2010

Tracing VNC And RDP Protocol Artefacts on Windows Mobile and Windows Smartphone for Forensic Purpose

Paresh Kerai
Edith Cowan University

TRACING VNC AND RDP PROTOCOL ARTEFACTS ON WINDOWS MOBILE AND WINDOWS SMARTPHONE FOR FORENSIC PURPOSE

Paresh Kerai

School of Computer and Security Science
Edith Cowan University
Perth, Western Australia
pkerai@our.ecu.edu.au

Abstract

Remote access is the means of acquiring access to a computer or network remotely or from distance. It is typically achieved through the internet which connects people, corporate offices and telecommuters to the internal network of organizations or individuals.

In recent years there has been a greater adoption of remote desktop applications that help administrators to configure and repair computers remotely over the network. However, this technology has also benefited cyber criminals. For example they can connect to computers remotely and perform illegal activity over the network. This research will focus on Windows mobile phones and the Paraben forensics software will be used to analyse the phones. The analysis will focus on any related Virtual Network Computing (VNC) and Remote Desktop protocol (RDP) artefacts left behind by the remote connection.

Keywords: VNC, RDP, RBF protocol, forensic, artefacts, registry files and log files, Windows Mobile smart phones and mobile PC.

INTRODUCTION

Most organisations, computer technicians or administrators are using the remote access features of VNC and RDP technology to solve remote computer system problems.

Windows Mobile devices such as pocket PC and smart phones can pose a challenge for forensic practitioners. These devices are fundamentally similar to computers however they are fully portable and are able to be taken to locations that more traditional computers cannot go to. Because of their broad uses these devices contains significant amount of information that can be useful from a forensic perspective. (Casey, Bann, & Doyle, 2010) Forensic investigators must be able to detect the presence of remote applications on the devices that permit remote log in and monitoring of networks. As the mobile devices are used by computer administrators and organisations to remotely log-in and monitor remote company networks, this can represent a threat to the organisation as; such connections can be used to perform illegal activities. New acquisition methods and techniques have become available that give forensic investigators access to deleted data and the device file system, including SIM information (Casey, et al., 2010). However, since Windows Mobile devices are relatively new in the market, and the data format is unfamiliar (such as volume files and embedded database), this poses a challenge for the forensic investigators. (Casey, et al., 2010)

This paper is going to focus on the ability to find any artefacts left behind by remote desktop protocol or VNC protocol, on the Windows Mobile devices file system, using both commercial and open source tools for acquisition and investigation.

VIRTUAL NETWORK COMPUTING (VNC)

VNC uses remote framebuffer (RBF) which is a simple protocol used by the system for remote access to graphical user interface (Tristan, Quentin, Kenneth, & Andy, 1998). The protocol is available to most operating systems including X11, Windows, Macintosh and Linux. (Richardson, 2009) The protocol allows remote desktop connections where one computer can connect to another with full view and control of the host computer. The application provides access to home and office computing environment from anywhere in the world that is connected to the internal network or internet.(Tristan, et al., 1998) This provides the user with user privileges and a uniform view of the computing infrastructure wherever they go (Richardson, 2009). The RBF protocol will run over any reliable transport such as TCP/IP protocol. By default VNC uses TCP ports 5900 through 5903. As the protocol has low bandwidth requirements it is a true thin-client protocol, which can run on

a wide range of hardware (Richardson, 2009). The communication over the network can be encrypted by Secure Shell (SSH) layer encryption and together with the encrypted client and server passwords provides stronger security. However, despite the encrypted passwords and network, any communication over the network is typically vulnerable and can be attacked by few tools and techniques. There are two components consisted in VNC: the viewer and the server.

