stores the history of the clients private IP addresses the local computer connected to.

Table 8 VNC applications, TeamViewer and RDP settings stored under the registry system

4.1.3 Image 3 (Windows XP service pack 3)

The table below summarises the artefacts left behind by the VNC applications and RDP under the registry system of Windows XP service pack 3.

VNC applications/ RDP	Artefacts left under registry system
Ultra VNC	- Under `HKEY_CURRENT_USER\Software\ORL\VNCviewer\History`, the application stores client private IP addresses the computer connected. - Under `HKEY_CURRENT_USER\Software\ORL\WinVNC`, the application stores the computer's VNC server password which is typically encrypted. - Under HKEY_CURRENT_USER\Software\ORL\VNCviewer\History, the application stores the connection settings for each client IP addresses.
Real VNC	- Under `HKEY_LOCAL_MACHINE\software\RealVNC\WinVNC4`, the application stores the RSA private key generated by the VNC server during the connection. - Under `HKEY_CURRENT_USER \Software\RealVNC\VNCViewer4\MRU`, the application stores the history of the client private IP addresses the computer made connections to. - Under `HKEY_LOCAL_MACHINE\Software\RealVNC\WinVNC4`, the application stores the local computer VNC server session password which is encrypted. It also stores View only password and Admin password also encrypted under this value. - Under `HKEY_LOCAL_MACHINE\Software\RealVNC\VNC Address Book`, it stores the connection settings and connection password of a connection that the user saved for future quick connection.

Tight VNC	- Under `HKEY_LOCAL_MACHINE\Software\TightVNC\Server`, the Tight VNC application stores the VNC server session password of the local computer, which is typically encrypted. - Under `HKEY_CURRENT_USER \Software\TightVNC\Server`, application stores the VNC server session password of the local computer, which is typically encrypted. The application also stores the connection settings defined by the user.
Team Viewer	- Under `HKEY_CURRENT_USER \Software\TeamViewer\Version5`, the application stores the history of the client IDs, the local computer connected to. - Under `HKEY_LOCAL_MACHINE\Software\ TeamViewer\Version5`, the application stores the private and public keys of the remote connection and also other settings relating to the connection. - Under `HKEY_LOCAL_MACHINE\Software\ TeamViewer\Version5`, the application also stores the security password used for connection, typically encrypted with AES encryption standard.
RDP	- Under `HKEY_CURRENT_USER \Software\Microsoft\Terminal Server Client\Default`, the application stores the history of the clients private IP addresses the local computer connected to. - Under `HKEY_CURRENT_USER \Software\Microsoft\Terminal Server Client\Servers`, the service stores the username used for the connection and also the computer name of the client PC.

Table 9 VNC applications, TeamViewer and RDP settings stored under the registry system

4.2 Log File Analysis

Log files carry important and enormous amount of information regarding the remote connection. Log files are useful because of the information it consists such as date and time of logs and who the computer connected to and which computer disconnect or closed the connection. Figures in appendix D (pg 124 – 137) show some log files extracted from the images that contain important information on whether the computer had any remote connections. Event log explorer was used to view the log information of the image. All the event log files were extracted and exported to a computer for analysis. The hash values were created of the files for integrity purposes. The hashes of the files are located in the Appendix B (pg 71-74).

4.2.1 Image 1 (Windows XP service pack 1)

The table below summarises the artefacts left behind by VNC and RDP as log information on the Windows file system for Windows XP service pack 1.

VNC applications/ RDP	Artefacts left under file system
Ultra VNC	- Ultra VNC leaves log information under the application event viewer of receiving computer's IP address and not of the host computer. - Under C:\Program Files\UltraVNC, the application leaves a WInVNC log file that consists of debug information.
Real VNC	- Real VNC leaves log information under the application event viewer of receiving computer's IP address and not of the host computer. - Real VNC stores saved connections under the C:\Documents and Settings\Administrator\Application Data\RealVNC. The saved connection contains the connection settings including the password for the connection.
Tight VNC	- Tight VNC places a log file under C:\Documents and Settings\Administrator\Application Data\TightVNC. The folder contains a log file of the application, however the file is empty and no log information is displayed, despite the connections.
Team Viewer	- Team Viewer typically stores log information under C:\Documents and Settings\Administrator\Application Data\TeamViewer folder. The folder contains two files. Firstly connections file and TeamViewer5_log file, both files contain connection information including file transfer logs.

RDP	- RDP does not leave any log information on the system.
Firewall	- Firewall log is placed under the C:\WINDOWS\pfirewall.log. The log information contains the all incoming and outgoing network information of the local network.

Table 10 Image 1 log information summary

4.2.2 Image 2 (Windows XP service pack 2)

The table below summarises the artefacts left behind by VNC and RDP as log information on the Windows file system for Windows XP service pack 2.

VNC applications/ RDP	Artefacts left under file system
Ultra VNC	- Ultra VNC leaves log information under the application event viewer of receiving computer's IP address and not of the host computer. - Ultra VNC places a log file under C:\Program Files\UltraVNC named mslogon. However there was no log file located in Image 1, therefore the application does not have any log file in Windows XP service pack. The file consists of client IP address and date and time the connection was received and ended. - Under C:\Program Files\UltraVNC, the application leaves a WInVNC log file that consists of debug information.
Real VNC	- Real VNC leaves log information under the application event viewer of receiving computer's IP address and not of the host computer. - Real VNC stores saved connections under the C:\Documents and Settings\Administrator\Application Data\RealVNC. The saved connection contains the connection settings including the password for the connection.
Tight VNC	- Tight VNC places a log file under C:\Documents and Settings\Administrator\Application Data\TightVNC. The folder contains a log file of the application, however the file is empty and no log information is displayed, despite the connections.
Team Viewer	- Team Viewer typically stores log information under C:\Documents and Settings\Administrator\Application Data\TeamViewer folder. The folder contains two files. Firstly connections file and TeamViewer5_log file,

	both files contain connection information including file transfer logs.
RDP	- RDP does not leave any log information on the system.
Firewall	- Firewall log is placed under the C:\WINDOWS\pfirewall.log. The log information contains the all incoming and outgoing network information of the local network.

Table 11 Image 2 log information summary

4.2.3 Image 3 (Windows XP service pack 3)

The table below summarises the artefacts left behind by VNC and RDP as log information on the Windows file system for Windows XP service pack 3.

VNC applications/ RDP	Artefacts left under file system
Ultra VNC	- Ultra VNC leaves log information under the application event viewer of receiving computer's IP address and not of the host computer. - Ultra VNC places a log file under C:\Program Files\UltraVNC named mslogon. However there was no log file located in Image 1, therefore the application does not have any log file in Windows XP service pack. The file consists of client IP address and date and time the connection was received and ended. - Under C:\Program Files\UltraVNC, the application leaves a WInVNC log file that consists of debug information.
Real VNC	- Real VNC leaves log information under the application event viewer of receiving computer's IP address and not of the host computer. - Real VNC stores saved connections under the C:\Documents and Settings\Administrator\Application Data\RealVNC. The saved connection contains the connection settings including the password for the connection.
Tight VNC	- Tight VNC places a log file under C:\Documents and Settings\Administrator\Application Data\TightVNC. The folder contains a log file of the application, however the file is empty and no log information is displayed, despite the connections.
Team Viewer	- Team Viewer typically stores log information under C:\Documents and

	Settings\Administrator\Application Data\TeamViewer folder. The folder contains two files. Firstly connections file and TeamViewer5_log file, both files contain connection information including file transfer logs.
RDP	- RDP does not leave any log information on the system.
Firewall	- Firewall log is placed under the C:\WINDOWS\pfirewall.log. The log information contains the all incoming and outgoing network information of the local network.

Table 12 Image 3 log information summary

5.0 DISCUSSION OF RESULTS

The information and data collected from analysed images as shown in chapter 5 and 6 clearly state what types of artefacts can be left behind by the VNC and RDP applications. This chapter will outline the recovered data and possible implications of the uses of each type of recovered data. The chapter explains the limitations during the analysis, discusses the results on the three images and answering the research questions outlined earlier in the thesis.

5.1 Limitations

The first thing that can be concluded from the results is that firewall and VNC applications must be enabled on the systems in order to read the application logs of remote connections. On Windows XP service pack 1 firewall does not allows remote connections unless configured to open ports, therefore the firewall was configured to allow the remote connections.

Therefore the user will have to allow both remote connection and change firewall settings to allow VNC and RDP to connect to the internet.

Secondly, the VNC applications and firewall does not log connection information on the computer system by default. For example if the user does not enable logging on the applications, then no logging information will be retrievable or found.

During the experiment and analysis process, Windows XP service packs 1, 2 & 3 must enable on the computers to allow remote desktop using RDP protocol for connection. It is very important that the limitations are clear and understood as it can have a significant impact on the way that acquired data and information can be used as artefact.

5.2 Ultra VNC

5.2.1 Windows Registry

As mentioned in chapter 6 under the result section that ultra VNC leaves important information behind about the remote connection initiated between the host and the client. The application stores the history of the clients the host computer initiated a remote connection with and the settings used for the connection. This is typically stored under the values `HKEY_CURRENT_USER\Software\ORL\VNCviewer\MRU` and `HKEY_CURRENT_USER\Software\ORL\VNCviewer\History`. This information is found under all the Windows XP service packs. This information can be important for an investigator or for forensics purposes, this is because the client can be tracked down by the private IP address, which is stored under the registry value. Further analyse the client computer for any misconduct activities or behaviour.

Furthermore with image 2 and 3 the application leaves a host computer's Ultra VNC server password under the registry value `HKEY_CURRENT_USER\Software\ORL\WinVNC`. This was not the case for image 1, and no server password was stored under the registry value. The password is typically encrypted by 3DES (Data Encryption Standard), however the encryption standard is vulnerable to brute force and dictionary attacks. Abel and Cain tool was used to crack the server password. The tool has a feature to crack VNC password of up to 8 characters long, therefore if the password is more than 8 characters then, the tool cannot crack the password. VNC password decryptor by (Shadow Production) is also capable of decrypting the Ultra VNC server password.

Under Appendix C in figures 25 and 39 shows decrypted passwords of the Ultra VNC server for images 2 and 3 respectively. Basically to decrypt the password, just type in the encrypted password stored under the registry value in the tool and the tool will decrypt the password and show it in clear text.

5.2.2 File System

Ultra VNC stores two files in the Widows file system under C:\Program Files\UltraVNC, namely; WinVNC log and mslogon. For image 1 (Windows XP service pack 1) the application only stores WinVNC log and not the mslogon file.

WinVNC log contains the debug information about the application and the remote connections initiated with different clients. After analysis on the file, the file did not have any important information left behind for forensic purpose. This is because the debug information left on the file does not leave any connection information on what happens during the connection with each client. However the mslogon file has information that may be of importance for forensic investigators, as the file contains the log information on the time and date the host computer connected to the client computer with the IP address shown. This information is vital for investigation purposes as you can see the times and client IP addresses the host computer connected to. As mentioned earlier that this log file is only present in the Widows XP service pack 2 & 3. Despite the log information left by the application, however the logs does not contain any file transfer information on what file was transferred and where the file was placed on the host or client computer.

The application also leaves log information under event viewer in application logs. The log information contains the client IP address and what time and date the connection was received by the computer. The application does not log information about the connection going out, but instead the connection coming to the local network. The log also contains whether the client or host computer disconnected.

5.3 Real VNC

5.3.1 Windows Registry

Real VNC also leaves crucial artefacts and information on the Windows registry system on all three images analysed. The application leaves the same information on all three images. Under `HKEY_LOCAL_MACHINE\software\RealVNC\WinVNC4`, the application stores the RSA private key. This key is usually encrypted and is generated by the host computer's Real VNC server during the remote connection session.

Real VNC has three options on what encryption to use. Firstly is always on, then prefer encryption on and lastly prefer encryption off. The user has an option to choose on whether to use encryption or not. The RSA key is generated if the first option is selected.

Under `HKEY_CURRENT_USER \Software\RealVNC\VNCViewer4\MRU`, the application stores the history of the clients private IP addresses the host computer connected to. This information can investigator to find the clients, since their private IP addresses is displayed.

Under `HKEY_LOCAL_MACHINE\software\RealVNC\WinVNC4`, the application stores the host computer Real VNC server password which encrypted by 3DES encryption standard. This password is used by the client to connect to the host computer. The encryption is vulnerable to attacks as to Ultra VNC and Abel and Cain is easily able to decrypt and crack the server password within seconds. Figures 16, 30 and 42 in appendix C shows the cracked passwords of Real VNC server for all three images. VNC password decryptor by (Shadow Production) is also capable of decrypting the Real VNC server password.

The application also stores View only password and Admin password typically encrypted under this value. This is an extra feature in Real VNC that the user can set ViewOnly password or Admin password. With ViewOnly feature the client can only perform limited functions defined by the other computer administrator and Admin feature gives the client, admin privileges with few or no limits on the host computer. Therefore he/she can perform admin functions. This sets a default setting for different users who connect to the computer remotely.

Under `HKEY_LOCAL_MACHINE\Software\RealVNC\VNC Address Book`, this is a saved connection of a client for future quick connection; it typically behaves like a bookmark. Under this registry key the application saves an encrypted master password. This password encrypts the address book which contains the connection settings including the remote connection password. However the master password had strong encryption used by the application and could not be decrypted to view the connection settings and password.

5.3.2 File System

Real VNC leaves log information under event viewer in application log the same way as Ultra VNC. The log information contains the client IP address and what time and date the connection was received by the computer. Therefore the log contains only the receiving client IP address and not showing that the host computer sent the remote connection to the client. The log also contains whether the client disconnected or host computer discontinued the connection. This is same to Ultra VNC application. This information can be useful as investigators can check the date and time of the connections made.

Real VNC stores address book under C:\Documents and Settings\Administrator\Application Data\RealVNC, the address book is like a bookmark that contains saved VNC connections for quick future connection. The address book is typically encrypted unless the user disables the encryption while saving the address book. Real VNC does not save any other log information under the file system. Since the application is capable and supports file transfer, it does not log any information relating to file transfer.

5.4 Tight VNC

5.4.1 Windows Registry

Tight VNC only leaves the application server session password which is usually encrypted by 3DES and is placed under `HKEY_LOCAL_MACHINE\Software\TightVNC\Server`. The key value only contains the server password and connection settings. The application does not leave any history of client IP addresses the host computer initiated remote connection with. The application has same features in all three images. As like Ultra VNC and Real VNC Tight VNC's server password vulnerable too and can be decrypted by Abel & Cain and VNC password decryptor tool. This is because of the weak encryption standards used by the applications. Figures 20, 34 and 46 placed under appendix C shows the decrypted passwords of the Tight VNC server for three images respectively.

5.4.2 File System

Tight VNC places a log file under C:\Documents and Settings\Administrator\Application Data\TightVNC. The folder contains a log file of the application, however the file is empty and no log information is displayed, despite the connections. This came to a surprise as the application has an option of enabling the log file, but still no connection information is logged in the file. The application does not leave any log information under the event viewer. The application also supports file transfer feature but no log information is kept on the computer. This is a drawback for a forensic investigator as no important artefacts are left behind the application.

5.5 Team Viewer

5.5.1 Windows Registry

Team Viewer does not work like the VNC applications and it uses TCP protocol and HTTP port 80 for remote connection. Therefore the settings and display is different from VNC applications mentioned above. The application usually stores and leaves some artefacts in the registry. Under `HKEY_CURRENT_USER \Software\TeamViewer\Version5`, the application stores the history of the client IDs, the local computer connected to. Now Team Viewer does not use client IP addresses for connection, instead it generates a client ID for connection and the ID needs to be passed to the host computer for the connection to work. Also the password for the connection is generated by the application and needs to be passed to the host computer for connection. The password is typically four characters long and normally figures. The application uses Advanced Encryption Standard (AES) to encrypt the remote session password.

Under `HKEY_LOCAL_MACHINE\Software\ TeamViewer\Version5`, the application stores the private and public keys of the remote connection and also other settings relating to the connection. The private and public keys are generated during the connection initiation; the encryption is based on RSA public/ private key exchange and is used in a similar form of https/SSL. The PKI (public key infrastructure) prevents Man-in-the-middle attacks between the remote connections.

Under `HKEY_LOCAL_MACHINE\Software\ TeamViewer\Version5`, the application also stores the security password used for connection, typically encrypted with AES encryption standard. The session password is only stored in image 3 and not on other images. However cracking or decrypting the password was not possible as the encryption used is strong.

5.5.2 File System

Team Viewer usually stores the log files under the C:\Documents and Settings\Administrator\Application Data\TeamViewer folder. The folder contains two log files namely; connection file and TeamViewer5_log file. The connection file contains the history of the connections made by the application to the client computer including the date and time for the connection.

TeamViewer5_log file contains all connection information from the point the host computer initiated remote connection with the client computer. The file contains connection settings such date, time of connection, IP address of the host computer, and IP address of the client computer, display settings, keyboard and mouse settings, Team Viewer server IP address, and file transfer log information. This information is important to a forensic investigator as he/she can retrieve the client IP address and also the files transferred during the connection. The log file had information on what files were transferred and where they were placed on the computer.

5.6 Remote Desktop Protocol (RDP)

5.6.1 Windows Registry

Remote desktop protocol by Microsoft does leave artefacts under the registry system. Usually under `HKEY_CURRENT_USER \Software\Microsoft\Terminal Server Client\Default`, the application leaves the history of the clients private IP addresses. As compared to VNC applications, RDP just leaves only client IP address history and no other connection settings. This is case on all images analysed.

In addition in image 3, RDP under `HKEY_CURRENT_USER \Software\Microsoft\Terminal Server Client\Servers`, the service stores the username used for the connection and also the computer name of the client PC. This is not the case on images 1 and 2. From the information one can get the username and the computer name, which the host computer connected to.

5.6.2 File System

RDP does not leave any log information of any kind on the file system.

5.7 Windows Firewall Analysis

Firewall log is another crucial place to find any remote connection log information. Windows firewall log is by default disabled by the Windows operating system, however for the purpose of the research the log was enabled to find any information about the remote connections made by the computer. Firewall log is normally placed under C:\WINDOWS\pfirewall.log, unless the user changes the path settings. The log contains information such as all incoming and outgoing network information of the local network including port numbers, protocols used, IP addresses and date and time. All remote access protocols and applications leave log information in the firewall log file.

5.8 Addressing Research Questions

The research questions mentioned earlier can be answered from the results found during the testing and analysis process. All three questions are addresses and answered individually in this section.

Question 1 – Does the use of remote access protocols on a Windows platform PC produce artefacts?

During the research and analysis of the images, it has been noted that different VNC remote access applications impact differently on Windows platform PC. The applications can also have different impacts on older and newer versions of Windows operating systems.

Therefore to the answer the question we need to understand two aspects. Firstly that it depends on which remote access application is used. This is because this research focused on Ultra VNC, Real VNC, Tight VNC, Team Viewer and RDP more; these are few from many other remote access applications available in the market. Therefore not knowing how other remote access applications behave on the Windows system is conclusive.

Secondly is that the research focused mainly on Windows XP system with different service packs and leaving out other version of Windows operating systems. Different operating systems have diverse impact on the remote access applications, and artefacts left behind these applications can be different from various VNC or remote access applications and various operating systems.

Therefore from the points mentioned above and the results and testing it can be concluded that yes, remote access protocols produce and leave artefacts on Windows platform PC.

Questions 1.1 – If remote access protocols produce any artefacts on a Windows platform PC, then what type of artefacts are produced?

This is a sub question to question 1 above. Remote access protocols leaves artefacts and information such as client private IP addresses the host computer had initiated connections with, date and time of the connections, file transfer log information, host computer VNC server passwords and also RSA private and public keys generated during the remote connection between the two computers.

However above mentioned in question 1 that different remote access protocols and applications produce different artefacts on Windows platform computers. Keeping this in mind a conclusive answer cannot be derived as not all remote access protocols and applications available in the market were analysed in the thesis.

Question 3 – Can a forensic process be developed for the extraction of remote access protocol artefacts from a device using VNC and RDP clients and server?

Firstly a computer forensic procedure and guidelines needs to be understood to answer this question. The computer forensic procedure and guideline is explained earlier in section 4.2. The process of acquisition of the images and analysis used a cryptographic hashing to ensure the original evidence is not changed in any means.

Yes a forensic process can be developed to extract artefacts of remote access protocols form devices using VNC and RDP clients and servers. However the computer forensic procedure and guideline explained earlier needs to be used side by side to produce a forensic process of extraction of artefacts of the remote access protocols from devices.

5.9 Possible Implications of Results

Based on the results derived from the analysis, there are number of likely implications for forensic investigators making use of the method outlined within the thesis.

It was a significant result that remote access protocols and applications do produce and leave artefacts on Windows platform computer systems. In all the three images analysed, artefacts left behind by the remote access applications were found. However it was not possible to do remote desktop connection using RDP on all three images, because of the fact that Windows disables the feature. Also for image 1, VNC applications were not able to configure the Windows firewall automatically therefore connection could not be initiated. For all three images VNC applications and firewall logging in not enable by default, therefore logs cannot be retrieved if disabled. To overcome this, assumptions were made and all the features were enabled to perform successful remote connection between computers and also to retrieve log information about the connections.

However it is possible that the retrieved data and information about the remote access applications and protocols could be used as supportive evidence in court of law. Then again the information could also be used in conjunction to provide additional information to assist during or in an investigation. For example is a computer was seized because of illegal content on the computer and the computer had a remote access application installed, then this means that the host computer made remote connections. If the investigators can be able to retrieve the private IP address used for connection, then they can track the remote computer and seize the computer for analysis of illegal content.

There are few limitations of the data and information retrieved from the images, which may prevent its use as potential primary evidence in court of law. However, this does not signify that the artefacts found during the analysis are not of a practical value to a potential forensic investigator.

6.0 CONCLUSION

Remote access protocols and applications provide a unique graphical user interface access to users to remote computers. Therefore the users can connect to a remote computer using remote desktop applications and perform tasks and functions as if they are sited next to the computer. Remote access simply uses a protocol over a TCP/IP connection. Many organisations and individuals use this protocol to monitor and troubleshoot remote computers and systems.

Remote access can be exploited by criminals and internet fraudsters to perform illegal activities and commit crime over the internet. Therefore this has significant potential to law enforcement agencies, government and other investigative agencies, as analysis on the applications may provide a way to track down the suspected cyber criminals.

As the adaption of the remote technologies is increasing, as such the investigators are also gathering forensic methods to recover potential artefacts left behind by theses remote technologies.

Future research in this area needs to be done to find out the degree of information and artefacts left behind by remote access protocols. The reason why further research is needed is that still a large amount of information can be retrieved from different remote applications and on different operating system platforms. Further analysis could potentially provide necessary or important information that is of forensic interest to investigators.

The research conducted and explained in this thesis has demonstrated that it is possible to retrieve any artefacts produced and left behind by the remote access protocols and applications in forensic sound manner. Information such as IP addresses and the server name it connected to, is still important information as the other party can be identified by their private IP address that was used to connect to the computer.

The analysis explained in this thesis will help forensic analysts and investigators to fight cyber crime over the internet.

7.0 REFERENCES

About TCP/IP. (1995). *InformationWeek*, 118.

Arce, I. (2001). Weak authentication in ATT VNC allows man-in-the-middle attack. Retrieved 6 May 2010, from http://www.securiteam.com/securitynews/5ZP0P1535W.html

AT&T Laboratories Cambridge. (1999). VNC - How it works. Retrieved 4th May 2010, 2010, from http://virtuallab.tu-freiberg.de/p2p/p2p/vnc/ug/howitworks.html

Auriemma, L. (2003). Password Recovery. Retrieved 16 April 2010, from http://aluigi.altervista.org/pwdrec.htm

Backfield, J., & Bambenek, J. (2008). Network Security Model. Retrieved 25th August 2010, from http://www.sans.org/reading_room/whitepapers/modeling/network-security-model_32843

Basta, A., & Halton, W. (2008). *Computer security and penetration testing*. United States: Thomson.

Bezroukov, D. N. (2009). VNC -- The Essential Sysadmin Tool. Retrieved 5th August 2010, from http://www.softpanorama.org/Xwindows/vnc.shtml

Briscoe, N. (2000). Understanding The OSI 7-Layer Model. *PC Network Advisor*(120), 2.

Brown, C. L. T. (2006). *Computer evidence collection & preservation*. Hingham, Mass: Charles River Media.

Bunyan, T. (2009). Watching the computers: Function creep allows EU states to use intrusive remote computer searches to target any crime, however minor. *Guardian*. Retrieved from http://www.guardian.co.uk/commentisfree/libertycentral/2009/jun/09/remote-access-surveillance-rootkit

Cain, & Abel. (2010). Cain & Abel. Retrieved 12th June 2010, from http://www.oxid.it/cain.htm

Casey, E. (2002). *Handbook of computer crime investigation*. San Diego, Calif: Academic Press.

Chappell, L., & Tittel, E. (2007). *Guide to TCP/IP*. Boston, Mass: Course Technology.

Ciampa, M. D. (2005). *Security+ guide to network security fundamentals*. Boston, Mass: Thomson/Course Technology.

Ciccarelli, P., & Faulkner, C. (2004). *Networking foundations*. Carlifornia: SYBEX Inc.

Cisco. (2010). Internetworking Technology Handbook Available from http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Intro-to-Internet.html#wp1023945

Comer, D. E. (2006). *Internetworking with TCP/IP, Principles, Protocols, and Architecture*. New Jearsey: Pearson Prentice Hall.

ElcomSoft. (2010). Corporate & forensic solutions. Retrieved 12 April 2010, from http://www.elcomsoft.com/products.html

Family Health International. (2010). Qualitative Research Methods: A Data Collector's Field Guide. Retrieved 15th September 2010, from http://www.fhi.org/nr/rdonlyres/etl7vogszehu5s4stpzb3tyqlpp7rojv4waq37elpbyei3tgmc4ty6dunbccfzxtaj2rvbaubzmz4f/overview1.pdf

Garfinkel, S., & Spafford, G. (2002). *Web Security, Privacy and Commerce*. California: O'Reilly & Associates, Inc.

Green, R. (2004). Using Virtual Network Computing (VNC) to remotely access ODB. Retrieved 4th August 2010, from organizersdb.org/0.9/odbremote.pdf

Hannay, P. (2007). *Acquisition of historical location data in a forensically sound and non-invasive manner for the TomTom One Satellite Navigation Unit.* Edith Cowan University, Perth.

HB171. (2003). *HB171: Guidelines for the management of IT evidence : handbook.* Sydney: Standards Australia.

Hopkins, W. (2000). Quantitative Research Design. Retrieved 10th September 2010, from http://www.sportsci.org/jour/0001/wghdesign.html

Horsfall, B. (2010). *Images of children and young people online*: Australian Criminology of Crime.

Kahate, A. (2003). *Cryptography and Network Security*. New Delhi: Tata McGraw-Hill.

Kozierok, C. M. (2005). The TCP/IP Guide. Retrieved 14th August 2010, from http://www.tcpipguide.com/free/t_IPDatagramGeneralFormat.htm

Kruse, W. G., & Heiser, J. G. (2002). *Computer Forensics: Incident Response Essentials*. Boston, MA: Addison-Wesley.

LaRose, M. (2010). What Are Remote Access Technologies? Retrieved 4th August 2010, 2010, from http://www.ehow.com/about_5046061_remote-access-technologies.html

Longzheng, C., Shengsheng, Y., & Jing-li, Z. (2004). *Research and Implementation of Remote Desktop Protocol Service Over SSL VPN.* Paper presented at the IEEE International Conference on Services Computing.

Luo, V. C. (2007). *Tracing USB Device artefacts on Windows XP operating system for forensic purpose.* Paper presented at the Australian Digital Forensics Conference, Perth.

Mayur, S. D., Thomas, C. R., & Thomas von der, E. (2002). System insecurity â€“ firewalls. *Information Management & Computer Security, 10*(3), 135.

McNab, C. (2008). *Network Security Assessment*. Sebastopol: O'Reilly.

Microsoft Support. (2007). How to view and manage event logs in Event Viewer in Windows XP. Retrieved 13th September 2010, 2010, from http://support.microsoft.com/kb/308427

Microsoft support. (2008). Windows registry information for advanced users. Retrieved 5th May 2010, 2010, from http://support.microsoft.com/kb/256986

MicrosoftSupport. (2007). Understanding the Remote Desktop Protocol. Retrieved 4 April 2010, from http://support.microsoft.com/kb/186607

MicrosoftTechNet. (2005). Configuring Remote Desktop. Retrieved 8 April 2010, from http://technet.microsoft.com/en-us/library/bb457106.aspx

Mike. (2007). Beginners Guide: Remote Access to Computers.   Retrieved 3rd August 2010, 2010, from http://www.pcstats.com/articleview.cfm?articleID=1441

Miller, R. L. (2001). The OSI Model: An Overview.   Retrieved 23th August 2010, from http://www.sans.org/reading_room/whitepapers/standards/osi-model-overview_543

Montoro, M. (2005). Remote Desktop Protocol, the Good the Bad and the Ugly.   Retrieved 9 April 2010, from http://www.oxid.it/downloads/rdp-gbu.pdf

Morris, P. (2001). Understanding Virtual Network Computing. *PC Network Advisor*(130), 9-13.

Nelson, B., Phillips, A., & Steuart, C. (2010). *Guide to computer forensics and investigations*. Boston, Mass: Course Technology.

Nguyen, B. (2004). Linux Dictionary. from http://www.tldp.org/LDP/Linux-Dictionary/html/i.html

Remote PC Access. (2009). The Authorities Have A Tough Time With Remote Access. Retrieved 21st August 2010, from http://www.remotepcaccess.org/authorities-remote-access.html

Richardson, T. (2009). The RFB Protocol.   Retrieved 14 March 2010, from http://www.realvnc.com/docs/rfbproto.pdf

Rita, M. (2003). Denial of Service Attacks. *Beyond Numbers*(429), 20.

Ross, J. (1999). Ways of approaching research : Quantitative Designs.   Retrieved 1st September 2010, 2010, from http://www.fortunecity.com/greenfield/grizzly/432/rra2.htm

Russell, K. (2006). Computer Forensics. *Computerworld, 40*(16), 49.

Russinovich, M. (2000). Inside the Registry *Windows NT magazine* Retrieved 10th September 2010, 2010, from http://technet.microsoft.com/en-us/library/cc750583.aspx

Russinovich, M. (2010). Sysinternals Suite.   Retrieved 14th May 2010, 2010, from http://technet.microsoft.com/en-us/sysinternals/bb842062.aspx

Simoneau, P. (2006). The OSI Model:Understanding the Seven Layers of Computer Networks. Retrieved 19th August 2010, from http://ww2.ost-us.com:5051/White%20Papers/OSIModel.pdf

Steel, C. (2006). *Windows Forensics. The field guide for conducting Corporate Computer Investigation*. Indiana: Wiley Publishing.

Sud, R., & Edelman, K. (2004). *SECUR*. Indiana: Que Publishing.

Technet, M. (2000). Remote Desktop Rrotocol (RDP) Features and Performance. Retrieved 5th May 2010, from http://download.microsoft.com/download/8/4/f/84fc80a7-661f-4c96-b5d6-cf73903b09f2/rdpfandp.doc

TopPasswordSoftwareInc. (2010). Top Password Software Inc. Retrieved 10 April 2010, from http://www.top-password.com/

Tristan, R., Quentin, S.-F., Kenneth, R. W., & Andy, H. (1998). Virtual Network Computing. *IEEE Internet Computing, 2*(1), 33.

Vacca, J. R. (2005). *Computer forensics*. Hingham, Mass: Charles River Media.

Wannous, M., Member, S., IEEE, & Nakano, H. (2010). NVLab, a Networking Virtual Web-Based

Laboratory that Implements Virtualization

and Virtual Network Computing Technologies. *IEEE TRANSACTIONS ON LEARNING TECHNOLOGIES, 3*.

Wannous, M., & Nakano, H. (2010). NVLab, a Networking Virtual Web-Based Laboratory that Implements Virtualization and Virtual Network Computing Technologies. *IEEE TRANSACTIONS ON LEARNING TECHNOLOGIES, 3*.

Watchguard. (2010). Remote Access Security Tops Australian IT Security Manager Priorities in 2011. Retrieved 16th August 2010, 2010, from http://www.computerworld.com.au/mediareleases/11290/remote-access-security-tops-australian-it/

Waugh, T. (2002). VNC Where it came from, where it's going. Retrieved 3/08/2010, from http://cyberelk.net/tim/articles/VNC/

Whitman, M. E., & Mattord, H. J. (2005). *Principles of Information Security*. Massachusetts: Thomson Course Technology.

Wiersma, W. (2000). *Research methods in education*. Boston: Allyn and Bacon.

8.0 APPENDICES

8.1 Appendix A - Hash Values of Images

8.1.1 Image 1 (Windows XP service pack 1)

```
Created By AccessData® FTK® Imager 2.9.0.1385 100406

Case Number: 11.2

Evidence Number: 111

Unique Description:

Examiner: Paresh

----------------------------------------------------------

Information for Z:\C\Users\Kerai\XP1 Image\image1:

Physical Evidentiary Item (Source) Information:

[Drive Geometry]

 Bytes per Sector: 512

 Sector Count: 62,889,064

 Source data size: 30707 MB

 Sector count:    62889064

[Computed Hashes]

 MD5 checksum:    f2a91bafd9ee01d8a124a499a62dd1f4

 SHA1 checksum:   0f6eba6e613ccbf97ed3d1999d41d7dd04432b38

Image Information:

 Acquisition started:   Fri Sep 17 13:27:37 2010

 Acquisition finished:  Fri Sep 17 14:46:30 2010
```

```
Image Verification Results:
 Verification started:  Fri Aug 17 14:46:32 2010
 Verification finished: Fri Aug 17 16:04:20 2010
 MD5 checksum:    f2a91bafd9ee01d8a124a499a62dd1f4 : verified
 SHA1 checksum:   0f6eba6e613ccbf97ed3d1999d41d7dd04432b38 : verified
```

8.1.2 Image 2 (Windows XP service pack 2)

```
Created By AccessData® FTK® Imager 2.9.0.1385 100406
Case Number: 22.2
Evidence Number: 2.02
Examiner: Paresh
--------------------------------------------------------------
Information for Z:\C\Users\Kerai\XP2 Image\image2:
Physical Evidentiary Item (Source) Information:
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 83,866,384
 Source data size: 40950 MB
 Sector count:    83866384
[Computed Hashes]
 MD5 checksum:    d6d402514f01069a0a35481e3dfef7ee
 SHA1 checksum:   c1b5bff1a2204628d4e0347a55f07898b3f9aad4
Image Information:
```

Acquisition started: Fri Sep 17 13:28:30 2010

Acquisition finished: Fri Sep 17 14:23:02 2010

Image Verification Results:

Verification started: Fri Aug 17 14:23:07 2010

Verification finished: Fri Aug 17 16:01:17 2010

MD5 checksum: **d6d402514f01069a0a35481e3dfef7ee** : verified

SHA1 checksum: **c1b5bff1a2204628d4e0347a55f07898b3f9aad4** : verified

8.1.3 Image 3 (Windows XP service pack 3)

Created By AccessData® FTK® Imager 2.9.0.1385 100406

Case Number: 33.3

Evidence Number: 3.03

Examiner: Paresh

Information for Z:\C\Users\Kerai\XP3 Image\image3:

Physical Evidentiary Item (Source) Information:

[Drive Geometry]

Bytes per Sector: 512

Sector Count: 83,866,384

Source data size: 40950 MB

Sector count: 83866384

[Computed Hashes]

MD5 checksum: **5e8488af6f272df4e3571873c6fdae23**

SHA1 checksum: **583c0cea72f74c1a42ba0a6aa9f282cd6ec2b282**

Image Information:

Acquisition started: Fri Aug 17 13:29:25 2010

Acquisition finished: Fri Aug 17 14:30:42 2010

Image Verification Results:

Verification started: Fri Sep 17 14:30:48 2010

Verification finished: Fri Sep 17 15:58:48 2010

MD5 checksum: **5e8488af6f272df4e3571873c6fdae23** : verified

SHA1 checksum: **583c0cea72f74c1a42ba0a6aa9f282cd6ec2b282** : verified

8.2 Appendix B – Files Hash Values

8.2.1 Image 1

8.2.1.1Registry Files

C:\Documents and Settings\Administrator\Desktop\WinXP1 files\Registry files\NTUSER[10857].DAT

MD5: 5b5f05fb894c4e287aa5b6b7012049c0

C:\Documents and Settings\Administrator\Desktop\WinXP1 files\Registry files\SAM[3387]

MD5: 384145787336bc1e1cf51d0ec8a01ff8

C:\Documents and Settings\Administrator\Desktop\WinXP1 files\Registry files\default[3981]

MD5: 20d374c798e34937ac6d548e27efdbad

C:\Documents and Settings\Administrator\Desktop\WinXP1 files\Registry files\system[3184]

MD5: 092521bbfc9f2a1a66acbf3a4da8851e

C:\Documents and Settings\Administrator\Desktop\WinXP1 files\Registry files\software[3212]

MD5: 2d3b5d80abf0bcd9f76866d2e1ba74cb

C:\Documents and Settings\Administrator\Desktop\WinXP1 files\Registry files\userdiff[3370]

MD5: 1fab80c309d2f83fa77c2e7a1f0487c6

C:\Documents and Settings\Administrator\Desktop\WinXP1 files\Registry files\SECURITY[3386]

MD5: bfec81114f03e810257804b295efd355

8.2.1.2Log Files

C:\Documents and Settings\Administrator\Desktop\WinXP1 files\Logs Files\TeamViewer5_Logfile[18804].log

MD5: a21d4f023744d251c99281ee12a99903

C:\Documents and Settings\Administrator\Desktop\WinXP1 files\Logs Files\pfirewall[45017].log

MD5: 96fd3b449c1a8989fda4d3993680e4e1

C:\Documents and Settings\Administrator\Desktop\WinXP1 files\Logs Files\Connections[45057].txt

MD5: d37e1ace413e7f2a2a1bf46e3dc1b49e

C:\Documents and Settings\Administrator\Desktop\WinXP1 files\Logs Files\WinVNC[45025].log

MD5: cec3aa75382c3ac49cb8b9d8ef173cad

8.2.1.3Event viewer log files

C:\Documents and Settings\Administrator\Desktop\WinXP1 files\Event Log files\SysEvent[3402].Evt

MD5: 915be121d5586cce366191ac50c4aca0

C:\Documents and Settings\Administrator\Desktop\WinXP1 files\Event Log files\SecEvent[3401].Evt

MD5: 4407052e2885c8319711f5112fafaf5c

C:\Documents and Settings\Administrator\Desktop\WinXP1 files\Event Log files\AppEvent[3400].Evt

MD5: bb598b69b27ddf3b2b2ba73749bb641c

8.2.2 Image 2

8.2.2.1Registry Files

C:\Documents and Settings\Administrator\Desktop\WinxXP2 files\Registry Files\system[1984]

MD5: 9170c77cb552d580bc66dd084c4ff3c2

C:\Documents and Settings\Administrator\Desktop\WinxXP2 files\Registry Files\software[3530]

MD5: 572f1db209708a3c11500edb279f787d

C:\Documents and Settings\Administrator\Desktop\WinxXP2 files\Registry Files\SECURITY[3669]

MD5: 8d74376143063d448098b145486c9b81

C:\Documents and Settings\Administrator\Desktop\WinxXP2 files\Registry Files\SAM[3670]

MD5: e12bd3be4b5f7dc1d58f18b04b8236f6

C:\Documents and Settings\Administrator\Desktop\WinxXP2 files\Registry Files\NTUSER[11136].DAT

MD5: 4dc97f85b3d2dc3b17bd2e799d8385a2

C:\Documents and Settings\Administrator\Desktop\WinxXP2 files\Registry Files\default[4379]

MD5: a9582516acc281b3b793c868e724eb8e

8.2.2.2Log Files

C:\Documents and Settings\Administrator\Desktop\WinxXP2 files\Log files\WinVNC[25353].log

MD5: d46c3d0cfb9cb0fd8f888365b868b944

C:\Documents and Settings\Administrator\Desktop\WinxXP2 files\Log files\TeamViewer5_Logfile[20141].log

