TeamViewer Forensics

Written by:
Colby Lahaie

Researched by:
Colby Lahaie & David Leberfinger

The Senator Patrick Leahy Center for Digital Investigation

Champlain College

Date Jan 29, 2013

Disclaimer:

This document contains information based on research that has been gathered by employee(s) of The Senator Patrick Leahy Center for Digital Investigation (LCDI). The data contained in this project is submitted voluntarily and is unaudited. Every effort has been made by LCDI to assure the accuracy and reliability of the data contained in this report. However, LCDI nor any of our employees make no representation, warranty or guarantee in connection with this report and hereby expressly disclaims any liability or responsibility for loss or damage resulting from use of this data. Information in this report can be downloaded and redistributed by any person or persons. Any redistribution must maintain the LCDI logo and any references from this report must be properly annotated.

Contents

1 Introduction

Remote viewing or remote access software allows individual access to a computer when physical access to the computer is not possible or convenient. With remote viewing software, a user can access his or her computer from wherever he or she is instead. Unlike typical File Transfer Protocols (FTP), which only allows you to transfer files, you have the ability to edit, modify, and view everything on the hosting computer, without having to save or move information to a flash drive for later use. If a user needs to share his or her desktop or transfer files between computers, remote access software is one option. There are many varieties of remote viewing and remote accessing software around, but there is one tool in particular that we will be looking at, the software TeamViewer. Remote desktop software is widely used because of its many capabilities and low cost to users. TeamViewer has many different versions, which are available for Windows, Mac, Linux, Android, and iOS and is available in both purchased and free versions. For our tests, we chose to use the full version of TeamViewer (see 3.1.1 for other versions), as it appeals to the typical user and provides the most functionality. Although both remote viewing and remote access software can be helpful, they can also pose a serious threat to a person or business. If an unauthorized individual uses the software to remotely access a person or company's computers or networks, he or she could steal sensitive, confidential data. Understanding how this software works is extremely important and provides forensic investigators and law enforcement officials with data that can help them understand what type of information is left behind, as well as how to figure out if it was used during a crime.

1.1 Background

When we first started the TeamViewer Forensics project, there was no prior in-depth research that had been done on the artifacts of TeamViewer. Throughout the course of our research, we came across a website, forensicartifacts.com, which contained an article by Matt Nelson called "TeamViewer 8," providing a list of all of the artifacts found on a computer (Nelson, 2012). Although this has been done, we want to provide a paper on where the artifacts are stored and how to find them using forensic software from a student's perspective.

1.2 Terminology

The area that we are researching is the remote viewing and access of computers.

File Box – The file box is one of the two ways to transfer files using TeamViewer. File sizes are limited to 25 MB, but the file box is available in every TeamViewer session, including meetings. The file box is accessible to the host and client via the File Transfer drop down menu on the tool bar, as well as to the victim via the file box button on the TeamViewer panel.

File Transfer – The file transfer service is the second method of transferring files through TeamViewer. There is no apparent limit on the size of files transferred with this method. This service is available during one-on-one sessions only. Through the file transfer service, users can transfer files from almost anywhere on their system or from the remote system. However, certain files, such as system files, cannot be transferred. The file transfer service is only available to the person currently remotely accessing the computer.

Remote Access – Remote access is the connection to a system from a secondary location other than that of the primary location of the system being accessed.

Remote Control – Remote control is the ability to control a system from a secondary location other than that of the primary location of the system being accessed.

Suspect (client) – The client is the user that remotely accesses the host's (victim's) system.

TeamViewer v.8.0.16642.0 (full version) – This version provides the most functionality and use. A user can control other computers, hold meetings, and allow others to control his or her computer. This is the version that was used for the report.

Victim (host) – The victim, or host, is the user that hosts the incoming remote session.

1.3 Research Questions

1) Will a user be alerted by TeamViewer if someone is remotely accessing his or her computer and/or taking his or her files? Will the victim see the mouse moving or the keystrokes of the person remotely accessing his or her computer? Also, if the victim opens up Windows Task Manager, will they see TeamViewer running?

2) Is it possible for a user to record the screen of the remotely accessed computer? Will the person remote into the other's computer be able to watch what the other user is doing and/or view the history of the other user?

3) How much information or data can be transferred between the two computers? Is it possible to transfer data without notifying the victim?

4) What artifacts are stored and where are they stored?

5) Once TeamViewer is deleted, what artifacts are left behind?

2 Methodology and Methods

We began this project by creating two Windows 7 virtual machines (VM). We used two VMs to simulate the host computer, which we called the "victim's computer" (see 3.2.2), and the client (or connecting computer), which we called the "suspect's computer" (see 3.2.3). We started by taking snapshots and registry shots of the fresh installation of Windows 7 for both VMs. Then, we proceeded to install TeamViewer 8 on both the "suspect's" VM and the "victim's" VM. Once we installed TeamViewer, we created a folder labeled "Victim" on the Host VM and a folder labeled "Suspect" on the Client VM. We transferred files between these folders.

Through multiple sessions using the full version of TeamViewer, we transferred files via the "File Box" and "File Transfer" actions, set up and joined a meeting, sent messages via the chat feature, used the remote log off action, used the disable remote input action, allowed remote control during a meeting, and denied remote control during a meeting. By taking registry shots and snapshots of each VM before and after completing each task, we can determine what artifacts are generated by each action.

3 Results

3.1 Versions of TeamViewer

All research was done using the full version of TeamViewer. Other versions of TeamViewer can be found on the TeamViewer website: http://www.teamviewer.com/en/download/windows.aspx.

3.1.1 Versions of Teamviewer

Verison	What it does
TeamViewer QuickSupport	"Simple and small customer module, runs immediately without installation and does not require administrative rights - *optimized for instant support."* (TeamViewer, 2013)
TeamViewer Host	"TeamViewer Host is running as a system service and is used for 24/7 access to remote computers, including login/logout and remote reboot - *optimized for server maintenance or home-office access."* (TeamViewer, 2013)
TeamViewer QuickJoin	"With the application QuickJoin, your customers can easily participate in your presentations. Your customers start the QuickJoin module and log in with their session data - ideal for quick and easy online presentations." (TeamViewer, 2013)
TeamViewer Portable	"TeamViewer Portable can be run directly from a USB stick or a CD - *the perfect solution if you are on the road*." (TeamViewer, 2013)
TeamViewer Manager	"TeamViewer Manager is an optional tool for the administration of your computers and contacts in a database. It also includes logging and reporting functionality for your connections." (TeamViewer, 2013)
TeamViewer MSI package	"TeamViewer MSI is an alternative installation package for the full version or TeamViewer Host. It's used for deploying TeamViewer via Group Policy (GPO) in an Active Directory domain. *TeamViewer MSI is only included in the Corporate license."* (TeamViewer, 2013)

3.2 Specifications

TeamViewer does not specify any requirements to use their software. Sections 3.2.1, 3.2.2, and 3.2.3 list the specifications of the test physical computer and the VMs used.