VNC Viewer

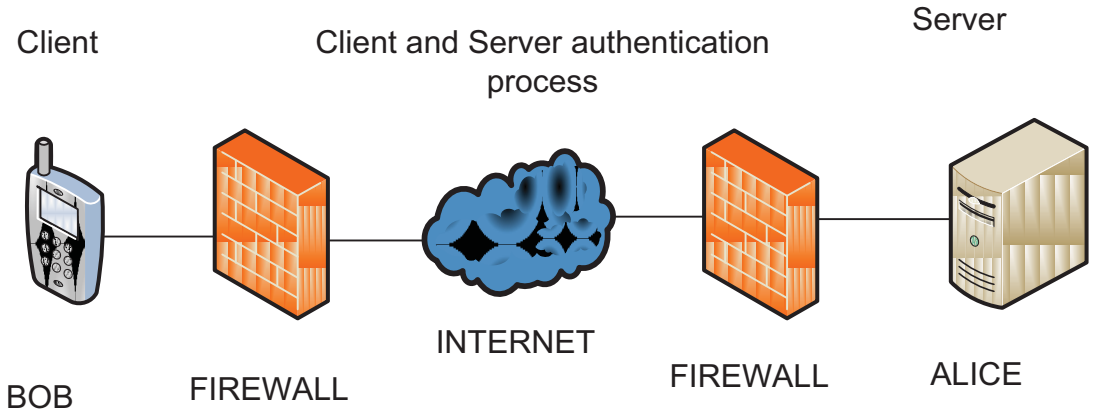
The viewer will connect to the server which in turn will allow the user or administrator to connect to the remote server system and view the system. The viewer is currently available in many operating systems such as Unix X window, Java, Windows, Macintosh 7.1 or higher and Windows CE 2.0 or later (Morris, 2001). The advantage of the viewer is that it does not require any installation and configuration, unlike the server, and can be run from a hard drive or any external electronic device (Morris, 2001). The most interesting point is that 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).

VNC Server

The server needs to be installed on the host system or machine and has to be defined and configured so that the viewer has something to connect to. The server is currently available on Unix X window, Windows and Macintosh computer systems. But is currently unavailable for Windows mobile PC and smart phones and therefore, cannot be installed on these devices. You can only install the viewer to access the remote server or similar client using the same features and applications configured to support the remote mobile device connections.

VNC Session Initiation

The following is a diagram of the session initiation and authentication process that takes place between the viewer and the server.



- *A Data Encryption Standard (DES) key (Luo, 2007) is used by Alice endpoint 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 is 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).

However in the Windows mobile some of the VNC applications leave the session password in the clear text on the phone registry. This is explained in more detail below under the "Registry Analysis".

REMOTE DESKTOP PROTOCOL (RDP)

Remote desktop protocol is similar to the VNC computing system. Like VNC, RDP provides similar access to remote computers from another remote computer or server running the same service. However Remote Desktop is based on Terminal Services Technology such as VNC uses RBF protocol for remote connections (MicrosoftTechNet, 2005). The feature is based on and an extension of T-120 family of protocol standards (MicrosoftSupport, 2007). Remote Desktop consists of following components:

a) 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 network, wide area network, dial-up, direct subscriber line or even with virtual private network (VPN). (MicrosoftTechNet, 2005). TCP/IP port 3389 is used by default by RDP.

b) Client software – software that is installed by default in 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 as to the server, just install and then the dialog box will prompt for IP address of server and password to connect to the remote computer. (MicrosoftTechNet, 2005)

c) 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 on older Windows operating systems.

d) Remote desktop web connection – this type of connection works the same way as remote desktop connection, the only difference is that the features are delivered over the web through Microsoft ActiveX technology. Remote desktop web connection ActiveX can start a remote desktop session on the remote computer through an embedded on a web page, with the computer not having installed 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.

By default, the data and information that travels over the network using the connection between the client and the server is protected by RC4 symmetric encryption algorithm which provides three level of security (Montoro, 2005):

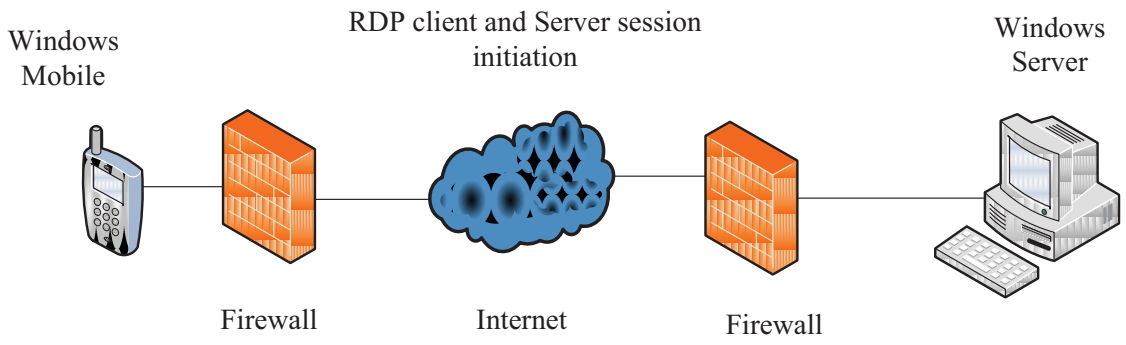
- *High level* – encrypts data sent from both clients to server and server to clients using 128-bit key.
- *Medium* - encrypts data sent from both clients to server and serve to clients using 56-bit key.
- *Low* – this encrypts on the data sent from the client to server using either 56 or 40-bit keys depending on the version of the client.