MD5: 5b32650d62e6e2f4a89d013747b4c647

C:\Documents and Settings\Administrator\Desktop\WinxXP2 files\Log files\pfirewall[25315].log

MD5: 8a3d89ffd21f0e8b38ab73238c0942fa

C:\Documents and Settings\Administrator\Desktop\WinxXP2 files\Log files\mslogon[20170].log

MD5: b839fd303484f396cef8dc4121f1d259

C:\Documents and Settings\Administrator\Desktop\WinxXP2 files\Log files\Connections_incoming[20295].txt

MD5: dea50d23214f3774896cc863115744dd

C:\Documents and Settings\Administrator\Desktop\WinxXP2 files\Log files\Connections[18432].txt

MD5: fa9b5376fb1e832ddda7d2a7afebd892

8.2.2.3Event viewer log files

C:\Documents and Settings\Administrator\Desktop\WinxXP2 files\Event log files\AppEvent[3684].Evt

MD5: 901d9a778151802787b598ca6e625e8e

C:\Documents and Settings\Administrator\Desktop\WinxXP2 files\Event log files\SysEvent[3686].Evt

MD5: c0f699d332db06468af9d8e0ce2d9bd4

C:\Documents and Settings\Administrator\Desktop\WinxXP2 files\Event log files\SecEvent[3685].Evt

MD5: 4407052e2885c8319711f5112fafaf5c

8.2.3 Image 3

8.2.3.1Registry Files

C:\Documents and Settings\Administrator\Desktop\WinXP3 files\Registry files\system[1863]

MD5: 7df5d9bda3349d2d9fbe2906c936d04d

C:\Documents and Settings\Administrator\Desktop\WinXP3 files\Registry files\software[3668]

MD5: f9f9bf5d147ab43e373e5378294d0e13

C:\Documents and Settings\Administrator\Desktop\WinXP3 files\Registry files\SECURITY[3826]

MD5: 21da7de2ef9392e0262744f114545960

C:\Documents and Settings\Administrator\Desktop\WinXP3 files\Registry files\SAM[3827]

MD5: 2c4f39c511790ac68eaa329fc3f849c1

C:\Documents and Settings\Administrator\Desktop\WinXP3 files\Registry files\NTUSER[11724].DAT

MD5: 869c39e4509d7410a303069ca9321b7f

C:\Documents and Settings\Administrator\Desktop\WinXP3 files\Registry files\default[4535]

MD5: bdd6fd6cd17d93160ab01c9fdb0e421f

8.2.3.2Log Files

C:\Documents and Settings\Administrator\Desktop\WinXP3 files\Log files\WinVNC[17457].log

MD5: bcf17c95174a6a3d7b01e2e6444fab45

C:\Documents and Settings\Administrator\Desktop\WinXP3 files\Log files\vncchat[24112].xml

MD5: 3d396f69a5a5e528efcf492fedf06dda

C:\Documents and Settings\Administrator\Desktop\WinXP3 files\Log files\TeamViewer5_Logfile[13670].log

MD5: 51f5d56cde228dff3d288f3fcbf28dd6

C:\Documents and Settings\Administrator\Desktop\WinXP3 files\Log files\pfirewall[17467].log

MD5: b0c41ec13bc3e9b0bde6973a47452c31

C:\Documents and Settings\Administrator\Desktop\WinXP3 files\Log files\mslogon.log

MD5: 5c2c770c1caf67d3a6ca0803afdc858f

C:\Documents and Settings\Administrator\Desktop\WinXP3 files\Log files\Connections_incoming[52021].txt

MD5: 8b9699af6df64d16125c498a53f70345

C:\Documents and Settings\Administrator\Desktop\WinXP3 files\Log files\Connections[13673].txt

MD5: bc980ce05789031852c9514dc3f3e26f

8.2.3.3Event viewer log files

C:\Documents and Settings\Administrator\Desktop\WinXP3 files\Event log files\SecEvent[3842].Evt

MD5: 4407052e2885c8319711f5112fafaf5c

C:\Documents and Settings\Administrator\Desktop\WinXP3 files\Event log files\SysEvent[3843].Evt

MD5: aac1e0c0ac8ff4b0874a3f2d9dcc29eb

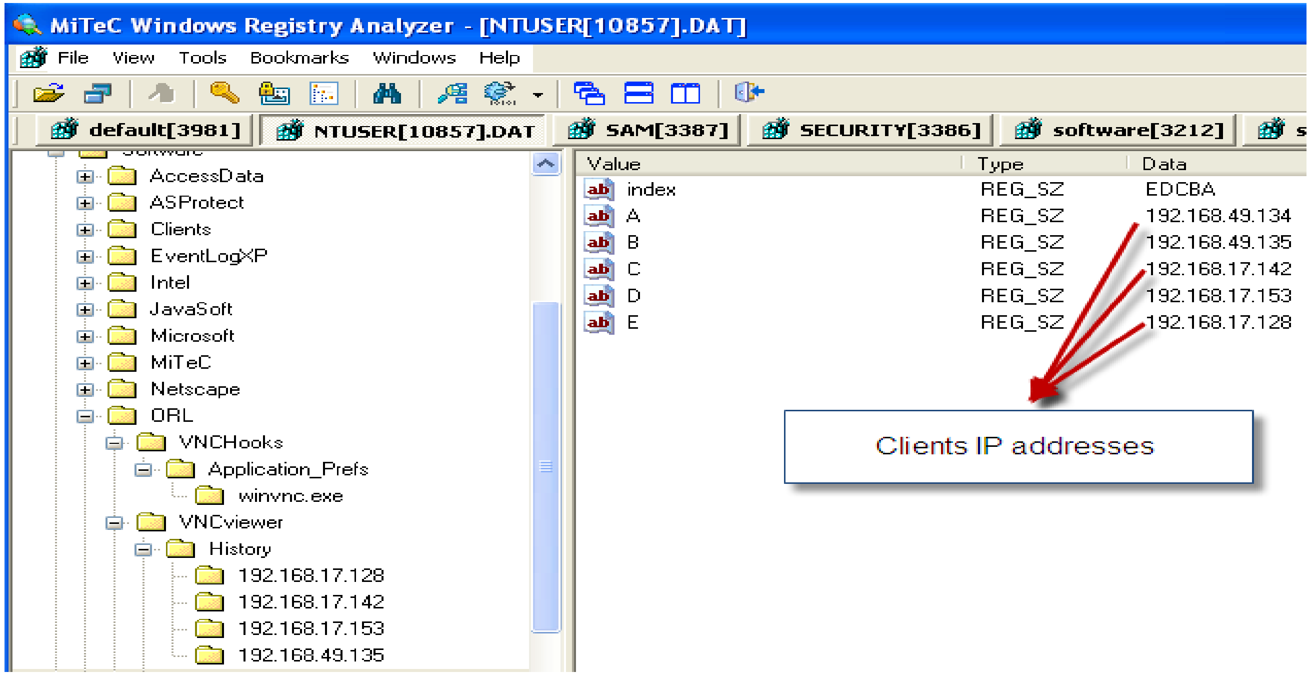
C:\Documents and Settings\Administrator\Desktop\WinXP3 files\Event log files\AppEvent[3841].Evt

MD5: fdfca99bc5b88e776dcaa8c72ac7ebaa

8.3 Appendix C - Registry Analysis

8.3.1 Image 1

Figure 10 shows how UltraVNC stores the client private IP addresses under regisrty HKEY_CURRENT_USER\Software\ORL\VNCviewer\History. The IP addresses shown are the addresses the local computer initiated remote connection using UltraVNC viewer.

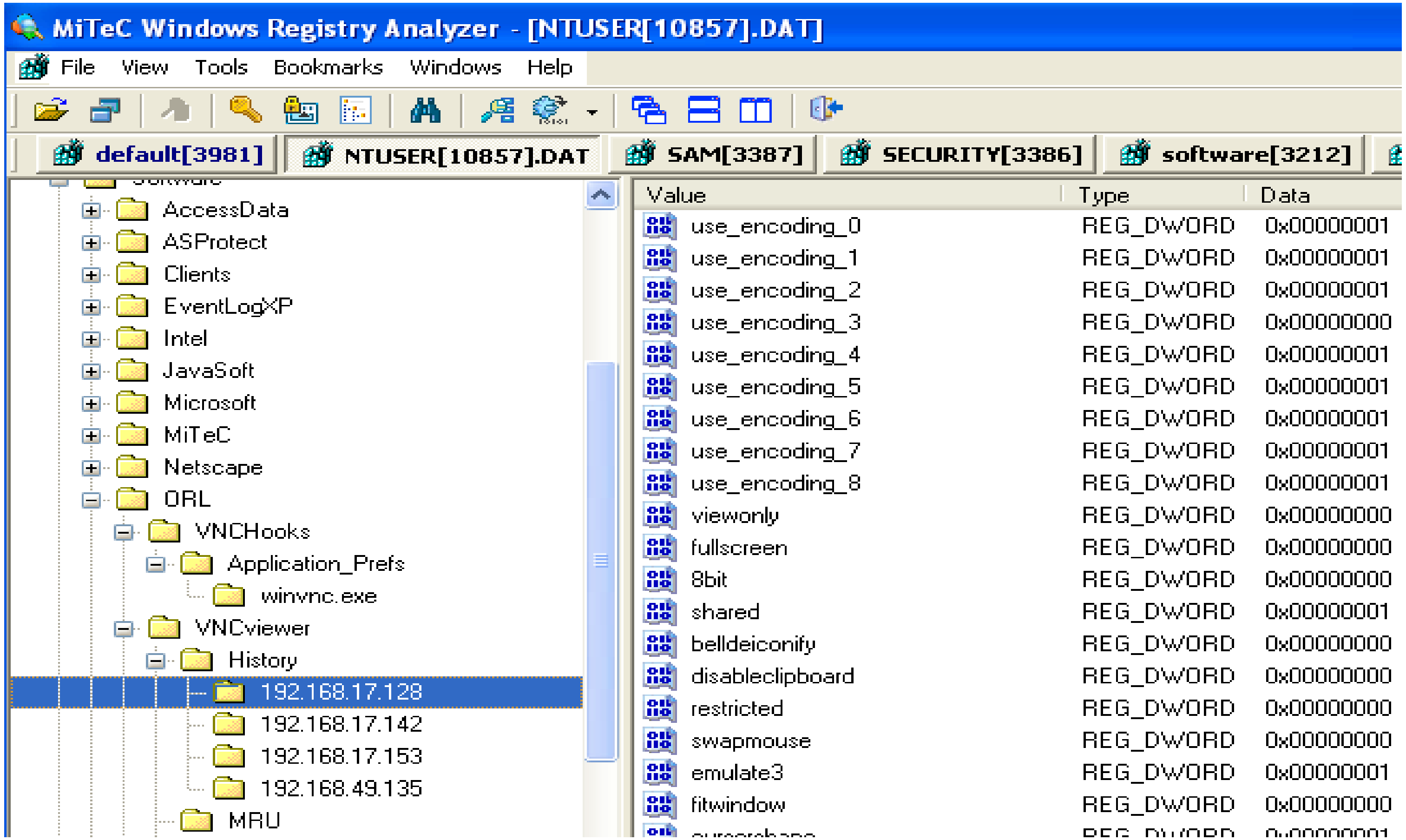


Value	Type	Data
index	REG_SZ	EDCBA
A	REG_SZ	192.168.49.134
B	REG_SZ	192.168.49.135
C	REG_SZ	192.168.17.142
D	REG_SZ	192.168.17.153
E	REG_SZ	192.168.17.128

Clients IP addresses

Figure 10 UltraVNC shows client IP addreses

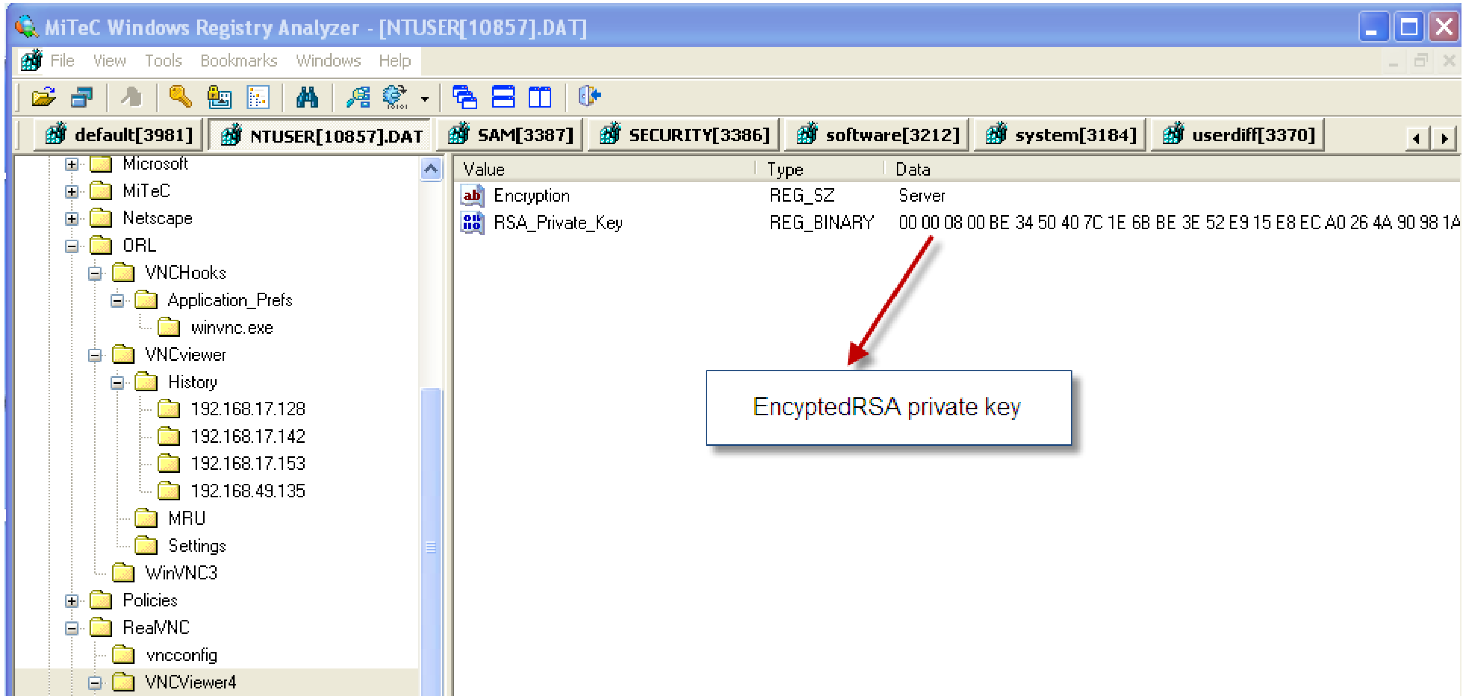
The figure 11 below shows the connection settings of a particular client that the local computer and the client computer negotiated during the connection.



Value	Type	Data
use_encoding_0	REG_DWORD	0x00000001
use_encoding_1	REG_DWORD	0x00000001
use_encoding_2	REG_DWORD	0x00000001
use_encoding_3	REG_DWORD	0x00000000
use_encoding_4	REG_DWORD	0x00000001
use_encoding_5	REG_DWORD	0x00000001
use_encoding_6	REG_DWORD	0x00000001
use_encoding_7	REG_DWORD	0x00000001
use_encoding_8	REG_DWORD	0x00000001
viewonly	REG_DWORD	0x00000000
fullscreen	REG_DWORD	0x00000000
8bit	REG_DWORD	0x00000000
shared	REG_DWORD	0x00000001
belldeiconify	REG_DWORD	0x00000000
disableclipboard	REG_DWORD	0x00000000
restricted	REG_DWORD	0x00000000
swapmouse	REG_DWORD	0x00000000
emulate3	REG_DWORD	0x00000001
fitwindow	REG_DWORD	0x00000000

Figure 11 UltraVNC client connection settings

Figure 12 below shows where the RealVNC stores RSA encrypted private key that was created during the connection in the registry under HKEY_CURRENT_USER \Software\RealVNC\vncconfig and also shows the encryption type the application is using. In this case the VNC server decides on the encryption type to use during the connection.

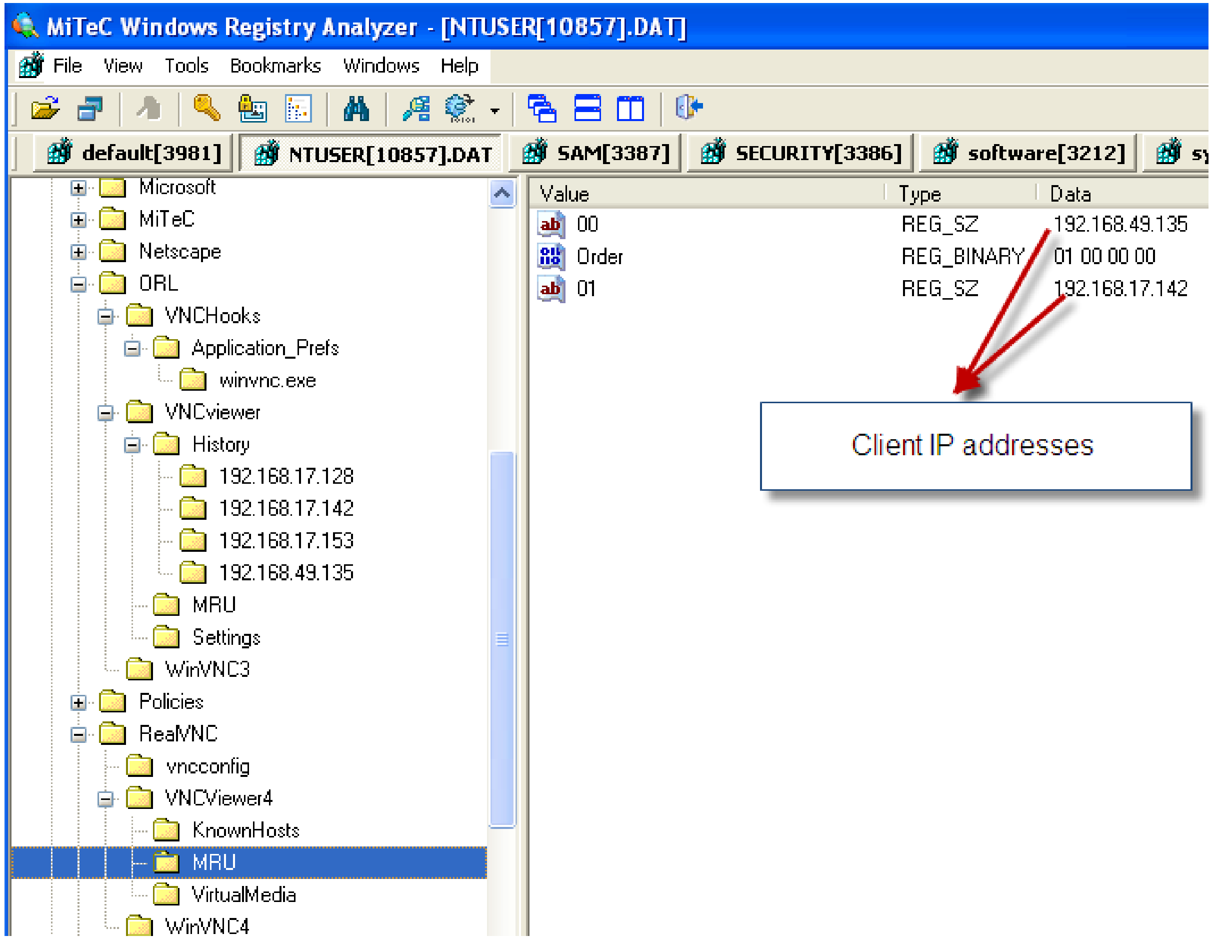


Value	Type	Data
Encryption	REG_SZ	Server
RSA_Private_Key	REG_BINARY	00 00 08 00 BE 34 50 40 7C 1E 6B BE 3E 52 E9 15 E8 EC A0 26 4A 90 98 1A

EncryptedRSA private key

Figure 12 RealVNC RSA Private Key in registry

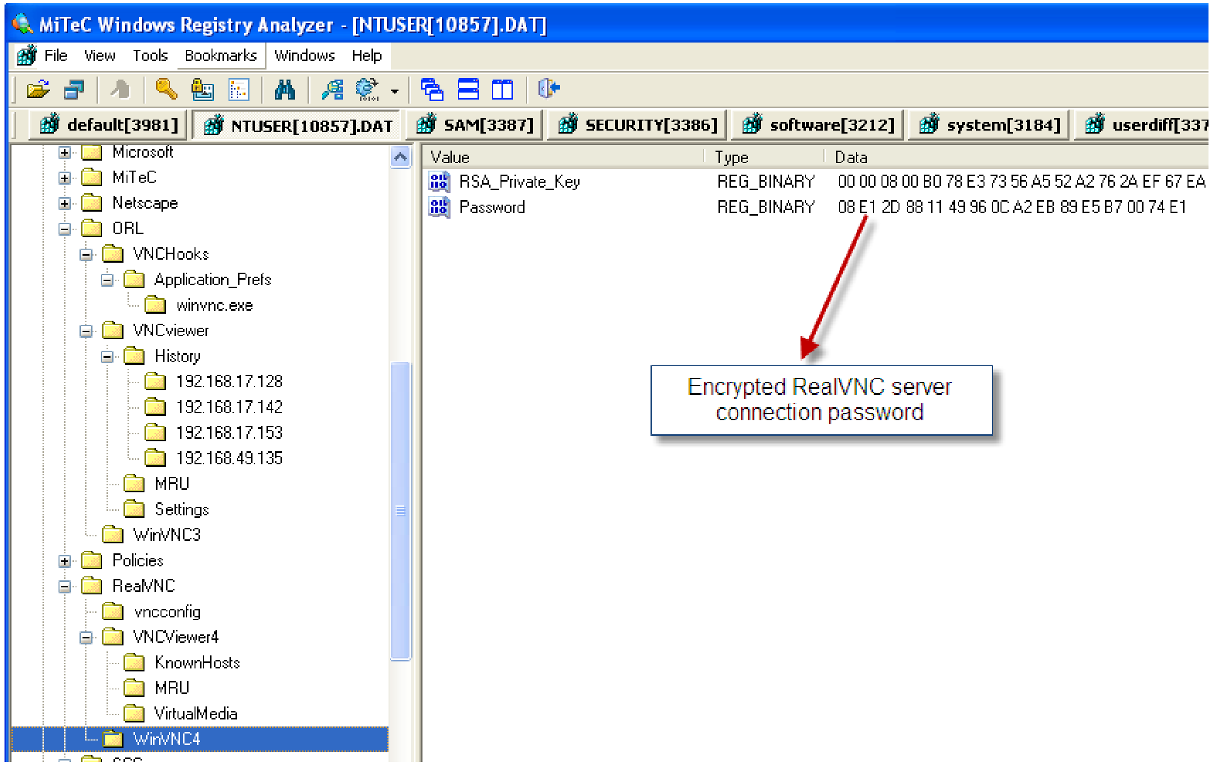
Figure 13 shows the RealVNC connection history of the client IP addresses the local computer initiated connection. The value is found under Under HKEY_CURRENT_USER \Software\RealVNC\VNCViewer4\MRU.



Value	Type	Data
00	REG_SZ	192.168.49.135
Order	REG_BINARY	01 00 00 00
01	REG_SZ	192.168.17.142

Figure 13 RealVNC Clients IP addresses

Figure 14 below shows where RealVNC places the local computer's VNC server password. It is typically encrypted with 3DES. Note that this password is of the local computer and not of the client's VNC server password. The values are stored under HKEY_LOCAL_MACHINE\Software\RealVNC\WinVNC4

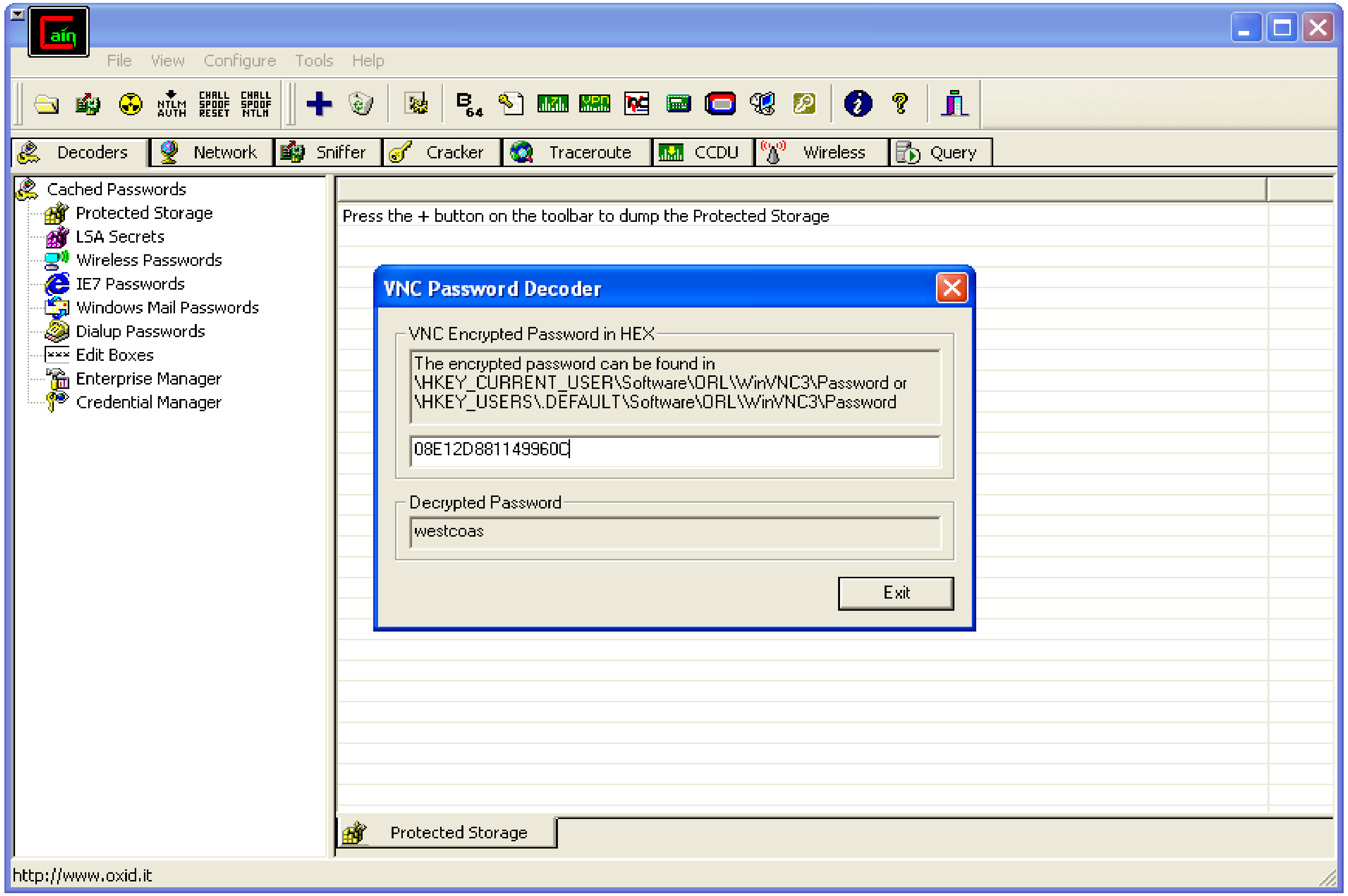


Value	Type	Data
RSA_Private_Key	REG_BINARY	00 00 08 00 B0 78 E3 73 56 A5 52 A2 76 2A EF 67 EA
Password	REG_BINARY	08 E1 2D 88 11 49 96 0C A2 EB 89 E5 B7 00 74 E1

Encrypted RealVNC server connection password

Figure 14 RealVNC server encrypted password in registry

Figure 15 below shows the decrypted password for the RealVNC found under the registry above using Abel and Cain software. The tool attacks VNC passwords of up to 8 character long and use 3DES encryption. Therefore it is the ideal tool to decrypt VNC server password. The decrypted password is westcoas



Press the + button on the toolbar to dump the Protected Storage

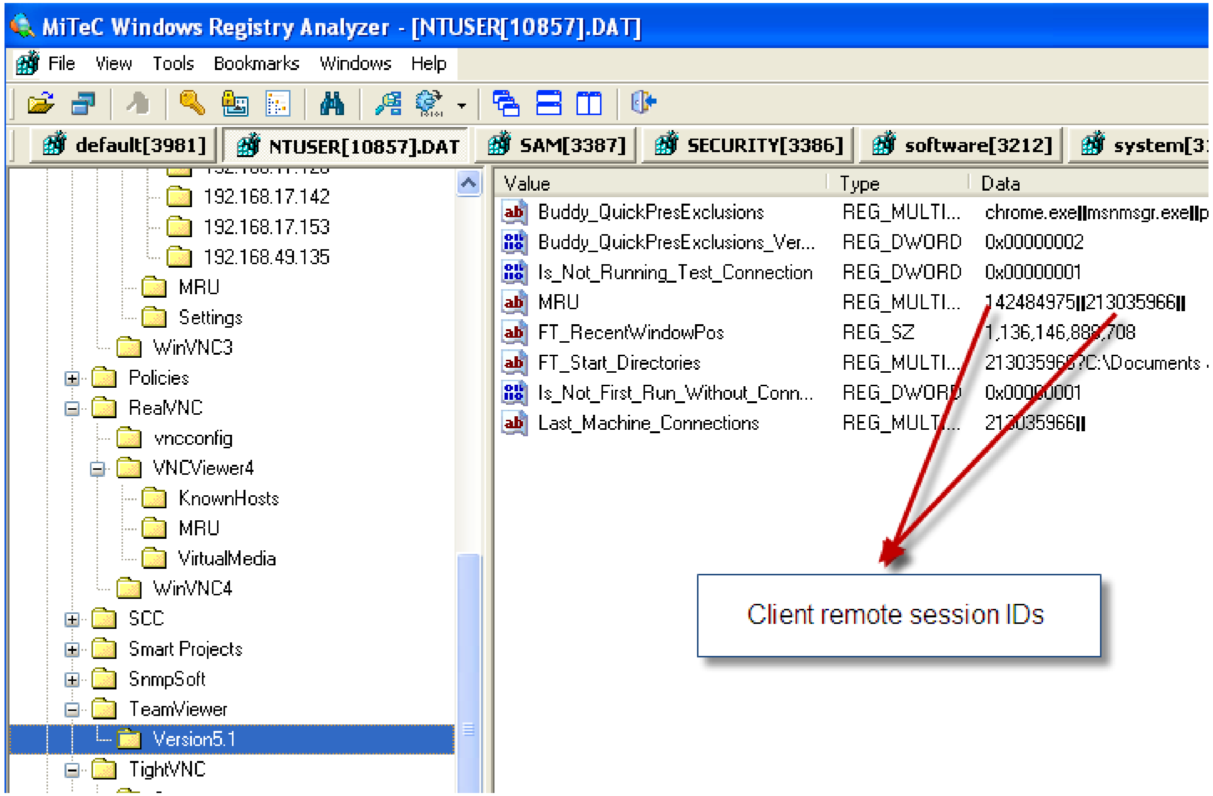
The encrypted password can be found in
\HKEY_CURRENT_USER\Software\ORL\WinVNC3\Password or
\HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3\Password

VNC Encrypted Password in HEX: 08E12D881149960C

Decrypted Password: westcoas

Figure 15 RealVNC decrypted password using Abel and Cain

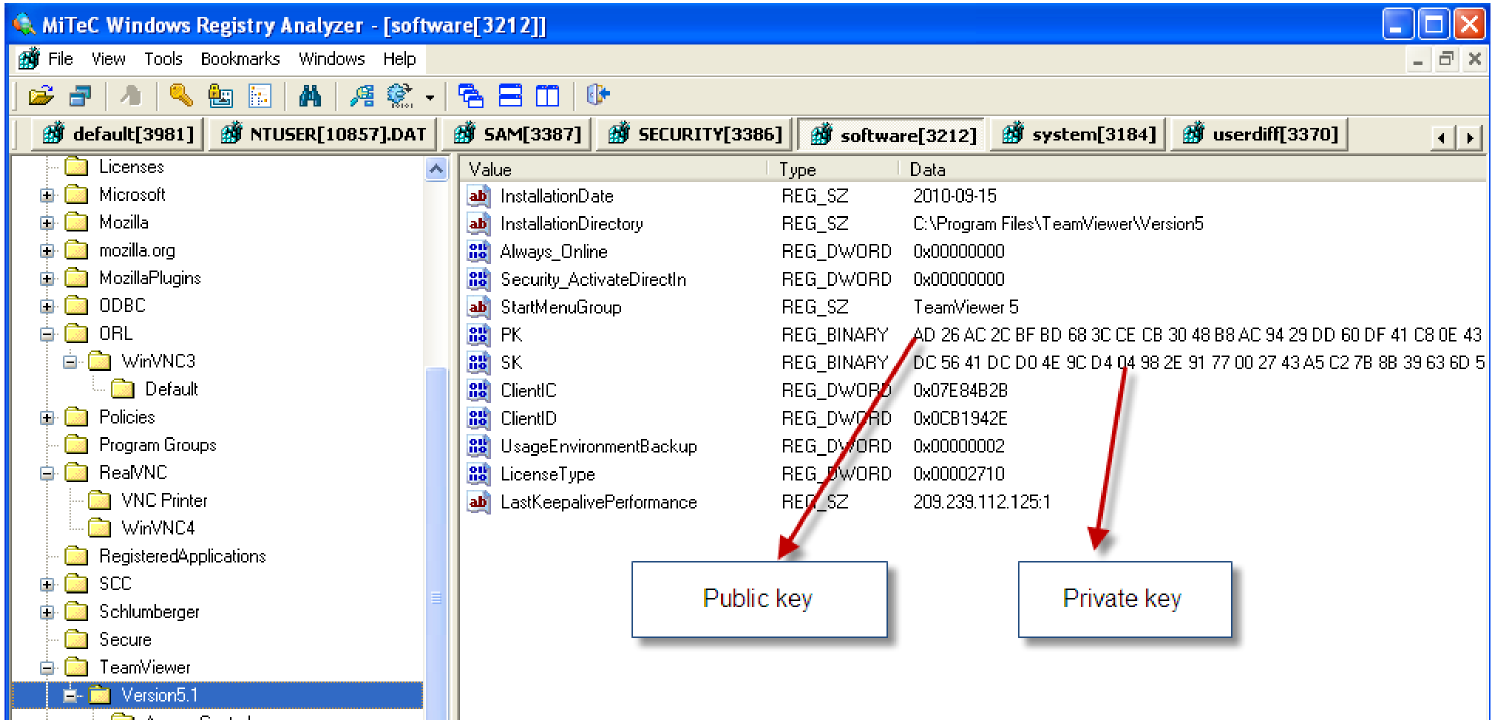
TeamViewer also stores the client connection IDs that the local computer connected to, and also the connection settings as shown in figure 16 below. This is typically stored under Under HKEY_CURRENT_USER \Software\TeamViewer\Version5.



Value	Type	Data
Buddy_QuickPresExclusions	REG_MULTI...	chrome.exe‖msnmsgr.exe‖p
Buddy_QuickPresExclusions_Ver...	REG_DWORD	0x00000002
Is_Not_Running_Test_Connection	REG_DWORD	0x00000001
MRU	REG_MULTI...	142484975‖213035966‖
FT_RecentWindowPos	REG_SZ	1,136,146,888,708
FT_Start_Directories	REG_MULTI...	213035966?C:\Documents
Is_Not_First_Run_Without_Conn...	REG_DWORD	0x00000001
Last_Machine_Connections	REG_MULTI...	213035966‖

Figure 16 TeamViewer client IDs

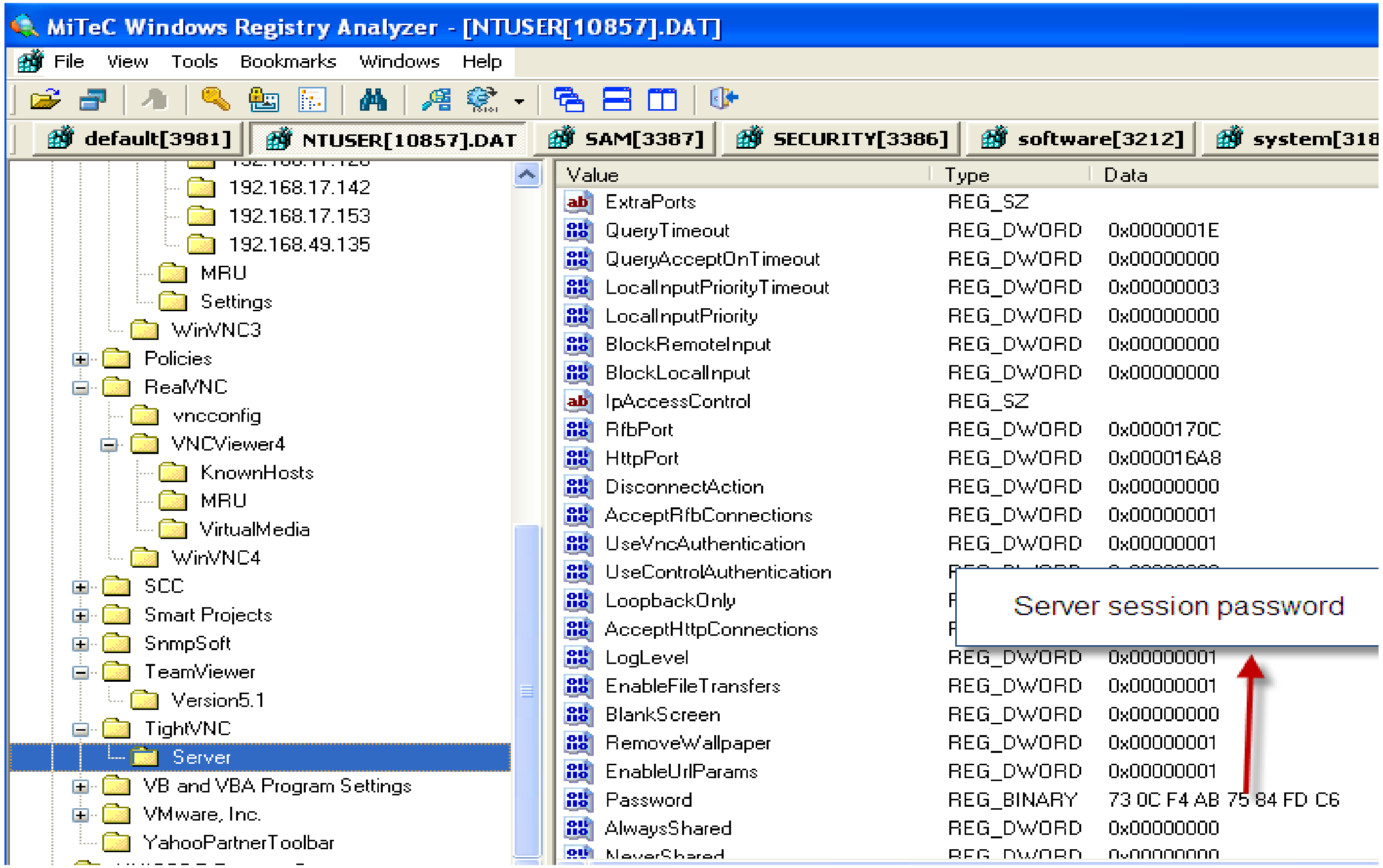
Figure 17 below shows the encrypted private and public keys stored in the registry under HKEY_LOCAL_MACHINE\Software\TeamViewer\Version5. These keys are generated when the client and local computer initiate the connection. The keys are typically encrypted with RSA cipher encryption algorithm.