3.2.1 Physical Test Computer Specifications

Memory	6GB
Processor	Single Processor Quad Core 2.66GHz
HDD	SCSI – 232GB

VMs:

3.2.2 Victim VM Specifications

Memory	2GB
Processor	Single processor 2 core

HDD	SCSI – 60GB
CD/DVD	IDE - Auto (connected at power on)
Floppy	Auto (not connected)
Network	NAT
USB	Auto connect
Sound Card	Default host card, connect at power on
Printer	Connected at power on

3.2.3 Suspect VM Specifications

Memory	2GB
Processor	Single processor 2 core
HDD	SCSI – 60GB
CD/DVD	IDE - Auto (connected at power on)
Floppy	Auto (not connected)
Network	NAT
USB	Auto connect
Sound Card	Default host card, connect at power on
Printer	Connected at power on

3.3 Installing TeamViewer

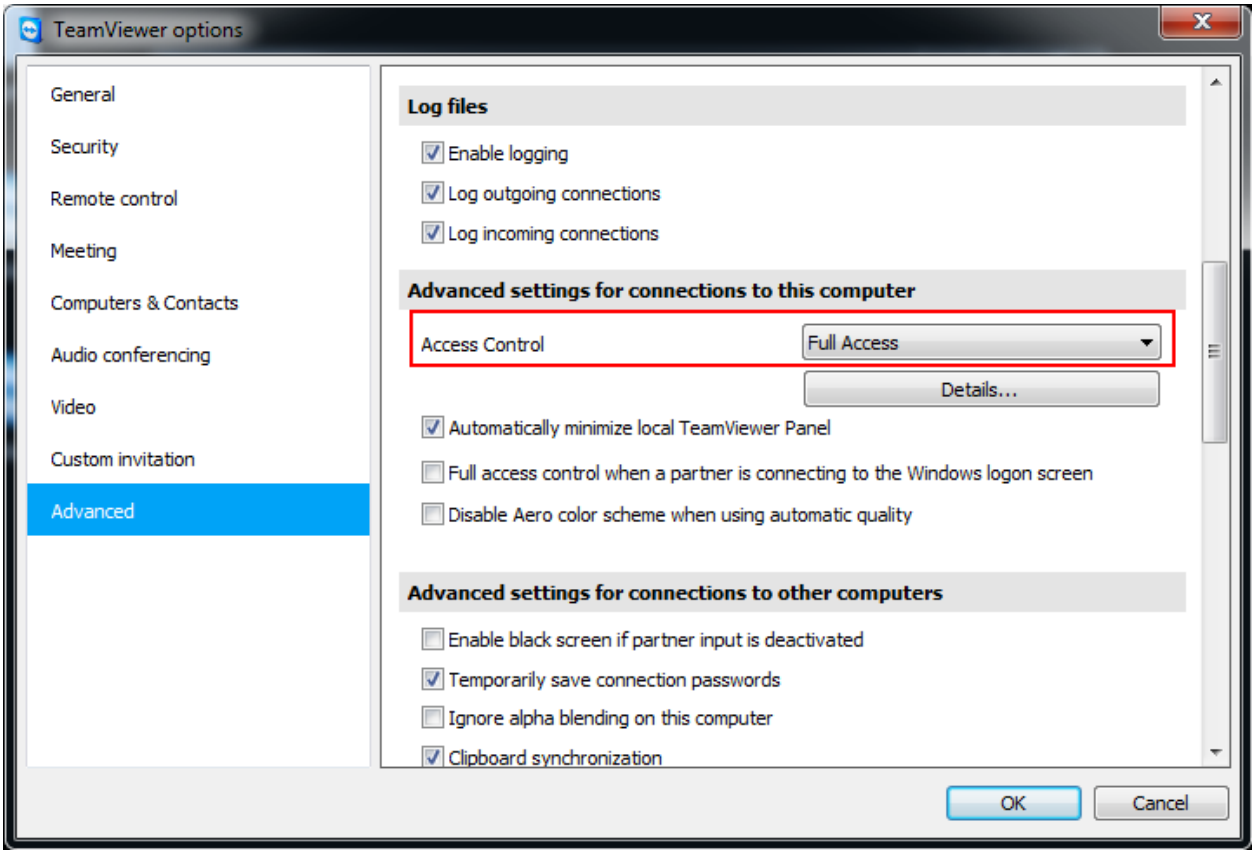
When first installing TeamViewer, the user is prompted with two options: “Full access (Recommended)” or “Confirm all.” “Confirm all” could be used if someone is trying to connect his or her computer while a family member is at home (see Figure 3.3.1 below). When “Full access” is selected, the suspect will have full access to the connected computer; no prompts will be displayed for actions the suspect attempts. By selecting the “Confirm all” option, the victim will be prompted every time the connecting user attempts to perform an action.

On install, the victim also has the choice to set up remote access, which allows him or her to remotely connect to his or her own system from anywhere in the world as long as TeamViewer is installed (see Figure 3.3.2 below). When TeamViewer is finished setting up, the victim and suspect are given a username and password, which they will use to remotely access their system, or another person’s system, in the future. Even if the suspect has full access, he or she will still have to obtain the ID and password (the given password will change every time TeamViewer is launched on the same computer) of the victim’s TeamViewer in order to first gain control of the victim’s computer. In order to start a TeamViewer session, the victim and suspect must both have a version of TeamViewer on their system. The person who initializes the session must have the full version of TeamViewer.