(Montoro, 2005):

Both the VNC and RDP work the similar way and have similar features but to use the applications the system must have an internet connection that can be used to connect to the client or server. Both applications use the standard Open System Interconnection model (OSI) seven layers for communication. (MicrosoftSupport, 2007)

> "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)

RDP Session Initiation



- *Windows mobile 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 mobile sends a random salt to server, encrypted with the Windows RSA server public key.*
- *Windows server receives the encrypted random salt from Windows mobile 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)

EXAMINING WINDOWS MOBILE REGISTRY

The registry in the Windows mobile PC and phones contains valuable information about the configurations and the use of devices (Casey, et al., 2010). Fig. 1 Illustrates and shows the structure of the registry on the Windows mobile devices, the registry is a hierarchical structure and is similar to the other Microsoft operating systems.

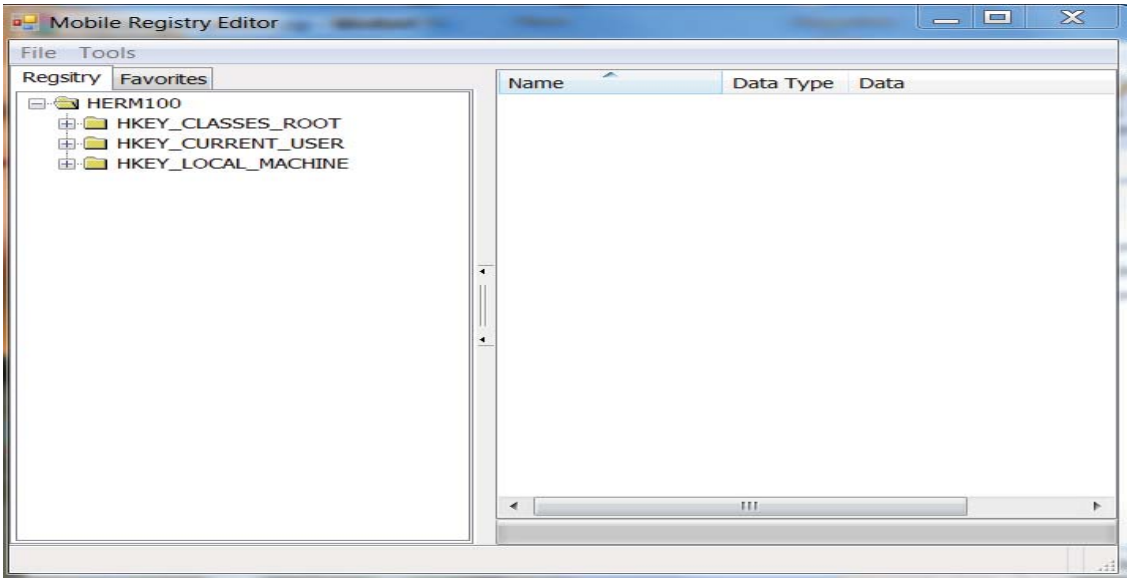


Fig. 1 Registry hives and values of HTC Dopod Windows mobile phone.

The devices have three hives when compared to the Windows operating systems which have 5 hierarchical hives. The Table below explains Windows PC and Windows Mobile registry values and what it stores under the each hives:

Windows PC	Settings stored	Windows Mobile	Settings stored
HKEY_LOCAL_MACHINE (**HKLM**)	Stores information about local computer, such as system memory, devices, drivers, and hardware settings.	HKEY_LOCAL_MACHINE (HKLM)	Stores information related mobile device system.
HKEY_CLASSES_ROOT (**HKCR**)	Stores information used by various OLE technologies, file association and COM object registration	HKEY_CLASSES_ROOT (HKCR)	Stores information regarding file association with applications.
HKEY_CURRENT_USER (**HKCU**)	Stores information about the current user logged on.	HKEY_CURRENT_USER (HKCU)	Stores information and settings about the current user of the mobile device.
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.		

(TechNet, 2005), (The Registry on Windows, 2009)

Mobile registry editor tool was used to view the device's registry system for analysis. The tool is free to download and runs directly from the file, therefore it does not require to be installed on the computer.

VNC artefacts on registry hives

Normally the VNC settings are placed under HKEY_CURRENT_USER\Software\ that is the same with the Remote desktop terminal. However not all VNC applications and softwares place the application configurations and settings under one registry key. In this paper the author used three different types of VNC applications on the device to see how each application behaves and what artefacts are left behind and from which VNC application.

a) VNC viewerv3.3.2 for Windows mobile

VNC viewerv3.3.2 is application is freeware and can be downloaded to the mobile device and anyone can use it for remote connections.