Value	Type	Data
InstallationDate	REG_SZ	2010-09-15
InstallationDirectory	REG_SZ	C:\Program Files\TeamViewer\Version5
Always_Online	REG_DWORD	0x00000000
Security_ActivateDirectIn	REG_DWORD	0x00000000
StartMenuGroup	REG_SZ	TeamViewer 5
PK	REG_BINARY	AD 26 AC 2C BF BD 68 3C CE CB 30 48 B8 AC 94 29 DD 60 DF 41 C8 0E 43
SK	REG_BINARY	DC 56 41 DC D0 4E 9C D4 04 98 2E 91 77 00 27 43 A5 C2 7B 8B 39 63 6D 5
ClientIC	REG_DWORD	0x07E84B2B
ClientID	REG_DWORD	0x0CB1942E
UsageEnvironmentBackup	REG_DWORD	0x00000002
LicenseType	REG_DWORD	0x00002710
LastKeepalivePerformance	REG_SZ	209.239.112.125:1

Figure 17 TeamViewer encrypted private and public stored under registry

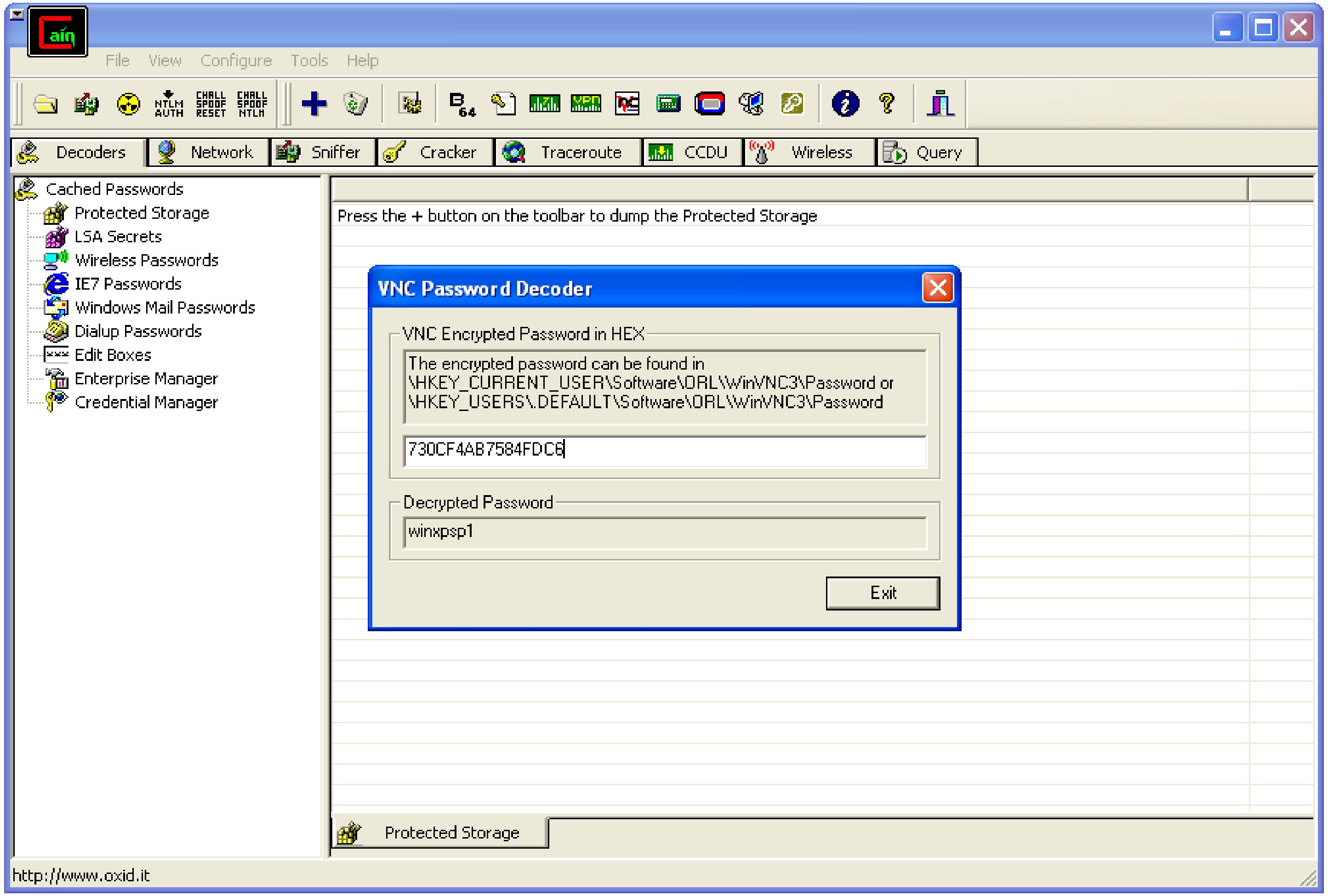
TightVNC also stores the local computers TightVNC server password in the registry under value HKEY_LOCAL_MACHINE\Software\TightVNC\Server. The application also stores the connection and application settings. However as to other VNC applications, it does not save any connection history of the client machines, that the local computer connected to. This is shown in the figure 18 below.



Value	Type	Data
ExtraPorts	REG_SZ	
QueryTimeout	REG_DWORD	0x0000001E
QueryAcceptOnTimeout	REG_DWORD	0x00000000
LocalInputPriorityTimeout	REG_DWORD	0x00000003
LocalInputPriority	REG_DWORD	0x00000000
BlockRemoteInput	REG_DWORD	0x00000000
BlockLocalInput	REG_DWORD	0x00000000
IpAccessControl	REG_SZ	
RfbPort	REG_DWORD	0x0000170C
HttpPort	REG_DWORD	0x000016A8
DisconnectAction	REG_DWORD	0x00000000
AcceptRfbConnections	REG_DWORD	0x00000001
UseVncAuthentication	REG_DWORD	0x00000001
UseControlAuthentication	[illegible]	[illegible]
LoopbackOnly	[illegible]	[illegible]
AcceptHttpConnections	[illegible]	[illegible]
LogLevel	REG_DWORD	0x00000001
EnableFileTransfers	REG_DWORD	0x00000001
BlankScreen	REG_DWORD	0x00000000
RemoveWallpaper	REG_DWORD	0x00000001
EnableUrlParams	REG_DWORD	0x00000001
Password	REG_BINARY	73 0C F4 AB 75 84 FD C6
AlwaysShared	REG_DWORD	0x00000000
NeverShared	REG_DWORD	0x00000000

Figure 18 TightVNC server session encrypted password stored in registry

The figure 19 below shows the TightVNC decrypted password by Abel and Cain tool. Basically just type in the encypted password found under the registry and Abel and Cain will decrypt and show the server password. As shown below winxpsp1 was the decrypted password.



Press the + button on the toolbar to dump the Protected Storage

VNC Password Decoder

VNC Encrypted Password in HEX

The encrypted password can be found in
\HKEY_CURRENT_USER\Software\ORL\WinVNC3\Password or
\HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3\Password

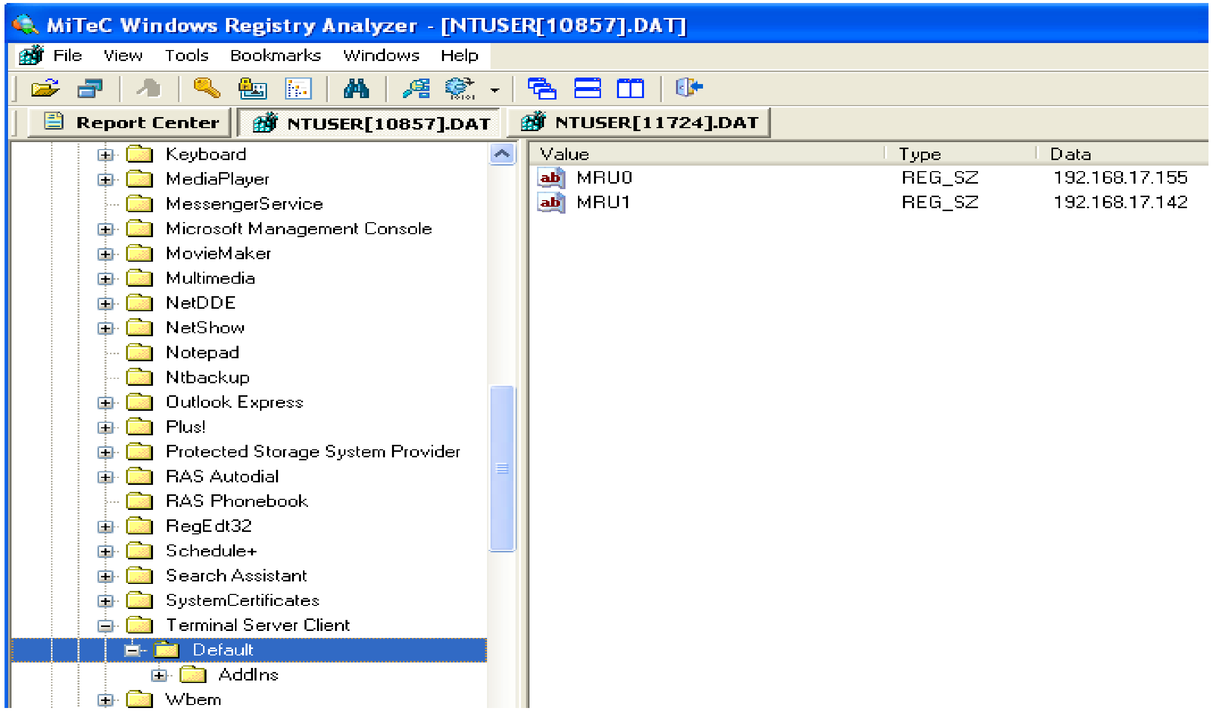
730CF4AB7584FDC6

Decrypted Password

winxpsp1

Figure 19 TightVNC decrypted password using Abel and Cain

Figure 20 shows the client connection history saved by the RDP under the value HKEY_CURRENT_USER \Software\Microsoft\Terminal Server Client\Default. These are again the private IP addresses of the client.



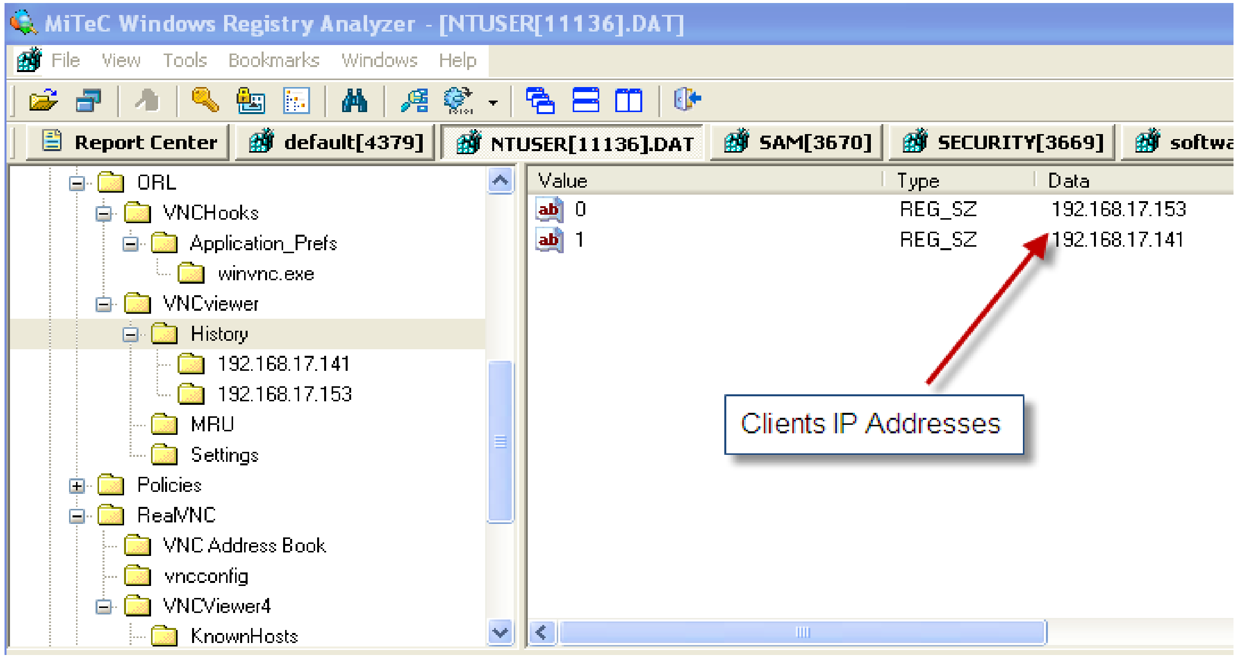
Value	Type	Data
MRU0	REG_SZ	192.168.17.155
MRU1	REG_SZ	192.168.17.142

Figure 20 Remote desktop protocol settings

8.3.2 Image 2

The figures below shows the settings and artefacts left behing by UltaVNC, RealVNC, TightVNC, TeamViewer and RDP on Windows XP serive pack 2.

Figure 21 shows how UltraVNC stores the client private IP addresses under regisrty HKEY_CURRENT_USER\Software\ORL\VNCviewer\History. The IP addresses shown are the addresses the local computer initiated remote connection using UltraVNC viewer.

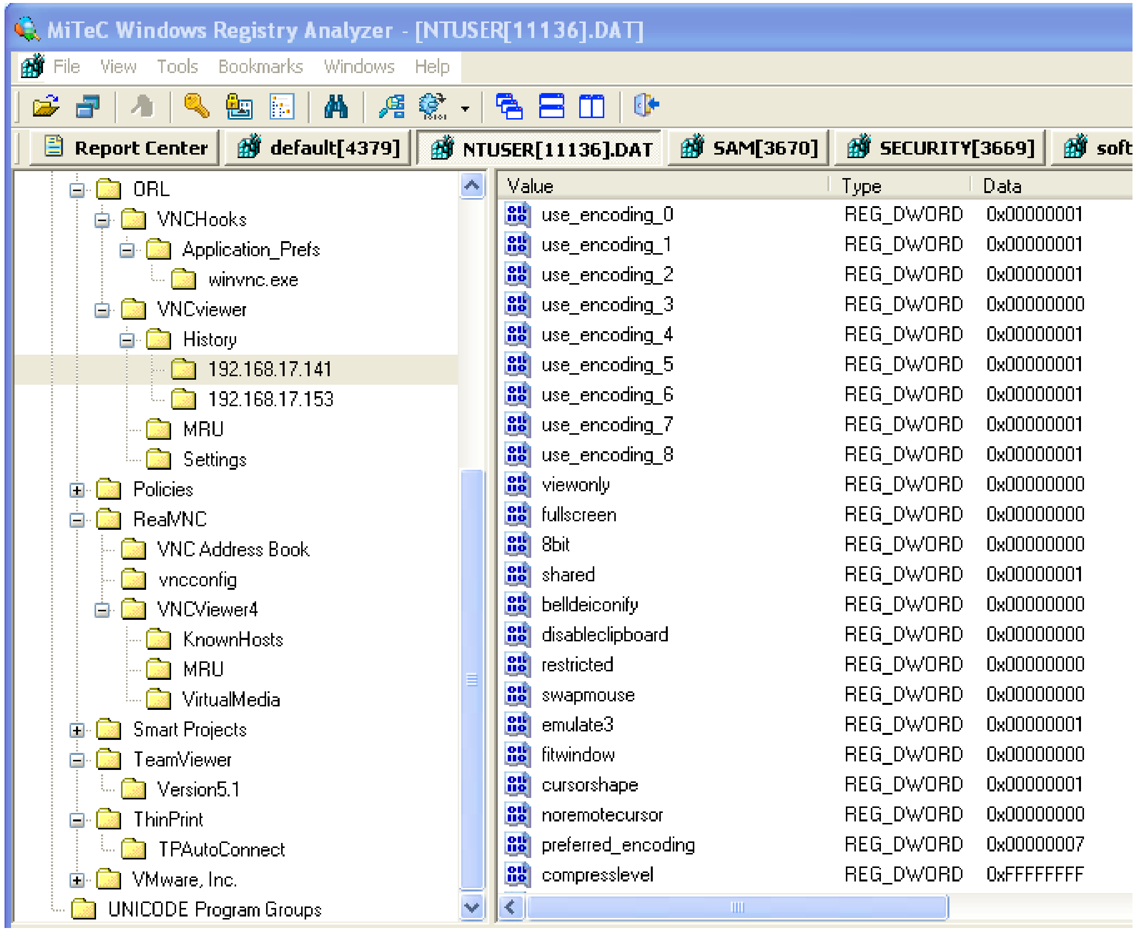


Value	Type	Data
ab 0	REG_SZ	192.168.17.153
ab 1	REG_SZ	192.168.17.141

Clients IP Addresses

Figure 21 UltraVNC shows client IP addresses

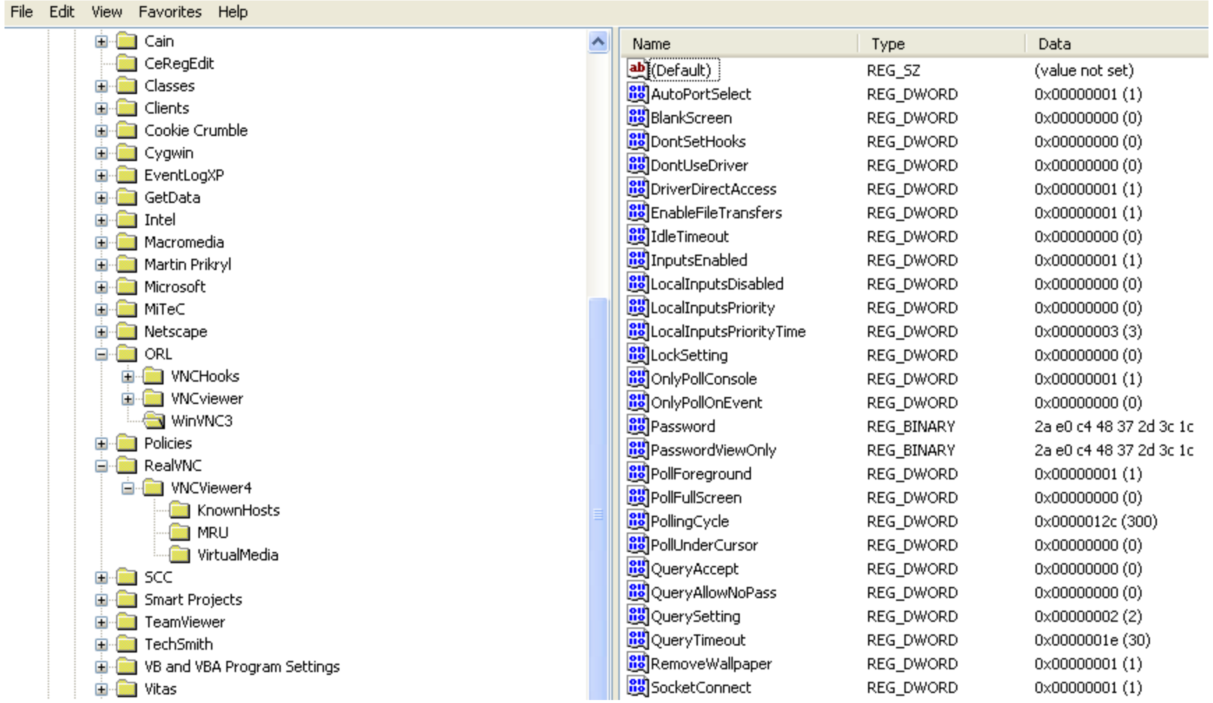
The figure 22 below shows the connection settings of a particular client that the local computer and the client computer negotiated during the connection.



Value	Type	Data
use_encoding_0	REG_DWORD	0x00000001
use_encoding_1	REG_DWORD	0x00000001
use_encoding_2	REG_DWORD	0x00000001
use_encoding_3	REG_DWORD	0x00000000
use_encoding_4	REG_DWORD	0x00000001
use_encoding_5	REG_DWORD	0x00000001
use_encoding_6	REG_DWORD	0x00000001
use_encoding_7	REG_DWORD	0x00000001
use_encoding_8	REG_DWORD	0x00000001
viewonly	REG_DWORD	0x00000000
fullscreen	REG_DWORD	0x00000000
8bit	REG_DWORD	0x00000000
shared	REG_DWORD	0x00000001
belldeiconify	REG_DWORD	0x00000000
disableclipboard	REG_DWORD	0x00000000
restricted	REG_DWORD	0x00000000
swapmouse	REG_DWORD	0x00000000
emulate3	REG_DWORD	0x00000001
fitwindow	REG_DWORD	0x00000000
cursorshape	REG_DWORD	0x00000001
noremotecursor	REG_DWORD	0x00000000
preferred_encoding	REG_DWORD	0x00000007
compresslevel	REG_DWORD	0xFFFFFFFF

Figure 22 UltraVNC client connection settings

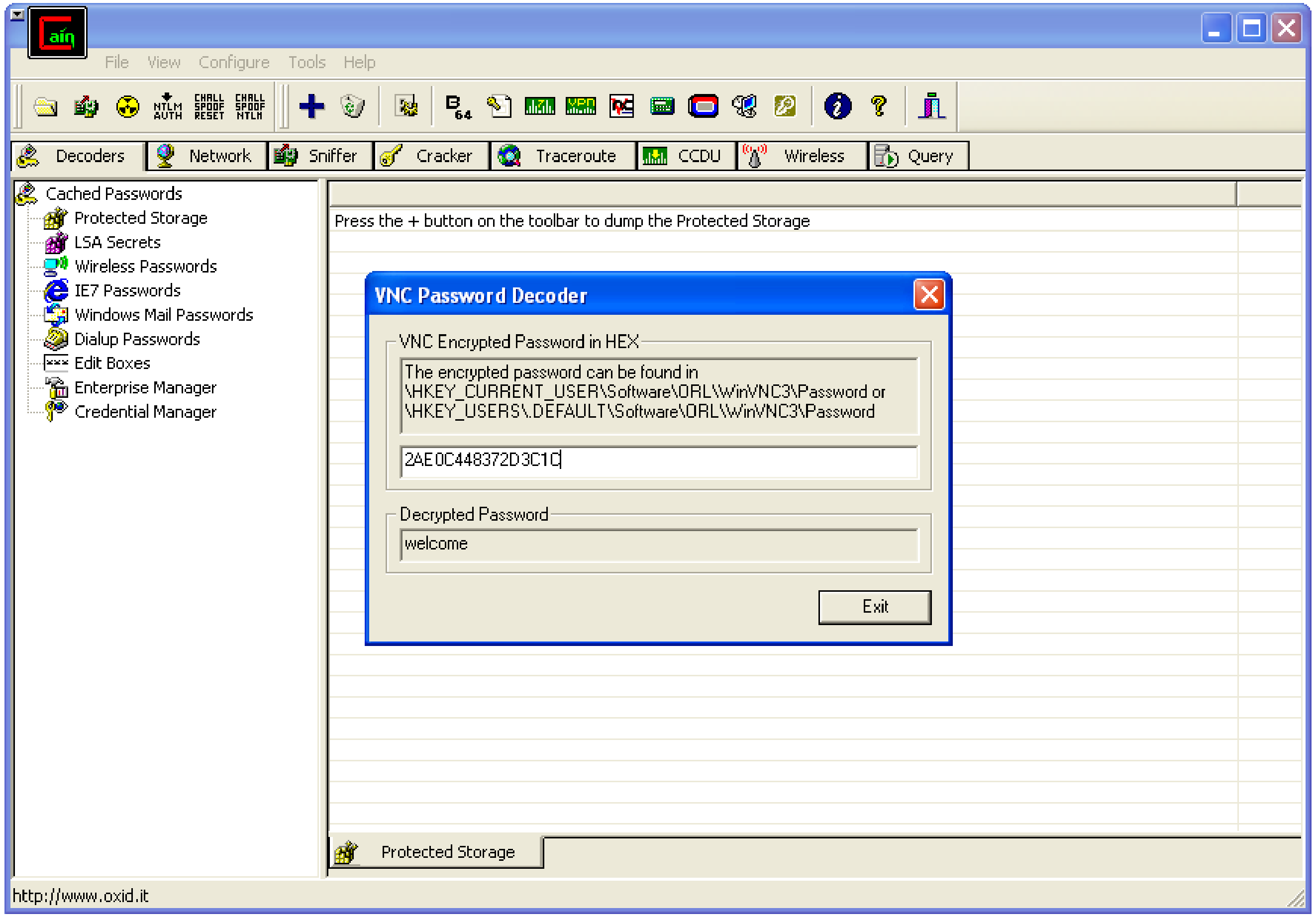
Figure 23 shows the encrypted UltraaVNC server password typically encrypted with 3DES under the value HKEY_CURRENT_USER\Software\ORL\WinVNC. This means that on the previous image of Windows XP service pack 1, UltrtaVNC does not store the server password in registry.



Name	Type	Data
(Default)	REG_SZ	(value not set)
AutoPortSelect	REG_DWORD	0x00000001 (1)
BlankScreen	REG_DWORD	0x00000000 (0)
DontSetHooks	REG_DWORD	0x00000000 (0)
DontUseDriver	REG_DWORD	0x00000000 (0)
DriverDirectAccess	REG_DWORD	0x00000001 (1)
EnableFileTransfers	REG_DWORD	0x00000001 (1)
IdleTimeout	REG_DWORD	0x00000000 (0)
InputsEnabled	REG_DWORD	0x00000001 (1)
LocalInputsDisabled	REG_DWORD	0x00000000 (0)
LocalInputsPriority	REG_DWORD	0x00000000 (0)
LocalInputsPriorityTime	REG_DWORD	0x00000003 (3)
LockSetting	REG_DWORD	0x00000000 (0)
OnlyPollConsole	REG_DWORD	0x00000001 (1)
OnlyPollOnEvent	REG_DWORD	0x00000000 (0)
Password	REG_BINARY	2a e0 c4 48 37 2d 3c 1c
PasswordViewOnly	REG_BINARY	2a e0 c4 48 37 2d 3c 1c
PollForeground	REG_DWORD	0x00000001 (1)
PollFullScreen	REG_DWORD	0x00000000 (0)
PollingCycle	REG_DWORD	0x0000012c (300)
PollUnderCursor	REG_DWORD	0x00000000 (0)
QueryAccept	REG_DWORD	0x00000000 (0)
QueryAllowNoPass	REG_DWORD	0x00000000 (0)
QuerySetting	REG_DWORD	0x00000002 (2)
QueryTimeout	REG_DWORD	0x0000001e (30)
RemoveWallpaper	REG_DWORD	0x00000001 (1)
SocketConnect	REG_DWORD	0x00000001 (1)

Figure 23 UltraVNC server encrypted password in registry

The figure 24 below shows the UltraVNC decrypted password by Abel and Cain tool. As shown below welcome was the decrypted password.



Press the + button on the toolbar to dump the Protected Storage

VNC Password Decoder

VNC Encrypted Password in HEX

The encrypted password can be found in
\HKEY_CURRENT_USER\Software\ORL\WinVNC3\Password or
\HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3\Password

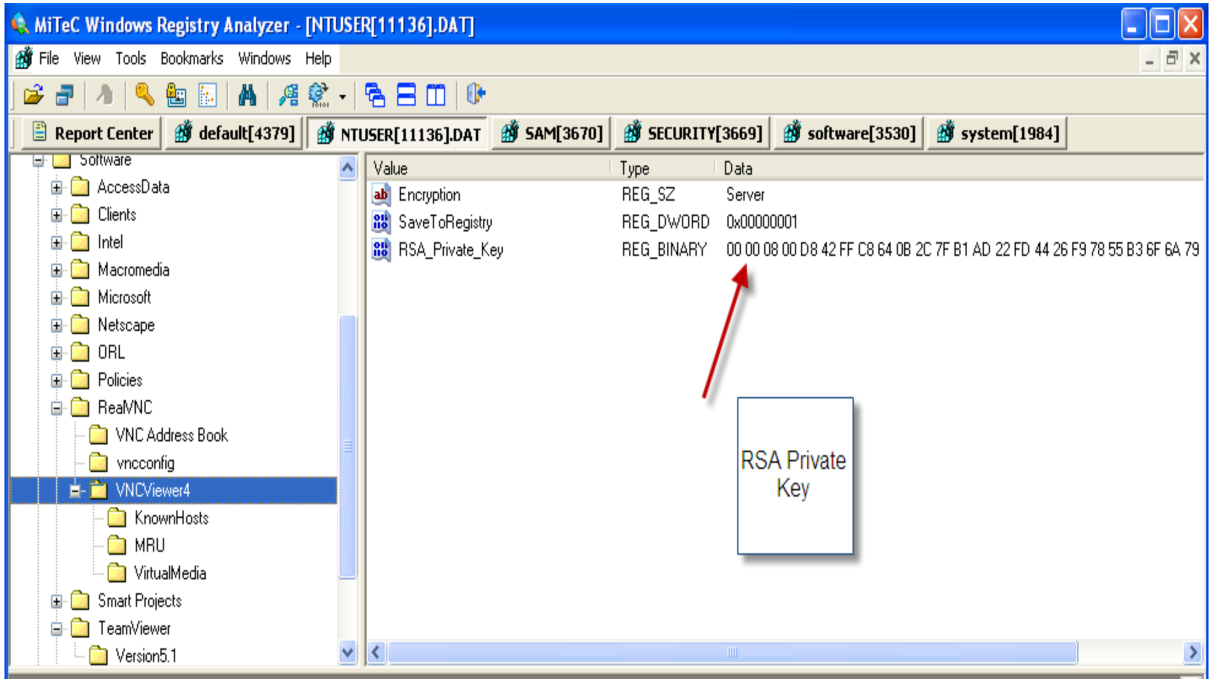
2AE0C448372D3C1C

Decrypted Password

welcome

Figure 24 UltraVNC decrypted password using Abel and Cain

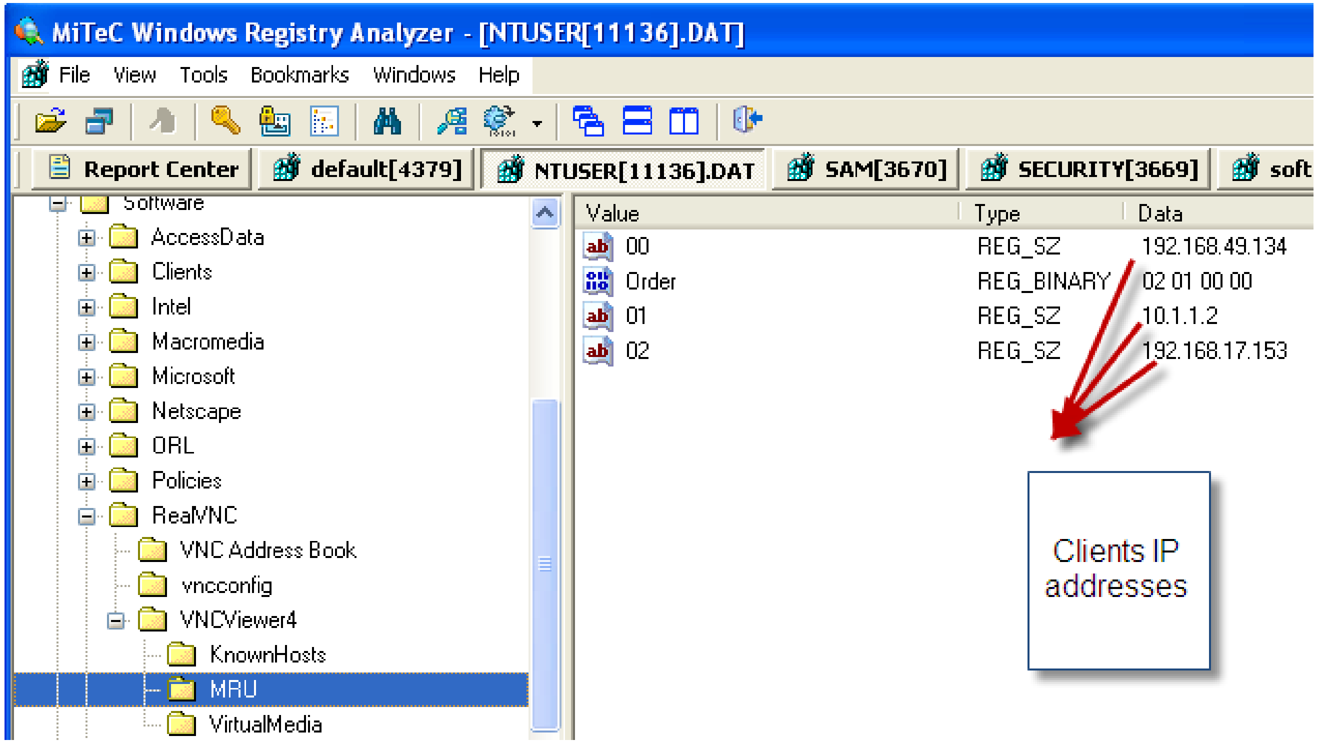
Figure 25 below shows where the RealVNC stores RSA encrypted private key that was created during the connection in the registry under HKEY_CURRENT_USER \Software\RealVNC\vncconfig and also shows the encryption type the application is using. In this case the VNC server decides on the encryption type to use during the connection.



Value	Type	Data
Encryption	REG_SZ	Server
SaveToRegistry	REG_DWORD	0x00000001
RSA_Private_Key	REG_BINARY	00 00 08 00 D8 42 FF C8 64 0B 2C 7F B1 AD 22 FD 44 26 F9 78 55 B3 6F 6A 79

Figure 25 RealVNC RSA Private Key in registry

Figure 26 shows the RealVNC connection history of the client IP addresses the local computer initiated connection. The value is found under Under HKEY_CURRENT_USER \Software\RealVNC\VNCViewer4\MRU.

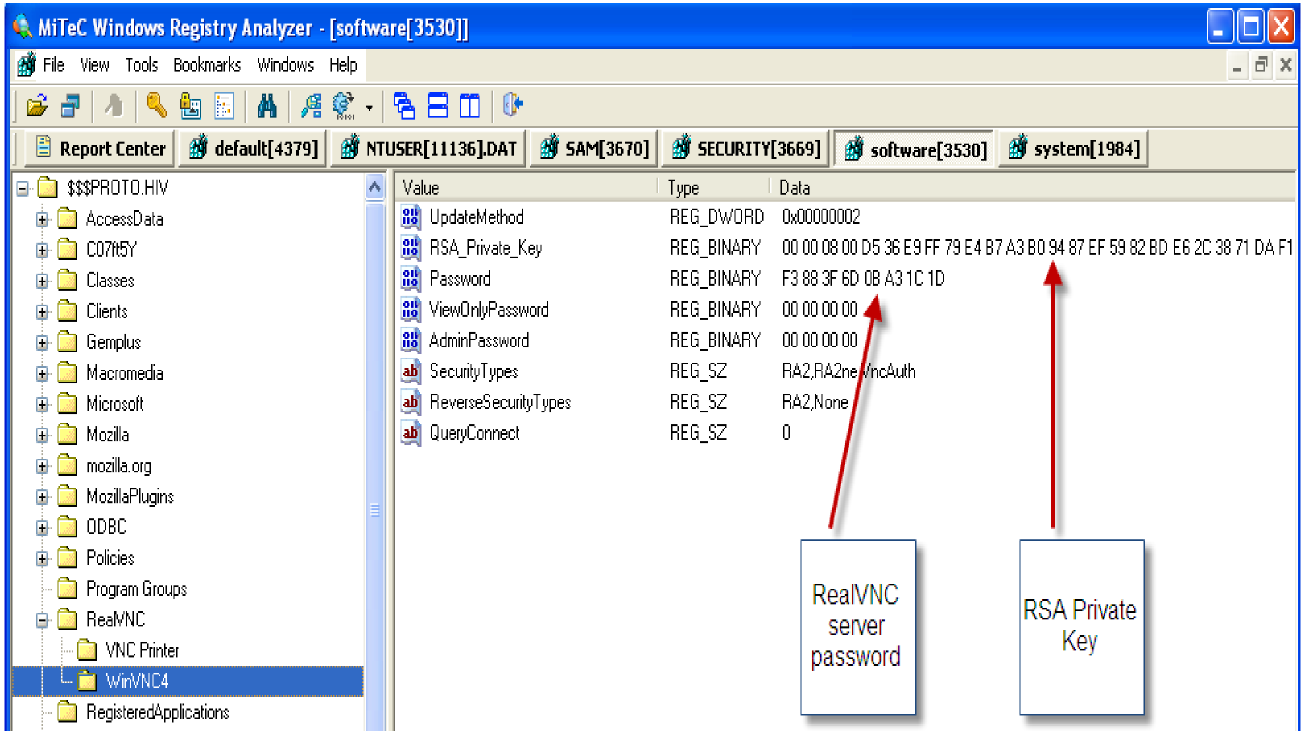


Value	Type	Data
00	REG_SZ	192.168.49.134
Order	REG_BINARY	02 01 00 00
01	REG_SZ	10.1.1.2
02	REG_SZ	192.168.17.153

Figure 26 RealVNC Clients IP addresses

Figure 27 below shows where RealVNC places the local computer’s VNC server password. It is typically encrypted with 3DES. Note that this password is of the local computer and not of the client’s VNC server password. The values are stored under HKEY_LOCAL_MACHINE\Software\RealVNC\WinVNC4.

However in Windows XP service pack 2, RealVNC also stores the Adminpassword and ViewOnly password if set, unlike to service pack 1 which does not store such values. The figure below shows the passwords are empty with all 00000000 values.



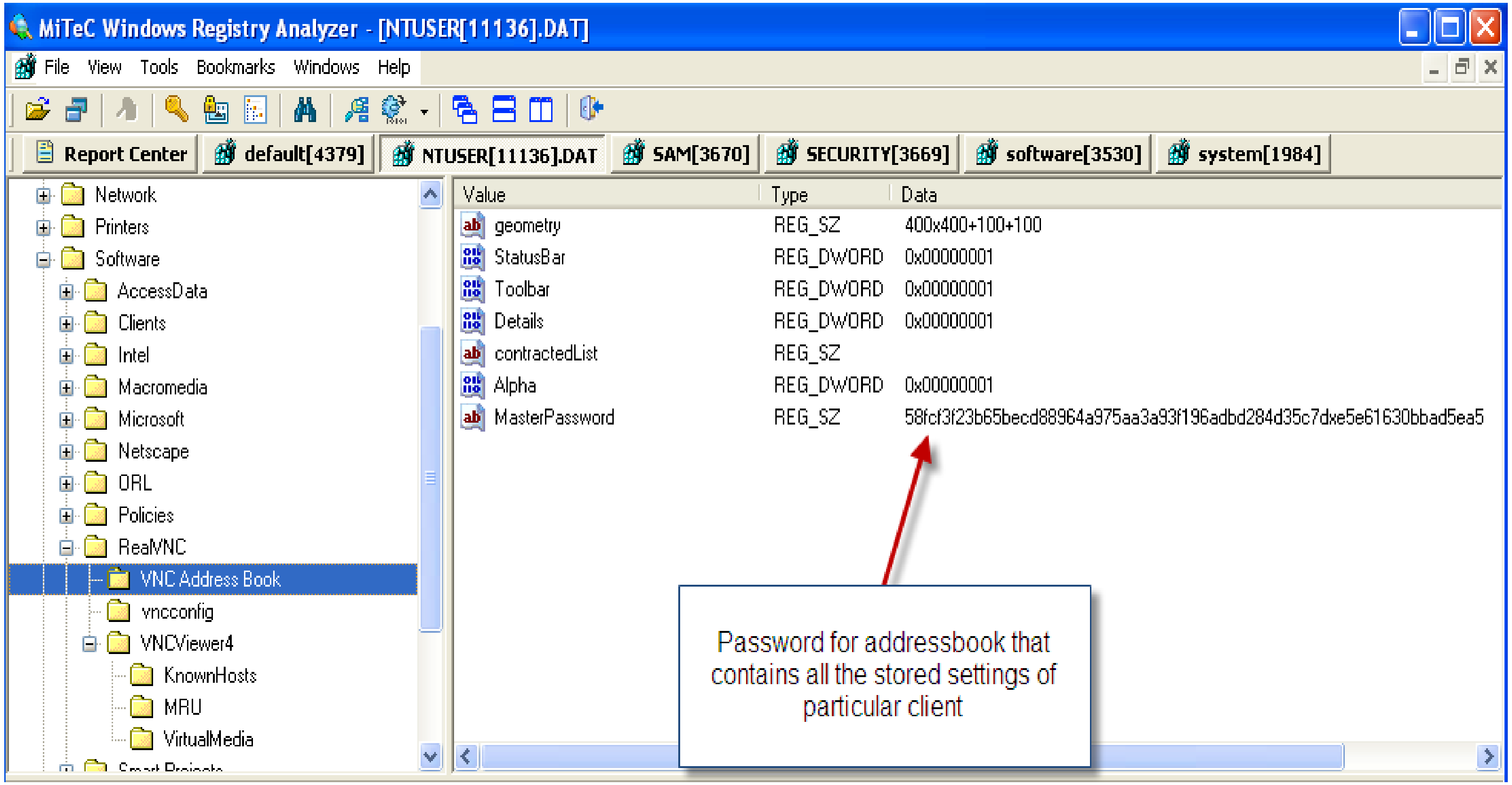
Value	Type	Data
UpdateMethod	REG_DWORD	0x00000002
RSA_Private_Key	REG_BINARY	00 00 08 00 D5 36 E9 FF 79 E4 B7 A3 B0 94 87 EF 59 82 BD E6 2C 38 71 DA F1
Password	REG_BINARY	F3 88 3F 6D 0B A3 1C 1D
ViewOnlyPassword	REG_BINARY	00 00 00 00
AdminPassword	REG_BINARY	00 00 00 00
SecurityTypes	REG_SZ	RA2,RA2ne,VncAuth
ReverseSecurityTypes	REG_SZ	RA2,None
QueryConnect	REG_SZ	0

RealVNC server password

RSA Private Key

Figure 27 RealVNC server encrypted password in registry

Figure 28 shows that RealVNC stores encrypted masterpassword under values HKEY_LOCAL_MACHINE\Software\RealVNC\VNC Address Book. This stores the connection settings and connection password of a connection that the user saved for future quick connection.