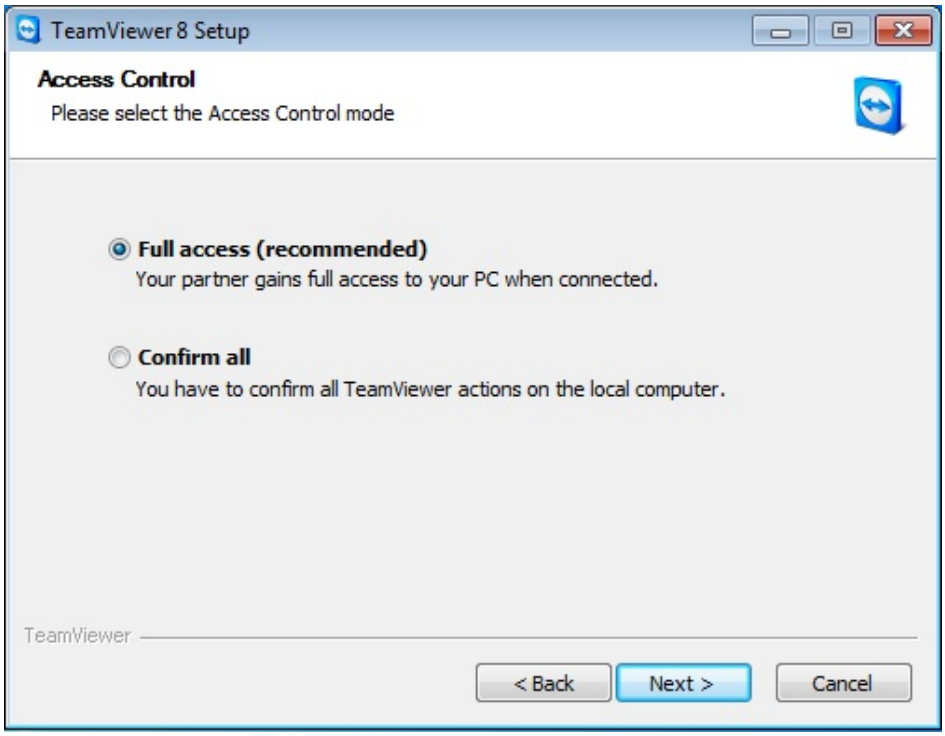
When we first installed TeamViewer, we chose to not allow full access, prompting a notification for every action (for the majority of the research we used the full access option). At any point after TeamViewer is installed, if the victim wishes to set up full access control for their system, they can do so by clicking on “Extras” -> “Options” -> “Advance”, as shown

in Figure 3.3.1 below. We chose to not allow full access at first, allowing us to be certain that we covered all of the options for the installation of the program. Later, after some research, we found that the options chosen do not make a difference in terms of artifacts left behind, nor do they change or add information in the logs. For maximum security, the user should choose the "Confirm all" option, especially when the remote session is being conducted with an unknown person. Note: It is not necessary to have a TeamViewer account to use TeamViewer.