The VNC settings and its registry values are normally placed under HKEY_CURRENT_USER\Software\ORL\VNCviewer, which can be viewed by the registry viewer. It is possible to view all the connections and IP addresses and the port used by the device connect to the corresponding server or viewer under the HKEY_CURRENT_USER\Software\ORL\VNCviewer\MRU as shown in Fig. 2 below.

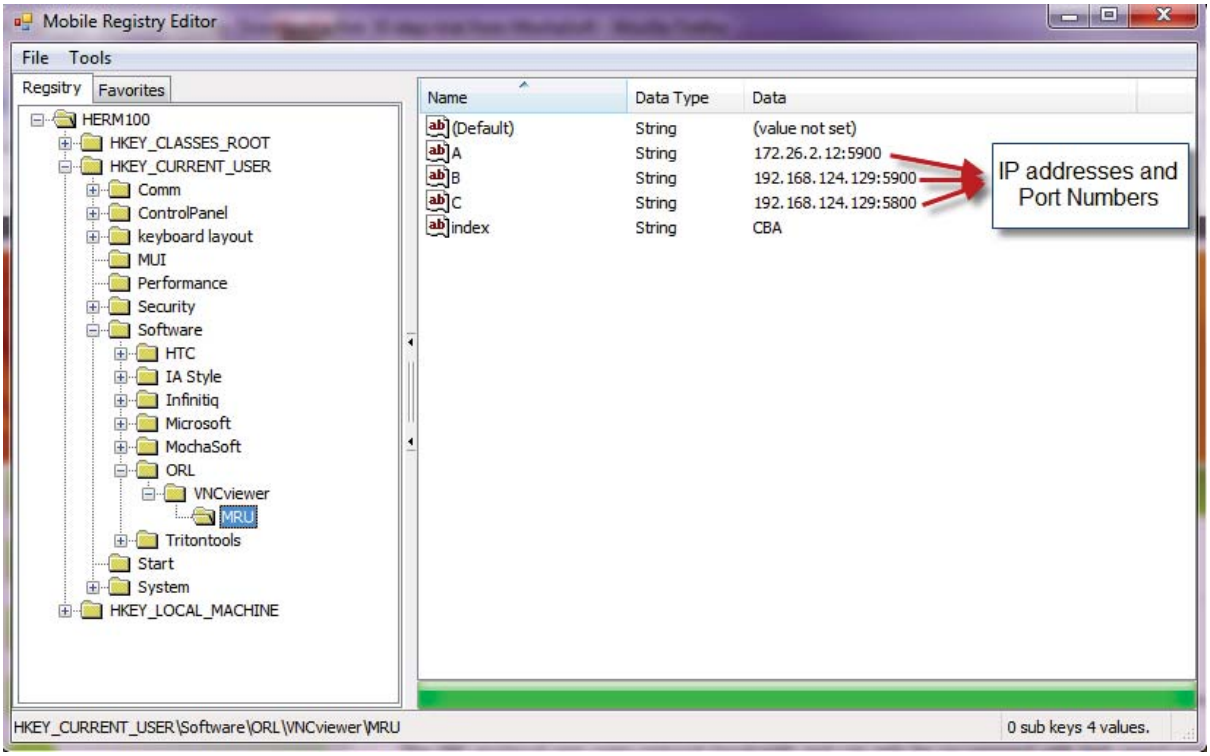


Fig. 2 VNC viewer registry values

The figure above shows the IP addresses and also the ports used by the device that it connected to. This can be used by the forensics investigators or law enforcement agencies to find and locate the corresponding party or computer system.

b) Mocha VNC (MochaSoft)

This application had good features in terms of screen resolution capability and other features like sending alt+cntl+del command, mouse right click, Esc, Window key, Del functions, protocol information and disconnect key. However, the application is not freeware and is worth US$ 20 for a single user license key. The application can be downloaded from the MochaVNC site (http://www.mochasoft.dk/vncce.htm). The application stores its configurations and settings under HKEY_CURRENT_USER\Software\MochaSoft\VNC as shown in Fig.3

The disadvantage of the application is that the password used for the connection is not encrypted and is placed under the registry hive in plain text. Fig.3 shows the IP addresses used to connect to and also other connection settings including the clear text password used to connect to the server.