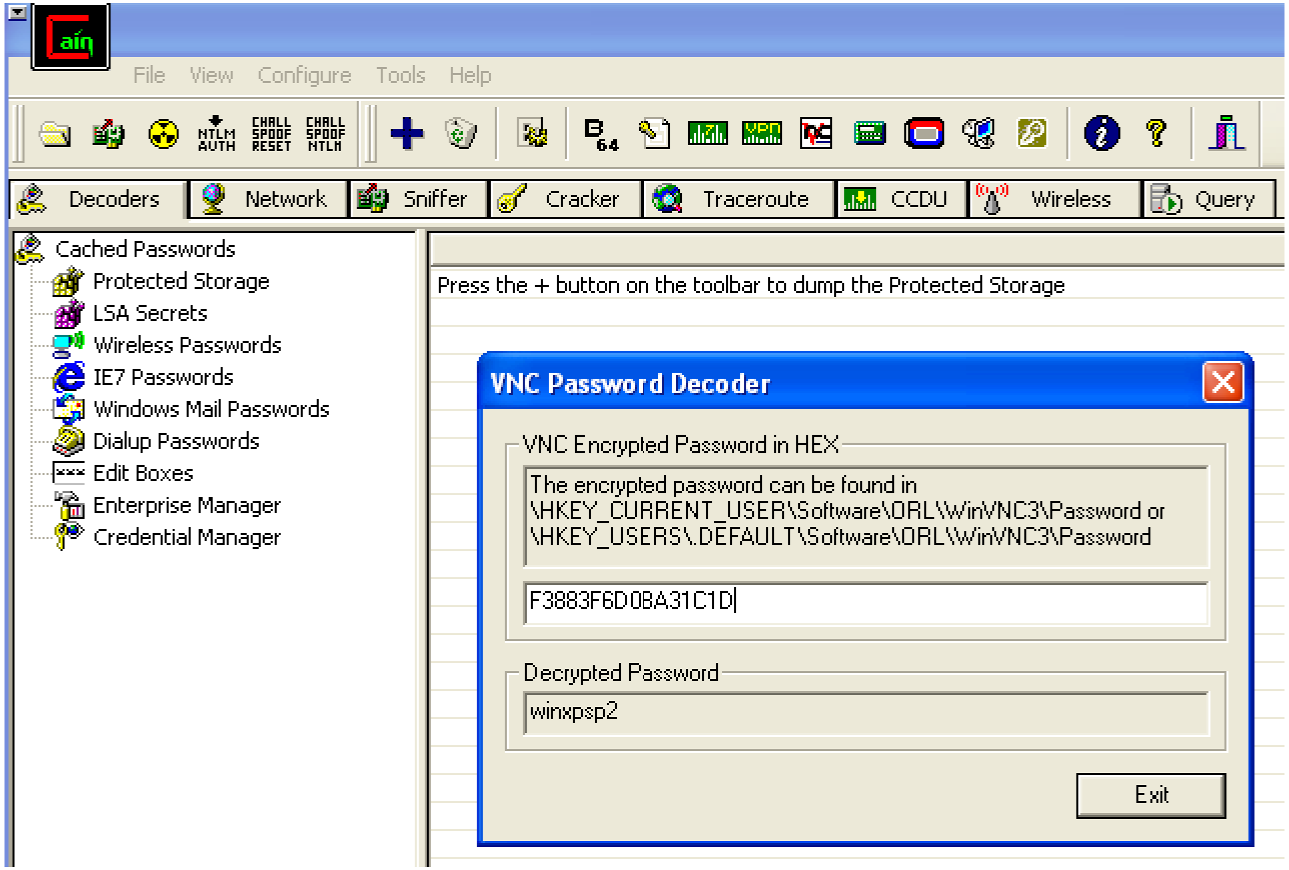


Value	Type	Data
geometry	REG_SZ	400x400+100+100
StatusBar	REG_DWORD	0x00000001
Toolbar	REG_DWORD	0x00000001
Details	REG_DWORD	0x00000001
contractedList	REG_SZ	
Alpha	REG_DWORD	0x00000001
MasterPassword	REG_SZ	58fcf3f23b65becd88964a975aa3a93f196adbd284d35c7dxe5e61630bbad5ea5

Password for addressbook that contains all the stored settings of particular client

Figure 28 RealVNC encrypted masterpassword in registry

Figure 29 below shows the decrypted password for the RealVNC found under the registry above, using Abel and Cain software. The decrypted password is winxpsp2



Press the + button on the toolbar to dump the Protected Storage

VNC Encrypted Password in HEX

The encrypted password can be found in
\HKEY_CURRENT_USER\Software\ORL\WinVNC3\Password or
\HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3\Password

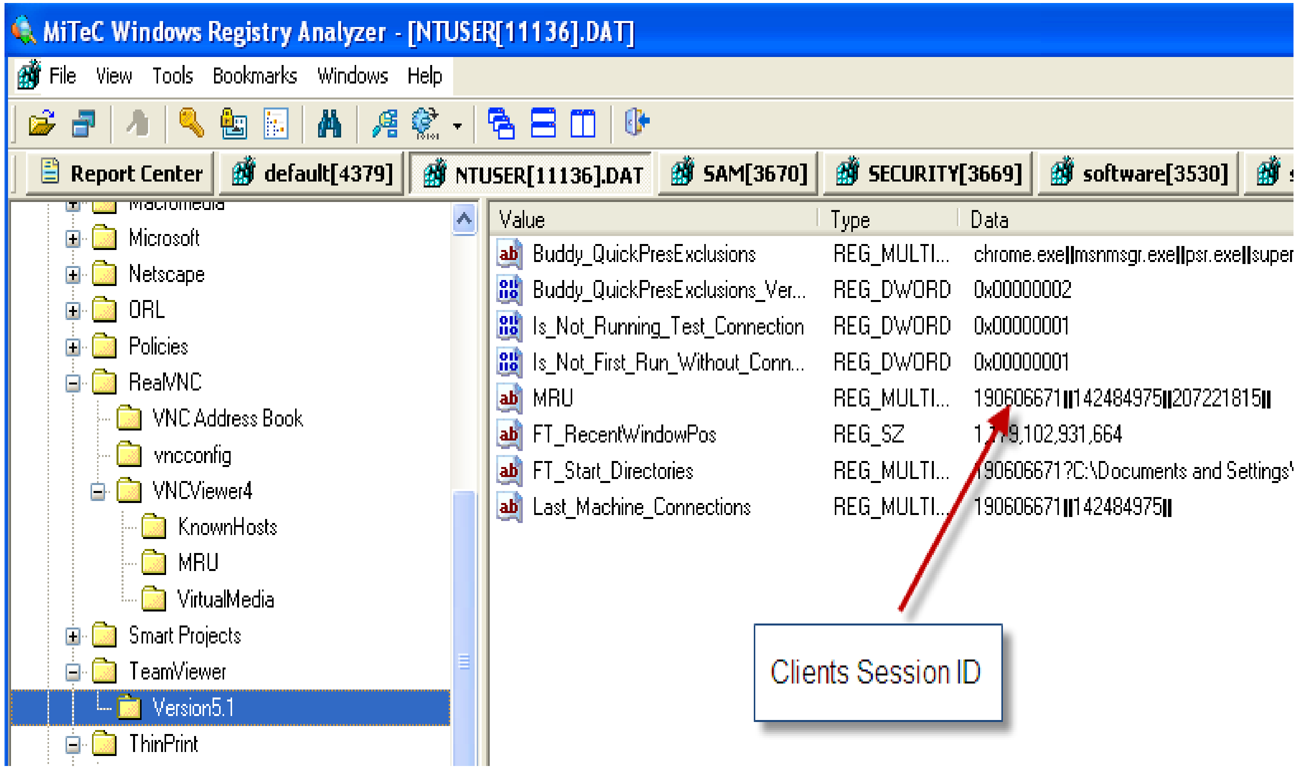
F3883F6D0BA31C1D

Decrypted Password

winxpsp2

Figure 29 RealVNC decrypted password using Abel and Cain

TeamViewer also stores the client connection IDs that the local computer connected to, and also the connection settings as shown in figure 30 below. This is typically stored under Under HKEY_CURRENT_USER \Software\TeamViewer\Version5.

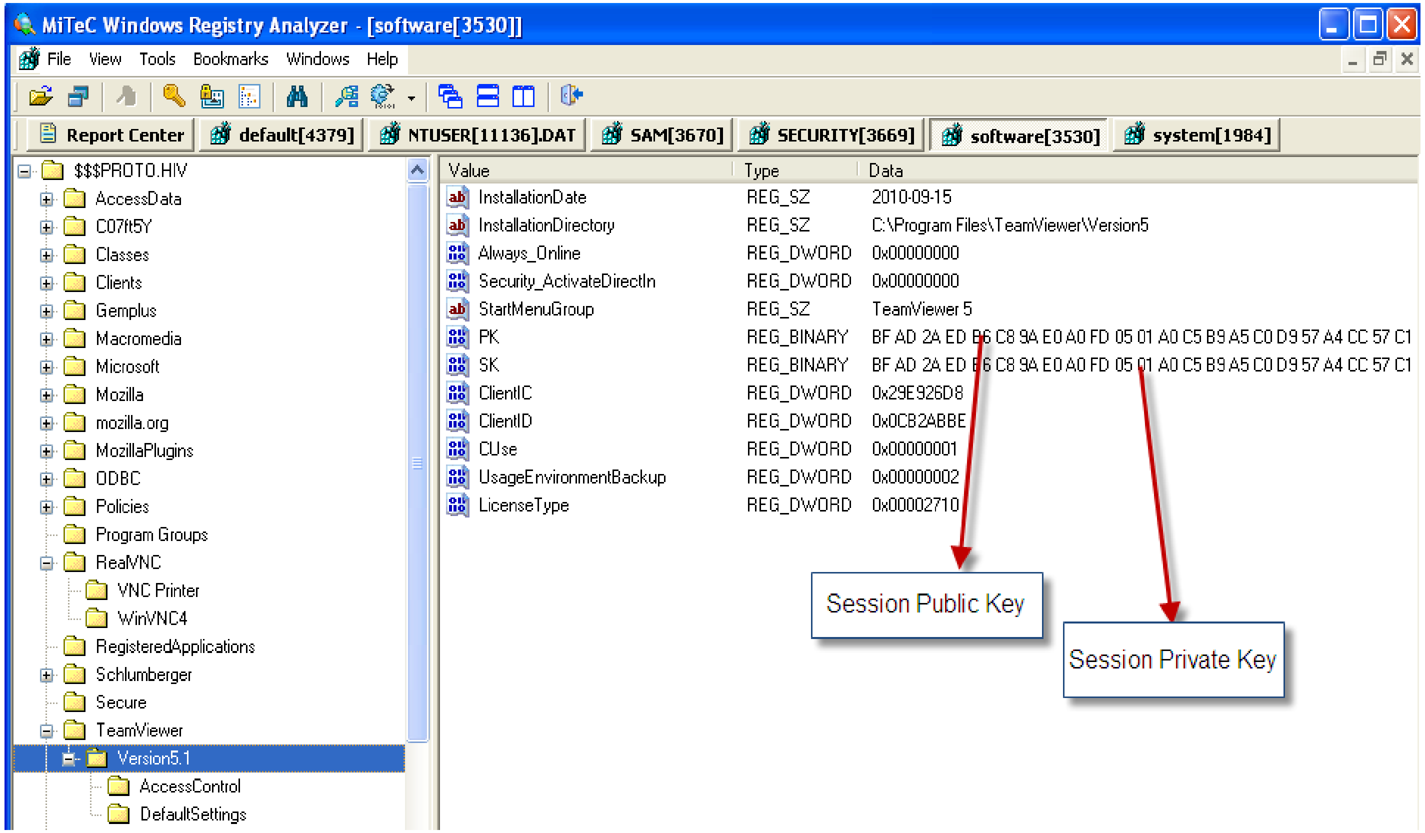


Value	Type	Data
Buddy_QuickPresExclusions	REG_MULTI...	chrome.exe‖msnmsgr.exe‖psr.exe‖super
Buddy_QuickPresExclusions_Ver...	REG_DWORD	0x00000002
Is_Not_Running_Test_Connection	REG_DWORD	0x00000001
Is_Not_First_Run_Without_Conn...	REG_DWORD	0x00000001
MRU	REG_MULTI...	190606671‖142484975‖207221815‖
FT_RecentWindowPos	REG_SZ	1,[illegible]9,102,931,664
FT_Start_Directories	REG_MULTI...	190606671?C:\Documents and Settings
Last_Machine_Connections	REG_MULTI...	190606671‖142484975‖

Clients Session ID

Figure 30 TeamViewer client IDs

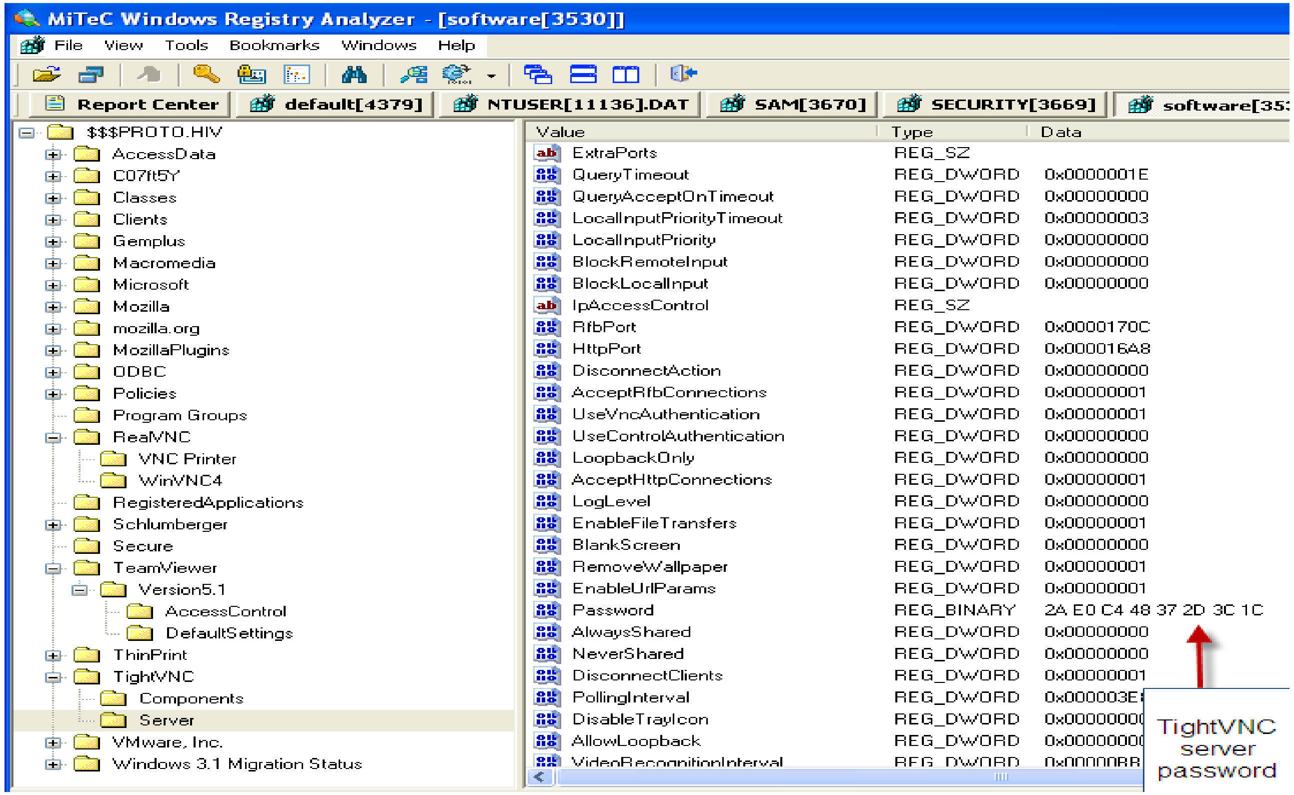
Figure 31 below shows the encrypted private and public keys stored in the registry under HKEY_LOCAL_MACHINE\Software\TeamViewer\Version5. These keys are generated when the client and local computer initiate the connection. The keys are typically encrypted with RSA cipher encryption algorithm.



Value	Type	Data
InstallationDate	REG_SZ	2010-09-15
InstallationDirectory	REG_SZ	C:\Program Files\TeamViewer\Version5
Always_Online	REG_DWORD	0x00000000
Security_ActivateDirectIn	REG_DWORD	0x00000000
StartMenuGroup	REG_SZ	TeamViewer 5
PK	REG_BINARY	BF AD 2A ED B6 C8 9A E0 A0 FD 05 01 A0 C5 B9 A5 C0 D9 57 A4 CC 57 C1
SK	REG_BINARY	BF AD 2A ED B6 C8 9A E0 A0 FD 05 01 A0 C5 B9 A5 C0 D9 57 A4 CC 57 C1
ClientIC	REG_DWORD	0x29E926D8
ClientID	REG_DWORD	0x0CB2ABBE
CUse	REG_DWORD	0x00000001
UsageEnvironmentBackup	REG_DWORD	0x00000002
LicenseType	REG_DWORD	0x00002710

Figure 31 TeamViewer encrypted private and public stored under registry

TightVNC stores the local computers TightVNC server password in the registry under value HKEY_LOCAL_MACHINE\Software\TightVNC\Server. The application also stores the connection and application settings. However as to other VNC applications, it does not save any connection history of the client machines that the local computer connected to. This is shown in the figure 32 below.



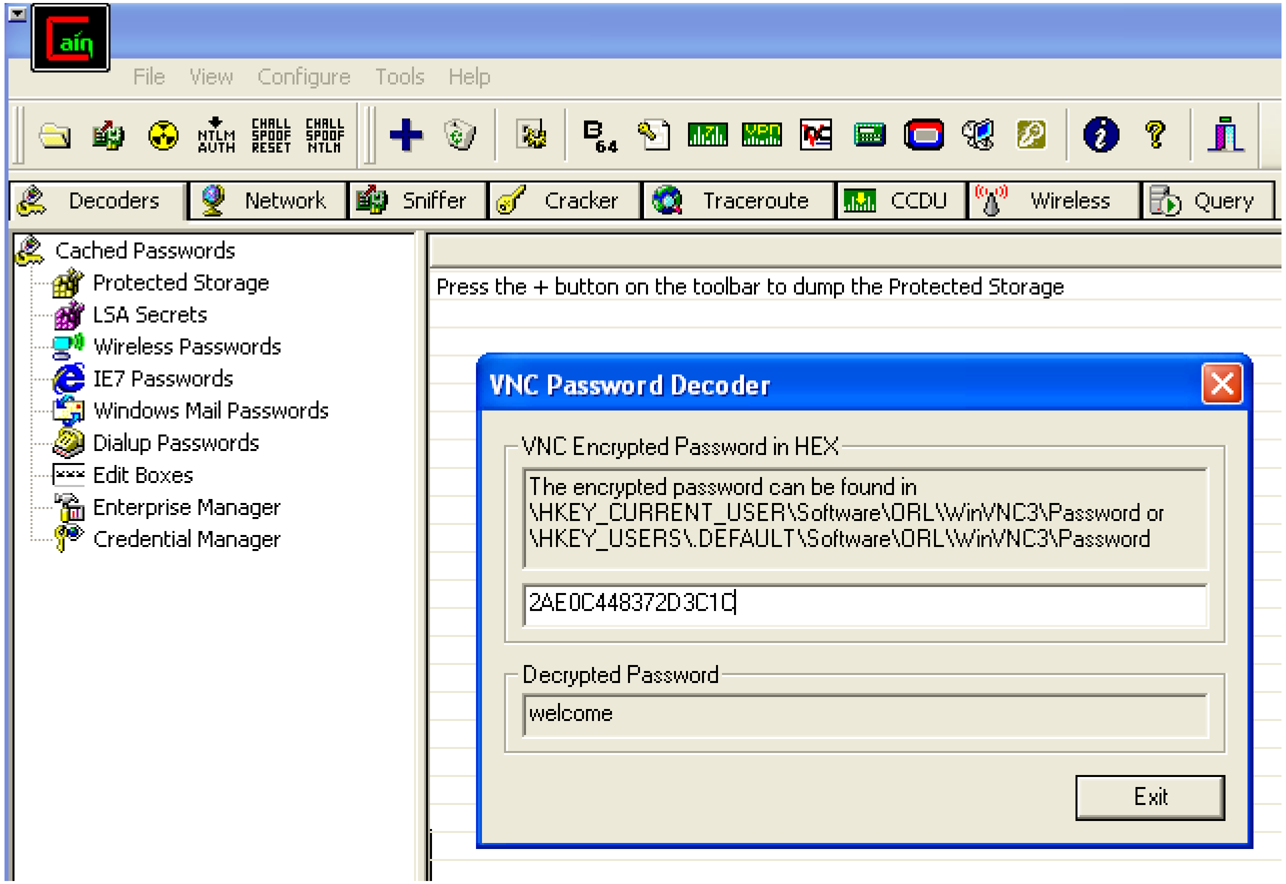
- $$$PROTO.HIV
  - AccessData
  - C07ft5Y
  - Classes
  - Clients
  - Gemplus
  - Macromedia
  - Microsoft
  - Mozilla
  - mozilla.org
  - MozillaPlugins
  - ODBC
  - Policies
  - Program Groups
  - RealVNC
    - VNC Printer
    - WinVNC4
  - RegisteredApplications
  - Schlumberger
  - Secure
  - TeamViewer
    - Version5.1
      - AccessControl
      - DefaultSettings
  - ThinPrint
  - TightVNC
    - Components
    - Server
  - VMware, Inc.
  - Windows 3.1 Migration Status

Value	Type	Data
ExtraPorts	REG_SZ	
QueryTimeout	REG_DWORD	0x0000001E
QueryAcceptOnTimeout	REG_DWORD	0x00000000
LocalInputPriorityTimeout	REG_DWORD	0x00000003
LocalInputPriority	REG_DWORD	0x00000000
BlockRemoteInput	REG_DWORD	0x00000000
BlockLocalInput	REG_DWORD	0x00000000
IpAccessControl	REG_SZ	
RfbPort	REG_DWORD	0x0000170C
HttpPort	REG_DWORD	0x000016A8
DisconnectAction	REG_DWORD	0x00000000
AcceptRfbConnections	REG_DWORD	0x00000001
UseVncAuthentication	REG_DWORD	0x00000001
UseControlAuthentication	REG_DWORD	0x00000000
LoopbackOnly	REG_DWORD	0x00000000
AcceptHttpConnections	REG_DWORD	0x00000001
LogLevel	REG_DWORD	0x00000000
EnableFileTransfers	REG_DWORD	0x00000001
BlankScreen	REG_DWORD	0x00000000
RemoveWallpaper	REG_DWORD	0x00000001
EnableUrlParams	REG_DWORD	0x00000001
Password	REG_BINARY	2A E0 C4 48 37 2D 3C 1C
AlwaysShared	REG_DWORD	0x00000000
NeverShared	REG_DWORD	0x00000000
DisconnectClients	REG_DWORD	0x00000001
PollingInterval	REG_DWORD	0x000003E
DisableTrayIcon	REG_DWORD	0x0000000
AllowLoopback	REG_DWORD	0x0000000
VideoRecognitionInterval	REG_DWORD	0x000000BB

TightVNC server password

Figure 32 TightVNC server session encrypted password stored in registry

The figure 33 below shows the TightVNC decrypted password by Abel and Cain tool. As shown below welcome was the decrypted password.



Press the + button on the toolbar to dump the Protected Storage

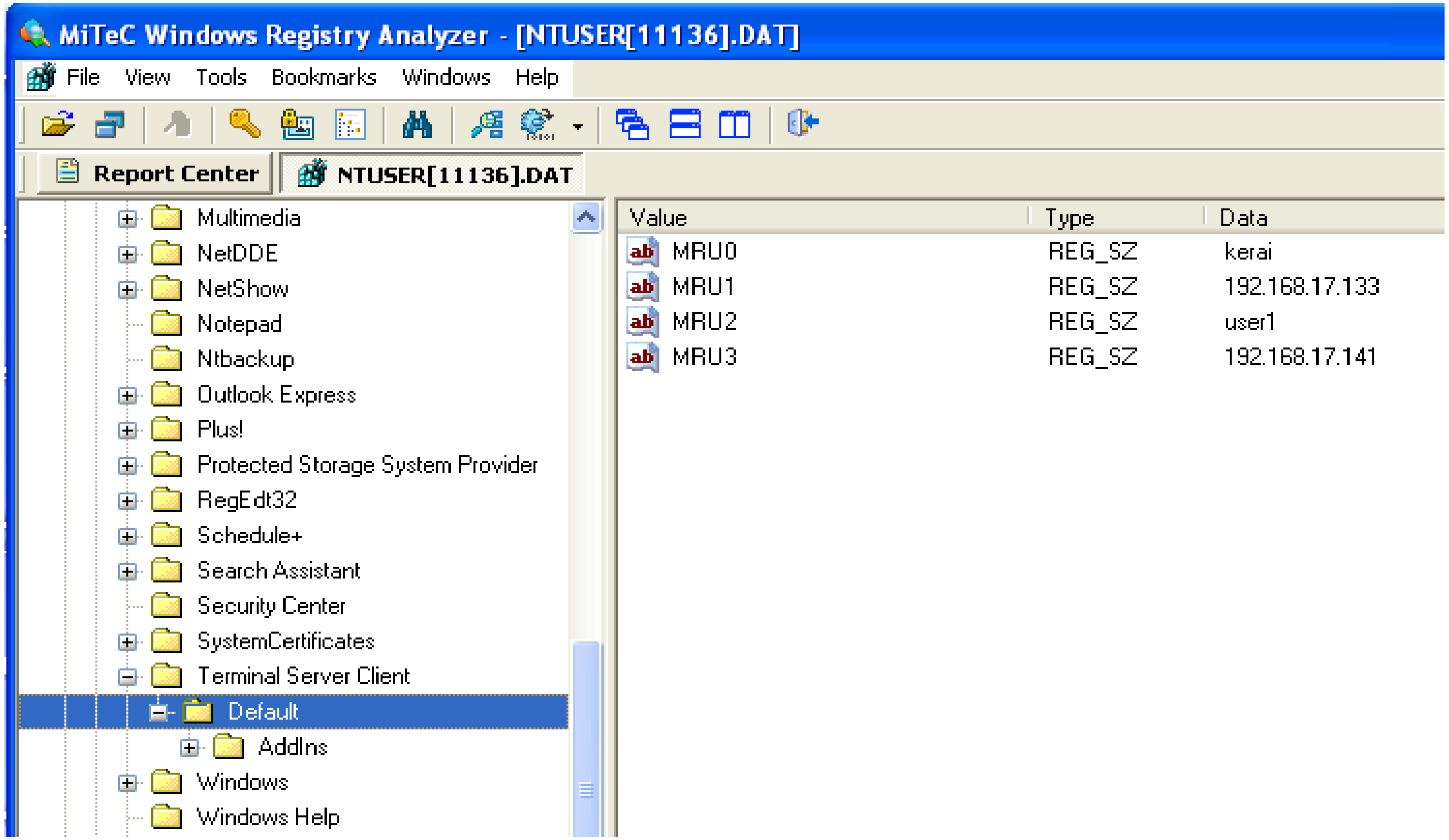
The encrypted password can be found in
\HKEY_CURRENT_USER\Software\ORL\WinVNC3\Password or
\HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3\Password

VNC Encrypted Password in HEX: 2AE0C448372D3C1C

Decrypted Password: welcome

Figure 33 TightVNC decrypted password using Abel and Cain

Figure 34 shows the client connection history saved by the RDP under the value HKEY_CURRENT_USER \Software\Microsoft\Terminal Server Client\Default. These are again the private IP addresses of the client.



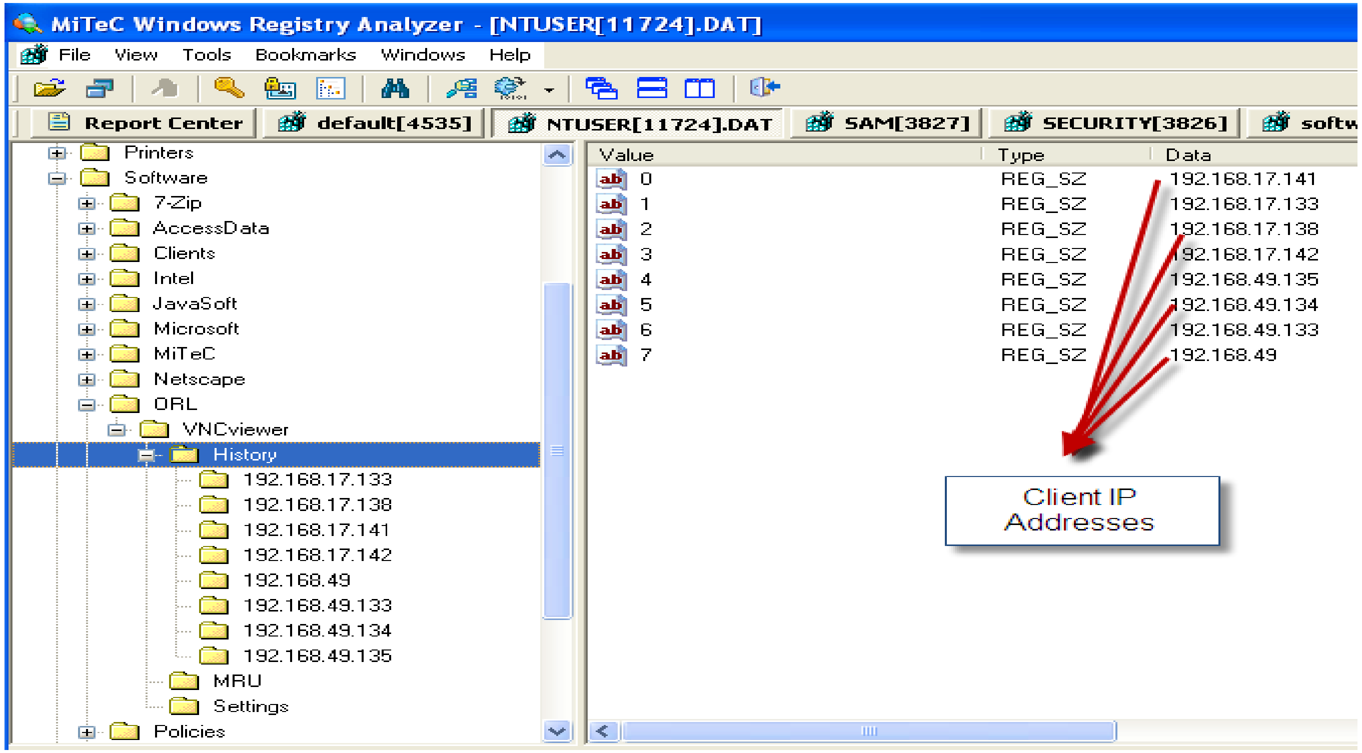
Value	Type	Data
MRU0	REG_SZ	kerai
MRU1	REG_SZ	192.168.17.133
MRU2	REG_SZ	user1
MRU3	REG_SZ	192.168.17.141

Figure 34 Remote desktop protocol settings

8.3.3 Image 3

The figures below shows the settings and artefacts left behing by UltaVNC, RealVNC, TightVNC, TeamViewer and RDP.

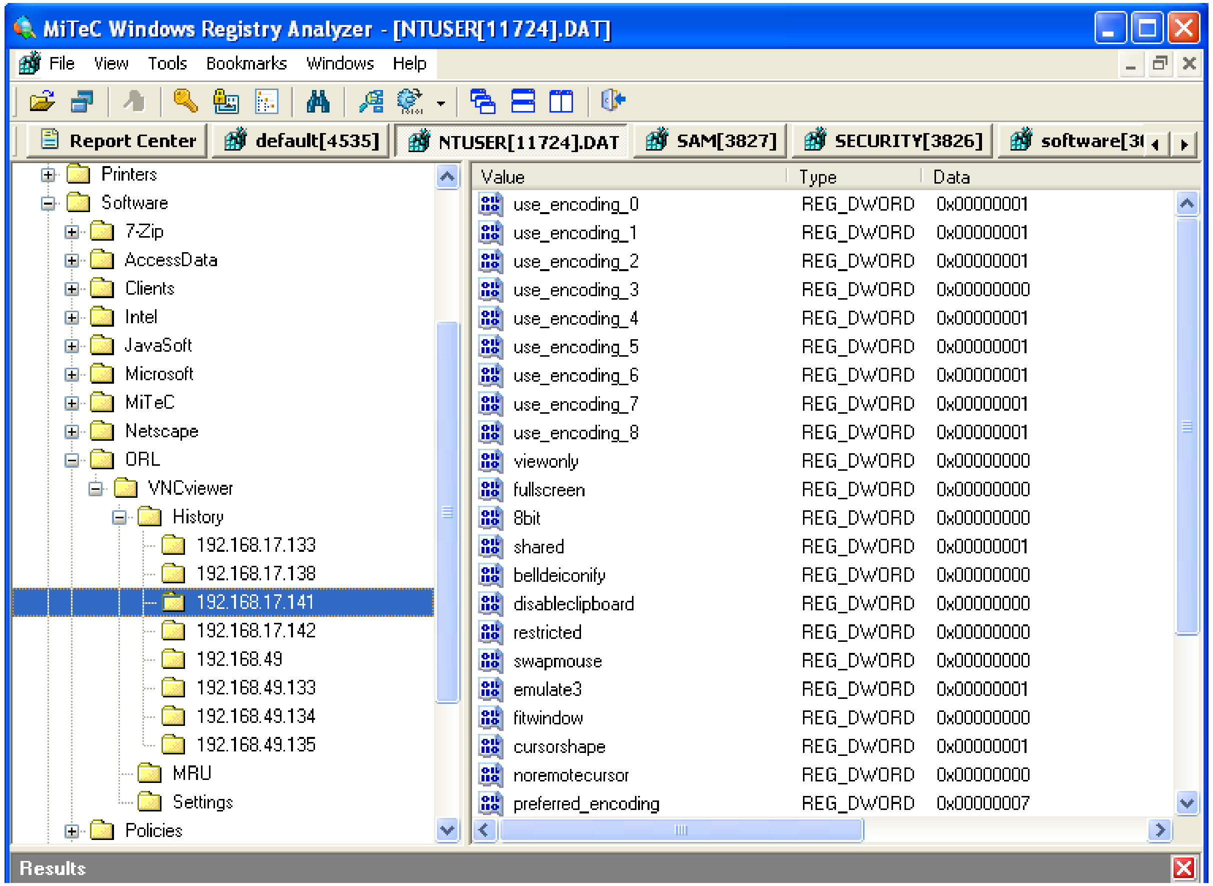
Figure 36 shows how UltraVNC stores the client private IP addresses under regisrty HKEY_CURRENT_USER\Software\ORL\VNCviewer\History. The IP addresses shown are the addresses the local computer initiated remote connection using UltraVNC viewer.



Value	Type	Data
0	REG_SZ	192.168.17.141
1	REG_SZ	192.168.17.133
2	REG_SZ	192.168.17.138
3	REG_SZ	192.168.17.142
4	REG_SZ	192.168.49.135
5	REG_SZ	192.168.49.134
6	REG_SZ	192.168.49.133
7	REG_SZ	192.168.49

Figure 35 UltraVNC shows client IP addresses

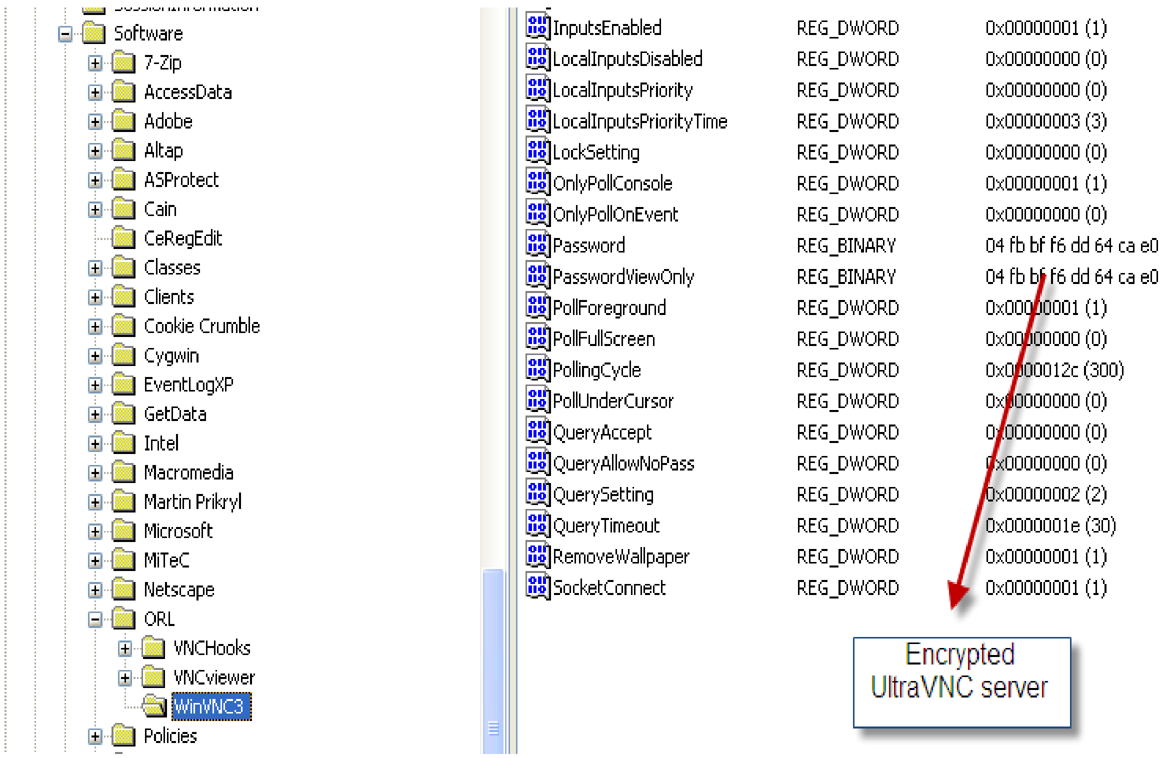
The figure 37 below shows the connection settings of a particular client that the local computer and the client computer negotiated during the connection.