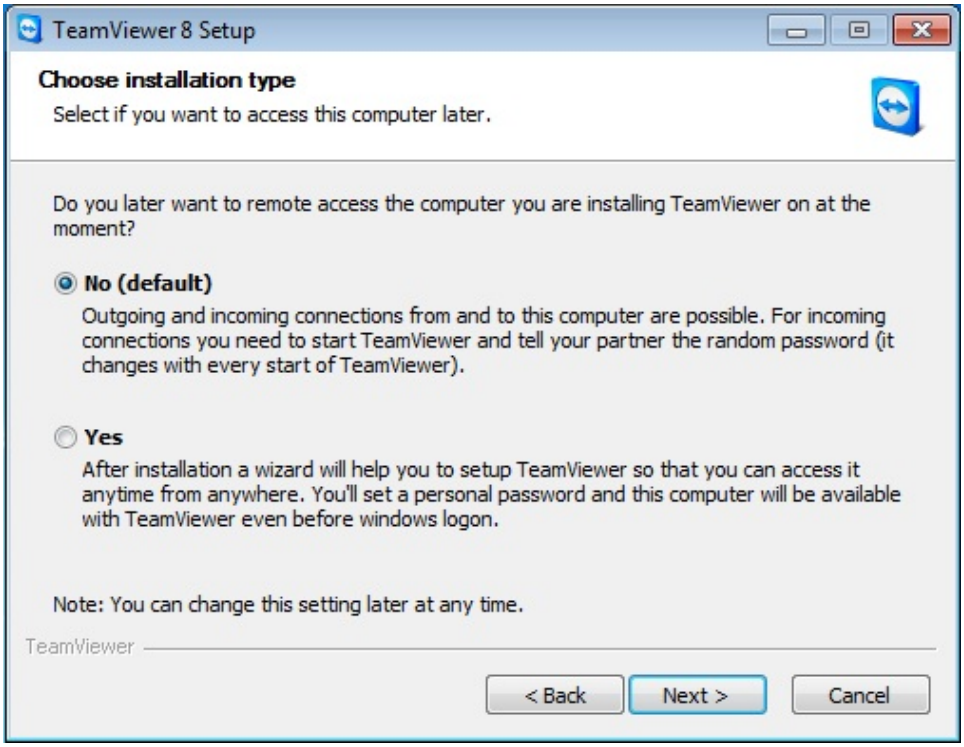
3.3.1 TeamViewer Options



3.3.2 TeamViewer Access Control



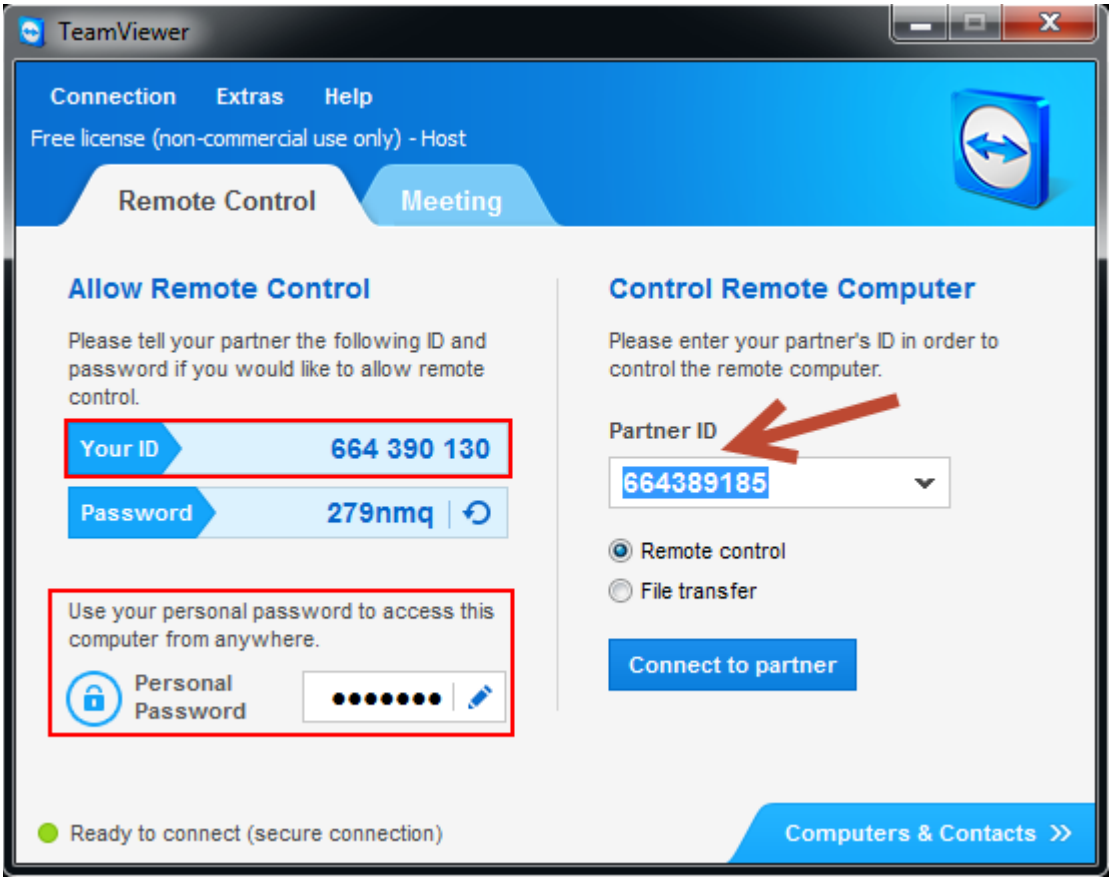
3.3.3 TeamViewer Installation Type



3.4 Remote Access

When a suspect first opens TeamViewer, he or she is prompted with a remote control window (see Figure 3.4.1 below). This window gives you an ID number and a password (the password changes every time you open TeamViewer on the same computer), which you would use to remote into your computer. This could make it hard, if not impossible, for a suspect to use TeamViewer to access a victim's computer, unless the victim has set up unattended access (see Figure 3.4.1). Unattended access allows the victim to enter his or her own personal password, making it easier for a suspect to access the victim's computer using TeamViewer. Additionally, this will allow the victim (or the suspect) to access the computer without needing someone to provide them with the generated password, enabling them to automatically connect to the system. If the suspect can obtain the victim's ID and password, they will enter the ID in the Partner ID window on the right and click "Connect to partner." Once they click this button, it will ask them for the victim's password, which will allow remote access to the victim's computer if the password is correct. This would allow the suspect to easily and readily access the victim's system whenever and wherever, without having to worry about asking the victim for the generated password.

3.4.1 TeamViewer Remote Control Window

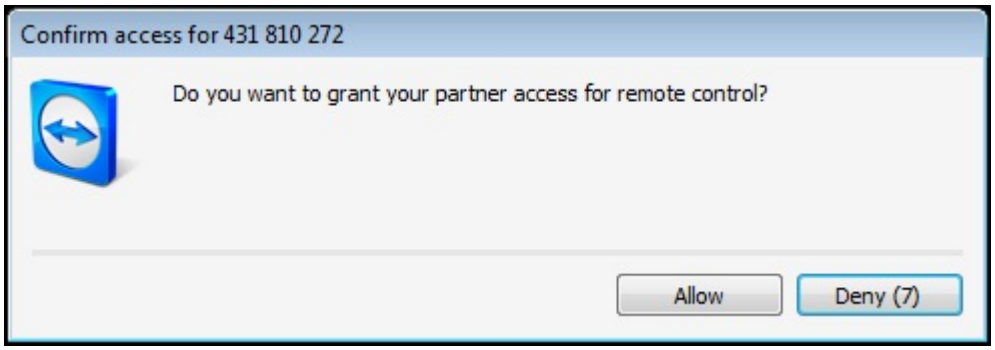


3.5 Remote Control

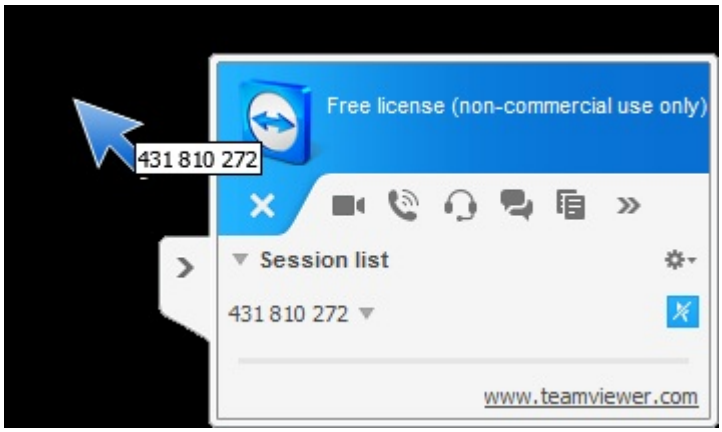
When a suspect first connects to a victim, they are immediately given remote access (with full access turned on); they do not have to get permission from the victim to complete actions such as transferring files or recording the screen. If the confirm all option is turned on and the suspect is attempting to access the victim's computer, the victim will be alerted and must confirm the action before the suspect can connect. All prompts are set on a 10 second timer that automatically denies the action if it is not allowed in the allotted time, as seen in Figure 3.5.1 below. Once the suspect is remotely viewing the victim's screen, the suspect's pointer will show his or her ID hovering nearby (this will occur only if

the confirm all action is turned on), as seen in Figure 3.5.2 below. If full access is turned on, the mouse pointer will look like a normal white mouse pointer. When the suspect is remotely accessing the victim's screen, the screen will show the movement of the mouse and all of the actions as if the suspect were physically present. If a victim is at the computer at the time, he or she will be able to see someone accessing the computer and can exit TeamViewer or turn off the computer. However, there is an option on the suspect's side of TeamViewer that allows him or her to disable remote input. In this case, the victim would not be able to click on anything or access his or her computer. Additionally, this allows the suspect to turn the victim's screen black so they cannot see what is taking place on their system (see Figure 3.5.3 below); however, although the victim cannot see what is going on, he or she can still see the mouse moving on the black screen.