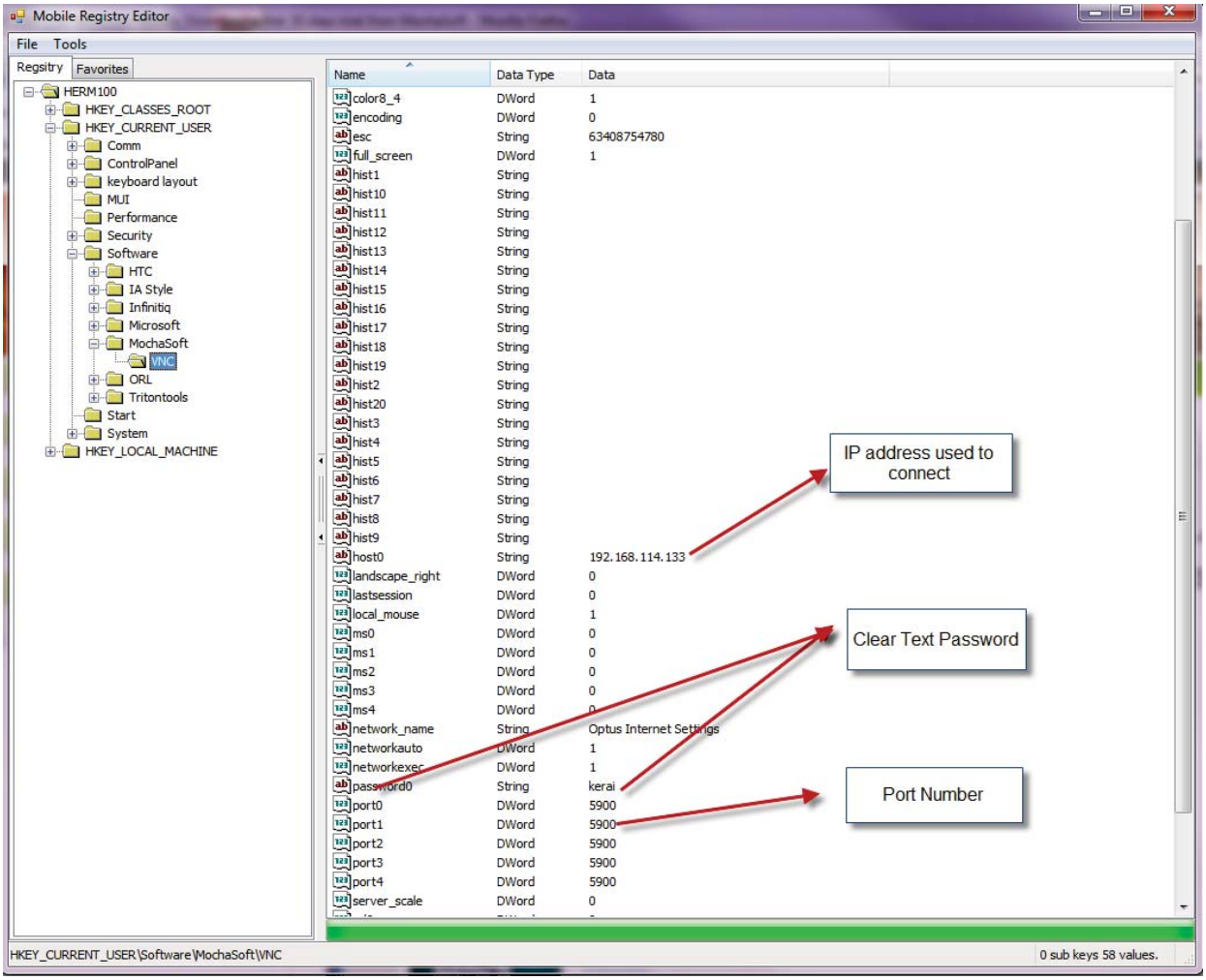


Fig. 3 Mocha VNC registry values

c) Smart VNC

This application has similar features and abilities to Mocha VNC, the difference is that the application is freeware. The application has features such as create multiple connections and also edit the connection settings; also you can configure the preferred encoding for the connection. The application places its connection settings and configurations under the key value HKEY_CURRENT_USER\Software\MochaSoft\Tritontools\SmartVNC\Connections.

The application has different configuration values for different connections. Fig. 4 and 5 shows the values stored under the registry hives.