Value	Type	Data
use_encoding_0	REG_DWORD	0x00000001
use_encoding_1	REG_DWORD	0x00000001
use_encoding_2	REG_DWORD	0x00000001
use_encoding_3	REG_DWORD	0x00000000
use_encoding_4	REG_DWORD	0x00000001
use_encoding_5	REG_DWORD	0x00000001
use_encoding_6	REG_DWORD	0x00000001
use_encoding_7	REG_DWORD	0x00000001
use_encoding_8	REG_DWORD	0x00000001
viewonly	REG_DWORD	0x00000000
fullscreen	REG_DWORD	0x00000000
8bit	REG_DWORD	0x00000000
shared	REG_DWORD	0x00000001
belldeiconify	REG_DWORD	0x00000000
disableclipboard	REG_DWORD	0x00000000
restricted	REG_DWORD	0x00000000
swapmouse	REG_DWORD	0x00000000
emulate3	REG_DWORD	0x00000001
fitwindow	REG_DWORD	0x00000000
cursorshape	REG_DWORD	0x00000001
noremotecursor	REG_DWORD	0x00000000
preferred_encoding	REG_DWORD	0x00000007

Figure 36 UltraVNC client connection settings

Figure 38 shows the encrypted UltraaVNC server password typically encrypted with 3DES under the value HKEY_CURRENT_USER\Software\ORL\WinVNC. This means that on the previous image of Windows XP service pack 1, UltrtaVNC does not store the server password in registry.

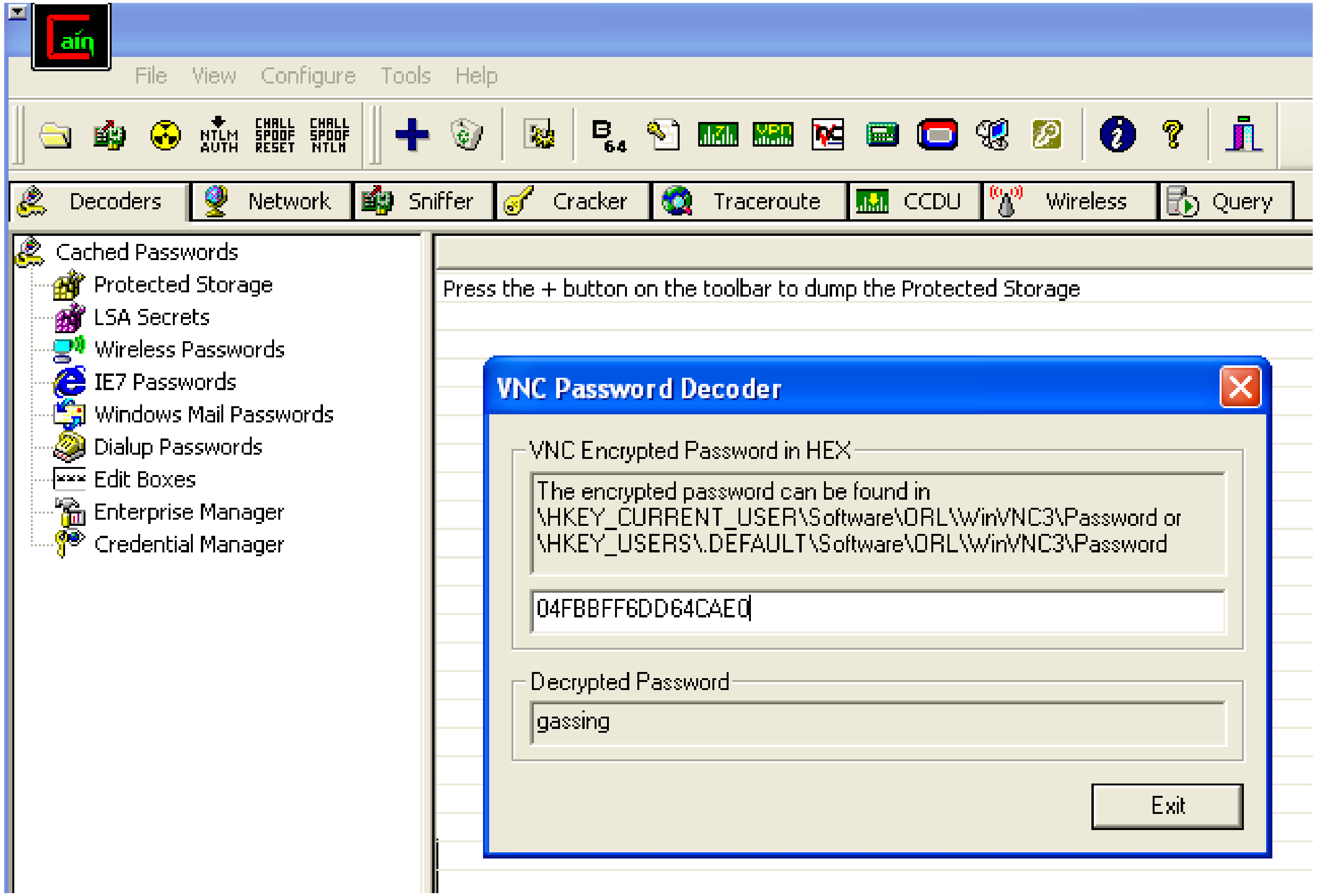


InputsEnabled	REG_DWORD	0x00000001 (1)
LocalInputsDisabled	REG_DWORD	0x00000000 (0)
LocalInputsPriority	REG_DWORD	0x00000000 (0)
LocalInputsPriorityTime	REG_DWORD	0x00000003 (3)
LockSetting	REG_DWORD	0x00000000 (0)
OnlyPollConsole	REG_DWORD	0x00000001 (1)
OnlyPollOnEvent	REG_DWORD	0x00000000 (0)
Password	REG_BINARY	04 fb bf f6 dd 64 ca e0
PasswordViewOnly	REG_BINARY	04 fb bf f6 dd 64 ca e0
PollForeground	REG_DWORD	0x00000001 (1)
PollFullScreen	REG_DWORD	0x00000000 (0)
PollingCycle	REG_DWORD	0x0000012c (300)
PollUnderCursor	REG_DWORD	0x00000000 (0)
QueryAccept	REG_DWORD	0x00000000 (0)
QueryAllowNoPass	REG_DWORD	0x00000000 (0)
QuerySetting	REG_DWORD	0x00000002 (2)
QueryTimeout	REG_DWORD	0x0000001e (30)
RemoveWallpaper	REG_DWORD	0x00000001 (1)
SocketConnect	REG_DWORD	0x00000001 (1)

Encrypted UltraVNC server

Figure 37 UltraVNC server encrypted password in registry

The figure 38 below shows the UltraVNC decrypted password by Abel and Cain tool. As shown below GASSING was the decrypted password.



Press the + button on the toolbar to dump the Protected Storage

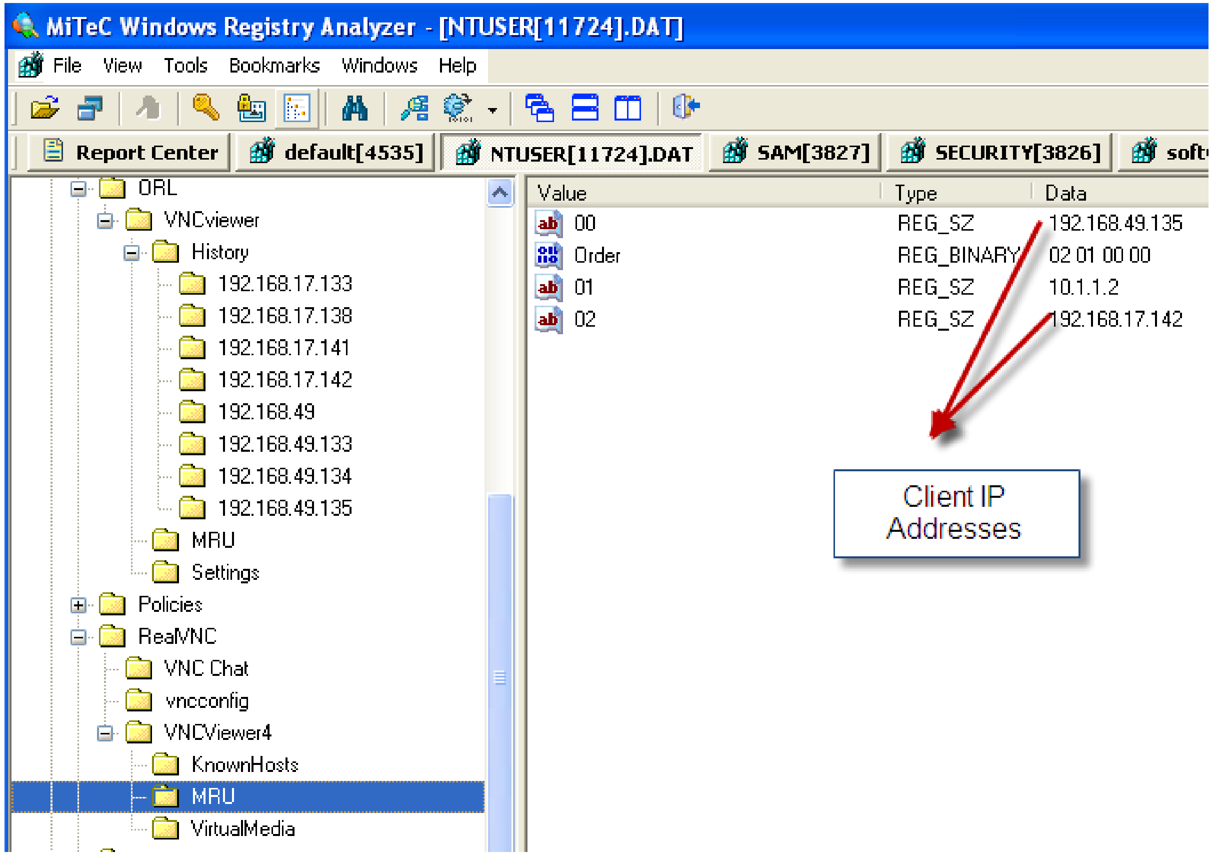
The encrypted password can be found in
\HKEY_CURRENT_USER\Software\ORL\WinVNC3\Password or
\HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3\Password

04FBBFF6DD64CAE0

gassing

Figure 38 UltraVNC decrypted password using Abel and Cain

Figure 39 shows the RealVNC connection history of the client IP addresses the local computer initiated connection. The value is found under Under HKEY_CURRENT_USER \Software\RealVNC\VNCViewer4\MRU.

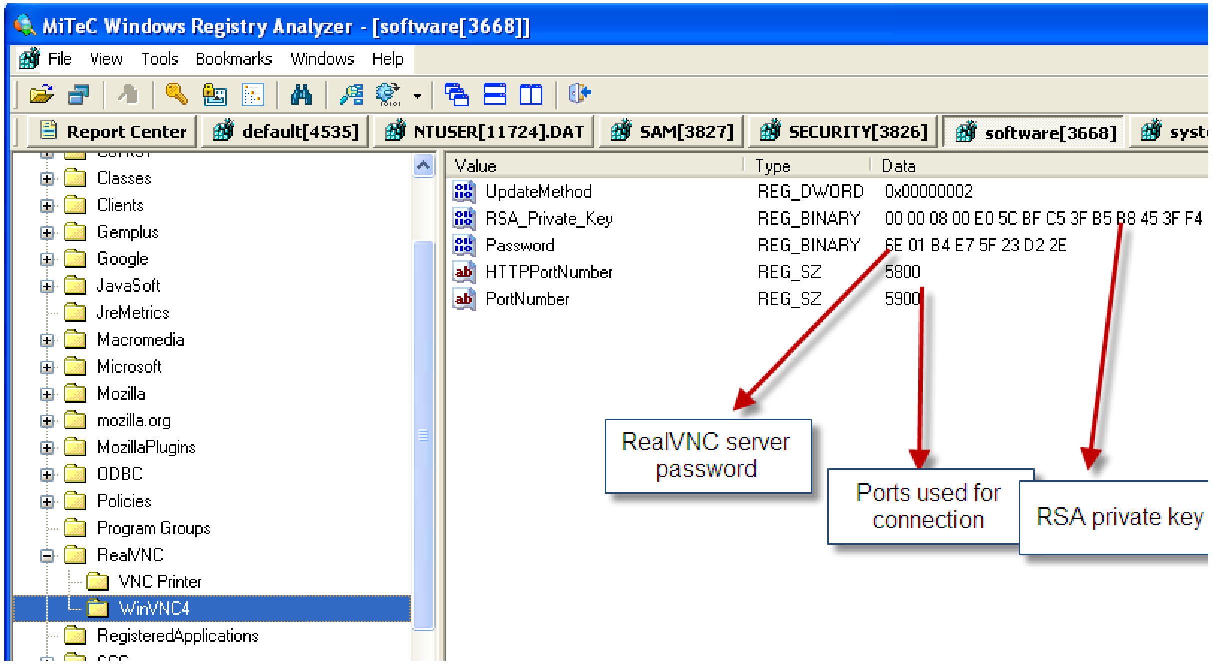


Value	Type	Data
00	REG_SZ	192.168.49.135
Order	REG_BINARY	02 01 00 00
01	REG_SZ	10.1.1.2
02	REG_SZ	192.168.17.142

Client IP Addresses

Figure 39 RealVNC Clients IP addresses

Figure 40 below shows where RealVNC places the local computer's VNC server password. It is typically encrypted with 3DES. Note that this password is of the local computer and not of the client's VNC server password. The values are stored under HKEY_LOCAL_MACHINE\Software\RealVNC\WinVNC4 and also the RSA private key.



Value	Type	Data
UpdateMethod	REG_DWORD	0x00000002
RSA_Private_Key	REG_BINARY	00 00 08 00 E0 5C BF C5 3F B5 B8 45 3F F4
Password	REG_BINARY	6E 01 B4 E7 5F 23 D2 2E
HTTPPortNumber	REG_SZ	5800
PortNumber	REG_SZ	5900

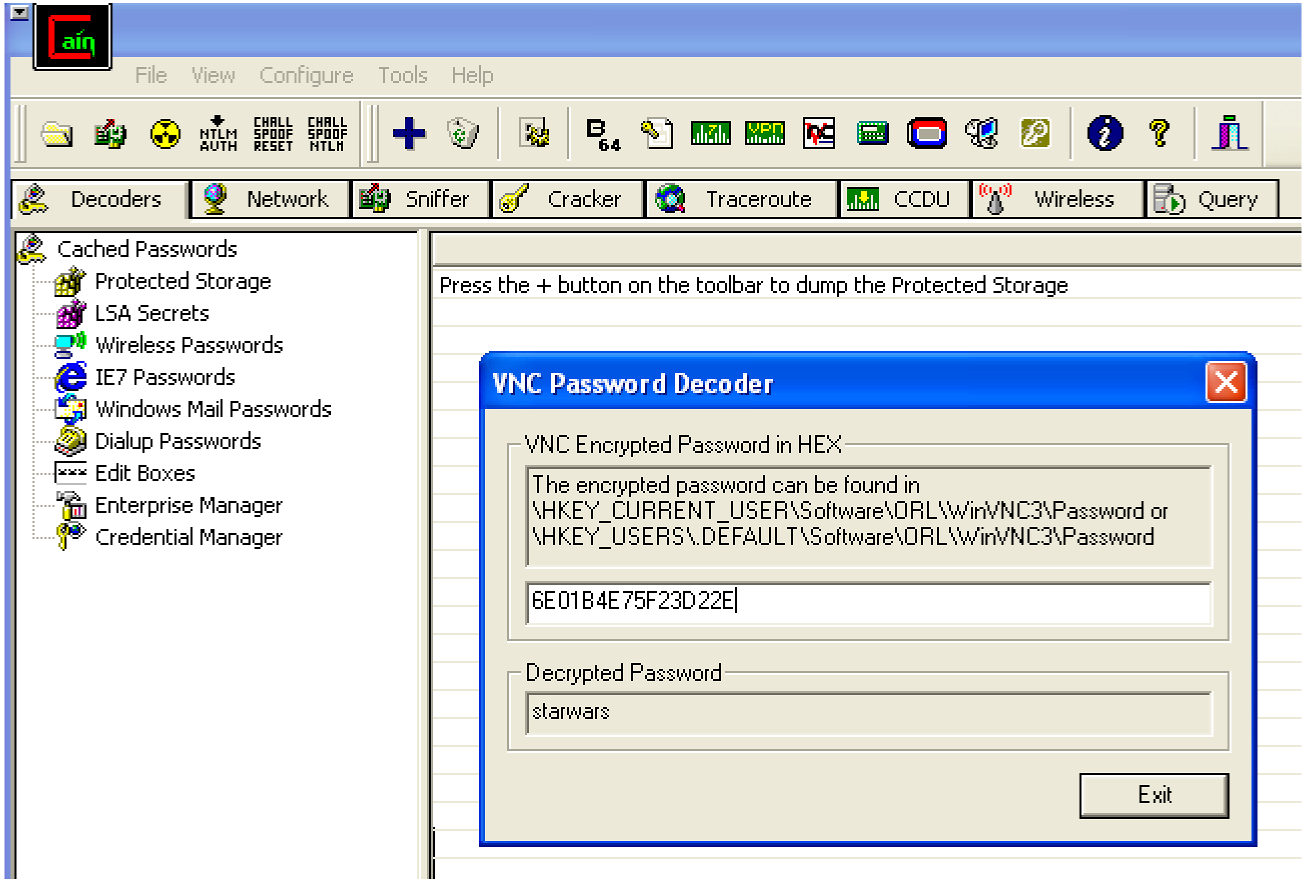
RealVNC server password

Ports used for connection

RSA private key

Figure 40 RealVNC server encrypted password in registry

Figure 41 below shows the decrypted password for the RealVNC found under the registry above using Abel and Cain software. The decrypted password is starwars as shown below.



Press the + button on the toolbar to dump the Protected Storage

VNC Encrypted Password in HEX

The encrypted password can be found in
\HKEY_CURRENT_USER\Software\ORL\WinVNC3\Password or
\HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3\Password

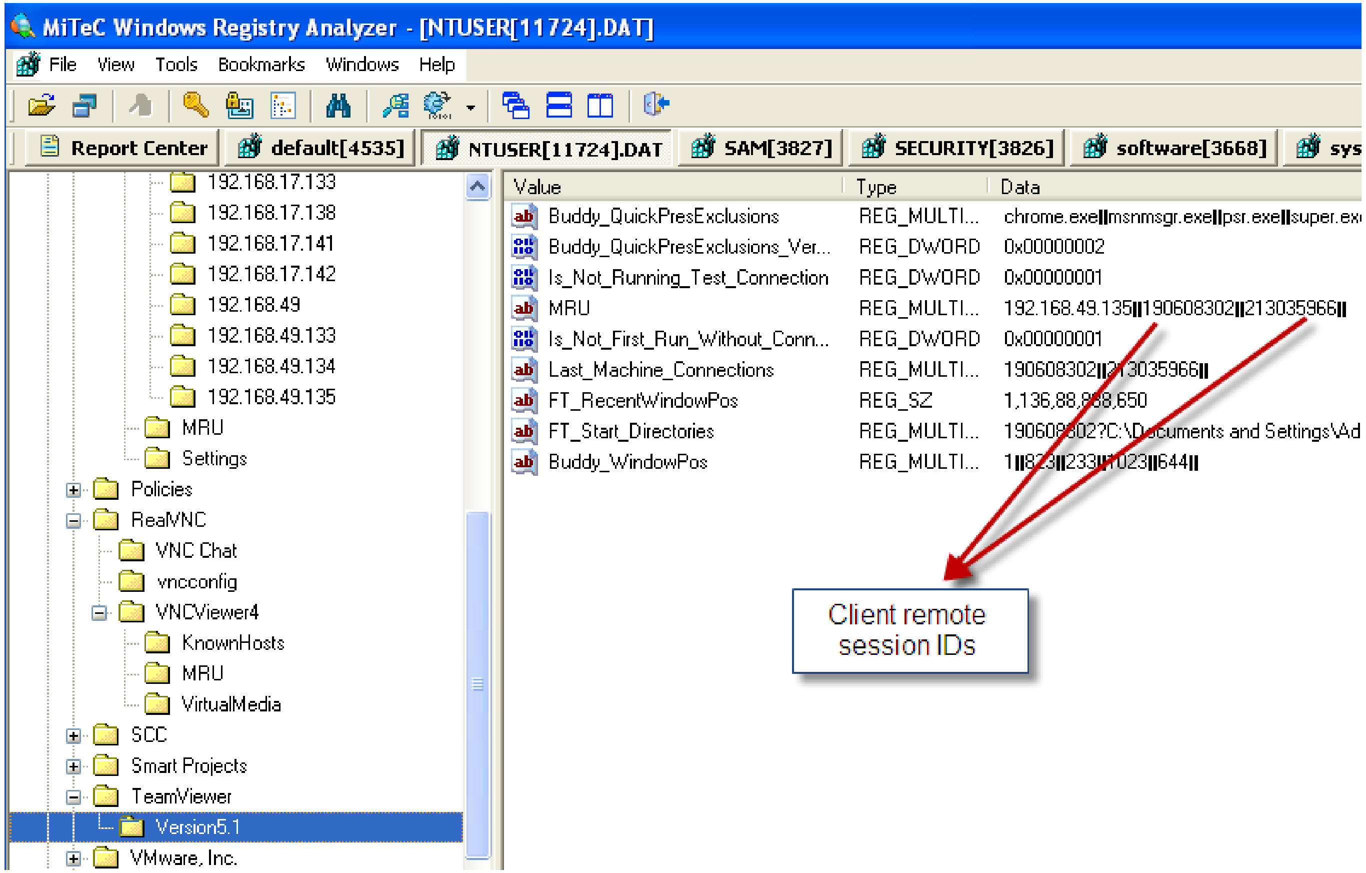
6E01B4E75F23D22E

Decrypted Password

starwars

Figure 41 RealVNC decrypted password using Abel and Cain

TeamViewer also stores the client connection IDs that the local computer connected to, and also the connection settings as shown in figure 42 below. This is typically stored under Under HKEY_CURRENT_USER \Software\TeamViewer\Version5.

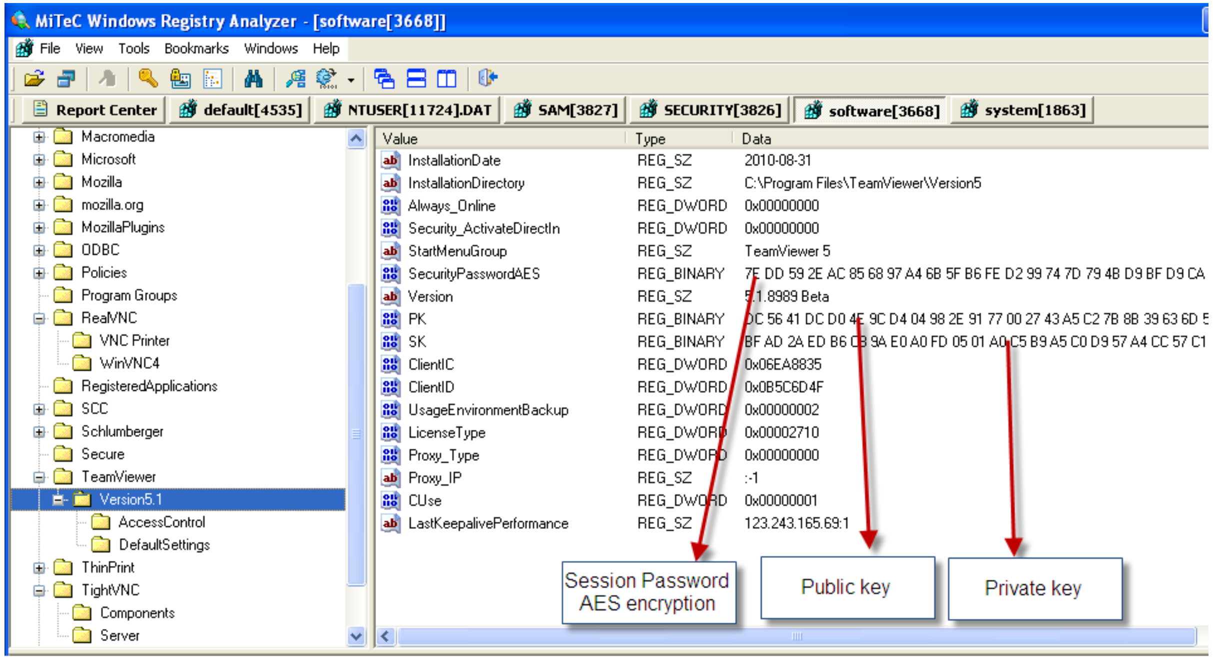


Value	Type	Data
Buddy_QuickPresExclusions	REG_MULTI...	chrome.exe‖msnmsgr.exe‖psr.exe‖super.ex
Buddy_QuickPresExclusions_Ver...	REG_DWORD	0x00000002
Is_Not_Running_Test_Connection	REG_DWORD	0x00000001
MRU	REG_MULTI...	192.168.49.135‖190608302‖213035966‖
Is_Not_First_Run_Without_Conn...	REG_DWORD	0x00000001
Last_Machine_Connections	REG_MULTI...	190608302‖2[illegible]3035966‖
FT_RecentWindowPos	REG_SZ	1,136,88,8[illegible]8,650
FT_Start_Directories	REG_MULTI...	19060[illegible]302?C:\Documents and Settings\Ad
Buddy_WindowPos	REG_MULTI...	1‖8[illegible]3‖233‖1023‖644‖

Client remote session IDs

Figure 42 TeamViewer client IDs

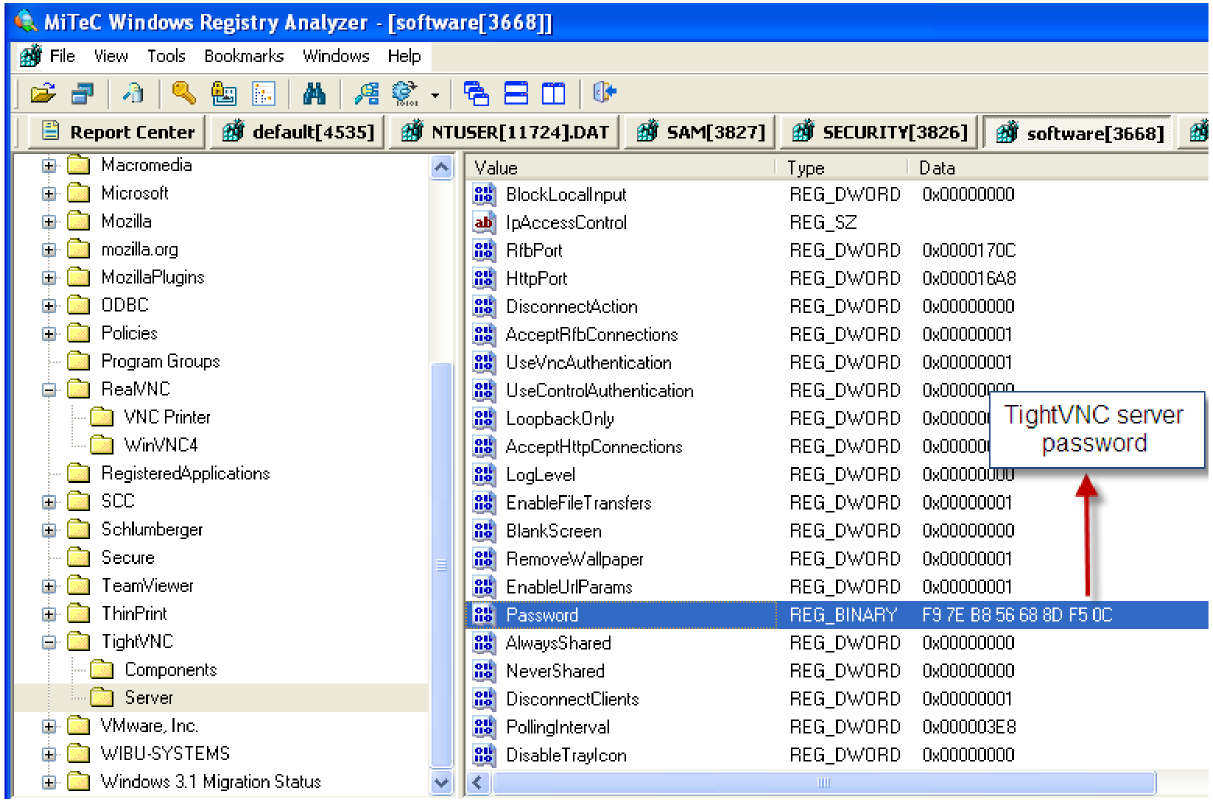
Figure 43 below shows the encrypted private and public keys stored in the registry under HKEY_LOCAL_MACHINE\Software\TeamViewer\Version5. These keys are generated when the client and local computer initiate the connection. The keys are typically encrypted with RSA cipher encryption algorithm. The application also stores session password for connection and is encrypted by AES standards. This was not the case in the earlier images of Windows XP service pack 1 and 2. Therefore Windows XP service pack 3 stores the session password in registry.



Value	Type	Data
InstallationDate	REG_SZ	2010-08-31
InstallationDirectory	REG_SZ	C:\Program Files\TeamViewer\Version5
Always_Online	REG_DWORD	0x00000000
Security_ActivateDirectIn	REG_DWORD	0x00000000
StartMenuGroup	REG_SZ	TeamViewer 5
SecurityPasswordAES	REG_BINARY	7E DD 59 2E AC 85 68 97 A4 6B 5F B6 FE D2 99 74 7D 79 4B D9 BF D9 CA
Version	REG_SZ	5.1.8989 Beta
PK	REG_BINARY	DC 56 41 DC D0 4E 9C D4 04 98 2E 91 77 00 27 43 A5 C2 7B 8B 39 63 6D 5
SK	REG_BINARY	BF AD 2A ED B6 CB 9A E0 A0 FD 05 01 A0 C5 B9 A5 C0 D9 57 A4 CC 57 C1
ClientIC	REG_DWORD	0x06EA8835
ClientID	REG_DWORD	0x0B5C6D4F
UsageEnvironmentBackup	REG_DWORD	0x00000002
LicenseType	REG_DWORD	0x00002710
Proxy_Type	REG_DWORD	0x00000000
Proxy_IP	REG_SZ	:-1
CUse	REG_DWORD	0x00000001
LastKeepalivePerformance	REG_SZ	123.243.165.69:1

Figure 43 TeamViewer encrypted private,public and session password in registry

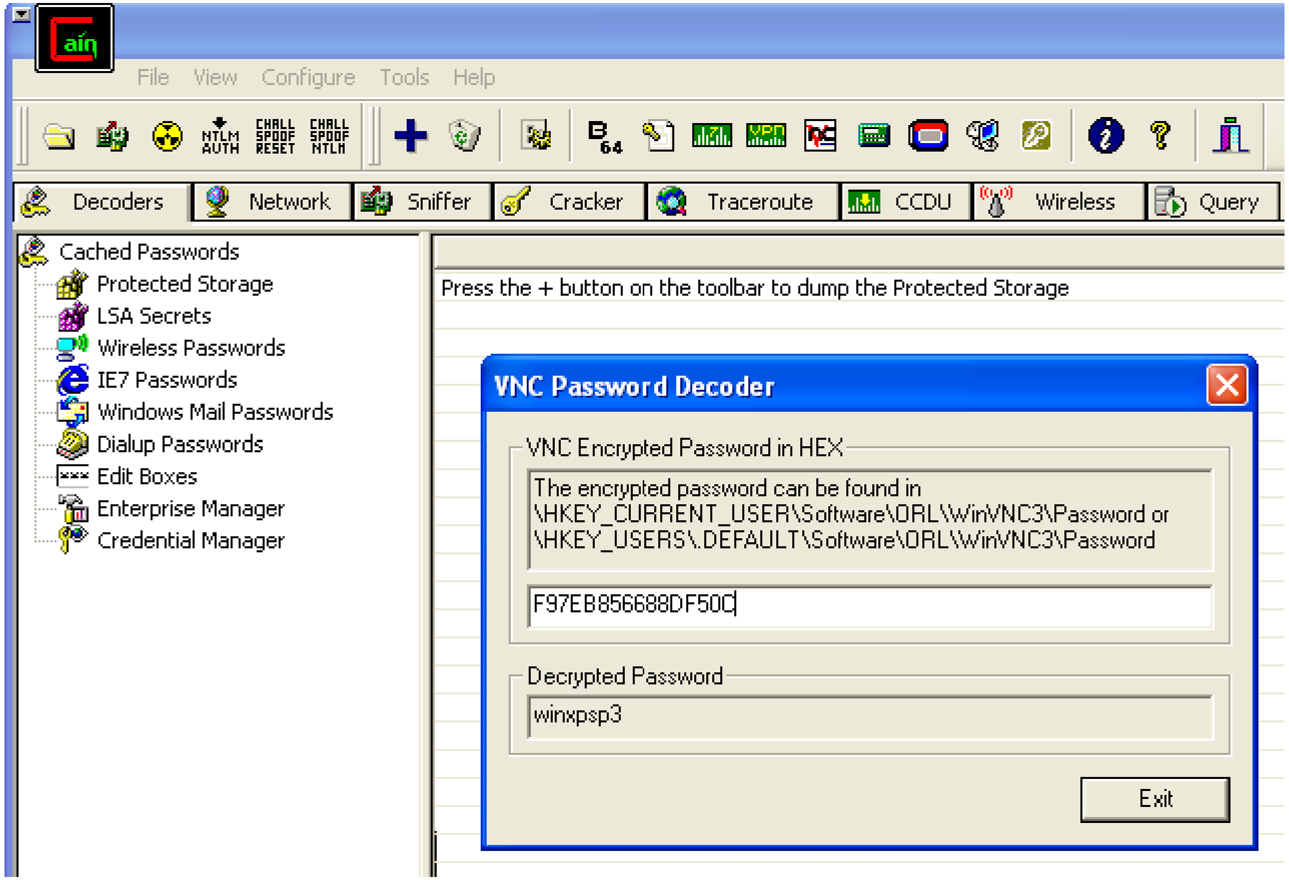
TightVNC also stores the local computers TightVNC server password in the registry under value HKEY_LOCAL_MACHINE\Software\TightVNC\Server. The application also stores the connection and application settings. However as to other VNC applications, it does not save any connection history of the client machines that the local computer connected to. This is shown in the figure 44 below.



Value	Type	Data
BlockLocalInput	REG_DWORD	0x00000000
IpAccessControl	REG_SZ	
RfbPort	REG_DWORD	0x0000170C
HttpPort	REG_DWORD	0x000016A8
DisconnectAction	REG_DWORD	0x00000000
AcceptRfbConnections	REG_DWORD	0x00000001
UseVncAuthentication	REG_DWORD	0x00000001
UseControlAuthentication	REG_DWORD	0x00000000
LoopbackOnly	REG_DWORD	0x00000
AcceptHttpConnections	REG_DWORD	0x00000
LogLevel	REG_DWORD	0x00000000
EnableFileTransfers	REG_DWORD	0x00000001
BlankScreen	REG_DWORD	0x00000000
RemoveWallpaper	REG_DWORD	0x00000001
EnableUrlParams	REG_DWORD	0x00000001
Password	REG_BINARY	F9 7E B8 56 68 8D F5 0C
AlwaysShared	REG_DWORD	0x00000000
NeverShared	REG_DWORD	0x00000000
DisconnectClients	REG_DWORD	0x00000001
PollingInterval	REG_DWORD	0x000003E8
DisableTrayIcon	REG_DWORD	0x00000000

Figure 44 TightVNC server session encrypted password stored in registry

The figure 45 below shows the TightVNC decrypted password by Abel and Cain tool. Basically just type in the encypted password found under the registry and Abel and Cain will decrypt and show the server password. As shown below ***winxpsp3*** was the decrypted password.



Press the + button on the toolbar to dump the Protected Storage

VNC Encrypted Password in HEX

The encrypted password can be found in
\HKEY_CURRENT_USER\Software\ORL\WinVNC3\Password or
\HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3\Password

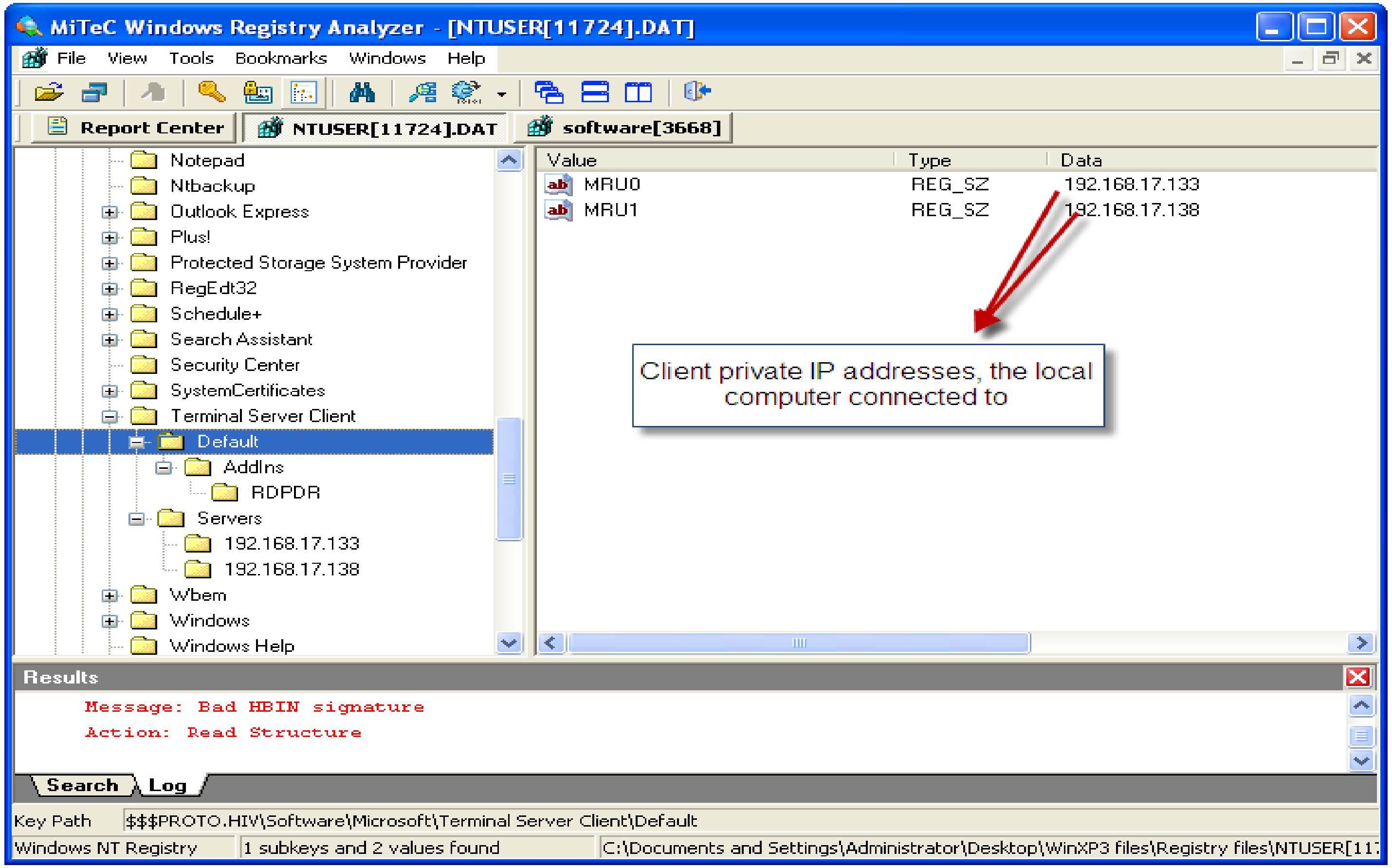
F97EB856688DF50C

Decrypted Password

winxpsp3

Figure 45 TightVNC decrypted password using Abel and Cain

Figure 46 shows the client connection history saved by the RDP under the value HKEY_CURRENT_USER \Software\Microsoft\Terminal Server Client\Default. These are again the private IP addresses of the client.