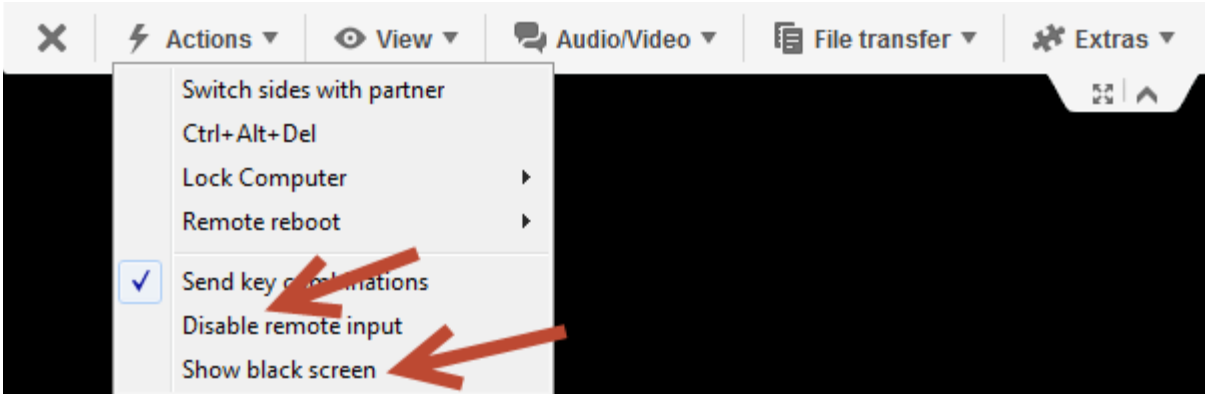
3.5.1 Remote Control Access Prompt



3.5.2 Suspect's Mouse Pointer

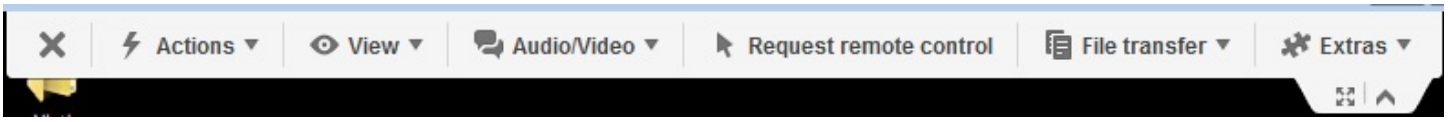


3.5.3 Disable Remote Input/Show black Screen



During remote control, the suspect has access to nearly every part of the system that a normal user would, including access to all hard drives on the system. The suspect is provided with a tool bar, which gives him or her different options to use while accessing the system (see Figure 3.5.4). With this toolbar, the suspect has the ability to lock the computer instantly or on session end, remote reboot, disable remote input on the victim's side, show a blank screen, start chats conference calls, start videos, transfer files, record the session, as well as access the files and use the computer like a normal user would. There are very few limitations to what the suspect can do. One of the only limitations that we have found in the course of our research is that the suspect cannot transfer system files via the file transfer features in TeamViewer, such as the NTUSER.dat files in the user's folders. System files are prohibited from being transferred via TeamViewer; however, he or she could use a freely available acquisition tool, or other such tool, and could access the system files and export them to his or her computer.

3.5.4 Suspect Tool Bar



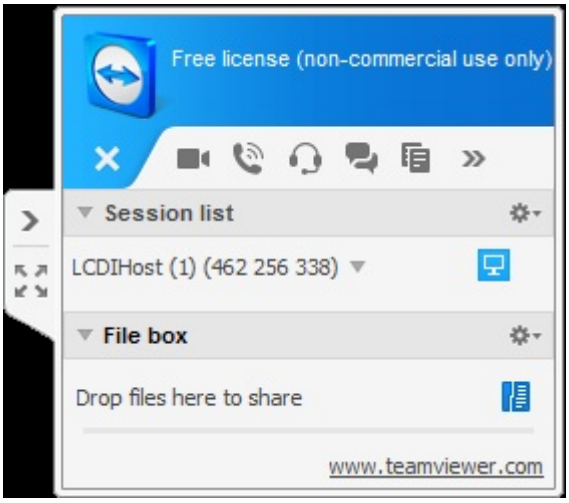
3.6 Transferring Files

There are two methods for transferring files in TeamViewer: the File Box and the File Transfer service.

3.6.1 File Box

The file box is a fast and convenient way to share files under 25 MB. The file box is available in every TeamViewer session, including meetings. The file box is accessible to the suspect via the File Transfer drop down menu on the tool bar, and to the victim via the file box button on the TeamViewer panel. Files in the file box remain there for the duration of the session and are removed when the session is ended. Files can be shared via the file box by dragging and dropping files into the file box. System files and files over 25 MB cannot be shared via the file box. Files dropped into the file box are shared to all individuals in the session, allowing all users to access the files during a meeting (see Figure 3.6.2 below).