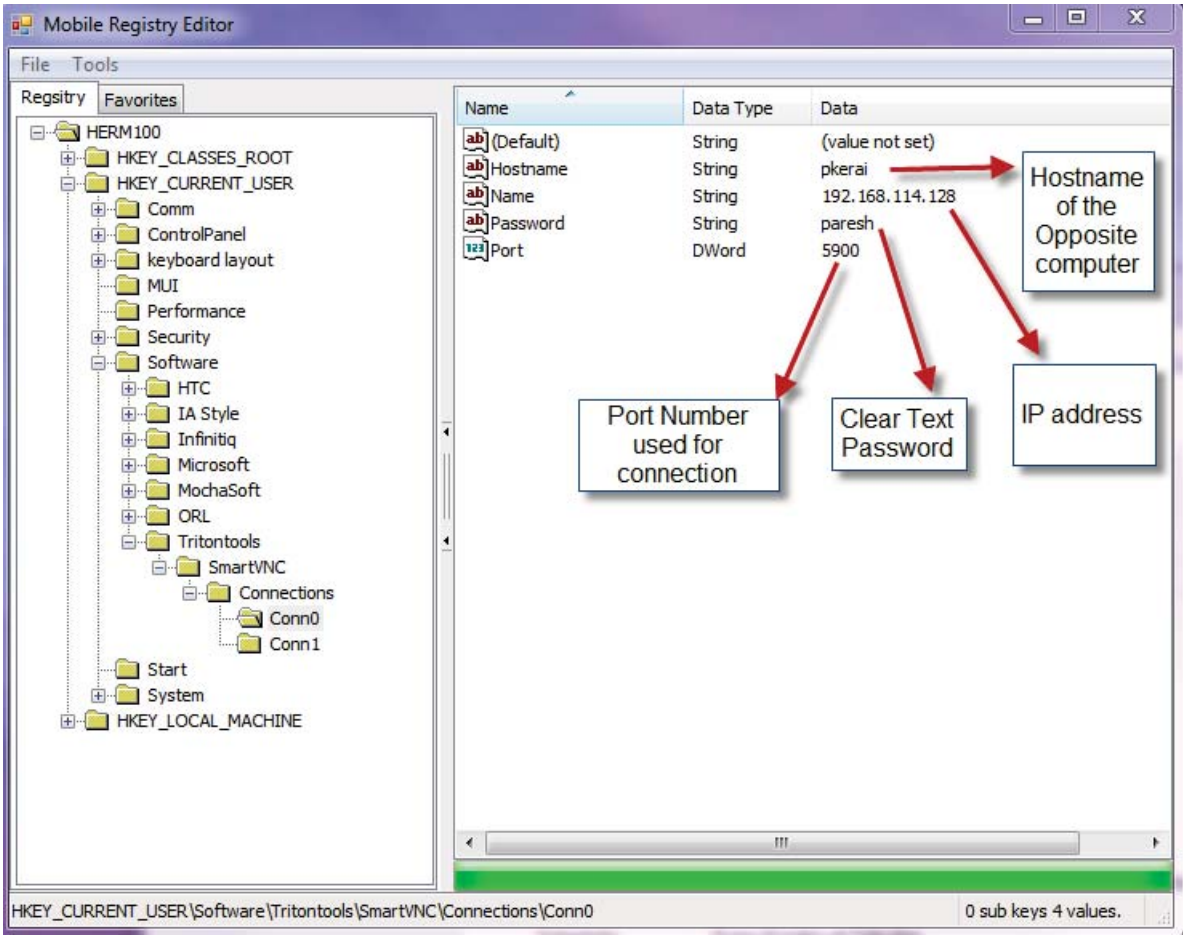


Fig.4 SmartVNC registry value Conn0

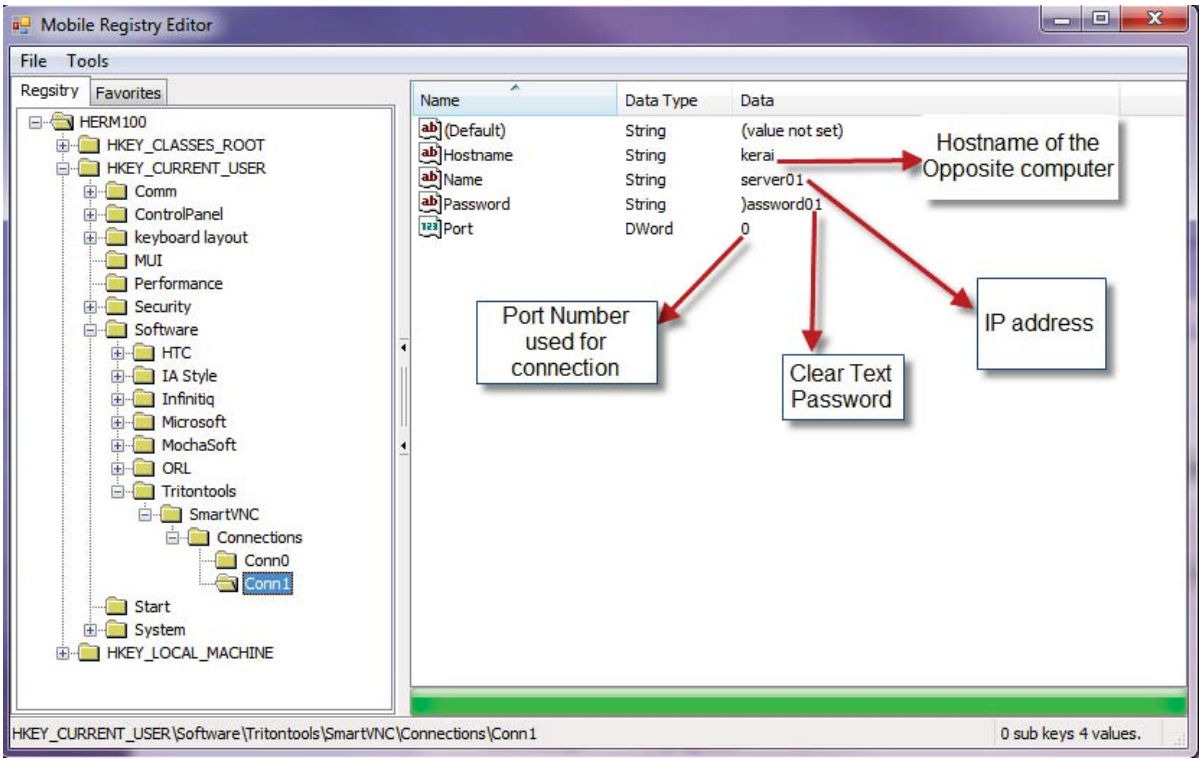


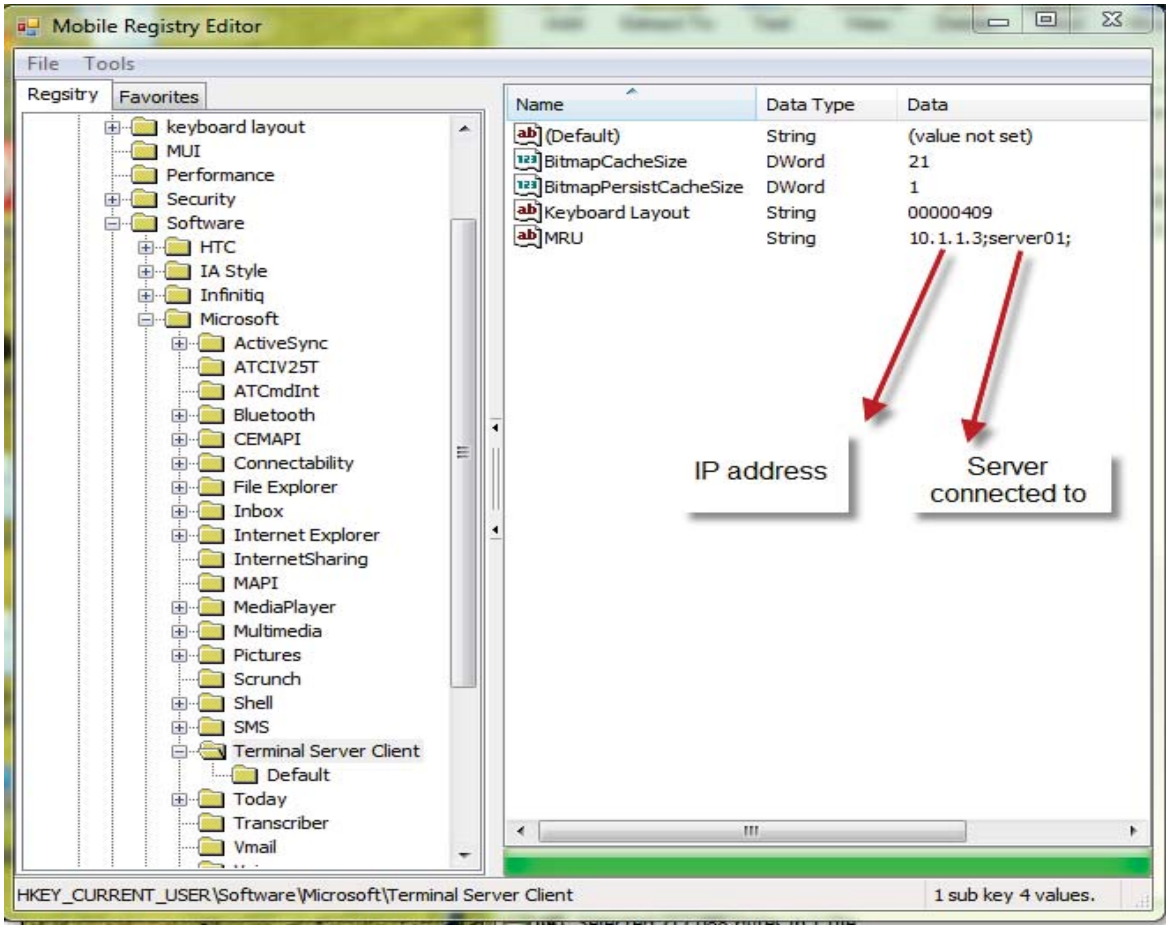
Fig. 5 SmartVNC registry value Conn1

As shown above in Fig. 4 and 5 the software also saves the password for the connection under registry hives in plain text. This is a major security threat and is an issue for anyone who uses the application for remote login. This password can be compromised by stealing the mobile device or from lost Windows mobile devices. It can then be used by a hacker to get access to the server or opposite client, using the password and IP address of the computers.

VNC viewer Applications	Artefacts left on Windows mobile registry
VNC Viewer v3.3.2	The application leaves IP addresses that the mobile device connected to, including the port number the connection used.
Mocha VNC	This application leaves the IP addresses it connected too with port numbers, but also it stores plain session connection password in the device registry. The application does not use any encryption standards to encrypt the session password.
Smart VNC	This application leaves the IP addresses it connected too with port numbers, also it stores plain clear text session connection password in the device registry. The application does not use any encryption standards to encrypt the session password.

RDP artefacts on registry hives

The settings of the remote desktop are normally under HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client. As for VNC applications, the Terminal server client application for remote desktop does not store or save any form of password either in plain text or encrypted. This is a good feature for security purposes. However under the registry value it does stores the IP addresses and the servers host name the mobile device it is connected to. This information can be useful to forensic investigators as they can track down the server or other opposite client through the IP address stored in the registry. Below is the snapshot of what is stored under the Terminal server client key value.