Value	Type	Data
MRU0	REG_SZ	192.168.17.133
MRU1	REG_SZ	192.168.17.138

Client private IP addresses, the local computer connected to

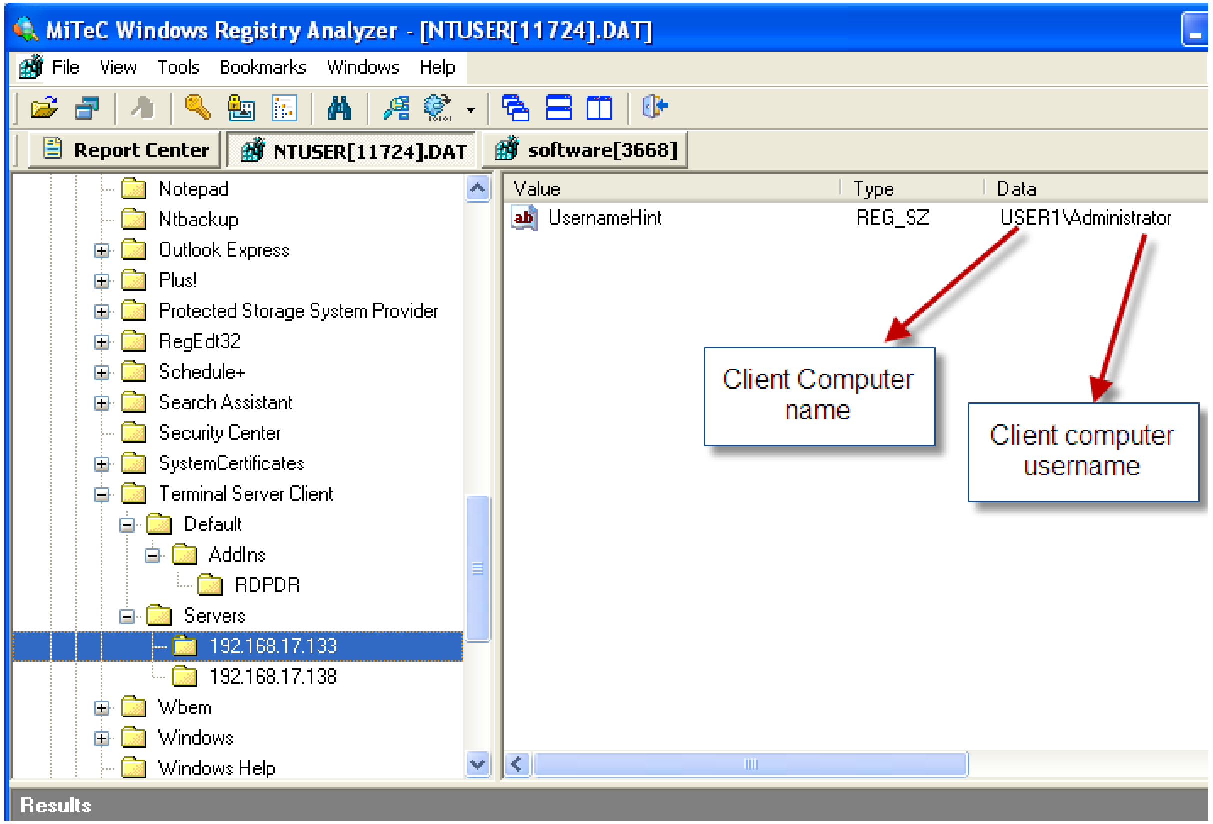
```
Message: Bad HBIN signature
Action: Read Structure
```

Key Path $$$PROTO.HIV\Software\Microsoft\Terminal Server Client\Default

Windows NT Registry | 1 subkeys and 2 values found | C:\Documents and Settings\Administrator\Desktop\WinXP3 files\Registry files\NTUSER[11

Figure 46 Remote desktop protocol settings

Figure 47below shows that RDP or terminal service client also stores the computer name and username of the client. This was not the case in earlier images. This can be important as you have the username and computer name of the client of computer which made a remote connection.



Value	Type	Data
UsernameHint	REG_SZ	USER1\Administrator

Client Computer name

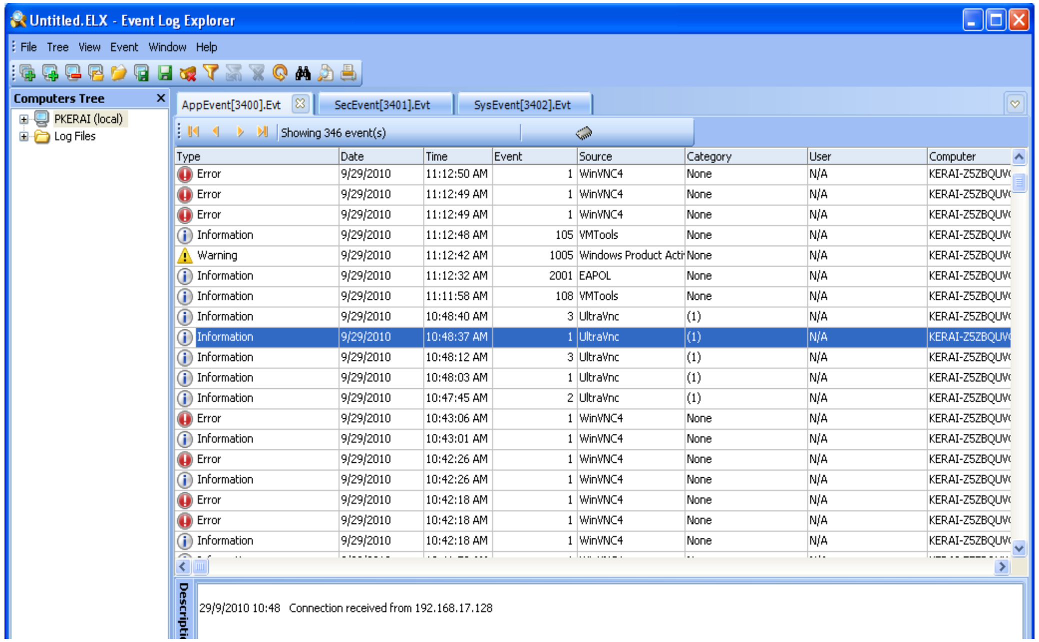
Client computer username

Figure 47 Remote desktop protocol client information

8.4 Appendix D - Log File Analysis

8.4.1 Image 1

Figure 48 below shows the application log under the event viewer of UltraVNC. UltraVNC logs information on the client computer only, therefore the application does not log connection information on the host computer. The log information consists of IP address and connection received and end date and time.

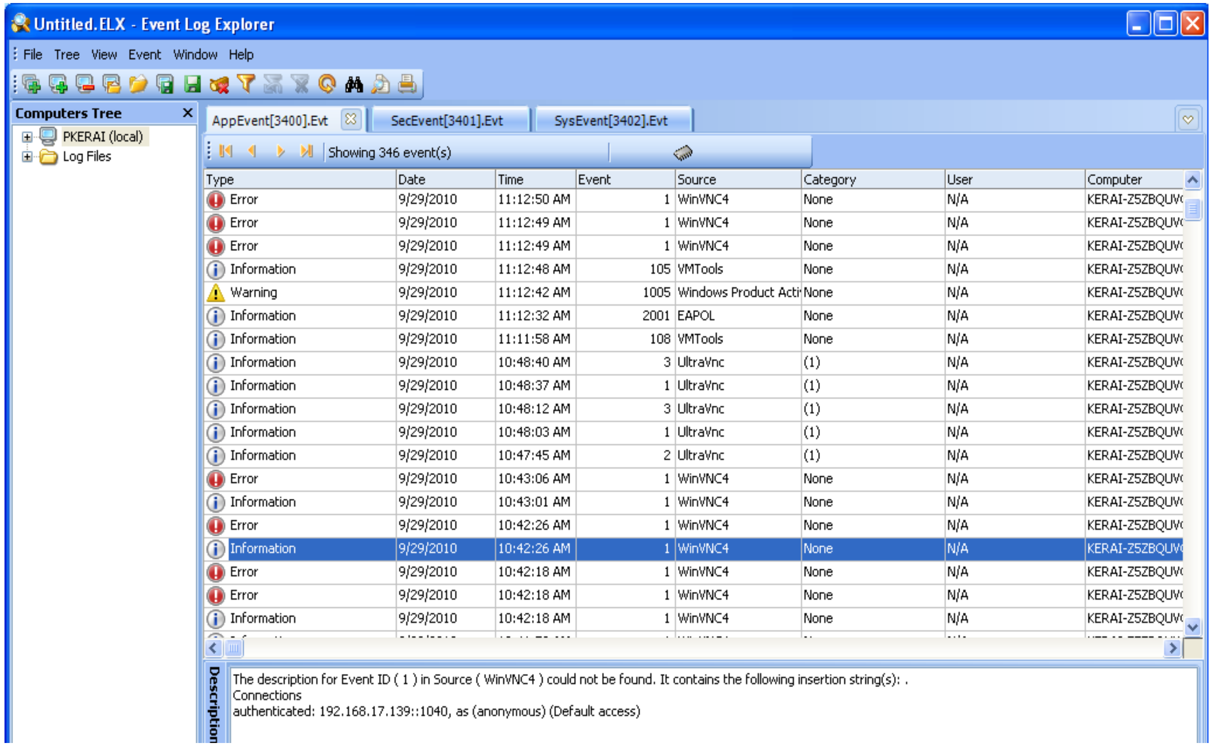


Type	Date	Time	Event	Source	Category	User	Computer
Error	9/29/2010	11:12:50 AM	1	WinVNC4	None	N/A	KERAI-Z5ZBQUV
Error	9/29/2010	11:12:49 AM	1	WinVNC4	None	N/A	KERAI-Z5ZBQUV
Error	9/29/2010	11:12:49 AM	1	WinVNC4	None	N/A	KERAI-Z5ZBQUV
Information	9/29/2010	11:12:48 AM	105	VMTools	None	N/A	KERAI-Z5ZBQUV
Warning	9/29/2010	11:12:42 AM	1005	Windows Product Acti	None	N/A	KERAI-Z5ZBQUV
Information	9/29/2010	11:12:32 AM	2001	EAPOL	None	N/A	KERAI-Z5ZBQUV
Information	9/29/2010	11:11:58 AM	108	VMTools	None	N/A	KERAI-Z5ZBQUV
Information	9/29/2010	10:48:40 AM	3	UltraVnc	(1)	N/A	KERAI-Z5ZBQUV
Information	9/29/2010	10:48:37 AM	1	UltraVnc	(1)	N/A	KERAI-Z5ZBQUV
Information	9/29/2010	10:48:12 AM	3	UltraVnc	(1)	N/A	KERAI-Z5ZBQUV
Information	9/29/2010	10:48:03 AM	1	UltraVnc	(1)	N/A	KERAI-Z5ZBQUV
Information	9/29/2010	10:47:45 AM	2	UltraVnc	(1)	N/A	KERAI-Z5ZBQUV
Error	9/29/2010	10:43:06 AM	1	WinVNC4	None	N/A	KERAI-Z5ZBQUV
Information	9/29/2010	10:43:01 AM	1	WinVNC4	None	N/A	KERAI-Z5ZBQUV
Error	9/29/2010	10:42:26 AM	1	WinVNC4	None	N/A	KERAI-Z5ZBQUV
Information	9/29/2010	10:42:26 AM	1	WinVNC4	None	N/A	KERAI-Z5ZBQUV
Error	9/29/2010	10:42:18 AM	1	WinVNC4	None	N/A	KERAI-Z5ZBQUV
Error	9/29/2010	10:42:18 AM	1	WinVNC4	None	N/A	KERAI-Z5ZBQUV
Information	9/29/2010	10:42:18 AM	1	WinVNC4	None	N/A	KERAI-Z5ZBQUV

```
29/9/2010 10:48   Connection received from 192.168.17.128
```

Figure 48 Application event log of UltraVNC

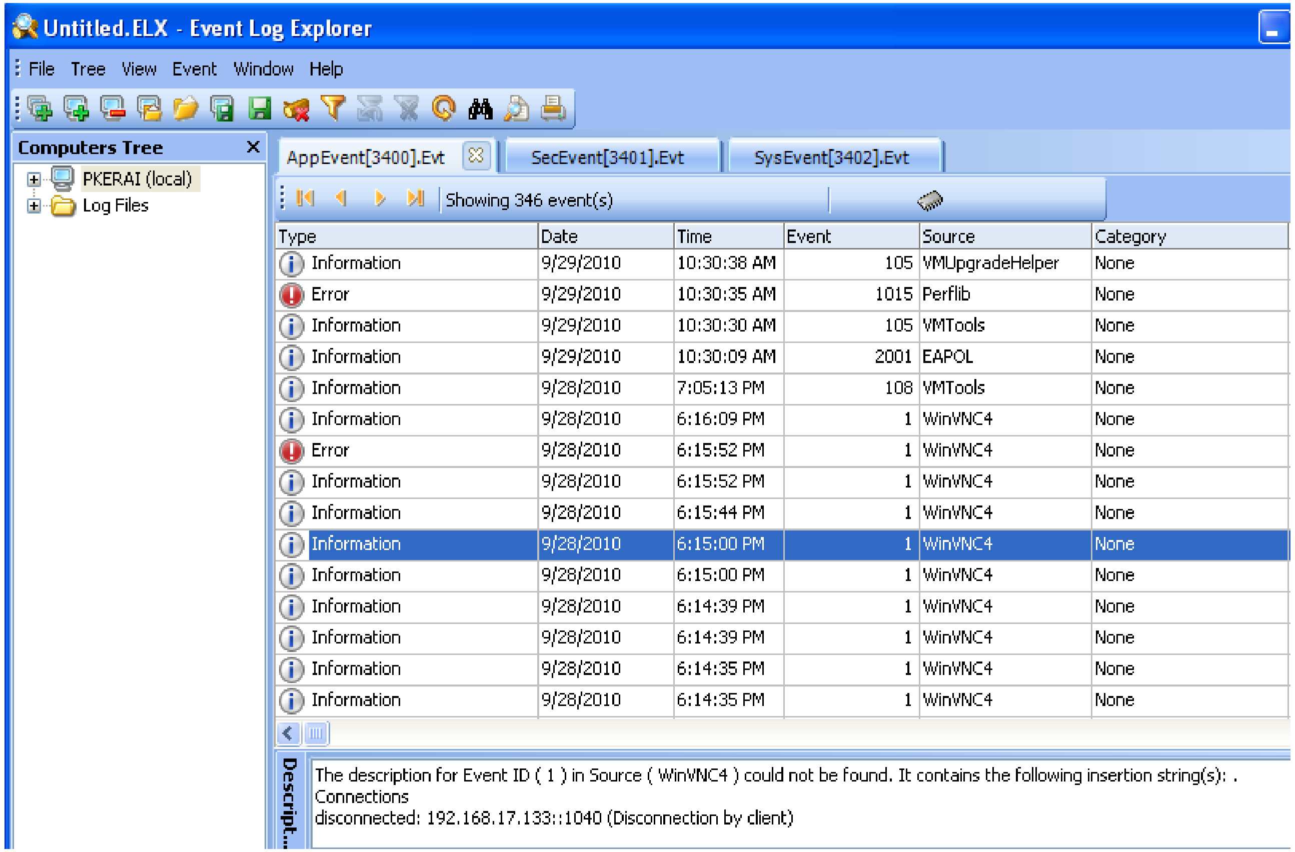
Figures 49-50 shows the application log information of RealVNC under the event viewer. RealVNC logs log information consists of IP address and connection received and end date and time. However the IP address in the log is of the client machine not of the host computer. The application does not log connection information on the host computer.



Type	Date	Time	Event	Source	Category	User	Computer
Error	9/29/2010	11:12:50 AM	1	WinVNC4	None	N/A	KERAI-Z5ZBQUV
Error	9/29/2010	11:12:49 AM	1	WinVNC4	None	N/A	KERAI-Z5ZBQUV
Error	9/29/2010	11:12:49 AM	1	WinVNC4	None	N/A	KERAI-Z5ZBQUV
Information	9/29/2010	11:12:48 AM	105	VMTools	None	N/A	KERAI-Z5ZBQUV
Warning	9/29/2010	11:12:42 AM	1005	Windows Product Acti	None	N/A	KERAI-Z5ZBQUV
Information	9/29/2010	11:12:32 AM	2001	EAPOL	None	N/A	KERAI-Z5ZBQUV
Information	9/29/2010	11:11:58 AM	108	VMTools	None	N/A	KERAI-Z5ZBQUV
Information	9/29/2010	10:48:40 AM	3	UltraVnc	(1)	N/A	KERAI-Z5ZBQUV
Information	9/29/2010	10:48:37 AM	1	UltraVnc	(1)	N/A	KERAI-Z5ZBQUV
Information	9/29/2010	10:48:12 AM	3	UltraVnc	(1)	N/A	KERAI-Z5ZBQUV
Information	9/29/2010	10:48:03 AM	1	UltraVnc	(1)	N/A	KERAI-Z5ZBQUV
Information	9/29/2010	10:47:45 AM	2	UltraVnc	(1)	N/A	KERAI-Z5ZBQUV
Error	9/29/2010	10:43:06 AM	1	WinVNC4	None	N/A	KERAI-Z5ZBQUV
Information	9/29/2010	10:43:01 AM	1	WinVNC4	None	N/A	KERAI-Z5ZBQUV
Error	9/29/2010	10:42:26 AM	1	WinVNC4	None	N/A	KERAI-Z5ZBQUV
Information	9/29/2010	10:42:26 AM	1	WinVNC4	None	N/A	KERAI-Z5ZBQUV
Error	9/29/2010	10:42:18 AM	1	WinVNC4	None	N/A	KERAI-Z5ZBQUV
Error	9/29/2010	10:42:18 AM	1	WinVNC4	None	N/A	KERAI-Z5ZBQUV
Information	9/29/2010	10:42:18 AM	1	WinVNC4	None	N/A	KERAI-Z5ZBQUV

```
The description for Event ID ( 1 ) in Source ( WinVNC4 ) could not be found. It contains the following insertion string(s): .
Connections
authenticated: 192.168.17.139::1040, as (anonymous) (Default access)
```

Figure 49 Application Log information of RealVNC

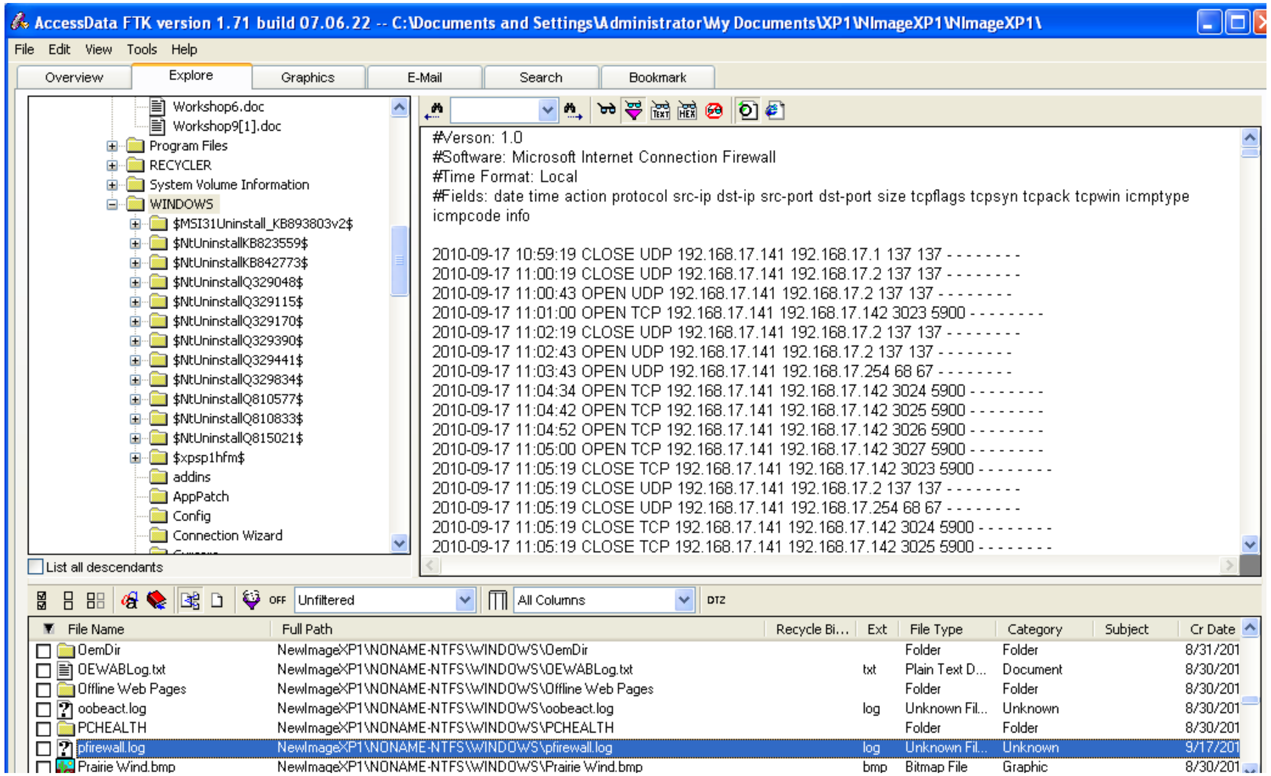


Type	Date	Time	Event	Source	Category
Information	9/29/2010	10:30:38 AM	105	VMUpgradeHelper	None
Error	9/29/2010	10:30:35 AM	1015	Perflib	None
Information	9/29/2010	10:30:30 AM	105	VMTools	None
Information	9/29/2010	10:30:09 AM	2001	EAPOL	None
Information	9/28/2010	7:05:13 PM	108	VMTools	None
Information	9/28/2010	6:16:09 PM	1	WinVNC4	None
Error	9/28/2010	6:15:52 PM	1	WinVNC4	None
Information	9/28/2010	6:15:52 PM	1	WinVNC4	None
Information	9/28/2010	6:15:44 PM	1	WinVNC4	None
Information	9/28/2010	6:15:00 PM	1	WinVNC4	None
Information	9/28/2010	6:15:00 PM	1	WinVNC4	None
Information	9/28/2010	6:14:39 PM	1	WinVNC4	None
Information	9/28/2010	6:14:39 PM	1	WinVNC4	None
Information	9/28/2010	6:14:35 PM	1	WinVNC4	None
Information	9/28/2010	6:14:35 PM	1	WinVNC4	None

```
The description for Event ID ( 1 ) in Source ( WinVNC4 ) could not be found. It contains the following insertion string(s): .
Connections
disconnected: 192.168.17.133::1040 (Disconnection by client)
```

Figure 50 Application Log information of RealVNC

Figure 51 shows the firewall log of image 1. In all Windows XP service packs firewall logging is by default disabled. Therefore logging was enabled on all the three image machines for logging purpose. The firewall log consists of all incoming and outgoing connection on the local network including connection data, time; ports used for connection, type of protocol and also IP addresses that the local computer connected to.

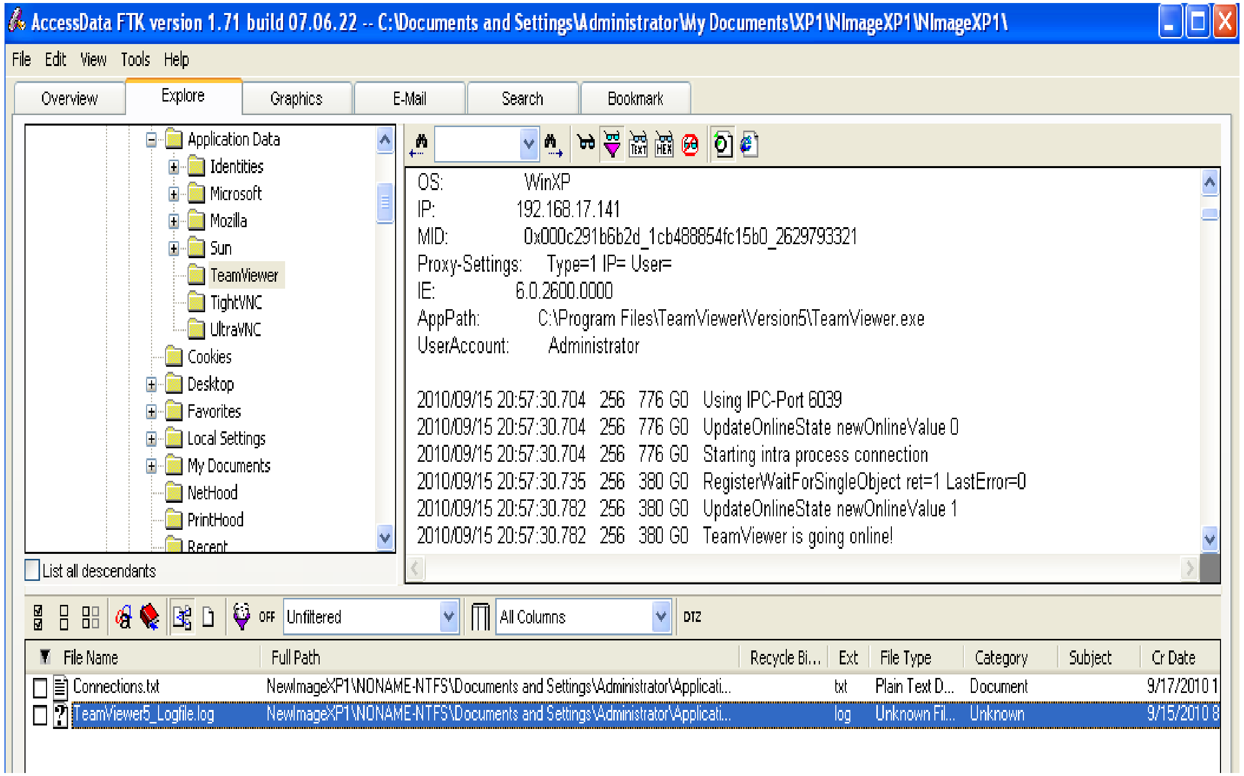


```
#Verson: 1.0
#Software: Microsoft Internet Connection Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype
icmpcode info

2010-09-17 10:59:19 CLOSE UDP 192.168.17.141 192.168.17.1 137 137 - - - - - - - -
2010-09-17 11:00:19 CLOSE UDP 192.168.17.141 192.168.17.2 137 137 - - - - - - - -
2010-09-17 11:00:43 OPEN UDP 192.168.17.141 192.168.17.2 137 137 - - - - - - - -
2010-09-17 11:01:00 OPEN TCP 192.168.17.141 192.168.17.142 3023 5900 - - - - - - - -
2010-09-17 11:02:19 CLOSE UDP 192.168.17.141 192.168.17.2 137 137 - - - - - - - -
2010-09-17 11:02:43 OPEN UDP 192.168.17.141 192.168.17.2 137 137 - - - - - - - -
2010-09-17 11:03:43 OPEN UDP 192.168.17.141 192.168.17.254 68 67 - - - - - - - -
2010-09-17 11:04:34 OPEN TCP 192.168.17.141 192.168.17.142 3024 5900 - - - - - - - -
2010-09-17 11:04:42 OPEN TCP 192.168.17.141 192.168.17.142 3025 5900 - - - - - - - -
2010-09-17 11:04:52 OPEN TCP 192.168.17.141 192.168.17.142 3026 5900 - - - - - - - -
2010-09-17 11:05:00 OPEN TCP 192.168.17.141 192.168.17.142 3027 5900 - - - - - - - -
2010-09-17 11:05:19 CLOSE TCP 192.168.17.141 192.168.17.142 3023 5900 - - - - - - - -
2010-09-17 11:05:19 CLOSE UDP 192.168.17.141 192.168.17.2 137 137 - - - - - - - -
2010-09-17 11:05:19 CLOSE UDP 192.168.17.141 192.168.17.254 68 67 - - - - - - - -
2010-09-17 11:05:19 CLOSE TCP 192.168.17.141 192.168.17.142 3024 5900 - - - - - - - -
2010-09-17 11:05:19 CLOSE TCP 192.168.17.141 192.168.17.142 3025 5900 - - - - - - - -
```

	File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date
☐	OemDir	NewImageXP1\NONAME-NTFS\WINDOWS\OemDir			Folder	Folder		8/31/201
☐	OEWABLog.txt	NewImageXP1\NONAME-NTFS\WINDOWS\OEWABLog.txt		txt	Plain Text D...	Document		8/30/201
☐	Offline Web Pages	NewImageXP1\NONAME-NTFS\WINDOWS\Offline Web Pages			Folder	Folder		8/30/201
☐	oobeact.log	NewImageXP1\NONAME-NTFS\WINDOWS\oobeact.log		log	Unknown Fil...	Unknown		8/30/201
☐	PCHEALTH	NewImageXP1\NONAME-NTFS\WINDOWS\PCHEALTH			Folder	Folder		8/30/201
☐	pfirewall.log	NewImageXP1\NONAME-NTFS\WINDOWS\pfirewall.log		log	Unknown Fil...	Unknown		9/17/201
☐	Prairie Wind.bmp	NewImageXP1\NONAME-NTFS\WINDOWS\Prairie Wind.bmp		bmp	Bitmap File	Graphic		8/30/201

Figure 51 Firewall log information for Image 1

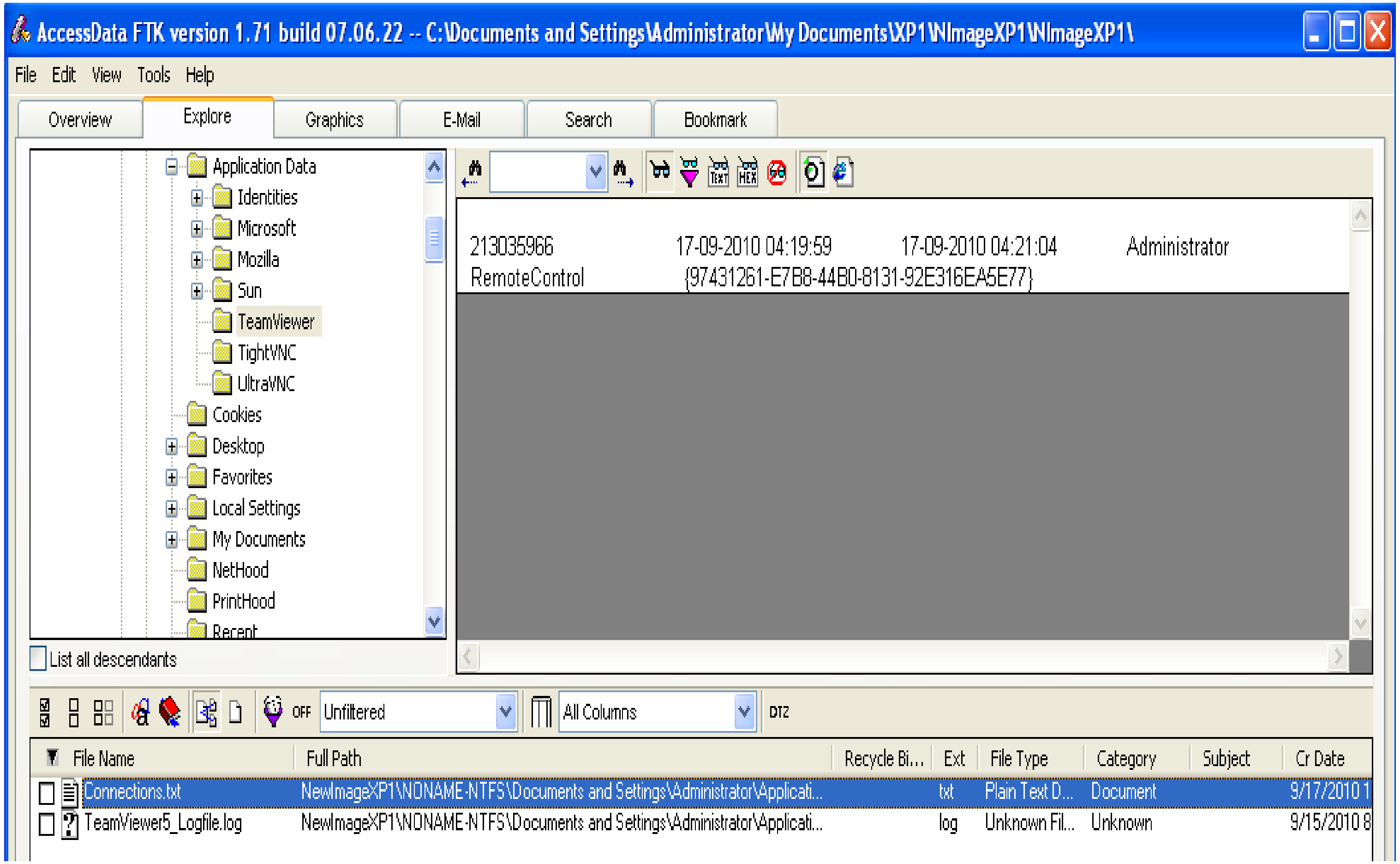
Figure 51-54 below shows the connection logs of Team viewer. Normally Team viewer log files are located under C:\Documents and Settings\Administrator\Application Data\TeamViewer. The folder consists of two files namely; connections.txt, this file consists of the client IDs used for connection including the date and time for connection.TeamViewer5_Logfile, this file consists of all the connection details such as connection settings, connection encryption, file transfer log and other connection related information. Figure 54 shows the files transferred using Team Viewer and where the files were placed.



```
OS:             WinXP
IP:            192.168.17.141
MID:            0x000c291b6b2d_1cb488854fc15b0_2629793321
Proxy-Settings:    Type=1 IP= User=
IE:            6.0.2600.0000
AppPath:          C:\Program Files\TeamViewer\Version5\TeamViewer.exe
UserAccount:       Administrator

2010/09/15 20:57:30.704   256   776 G0   Using IPC-Port 6039
2010/09/15 20:57:30.704   256   776 G0   UpdateOnlineState newOnlineValue 0
2010/09/15 20:57:30.704   256   776 G0   Starting intra process connection
2010/09/15 20:57:30.735   256   380 G0   RegisterWaitForSingleObject ret=1 LastError=0
2010/09/15 20:57:30.782   256   380 G0   UpdateOnlineState newOnlineValue 1
2010/09/15 20:57:30.782   256   380 G0   TeamViewer is going online!
```

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date
☐ Connections.txt	NewImageXP1\NONAME-NTFS\Documents and Settings\Administrator\Applicati...		txt	Plain Text D...	Document		9/17/2010 1
☐ TeamViewer5_Logfile.log	NewImageXP1\NONAME-NTFS\Documents and Settings\Administrator\Applicati...		log	Unknown Fil...	Unknown		9/15/2010 8

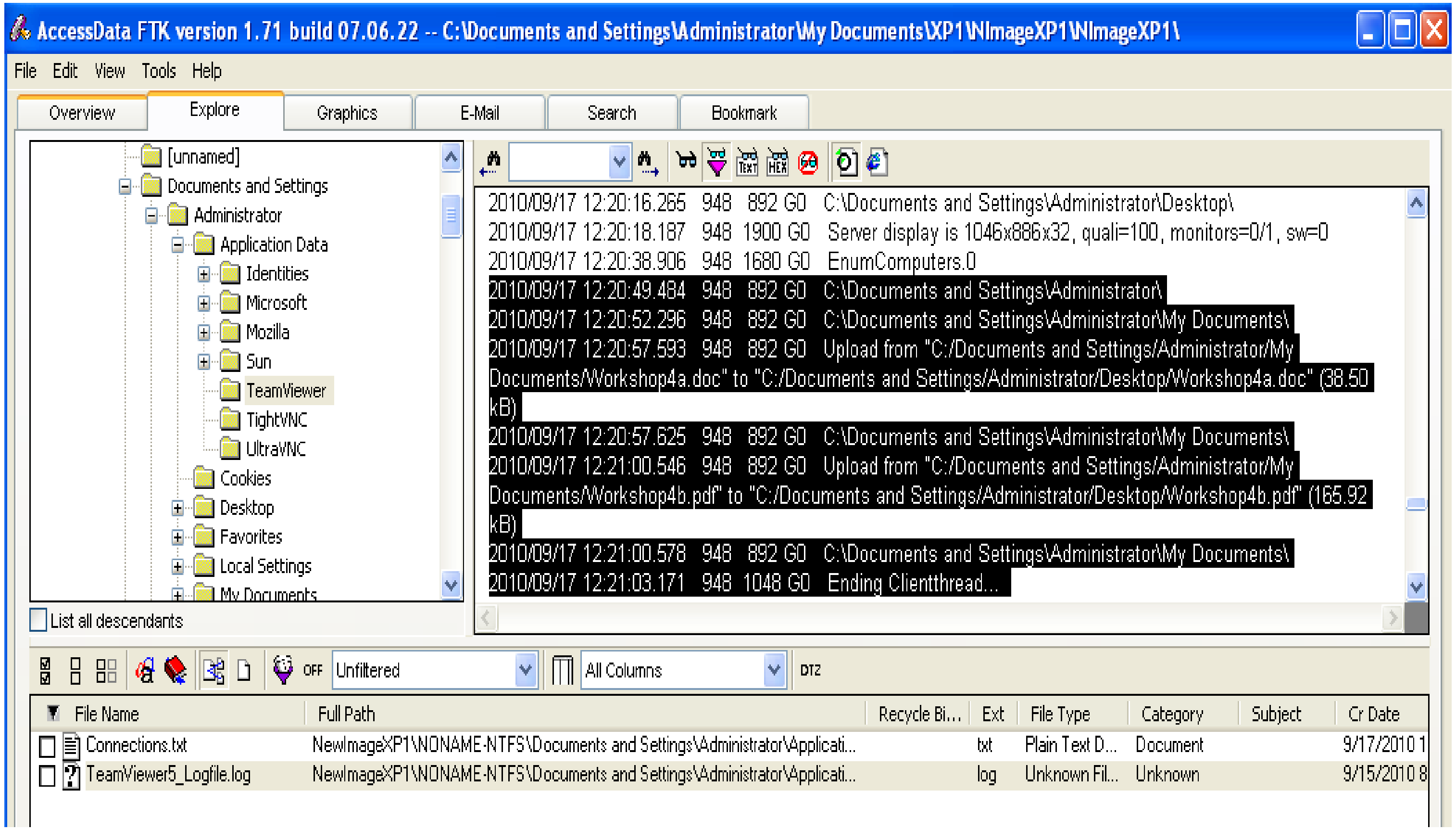
Figure 52 TeamViewer connection log information



```
213035966        17-09-2010 04:19:59        17-09-2010 04:21:04        Administrator
RemoteControl     {97431261-E7B8-44B0-8131-92E316EA5E77}
```

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date
☐ Connections.txt	NewImageXP1\NONAME-NTFS\Documents and Settings\Administrator\Applicati...		txt	Plain Text D...	Document		9/17/2010 1
☐ TeamViewer5_Logfile.log	NewImageXP1\NONAME-NTFS\Documents and Settings\Administrator\Applicati...		log	Unknown Fil...	Unknown		9/15/2010 8

Figure 53 Team Viewer connection log



```
2010/09/17 12:20:16.265   948   892 G0   C:\Documents and Settings\Administrator\Desktop\
2010/09/17 12:20:18.187   948  1900 G0   Server display is 1046x886x32, quali=100, monitors=0/1, sw=0
2010/09/17 12:20:38.906   948  1680 G0   EnumComputers.0
2010/09/17 12:20:49.484   948   892 G0   C:\Documents and Settings\Administrator\
2010/09/17 12:20:52.296   948   892 G0   C:\Documents and Settings\Administrator\My Documents\
2010/09/17 12:20:57.593   948   892 G0   Upload from "C:/Documents and Settings/Administrator/My
Documents/Workshop4a.doc" to "C:/Documents and Settings/Administrator/Desktop/Workshop4a.doc" (38.50
kB)
2010/09/17 12:20:57.625   948   892 G0   C:\Documents and Settings\Administrator\My Documents\
2010/09/17 12:21:00.546   948   892 G0   Upload from "C:/Documents and Settings/Administrator/My
Documents/Workshop4b.pdf" to "C:/Documents and Settings/Administrator/Desktop/Workshop4b.pdf" (165.92
kB)
2010/09/17 12:21:00.578   948   892 G0   C:\Documents and Settings\Administrator\My Documents\
2010/09/17 12:21:03.171   948  1048 G0   Ending Clientthread...
```

Unfiltered

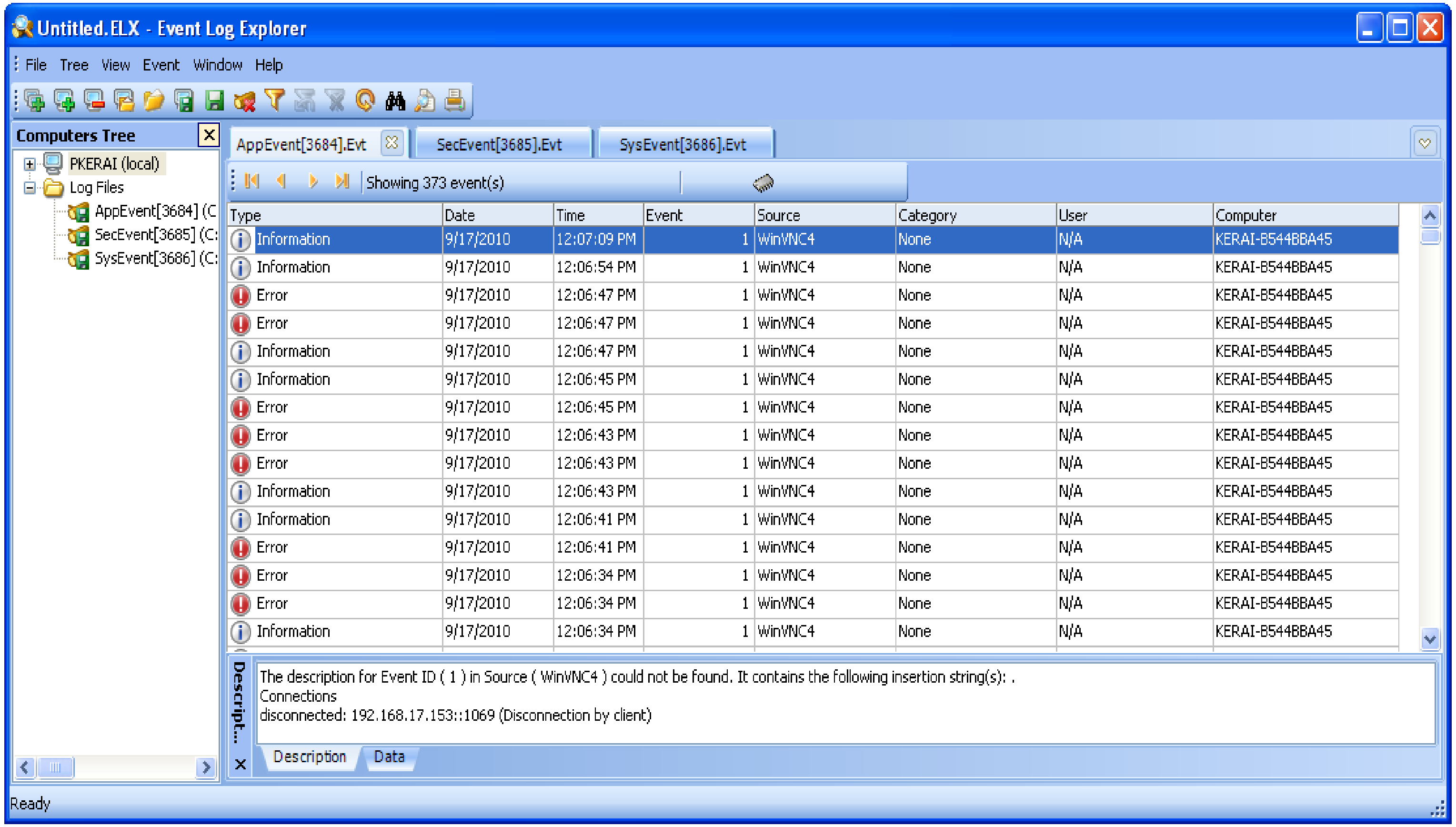
All Columns

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date
☐ Connections.txt	NewImageXP1\NONAME-NTFS\Documents and Settings\Administrator\Applicati...		txt	Plain Text D...	Document		9/17/2010 1
☐ TeamViewer5_Logfile.log	NewImageXP1\NONAME-NTFS\Documents and Settings\Administrator\Applicati...		log	Unknown Fil...	Unknown		9/15/2010 8

Figure 54 Team Viewer file transfer log information

8.4.2 Image 2 (Windows XP service pack 2)

Figures 55 shows the application log information of RealVNC under the event viewer. RealVNC logs log information consists of IP address and connection received and end date and time. However the IP address in the log is of the client machine not of the host computer. The application does not log connection information on the host computer.