3.6.2 TeamViewer File Box

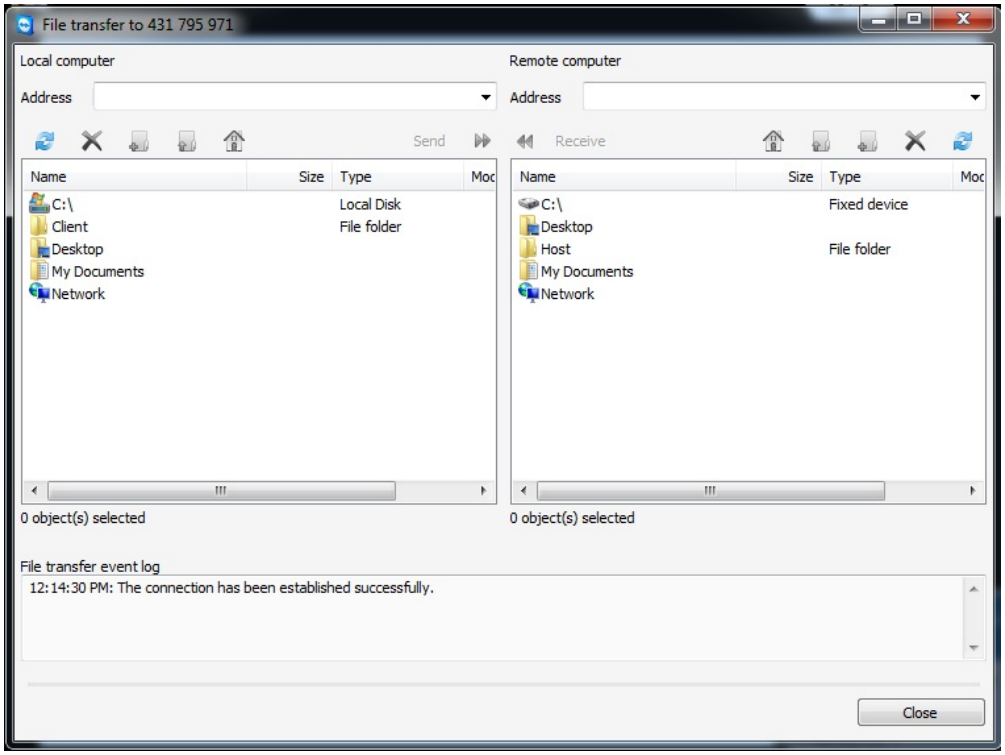


3.6.3 File Transfer

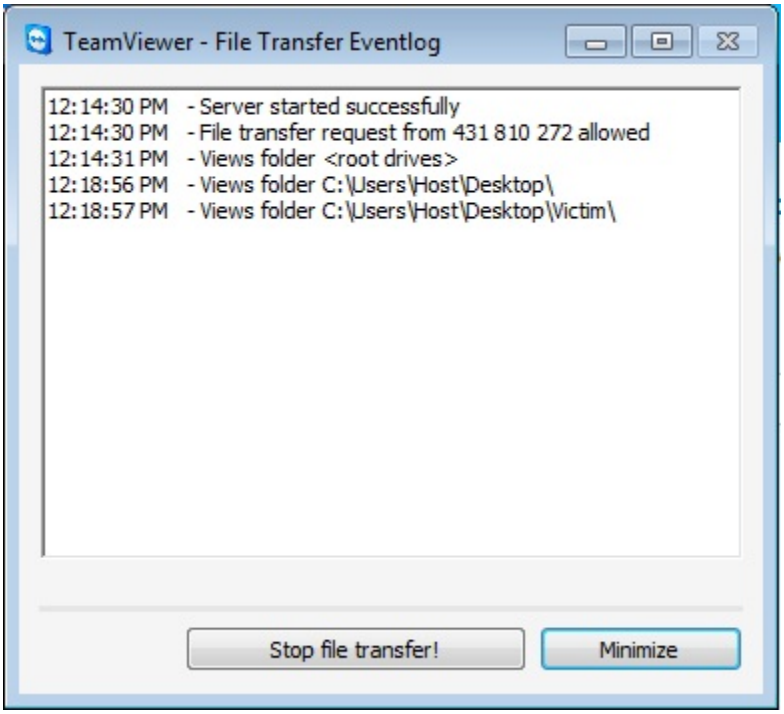
The file transfer service is a way to transfer multiple files easily, including files that are over 25 MBs. This service is available during one-on-one sessions only. Through the file transfer service, users can transfer files from almost

anywhere on their system or from the remote system. However, certain files, such as system files cannot be transferred. The file transfer service is only available to the suspect; he or she can open it via the file transfer menu, as seen in Figure 3.6.3.1 below. The file transfer menu is only visible on the suspect's screen. When a suspect is currently utilizing the file transfer service, the victim can see everything that is occurring via an active log. The active log will show the directories the client is going through, as well as what files they transfer to and from the system. The event log is saved in the TeamViewer log file and shows everything that is happening, including what file is being transferred and from where. Through the event log, the victim also has the ability to stop the file transfer at any time via the large "Stop file transfer!" command at the bottom of the event log (see Figure 3.6.3.2 below). This screen cannot be hidden by the suspect, only minimized or closed, which will stop the transfer. By looking back at the event log, law enforcement is able to see what files were sent to the victim, or taken from the victim, and also from where they were taken or where they were placed.

3.6.3.1 TeamViewer File Transfer



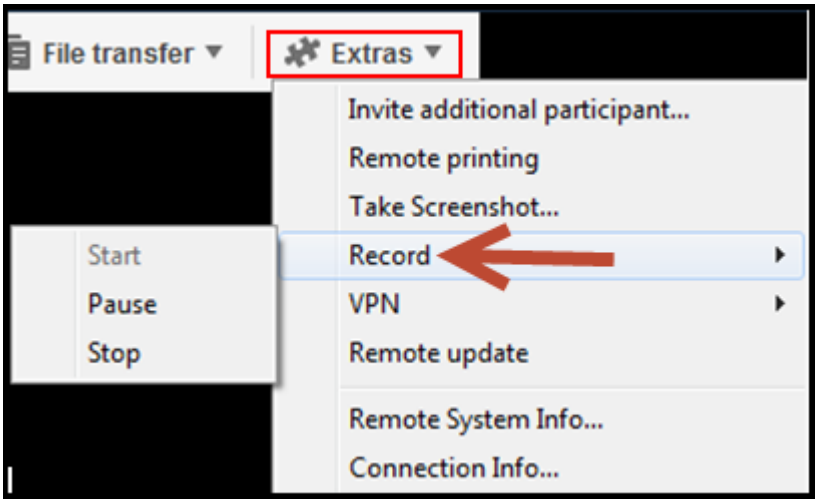
3.6.3.2 TeamViewer File Transfer Event Log



3.7 Recording Sessions

Recording of a TeamViewer session is possible from within the program. Recording can be started from the Extras menu on the suspect tool bar and is only accessible to the suspect (see Figure 3.7.1.1). A victim cannot record a session. A suspect has the ability to record the session without the consent of the victim, as long as they have it set to full access. If TeamViewer is setup to confirm all, the victim will be alerted.

3.7.1.1 Recording Option



Recordings through TeamViewer are saved in a .TVS format, which is proprietary to TeamViewer. The file can be viewed using TeamViewer. By default, the filename is formatted as VictimName (VideoNumber) (ID)_YEAR-MM-DD HH:MM.tvs. For example, LCDIHost (1) (431 795 971)_2013-02-04 13.33.tvs. The time is saved using a 24 hour format. The user is prompted to choose where to save these files after they stop the recording.