CONCLUSION

Despite the small size of the devices, users and administrators are able to connect to remote computers and networks through their Windows mobile phones. The devices contain a substantial amount of information about the user, applications, and mobile settings. This can be further analysed by the forensic investigators to retrieve substantial artefacts left on the mobile devices. As shows above, remote applications leave crucial information on the mobile devices including whom the device is connected to and what password they used for remote session connection.

Applications such as Mocha VNC and Smart VNC also leave the remote session connection password in clear and plain text, and no type of encryption standard is used by the applications. This shows how poorly the applications were developed and programmed by the vendors. Not only will this help forensic investigators, but it also poses a security threat to the organisation. If the mobile device was lost or stolen, then a person could retrieve the remote session password and use the password and IP address to connect to the remote server and then later perform malicious activities on the server or network.

The remote desktop protocol does not leave any kind of remote session password on the mobile device. However 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 mobile device.

Connection sessions such as log-in and log-out times can also be found on further analysis on the devices. This can be obtained through log file analysis on the device. As the research is still ongoing, the author of this paper is currently doing further analysis will be undertaken on the mobile devices to extract any other artefacts of the remote session by performing file system analysis.

The increase of in usage of mobile devices that can perform everyday computing is benefiting many organisations and individuals because of the portability and convenience the devices give to the organisations. However, this also brings with it threat as the mobile devices are portable and affordable.

As Windows mobile devices become more common and adapted by many individuals and organisations, there is a growing need for forensic investigators and analysts who can acquire and conduct forensics analysis on such devices for evidentiary purposes. The analysis explained in this paper will help forensic analysts to fight cyber crime over the internet.

REFERENCES

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
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

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

Boldwyn, C., Neumann, S. J., Panjwani, A., & Weiner, M. (2009). What is remote access. Retrieved 16 March 2010, from http://searchmidmarketsecurity.techtarget.com/sDefinition/0,,sid198_gci212887,00.html

Casey, E., Bann, M., & Doyle, J. (2010). Introduction to Windows Mobile Forensics. [Digital Investigation]. *Science Direct*, 136-146.

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.

Klaver, C. (2010). Windows Mobile advanced forensics. *Digital Investigation, 6*, 147-167.

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

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.

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

Technet. (2005). Registry structure. Retrieved 20th July 2010, 2010, from http://technet.microsoft.com/en-us/library/cc776231%28WS.10%29.aspx

The Registry on Windows. (2009). The Structure of the Registry Retrieved 20th July 2010, 2010, from http://www.registryonwindows.com/registry-structure.html

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