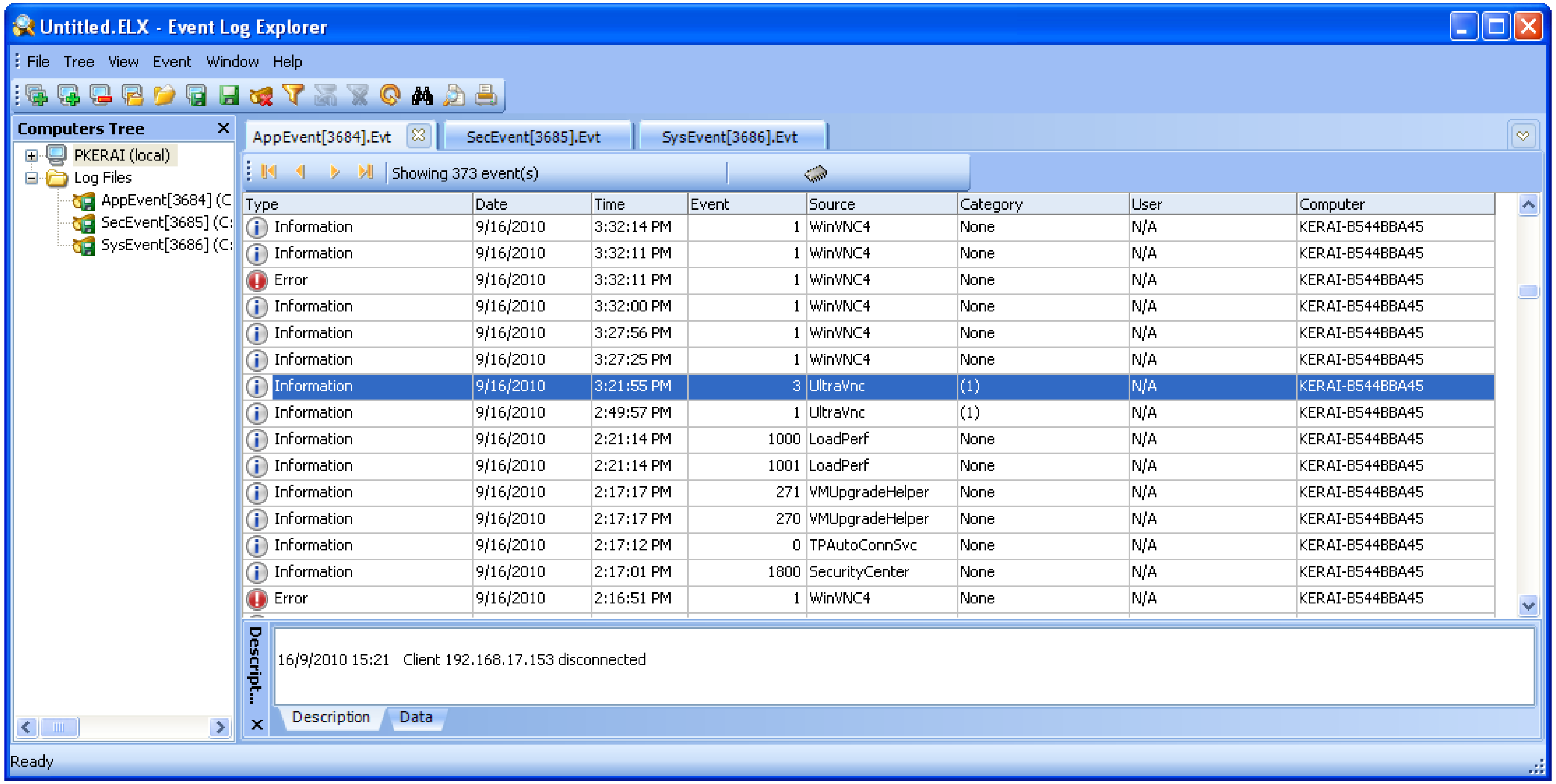


Type	Date	Time	Event	Source	Category	User	Computer
Information	9/17/2010	12:07:09 PM	1	WinVNC4	None	N/A	KERAI-B544BBA45
Information	9/17/2010	12:06:54 PM	1	WinVNC4	None	N/A	KERAI-B544BBA45
Error	9/17/2010	12:06:47 PM	1	WinVNC4	None	N/A	KERAI-B544BBA45
Error	9/17/2010	12:06:47 PM	1	WinVNC4	None	N/A	KERAI-B544BBA45
Information	9/17/2010	12:06:47 PM	1	WinVNC4	None	N/A	KERAI-B544BBA45
Information	9/17/2010	12:06:45 PM	1	WinVNC4	None	N/A	KERAI-B544BBA45
Error	9/17/2010	12:06:45 PM	1	WinVNC4	None	N/A	KERAI-B544BBA45
Error	9/17/2010	12:06:43 PM	1	WinVNC4	None	N/A	KERAI-B544BBA45
Error	9/17/2010	12:06:43 PM	1	WinVNC4	None	N/A	KERAI-B544BBA45
Information	9/17/2010	12:06:43 PM	1	WinVNC4	None	N/A	KERAI-B544BBA45
Information	9/17/2010	12:06:41 PM	1	WinVNC4	None	N/A	KERAI-B544BBA45
Error	9/17/2010	12:06:41 PM	1	WinVNC4	None	N/A	KERAI-B544BBA45
Error	9/17/2010	12:06:34 PM	1	WinVNC4	None	N/A	KERAI-B544BBA45
Error	9/17/2010	12:06:34 PM	1	WinVNC4	None	N/A	KERAI-B544BBA45
Information	9/17/2010	12:06:34 PM	1	WinVNC4	None	N/A	KERAI-B544BBA45

```
The description for Event ID ( 1 ) in Source ( WinVNC4 ) could not be found. It contains the following insertion string(s): .
Connections
disconnected: 192.168.17.153::1069 (Disconnection by client)
```

Figure 55 Application Log information of RealVNC

Figure 56 below shows the application log under the event viewer of UltraVNC. UltraVNC logs information on the client computer only, therefore the application does not log connection information on the host computer. The log information consists of IP address and connection received and end date and time.

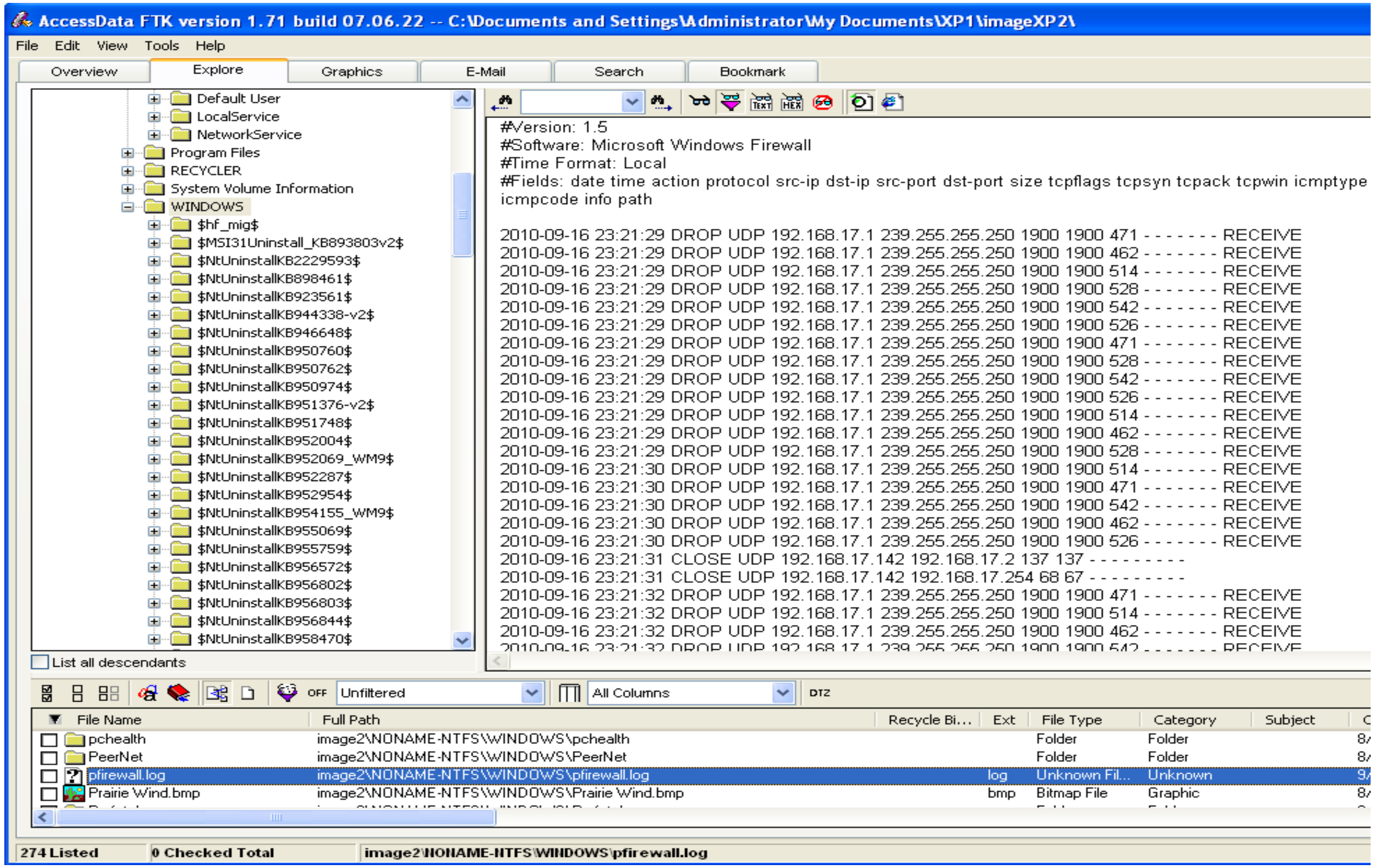


Type	Date	Time	Event	Source	Category	User	Computer
Information	9/16/2010	3:32:14 PM	1	WinVNC4	None	N/A	KERAI-B544BBA45
Information	9/16/2010	3:32:11 PM	1	WinVNC4	None	N/A	KERAI-B544BBA45
Error	9/16/2010	3:32:11 PM	1	WinVNC4	None	N/A	KERAI-B544BBA45
Information	9/16/2010	3:32:00 PM	1	WinVNC4	None	N/A	KERAI-B544BBA45
Information	9/16/2010	3:27:56 PM	1	WinVNC4	None	N/A	KERAI-B544BBA45
Information	9/16/2010	3:27:25 PM	1	WinVNC4	None	N/A	KERAI-B544BBA45
Information	9/16/2010	3:21:55 PM	3	UltraVnc	(1)	N/A	KERAI-B544BBA45
Information	9/16/2010	2:49:57 PM	1	UltraVnc	(1)	N/A	KERAI-B544BBA45
Information	9/16/2010	2:21:14 PM	1000	LoadPerf	None	N/A	KERAI-B544BBA45
Information	9/16/2010	2:21:14 PM	1001	LoadPerf	None	N/A	KERAI-B544BBA45
Information	9/16/2010	2:17:17 PM	271	VMUpgradeHelper	None	N/A	KERAI-B544BBA45
Information	9/16/2010	2:17:17 PM	270	VMUpgradeHelper	None	N/A	KERAI-B544BBA45
Information	9/16/2010	2:17:12 PM	0	TPAutoConnSvc	None	N/A	KERAI-B544BBA45
Information	9/16/2010	2:17:01 PM	1800	SecurityCenter	None	N/A	KERAI-B544BBA45
Error	9/16/2010	2:16:51 PM	1	WinVNC4	None	N/A	KERAI-B544BBA45

```
16/9/2010 15:21   Client 192.168.17.153 disconnected
```

Figure 56 Application event log of UltraVNC

Figure 57 shows the firewall log of image 2. In all Windows XP service packs firewall logging is by default disabled. Therefore logging was enabled on all the three image machines for logging purpose. The firewall log consists of all incoming and outgoing connection on the local network including connection data, time; ports used for connection, type of protocol and also IP addresses that the local computer connected to.



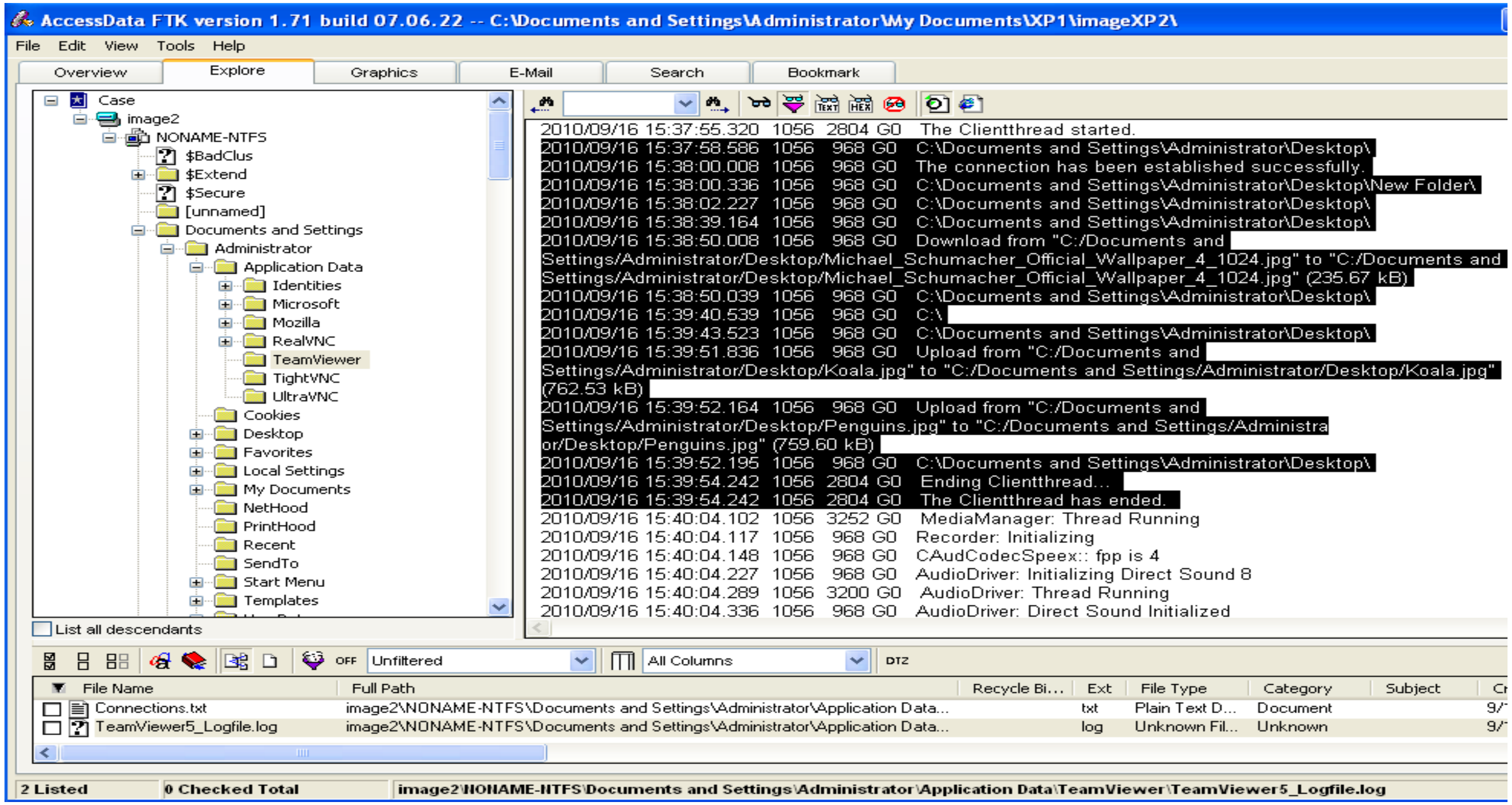
```
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype
icmpcode info path

2010-09-16 23:21:29 DROP UDP 192.168.17.1 239.255.255.250 1900 1900 471 - - - - - - - RECEIVE
2010-09-16 23:21:29 DROP UDP 192.168.17.1 239.255.255.250 1900 1900 462 - - - - - - - RECEIVE
2010-09-16 23:21:29 DROP UDP 192.168.17.1 239.255.255.250 1900 1900 514 - - - - - - - RECEIVE
2010-09-16 23:21:29 DROP UDP 192.168.17.1 239.255.255.250 1900 1900 528 - - - - - - - RECEIVE
2010-09-16 23:21:29 DROP UDP 192.168.17.1 239.255.255.250 1900 1900 542 - - - - - - - RECEIVE
2010-09-16 23:21:29 DROP UDP 192.168.17.1 239.255.255.250 1900 1900 526 - - - - - - - RECEIVE
2010-09-16 23:21:29 DROP UDP 192.168.17.1 239.255.255.250 1900 1900 471 - - - - - - - RECEIVE
2010-09-16 23:21:29 DROP UDP 192.168.17.1 239.255.255.250 1900 1900 528 - - - - - - - RECEIVE
2010-09-16 23:21:29 DROP UDP 192.168.17.1 239.255.255.250 1900 1900 542 - - - - - - - RECEIVE
2010-09-16 23:21:29 DROP UDP 192.168.17.1 239.255.255.250 1900 1900 526 - - - - - - - RECEIVE
2010-09-16 23:21:29 DROP UDP 192.168.17.1 239.255.255.250 1900 1900 514 - - - - - - - RECEIVE
2010-09-16 23:21:29 DROP UDP 192.168.17.1 239.255.255.250 1900 1900 462 - - - - - - - RECEIVE
2010-09-16 23:21:29 DROP UDP 192.168.17.1 239.255.255.250 1900 1900 528 - - - - - - - RECEIVE
2010-09-16 23:21:30 DROP UDP 192.168.17.1 239.255.255.250 1900 1900 514 - - - - - - - RECEIVE
2010-09-16 23:21:30 DROP UDP 192.168.17.1 239.255.255.250 1900 1900 471 - - - - - - - RECEIVE
2010-09-16 23:21:30 DROP UDP 192.168.17.1 239.255.255.250 1900 1900 542 - - - - - - - RECEIVE
2010-09-16 23:21:30 DROP UDP 192.168.17.1 239.255.255.250 1900 1900 462 - - - - - - - RECEIVE
2010-09-16 23:21:30 DROP UDP 192.168.17.1 239.255.255.250 1900 1900 526 - - - - - - - RECEIVE
2010-09-16 23:21:31 CLOSE UDP 192.168.17.142 192.168.17.2 137 137 - - - - - - - - -
2010-09-16 23:21:31 CLOSE UDP 192.168.17.142 192.168.17.254 68 67 - - - - - - - - -
2010-09-16 23:21:32 DROP UDP 192.168.17.1 239.255.255.250 1900 1900 471 - - - - - - - RECEIVE
2010-09-16 23:21:32 DROP UDP 192.168.17.1 239.255.255.250 1900 1900 514 - - - - - - - RECEIVE
2010-09-16 23:21:32 DROP UDP 192.168.17.1 239.255.255.250 1900 1900 462 - - - - - - - RECEIVE
```

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject
☐ pchealth	image2\NONAME-NTFS\WINDOWS\pchealth			Folder	Folder	
☐ PeerNet	image2\NONAME-NTFS\WINDOWS\PeerNet			Folder	Folder	
☐ pfirewall.log	image2\NONAME-NTFS\WINDOWS\pfirewall.log		log	Unknown Fil...	Unknown	
☐ Prairie Wind.bmp	image2\NONAME-NTFS\WINDOWS\Prairie Wind.bmp		bmp	Bitmap File	Graphic	

274 Listed | 0 Checked Total | image2\NONAME-NTFS\WINDOWS\pfirewall.log

Figure 57 Firewall log information for Image 2

Figure 58-59 below shows the connection logs of Team viewer. Normally Team viewer log files are located under C:\Documents and Settings\Administrator\Application Data\TeamViewer. The folder consists of two files namely; connections.txt, this file consists of the client IDs used for connection including the date and time for connection.TeamViewer5_Logfile, this file consists of all the connection details such as connection settings, connection encryption, file transfer log and other connection related information. Figure 54 shows the files transferred using Team Viewer and where the files were placed.

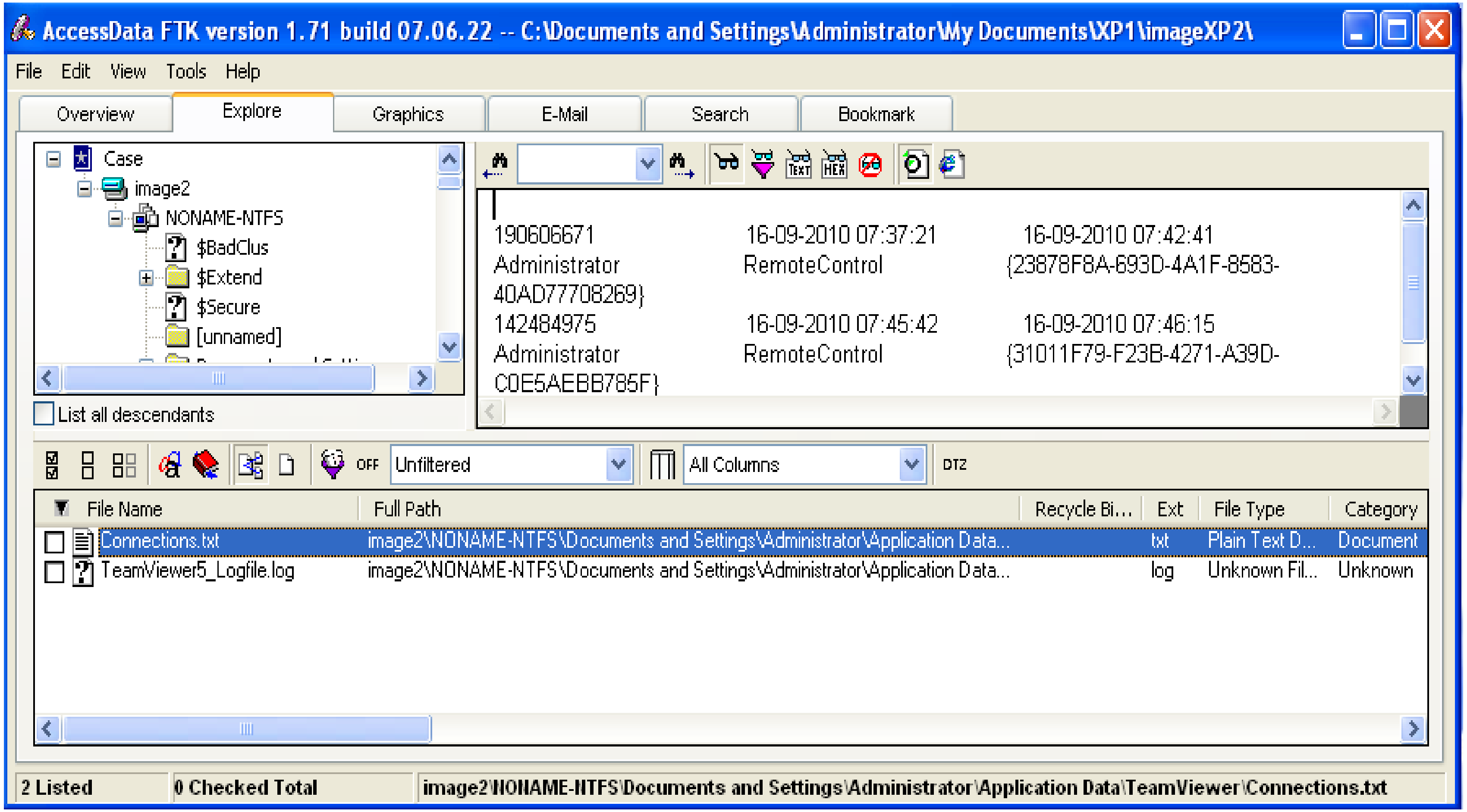


```
2010/09/16 15:37:55.320  1056  2804 G0   The Clientthread started.
2010/09/16 15:37:58.586  1056   968 G0   C:\Documents and Settings\Administrator\Desktop\
2010/09/16 15:38:00.008  1056   968 G0   The connection has been established successfully.
2010/09/16 15:38:00.336  1056   968 G0   C:\Documents and Settings\Administrator\Desktop\New Folder\
2010/09/16 15:38:02.227  1056   968 G0   C:\Documents and Settings\Administrator\Desktop\
2010/09/16 15:38:39.164  1056   968 G0   C:\Documents and Settings\Administrator\Desktop\
2010/09/16 15:38:50.008  1056   968 G0   Download from "C:/Documents and
Settings/Administrator/Desktop/Michael_Schumacher_Official_Wallpaper_4_1024.jpg" to "C:/Documents and
Settings/Administrator/Desktop/Michael_Schumacher_Official_Wallpaper_4_1024.jpg" (235.67 kB)
2010/09/16 15:38:50.039  1056   968 G0   C:\Documents and Settings\Administrator\Desktop\
2010/09/16 15:39:40.539  1056   968 G0   C:\
2010/09/16 15:39:43.523  1056   968 G0   C:\Documents and Settings\Administrator\Desktop\
2010/09/16 15:39:51.836  1056   968 G0   Upload from "C:/Documents and
Settings/Administrator/Desktop/Koala.jpg" to "C:/Documents and Settings/Administrator/Desktop/Koala.jpg"
(762.53 kB)
2010/09/16 15:39:52.164  1056   968 G0   Upload from "C:/Documents and
Settings/Administrator/Desktop/Penguins.jpg" to "C:/Documents and Settings/Administra
or/Desktop/Penguins.jpg" (759.60 kB)
2010/09/16 15:39:52.195  1056   968 G0   C:\Documents and Settings\Administrator\Desktop\
2010/09/16 15:39:54.242  1056  2804 G0   Ending Clientthread...
2010/09/16 15:39:54.242  1056  2804 G0   The Clientthread has ended.
2010/09/16 15:40:04.102  1056  3252 G0   MediaManager: Thread Running
2010/09/16 15:40:04.117  1056   968 G0   Recorder: Initializing
2010/09/16 15:40:04.148  1056   968 G0   CAudCodecSpeex:: fpp is 4
2010/09/16 15:40:04.227  1056   968 G0   AudioDriver: Initializing Direct Sound 8
2010/09/16 15:40:04.289  1056  3200 G0   AudioDriver: Thread Running
2010/09/16 15:40:04.336  1056   968 G0   AudioDriver: Direct Sound Initialized
```

	File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr
☐	Connections.txt	image2\NONAME-NTFS\Documents and Settings\Administrator\Application Data...		txt	Plain Text D...	Document		9/
☐	TeamViewer5_Logfile.log	image2\NONAME-NTFS\Documents and Settings\Administrator\Application Data...		log	Unknown Fil...	Unknown		9/

2 Listed | 0 Checked Total | image2\NONAME-NTFS\Documents and Settings\Administrator\Application Data\TeamViewer\TeamViewer5_Logfile.log

Figure 58 Team Viewer file transfer log information



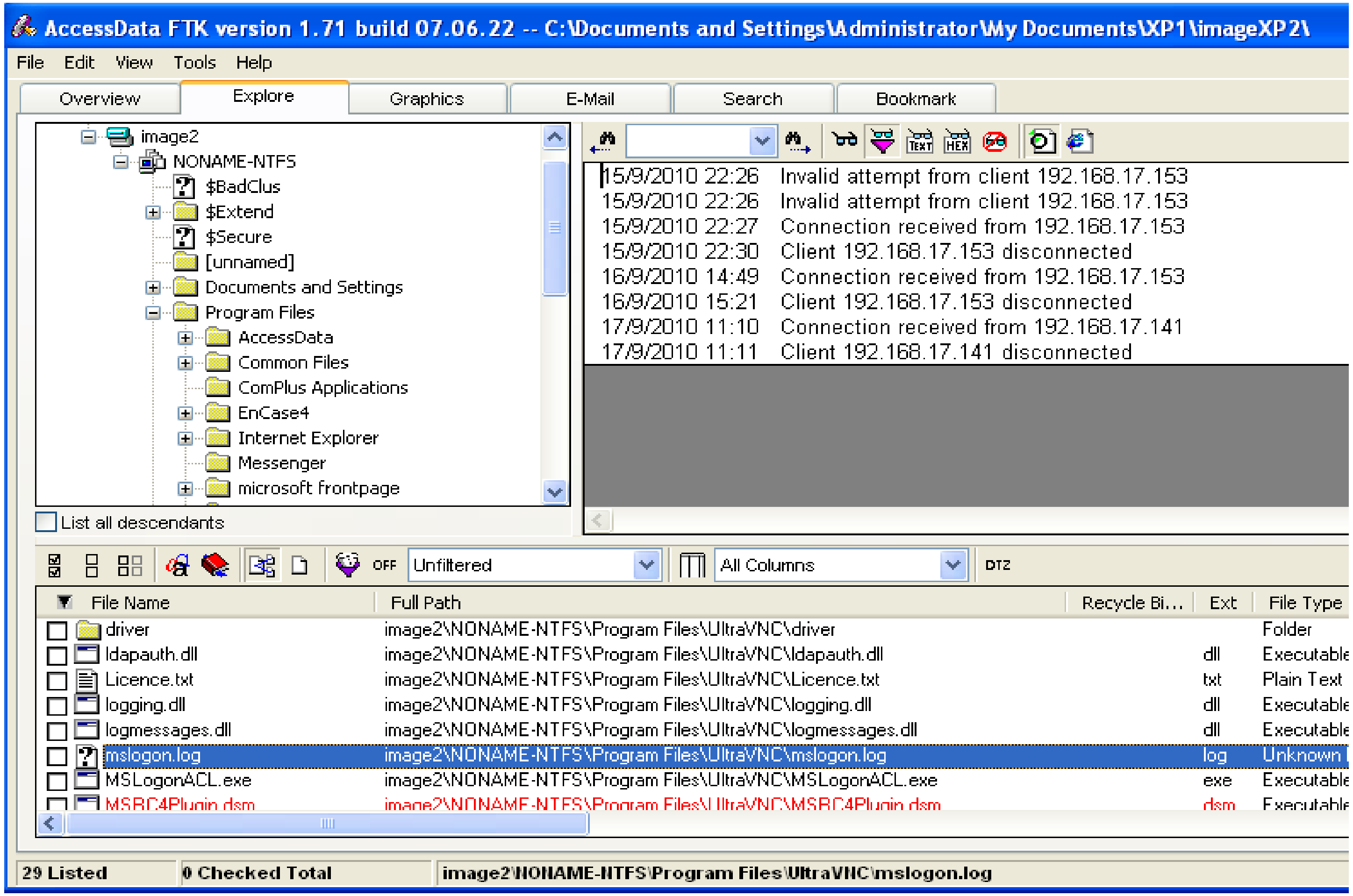
```
190606671          16-09-2010 07:37:21      16-09-2010 07:42:41
Administrator      RemoteControl           {23878F8A-693D-4A1F-8583-
40AD77708269}
142484975          16-09-2010 07:45:42      16-09-2010 07:46:15
Administrator      RemoteControl           {31011F79-F23B-4271-A39D-
C0E5AEBB785F}
```

File Name	Full Path	Recycle Bi...	Ext	File Type	Category
☐ Connections.txt	image2\NONAME-NTFS\Documents and Settings\Administrator\Application Data...		txt	Plain Text D...	Document
☐ TeamViewer5_Logfile.log	image2\NONAME-NTFS\Documents and Settings\Administrator\Application Data...		log	Unknown Fil...	Unknown

2 Listed | 0 Checked Total | image2\NONAME-NTFS\Documents and Settings\Administrator\Application Data\TeamViewer\Connections.txt

Figure 59 Team Viewer connection log

Figure 60 below shows the log file information of Ultra VNC placed under C:\Program Files\UltraVNC. The file is mslogon.log and contains the connections received and date and time of the connections. The file also gives information on who disconnected the remote connection.



```
15/9/2010 22:26  Invalid attempt from client 192.168.17.153
15/9/2010 22:26  Invalid attempt from client 192.168.17.153
15/9/2010 22:27  Connection received from 192.168.17.153
15/9/2010 22:30  Client 192.168.17.153 disconnected
16/9/2010 14:49  Connection received from 192.168.17.153
16/9/2010 15:21  Client 192.168.17.153 disconnected
17/9/2010 11:10  Connection received from 192.168.17.141
17/9/2010 11:11  Client 192.168.17.141 disconnected
```

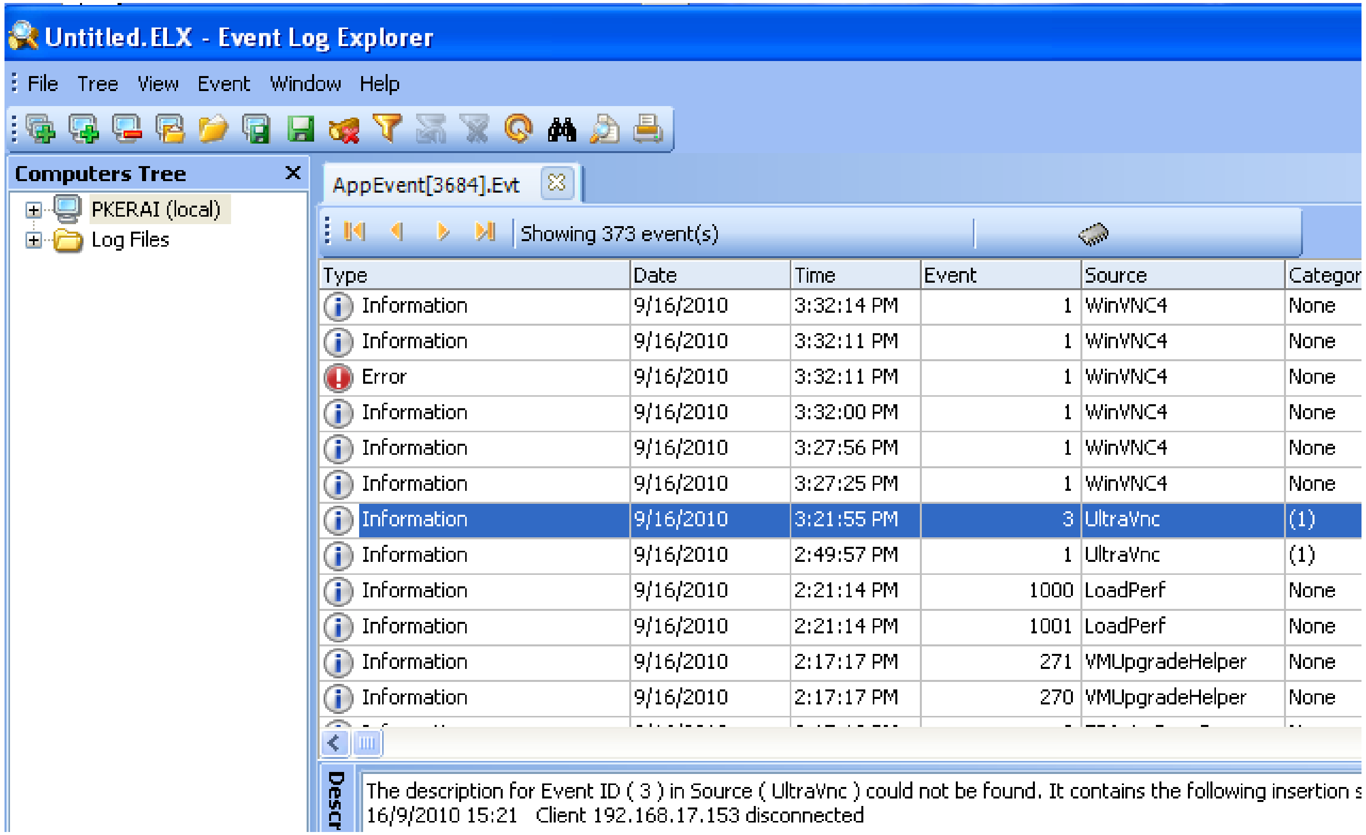
File Name	Full Path	Recycle Bi...	Ext	File Type
☐ driver	image2\NONAME-NTFS\Program Files\UltraVNC\driver			Folder
☐ ldapauth.dll	image2\NONAME-NTFS\Program Files\UltraVNC\ldapauth.dll		dll	Executable
☐ Licence.txt	image2\NONAME-NTFS\Program Files\UltraVNC\Licence.txt		txt	Plain Text
☐ logging.dll	image2\NONAME-NTFS\Program Files\UltraVNC\logging.dll		dll	Executable
☐ logmessages.dll	image2\NONAME-NTFS\Program Files\UltraVNC\logmessages.dll		dll	Executable
☐ mslogon.log	image2\NONAME-NTFS\Program Files\UltraVNC\mslogon.log		log	Unknown
☐ MSLogonACL.exe	image2\NONAME-NTFS\Program Files\UltraVNC\MSLogonACL.exe		exe	Executable
☐ MSRC4Plugin.dsm	image2\NONAME-NTFS\Program Files\UltraVNC\MSRC4Plugin.dsm		dsm	Executable

29 Listed | 0 Checked Total | image2\NONAME-NTFS\Program Files\UltraVNC\mslogon.log

Figure 60 Ultra VNC log information Image 2

8.4.3 Image 3 (Windows XP service pack 3)

Figure 61 below shows the application log under the event viewer of UltraVNC. UltraVNC logs information on the client computer only, therefore the application does not log connection information on the host computer. The log information consists of IP address and connection received and end date and time.