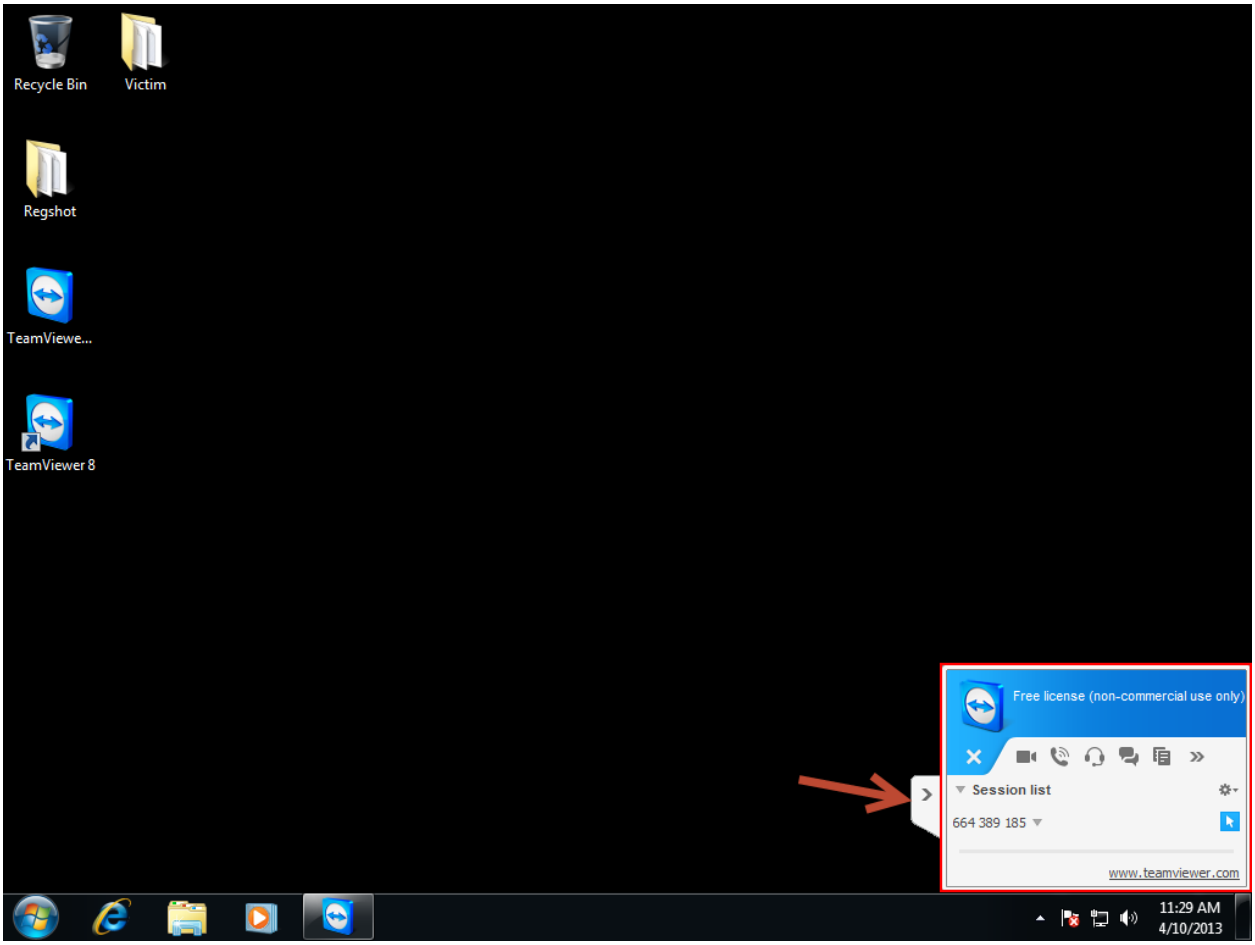
3.8 Malicious Intent

Due to the nature of TeamViewer, being a remote desktop program, it has its share of potential hazards. When a user is granted remote control access to a system, especially if the system has full control allowed by default, the remote system is at risk. The suspect who is connected has full access to the system and can delete files from the system or damage the system if they so choose. A more knowledgeable suspect could go so far as to transfer (or download) and launch a virus, key logger, or other malware onto the victim's system, shut down their firewall and/or anti-virus software, and steal files that contain personal or financial information without the user knowing. The suspect potentially has access to every part of the victim's computer. They have control of all of the actions of the remote computer, including transferring files, remote printing, taking screenshots, recording the screen, and inviting other participants. They even have the ability to disable remote input on the victim's computer, showing a black screen that will not allow the victim to see the suspect's actions. Also, although they cannot directly transfer system protected files, they could easily download software on the computer, such as FTK Imager (a free software), to get a copy of the system files, including the SAM registry hive (which contains password hashes of the user's Windows accounts). The suspect also has the ability to turn off log saving, leaving no log evidence of interactions. A suspect could even lock or logoff the computer, while still having access to it, leaving the victim unsuspecting of the suspect's activity. A suspect also has the ability to start TeamViewer and have it close to the tray menu, so that there is no icon showing on the dock bar; however, the side panel still shows up (see Figure 3.8.1) which is impossible to hide unless you install a third party software.

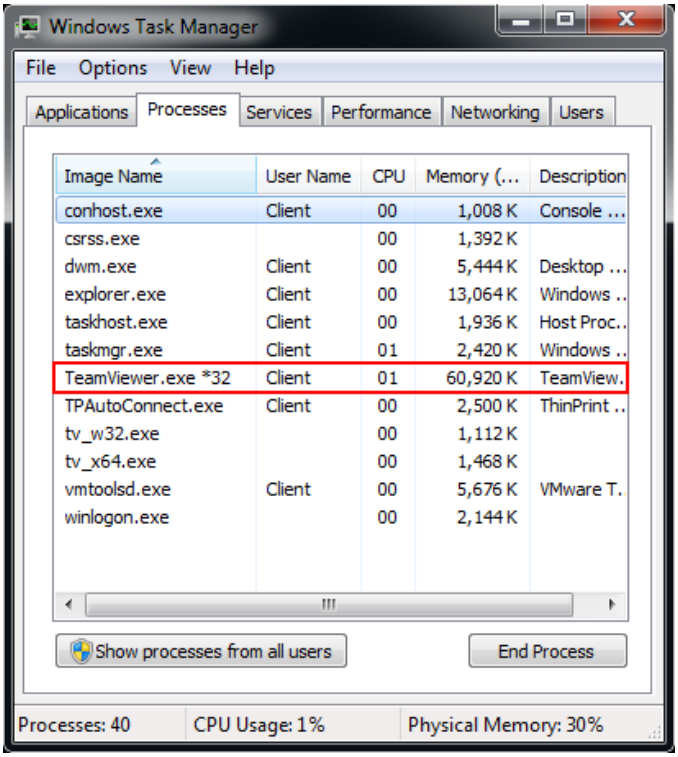
In order for a suspect to use this tool for malicious intent, they would have to know the victim personally. It would be very hard for a suspect to obtain the information from TeamViewer, such as the ID and password, to access the victim's system, unless they knew the individual and knew they had TeamViewer installed. A good example of this would be a wife suspecting her husband of cheating. Since she has physical access to the computer that she and her husband share, she could use TeamViewer to monitor her husband's activities on the computer while she was away. The wife would be

able to record the session and access any files that could contain information proving that her husband was cheating; however, it would be very hard for her to access the computer with TeamViewer if she didn't know the victim. Also, TeamViewer would not help a suspect obtain information from a suspect who is constantly monitoring his or her system. If the victim saw TeamViewer running and didn't run it or didn't have it installed on his or her computer, he or she would most likely realize that someone is trying to access the system and would terminate the process. Also, if a suspect was able to hide TeamViewer, it can still be found as a running process in the Windows Task Manager, as seen in Figure 3.8.2.

3.8.1 Side Panel



3.8.2 Task Manager



What does this mean for investigators and forensics analysts? There needs to be a valid and credible method to analyze systems that have or once had TeamViewer installed. The information generated and left behind by TeamViewer could assist in an investigation and can help show if a suspect used TeamViewer to access the victim's computer. However, it can be difficult to prove because the victim may have installed TeamViewer for his or her own personal use. Investigators can look for the logs files, if there are any, as it shows the IP address of the person connected. Again, in order for a suspect to access a victim's computer, they would most likely need to know the victim, as they would need to get the victim's ID and password.

3.9 Log Files

TeamViewer saves connection data in a log file that can be found in the TeamViewer install folder. For TeamViewer 8, that folder is "C:\Program Files (x86)\TeamViewer\Version8" by default. The log file is saved in a .log format, a common format, and is named "TeamViewer8_Logfile.log" in Version 8. The file constantly grows, adding a new line for every entry. The log saves program data, errors, and connection information. Every new session creates a new entry in the log file, separated by a heading that contains information about the session. The log file can provide extremely useful data if it is turned on. In TeamViewer, the logs are turned on by default; however, they can also be turned off. TeamViewer leaves very little information behind when the logs are turned off. If the suspect was decided to turn off logging, then an investigator would be unable to find information about the session from the suspect or the victim's computers.