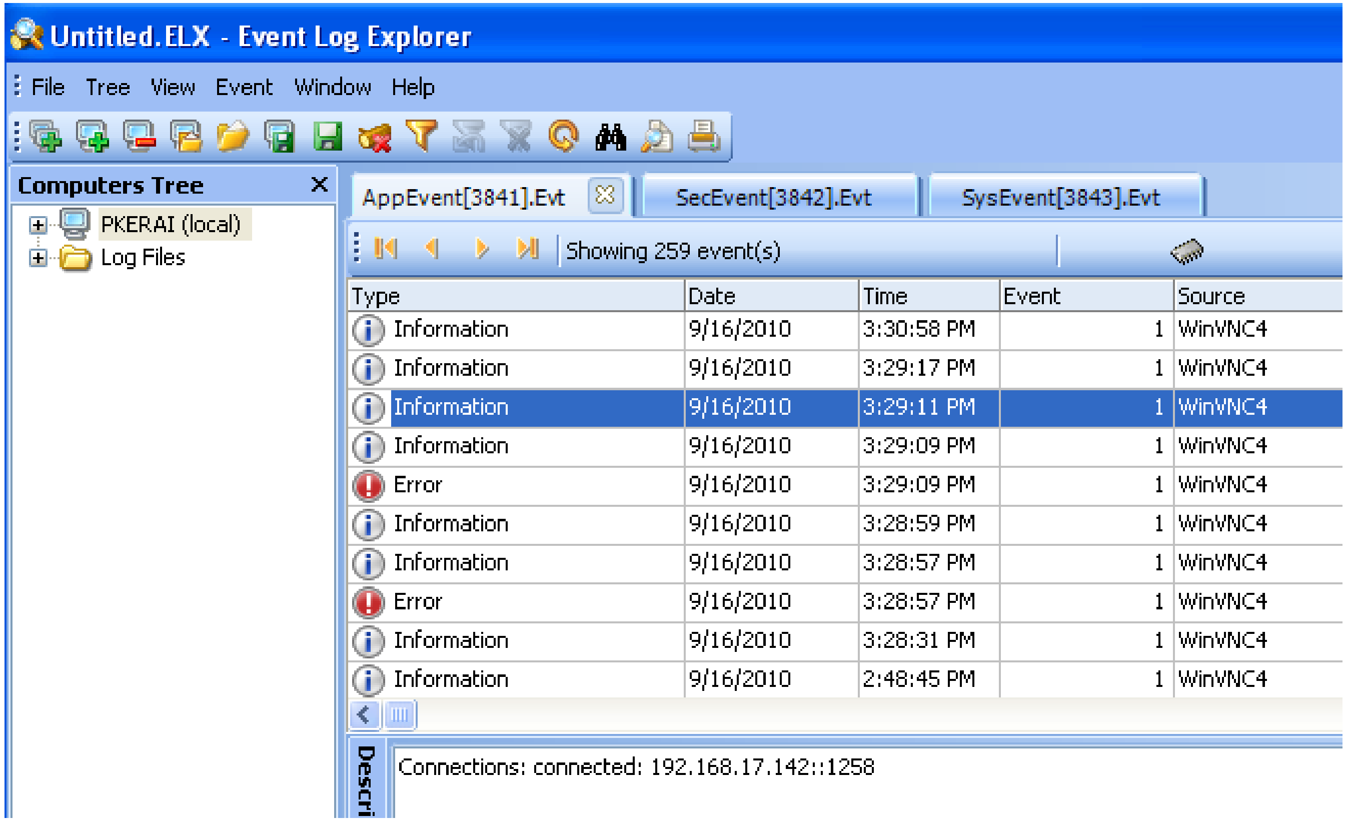


Type	Date	Time	Event	Source	Categor
Information	9/16/2010	3:32:14 PM	1	WinVNC4	None
Information	9/16/2010	3:32:11 PM	1	WinVNC4	None
Error	9/16/2010	3:32:11 PM	1	WinVNC4	None
Information	9/16/2010	3:32:00 PM	1	WinVNC4	None
Information	9/16/2010	3:27:56 PM	1	WinVNC4	None
Information	9/16/2010	3:27:25 PM	1	WinVNC4	None
Information	9/16/2010	3:21:55 PM	3	UltraVnc	(1)
Information	9/16/2010	2:49:57 PM	1	UltraVnc	(1)
Information	9/16/2010	2:21:14 PM	1000	LoadPerf	None
Information	9/16/2010	2:21:14 PM	1001	LoadPerf	None
Information	9/16/2010	2:17:17 PM	271	VMUpgradeHelper	None
Information	9/16/2010	2:17:17 PM	270	VMUpgradeHelper	None

The description for Event ID (3) in Source (UltraVnc) could not be found. It contains the following insertion s
16/9/2010 15:21 Client 192.168.17.153 disconnected

Figure 61 Application event log of UltraVNC

Figures 62-63 shows the application log information of RealVNC under the event viewer. RealVNC logs log information consists of IP address and connection received and end date and time. However the IP address in the log is of the client machine not of the host computer. The application does not log connection information on the host computer.

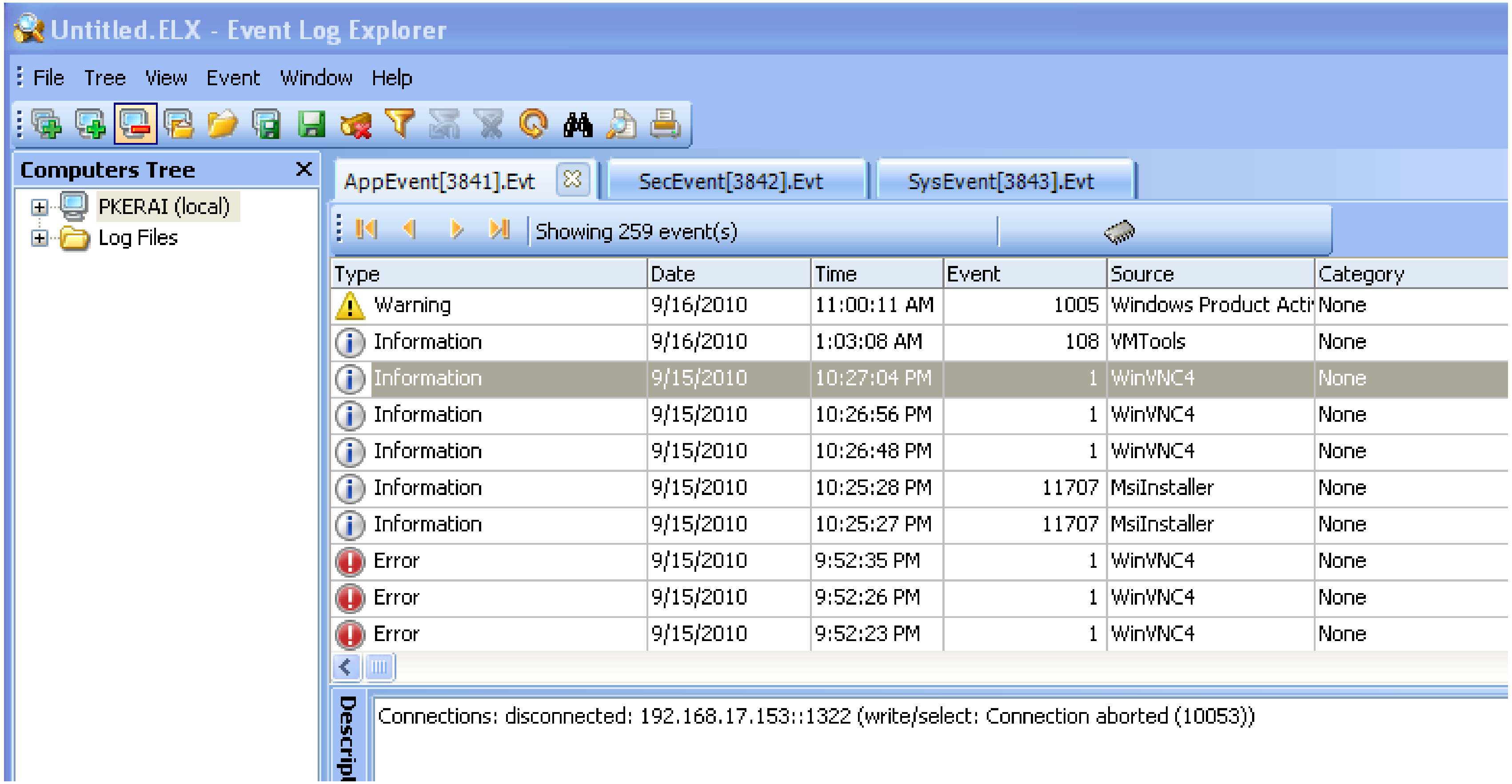


Showing 259 event(s)

Type	Date	Time	Event	Source
Information	9/16/2010	3:30:58 PM	1	WinVNC4
Information	9/16/2010	3:29:17 PM	1	WinVNC4
Information	9/16/2010	3:29:11 PM	1	WinVNC4
Information	9/16/2010	3:29:09 PM	1	WinVNC4
Error	9/16/2010	3:29:09 PM	1	WinVNC4
Information	9/16/2010	3:28:59 PM	1	WinVNC4
Information	9/16/2010	3:28:57 PM	1	WinVNC4
Error	9/16/2010	3:28:57 PM	1	WinVNC4
Information	9/16/2010	3:28:31 PM	1	WinVNC4
Information	9/16/2010	2:48:45 PM	1	WinVNC4

```
Connections: connected: 192.168.17.142::1258
```

Figure 62 Application Log information of RealVNC

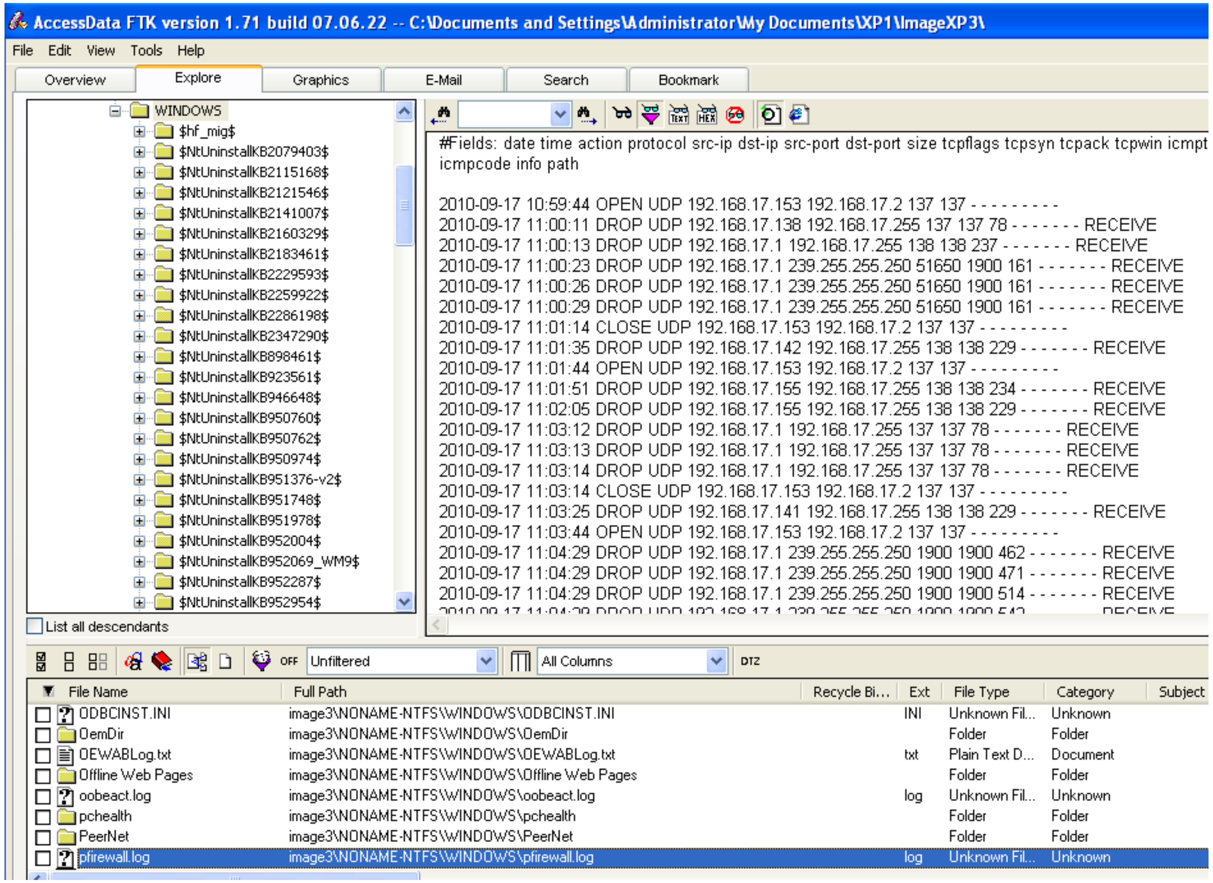


Type	Date	Time	Event	Source	Category
Warning	9/16/2010	11:00:11 AM	1005	Windows Product Acti	None
Information	9/16/2010	1:03:08 AM	108	VMTools	None
Information	9/15/2010	10:27:04 PM	1	WinVNC4	None
Information	9/15/2010	10:26:56 PM	1	WinVNC4	None
Information	9/15/2010	10:26:48 PM	1	WinVNC4	None
Information	9/15/2010	10:25:28 PM	11707	MsiInstaller	None
Information	9/15/2010	10:25:27 PM	11707	MsiInstaller	None
Error	9/15/2010	9:52:35 PM	1	WinVNC4	None
Error	9/15/2010	9:52:26 PM	1	WinVNC4	None
Error	9/15/2010	9:52:23 PM	1	WinVNC4	None

```
Connections: disconnected: 192.168.17.153::1322 (write/select: Connection aborted (10053))
```

Figure 63 Application Log information of RealVNC

Figure 64 shows the firewall log of image 3. In all Windows XP service packs firewall logging is by default disabled. Therefore logging was enabled on all the three image machines for logging purpose. The firewall log consists of all incoming and outgoing connection on the local network including connection data, time; ports used for connection, type of protocol and also IP addresses that the local computer connected to.

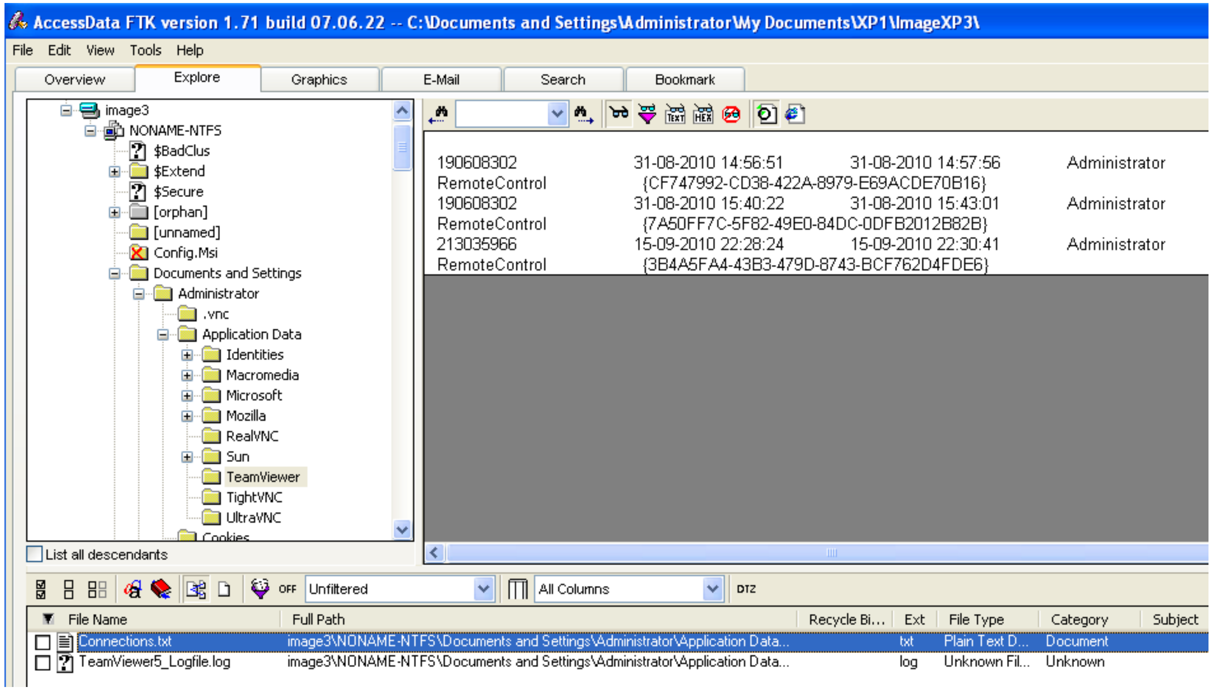


```
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmpt
icmpcode info path

2010-09-17 10:59:44 OPEN UDP 192.168.17.153 192.168.17.2 137 137 - - - - - - - - -
2010-09-17 11:00:11 DROP UDP 192.168.17.138 192.168.17.255 137 137 78 - - - - - - - RECEIVE
2010-09-17 11:00:13 DROP UDP 192.168.17.1 192.168.17.255 138 138 237 - - - - - - - RECEIVE
2010-09-17 11:00:23 DROP UDP 192.168.17.1 239.255.255.250 51650 1900 161 - - - - - - - RECEIVE
2010-09-17 11:00:26 DROP UDP 192.168.17.1 239.255.255.250 51650 1900 161 - - - - - - - RECEIVE
2010-09-17 11:00:29 DROP UDP 192.168.17.1 239.255.255.250 51650 1900 161 - - - - - - - RECEIVE
2010-09-17 11:01:14 CLOSE UDP 192.168.17.153 192.168.17.2 137 137 - - - - - - - - -
2010-09-17 11:01:35 DROP UDP 192.168.17.142 192.168.17.255 138 138 229 - - - - - - - RECEIVE
2010-09-17 11:01:44 OPEN UDP 192.168.17.153 192.168.17.2 137 137 - - - - - - - - -
2010-09-17 11:01:51 DROP UDP 192.168.17.155 192.168.17.255 138 138 234 - - - - - - - RECEIVE
2010-09-17 11:02:05 DROP UDP 192.168.17.155 192.168.17.255 138 138 229 - - - - - - - RECEIVE
2010-09-17 11:03:12 DROP UDP 192.168.17.1 192.168.17.255 137 137 78 - - - - - - - RECEIVE
2010-09-17 11:03:13 DROP UDP 192.168.17.1 192.168.17.255 137 137 78 - - - - - - - RECEIVE
2010-09-17 11:03:14 DROP UDP 192.168.17.1 192.168.17.255 137 137 78 - - - - - - - RECEIVE
2010-09-17 11:03:14 CLOSE UDP 192.168.17.153 192.168.17.2 137 137 - - - - - - - - -
2010-09-17 11:03:25 DROP UDP 192.168.17.141 192.168.17.255 138 138 229 - - - - - - - RECEIVE
2010-09-17 11:03:44 OPEN UDP 192.168.17.153 192.168.17.2 137 137 - - - - - - - - -
2010-09-17 11:04:29 DROP UDP 192.168.17.1 239.255.255.250 1900 1900 462 - - - - - - - RECEIVE
2010-09-17 11:04:29 DROP UDP 192.168.17.1 239.255.255.250 1900 1900 471 - - - - - - - RECEIVE
2010-09-17 11:04:29 DROP UDP 192.168.17.1 239.255.255.250 1900 1900 514 - - - - - - - RECEIVE
```

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject
☐ ODBCINST.INI	image3\NONAME-NTFS\WINDOWS\ODBCINST.INI		INI	Unknown Fil...	Unknown	
☐ OemDir	image3\NONAME-NTFS\WINDOWS\OemDir			Folder	Folder	
☐ OEWABLog.txt	image3\NONAME-NTFS\WINDOWS\OEWABLog.txt		txt	Plain Text D...	Document	
☐ Offline Web Pages	image3\NONAME-NTFS\WINDOWS\Offline Web Pages			Folder	Folder	
☐ oobeact.log	image3\NONAME-NTFS\WINDOWS\oobeact.log		log	Unknown Fil...	Unknown	
☐ pchealth	image3\NONAME-NTFS\WINDOWS\pchealth			Folder	Folder	
☐ PeerNet	image3\NONAME-NTFS\WINDOWS\PeerNet			Folder	Folder	
☐ pfirewall.log	image3\NONAME-NTFS\WINDOWS\pfirewall.log		log	Unknown Fil...	Unknown	

Figure 64 Firewall log information for Image 3

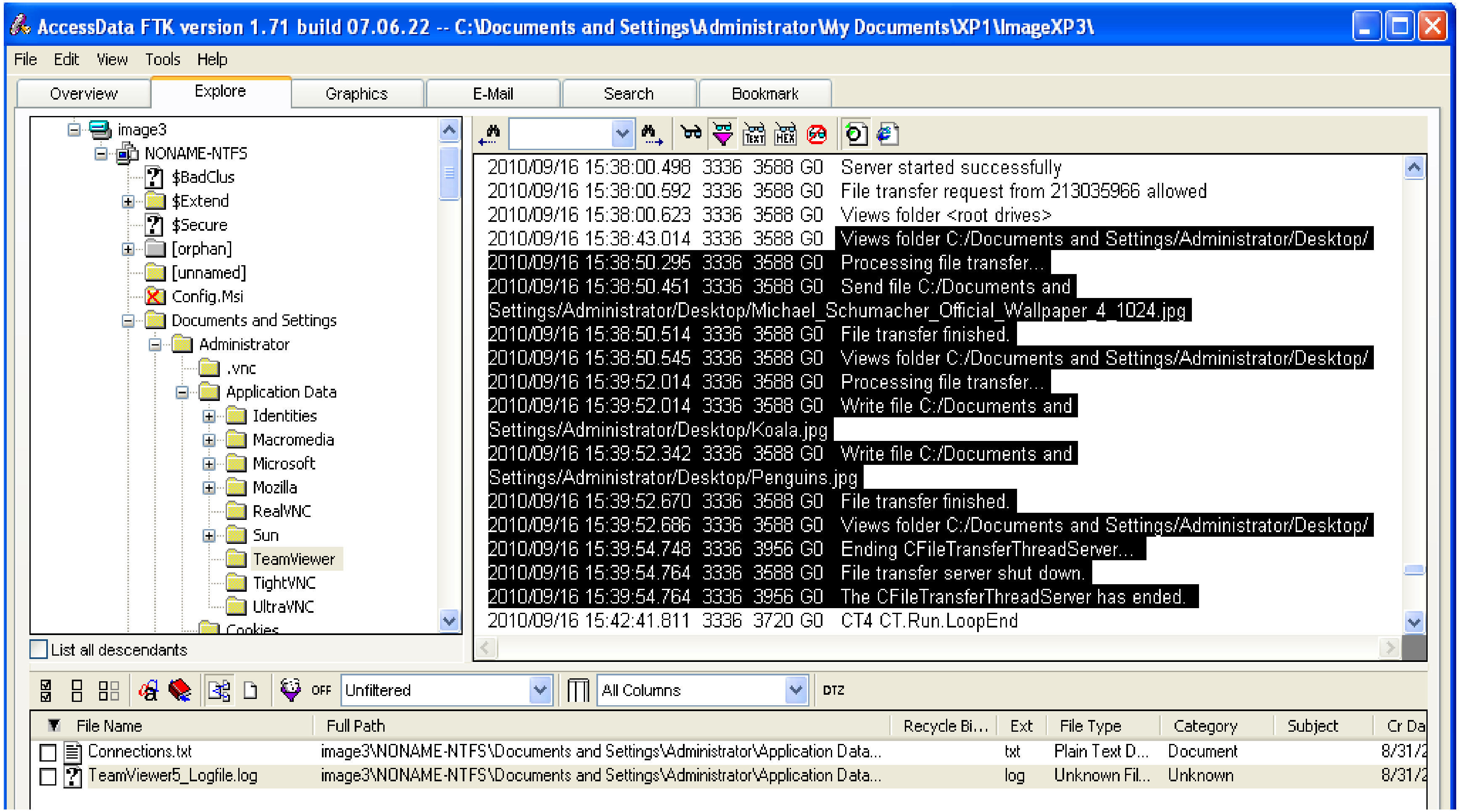
Figure 65-66 below shows the connection logs of Team viewer. Normally Team viewer log files are located under C:\Documents and Settings\Administrator\Application Data\TeamViewer. The folder consists of two files namely; connections.txt, this file consists of the client IDs used for connection including the date and time for connection.TeamViewer5_Logfile, this file consists of all the connection details such as connection settings, connection encryption, file transfer log and other connection related information. Figure 66 shows the files transferred using Team Viewer and where the files were placed.



```
190608302          31-08-2010 14:56:51        31-08-2010 14:57:56        Administrator
RemoteControl       {CF747992-CD38-422A-8979-E69ACDE70B16}
190608302          31-08-2010 15:40:22        31-08-2010 15:43:01        Administrator
RemoteControl       {7A50FF7C-5F82-49E0-84DC-0DFB2012B82B}
213035966          15-09-2010 22:28:24        15-09-2010 22:30:41        Administrator
RemoteControl       {3B4A5FA4-43B3-479D-8743-BCF762D4FDE6}
```

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject
☐ Connections.txt	image3\NONAME-NTFS\Documents and Settings\Administrator\Application Data...		txt	Plain Text D...	Document	
☐ TeamViewer5_Logfile.log	image3\NONAME-NTFS\Documents and Settings\Administrator\Application Data...		log	Unknown Fil...	Unknown	

Figure 65 Team Viewer connection log

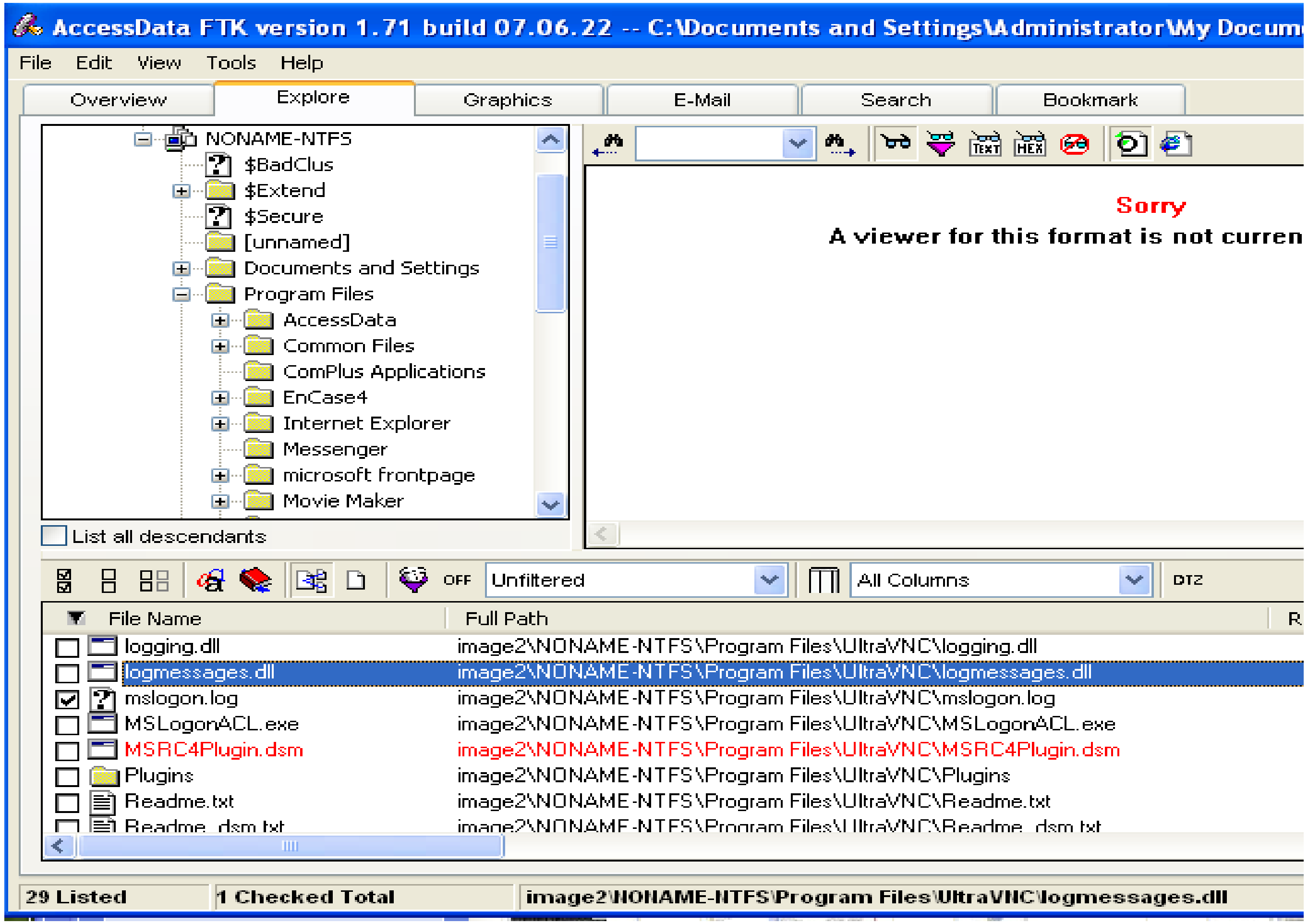


```
2010/09/16 15:38:00.498  3336  3588 G0   Server started successfully
2010/09/16 15:38:00.592  3336  3588 G0   File transfer request from 213035966 allowed
2010/09/16 15:38:00.623  3336  3588 G0   Views folder <root drives>
2010/09/16 15:38:43.014  3336  3588 G0   Views folder C:/Documents and Settings/Administrator/Desktop/
2010/09/16 15:38:50.295  3336  3588 G0   Processing file transfer...
2010/09/16 15:38:50.451  3336  3588 G0   Send file C:/Documents and
Settings/Administrator/Desktop/Michael_Schumacher_Official_Wallpaper_4_1024.jpg
2010/09/16 15:38:50.514  3336  3588 G0   File transfer finished.
2010/09/16 15:38:50.545  3336  3588 G0   Views folder C:/Documents and Settings/Administrator/Desktop/
2010/09/16 15:39:52.014  3336  3588 G0   Processing file transfer...
2010/09/16 15:39:52.014  3336  3588 G0   Write file C:/Documents and
Settings/Administrator/Desktop/Koala.jpg
2010/09/16 15:39:52.342  3336  3588 G0   Write file C:/Documents and
Settings/Administrator/Desktop/Penguins.jpg
2010/09/16 15:39:52.670  3336  3588 G0   File transfer finished.
2010/09/16 15:39:52.686  3336  3588 G0   Views folder C:/Documents and Settings/Administrator/Desktop/
2010/09/16 15:39:54.748  3336  3956 G0   Ending CFileTransferThreadServer...
2010/09/16 15:39:54.764  3336  3588 G0   File transfer server shut down.
2010/09/16 15:39:54.764  3336  3956 G0   The CFileTransferThreadServer has ended.
2010/09/16 15:42:41.811  3336  3720 G0   CT4 CT.Run.LoopEnd
```

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Da
☐ Connections.txt	image3\NONAME-NTFS\Documents and Settings\Administrator\Application Data...		txt	Plain Text D...	Document		8/31/2
☐ TeamViewer5_Logfile.log	image3\NONAME-NTFS\Documents and Settings\Administrator\Application Data...		log	Unknown Fil...	Unknown		8/31/2

Figure 66 Team Viewer file transfer log information

Figure 67-68 below shows the log file information of Ultra VNC placed under C:\Program Files\UltraVNC. The file is mslogon.log and contains the connections received and date and time of the connections. The file also gives information on who disconnected the remote connection.

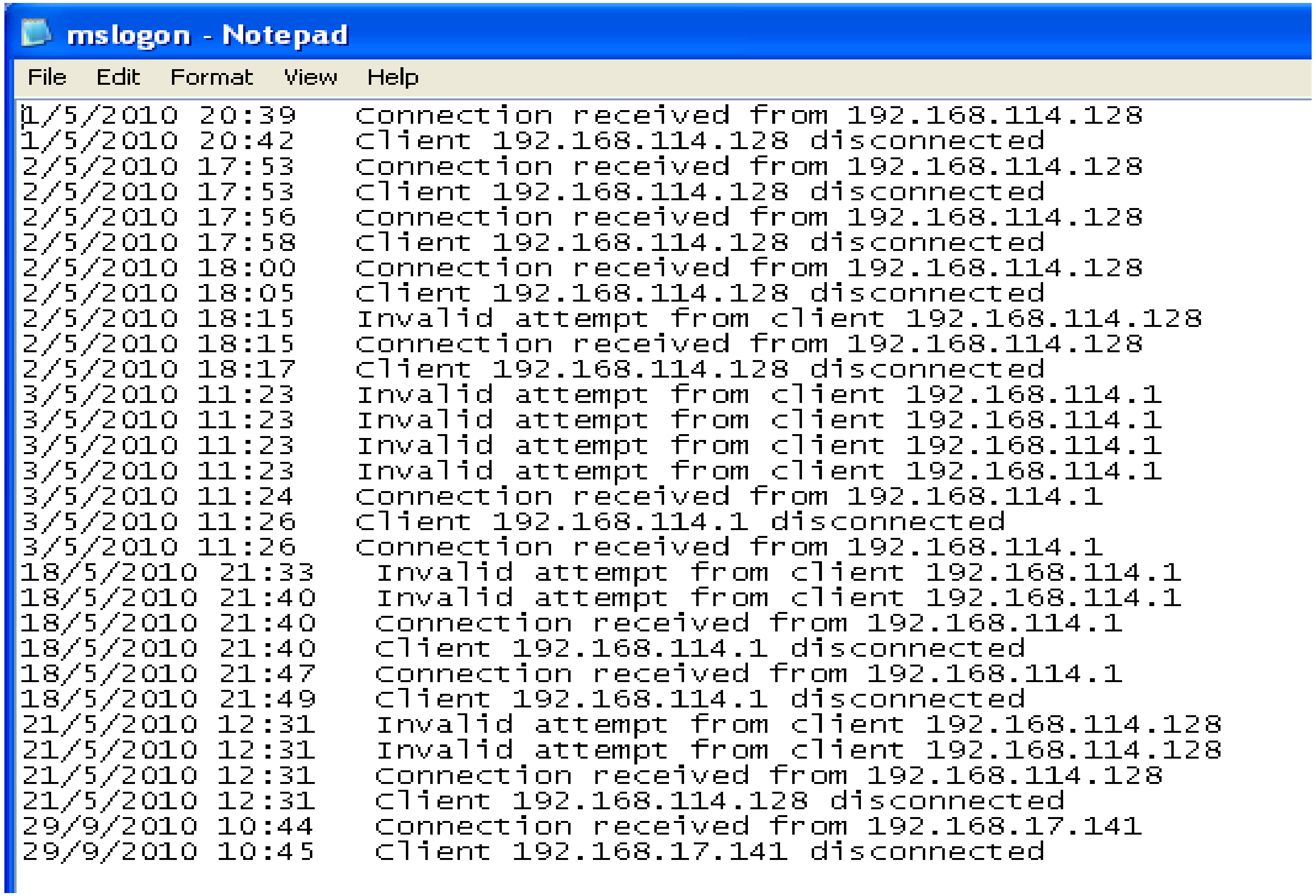


Sorry
A viewer for this format is not curren

File Name	Full Path
☐ logging.dll	image2\NONAME-NTFS\Program Files\UltraVNC\logging.dll
☐ logmessages.dll	image2\NONAME-NTFS\Program Files\UltraVNC\logmessages.dll
☑ mslogon.log	image2\NONAME-NTFS\Program Files\UltraVNC\mslogon.log
☐ MSLogonACL.exe	image2\NONAME-NTFS\Program Files\UltraVNC\MSLogonACL.exe
☐ MSRC4Plugin.dsm	image2\NONAME-NTFS\Program Files\UltraVNC\MSRC4Plugin.dsm
☐ Plugins	image2\NONAME-NTFS\Program Files\UltraVNC\Plugins
☐ Readme.txt	image2\NONAME-NTFS\Program Files\UltraVNC\Readme.txt
☐ Readme_dsm.txt	image2\NONAME-NTFS\Program Files\UltraVNC\Readme_dsm.txt

29 Listed | 1 Checked Total | image2\NONAME-NTFS\Program Files\UltraVNC\logmessages.dll

Figure 67 Ultra VNC log information Image 3



```
1/5/2010 20:39   Connection received from 192.168.114.128
1/5/2010 20:42   Client 192.168.114.128 disconnected
2/5/2010 17:53   Connection received from 192.168.114.128
2/5/2010 17:53   Client 192.168.114.128 disconnected
2/5/2010 17:56   Connection received from 192.168.114.128
2/5/2010 17:58   Client 192.168.114.128 disconnected
2/5/2010 18:00   Connection received from 192.168.114.128
2/5/2010 18:05   Client 192.168.114.128 disconnected
2/5/2010 18:15   Invalid attempt from client 192.168.114.128
2/5/2010 18:15   Connection received from 192.168.114.128
2/5/2010 18:17   Client 192.168.114.128 disconnected
3/5/2010 11:23   Invalid attempt from client 192.168.114.1
3/5/2010 11:23   Invalid attempt from client 192.168.114.1
3/5/2010 11:23   Invalid attempt from client 192.168.114.1
3/5/2010 11:23   Invalid attempt from client 192.168.114.1
3/5/2010 11:24   Connection received from 192.168.114.1
3/5/2010 11:26   Client 192.168.114.1 disconnected
3/5/2010 11:26   Connection received from 192.168.114.1
18/5/2010 21:33   Invalid attempt from client 192.168.114.1
18/5/2010 21:40   Invalid attempt from client 192.168.114.1
18/5/2010 21:40   Connection received from 192.168.114.1
18/5/2010 21:40   Client 192.168.114.1 disconnected
18/5/2010 21:47   Connection received from 192.168.114.1
18/5/2010 21:49   Client 192.168.114.1 disconnected
21/5/2010 12:31   Invalid attempt from client 192.168.114.128
21/5/2010 12:31   Invalid attempt from client 192.168.114.128
21/5/2010 12:31   Connection received from 192.168.114.128
21/5/2010 12:31   Client 192.168.114.128 disconnected
29/9/2010 10:44   Connection received from 192.168.17.141
29/9/2010 10:45   Client 192.168.17.141 disconnected
```

Figure 68 Ultra VNC log information Image