The log entry below shows a suspect browsing folders of a remote system with the File Transfer tool. The suspect who was controlling the remote computer started the file transfer service. The suspect requested to start the File Transfer at 12:14 and was allowed the request. The suspect then searched through multiple folders, starting at the root drive and finding their way to "C:\Users\Host\Desktop\Victim\." An investigator can trace the way a suspect went to the folder via the log. The suspect then transferred two files, PrivateInfo.txt from "C:\Users\Host\Desktop\Victim\" and also BadFile.txt from their system to the remote system. BadFile.txt was sent to "C:\Users\Host\Desktop\Victim\." The

suspect searched through additional files, ending in "C:\Users\Host\," where the suspect attempted to transfer a file. This file was not successfully transferred. The File Transfer was then shutdown at 12:40.

Every line of the log file, excluding line breaks and headers, begin with a timestamp starting with the date and followed by the time, down to a fraction of a second. The date is formatted as YEAR:MM:DD, and the time is formatted as HH:MM:SS.SSS. The timestamp uses a 24 hour system.

3.9.1 TeamViewer Log File

```
2013/01/25 12:14:30.337  2280  2656 G2   - File transfer request from 431 810 272 allowed
2013/01/25 12:14:31.387  2280  2656 G2   - Views folder <root drives>
2013/01/25 12:18:47.937  1244  1464 S0   CConnectionThread::PingRouter(): Router Ping started
2013/01/25 12:18:48.172  1244  1464 S0   CT4 CConnectionThread::CmdPingRouter(): Router Pong Received
with following Hops: 431795971 647933962
2013/01/25 12:18:56.227  2280  2656 G2   - Views folder C:\Users\Host\Desktop\
2013/01/25 12:18:57.602  2280  2656 G2   - Views folder C:\Users\Host\Desktop\Victim\
2013/01/25 12:28:26.752  2280  2656 G2   - Processing file transfer...
2013/01/25 12:28:26.862  2280  2656 G2   - Send file C:\Users\Host\Desktop\Victim\PrivateInfo.txt
2013/01/25 12:28:26.882  2280  2656 G2   - File transfer finished.
2013/01/25 12:30:45.702  2280  2656 G2   - Processing file transfer...
2013/01/25 12:30:45.702  2280  2656 G2   - Write file C:\Users\Host\Desktop\Victim\BadFile.txt
2013/01/25 12:30:45.737  2280  2656 G2   - File transfer finished.
2013/01/25 12:30:45.747  2280  2656 G2   - Views folder C:\Users\Host\Desktop\Victim\
2013/01/25 12:31:26.993  2280  2656 G2   - Views folder <root drives>
2013/01/25 12:31:30.953  2280  2656 G2   - Views folder C:\
2013/01/25 12:31:37.093  2280  2656 G2   - Views folder C:\Users\
2013/01/25 12:31:39.748  2280  2656 G2   - Views folder C:\Users\Host\
2013/01/25 12:32:18.218  2280  2656 G2   - Views folder C:\Users\
2013/01/25 12:32:20.488  2280  2656 G2   - Views folder C:\
2013/01/25 12:32:26.558  2280  2656 G2   - Views folder C:\Windows\
2013/01/25 12:32:32.893  2280  2656 G2   - Views folder C:\
2013/01/25 12:32:37.808  2280  2656 G2   - Views folder C:\Program Files\
2013/01/25 12:32:40.623  2280  2656 G2   - Views folder C:\
2013/01/25 12:32:41.393  2280  2656 G2   - Views folder C:\Program Files (x86)\
2013/01/25 12:32:43.208  2280  2656 G2   - Views folder C:\
2013/01/25 12:32:44.673  2280  2656 G2   - Views folder C:\Users\
2013/01/25 12:32:46.428  2280  2656 G2   - Views folder C:\Users\Host\
2013/01/25 12:32:47.418  2280  2656 G2   - Views folder C:\Users\Host\Documents\
2013/01/25 12:32:54.488  2280  2656 G2   - Views folder C:\Users\Host\
2013/01/25 12:33:06.713  2280  2656 G2   - Processing file transfer...
2013/01/25 12:33:06.813  2280  2656 G2   - File transfer finished.
2013/01/25 12:40:41.059  2280  2392 G2   Ending CFileTransferThreadServer...
2013/01/25 12:40:41.059  2280  2392 G2   The CFileTransferThreadServer has ended.
2013/01/25 12:40:41.059  2280  2656 G2   DragDropManager: Aborting 0 copy operations
2013/01/25 12:40:41.059  2280  2656 G2   - File transfer server shut down.
```

Below are two more lines from the log files that show some useful data. The data is color coded with a key to help distinguish the data in the line from the log file.

3.9.2 TeamViewer Log File

```
Key: Date, Time, IP Address, Port
2013/01/23 12:39:53.961  1932  2968 S0   CT3 CT.Connect.176.9.82.177:5938
Key: Display Device Name, Signal Type, Display Number, Resolution
```

3.10 Start of a new session in TeamViewer logfile

At the start of every new session with TeamViewer, a special heading is made in the log file that shows information about the computer that was connecting to the system that the log file is on. This not only makes the log file a bit more user friendly when searching for a particular session, but it can also provide some valuable information such as the date and time that the session began, the OS being used, the IP address, and the location of the TeamViewer executable on the system.

3.10.1 TeamViewer Log File

Start:	2013/01/23 12:09:17.197
Version:	8.0.16642
ID:	0
License:	0
Server:	master12.teamviewer.com
IC:	729358992
CPU:	Intel64 Family 6 Model 23 Stepping 7, GenuineIntel
OS:	Win7 (64-bit)
IP:	172.16.3.136
MID:	0x000c29ec87c2_1ca0431fd8ab1dc_4277033807
MIDv:	0
Proxy-Settings:	Type=1 IP= User=
IE:	8.0.7601.17514
AppPath:	C:\Program Files (x86)\TeamViewer\Version8\TeamViewer_Service.exe
UserAccount:	SYSTEM

3.11 Registry Changes

When uninstalling TeamViewer, the user is given the option to remove all settings or to keep the settings on the machine (this option generally would be used when upgrading versions). For law enforcement, the option a suspect chooses when uninstalling TeamViewer could be the difference between a conviction and the suspect getting away, if the suspect chooses a setting that removes information from the computer that could be pertinent to a case.

To compare the changes in the registry before the program was installed and after it was uninstalled, we used RegShot. We compared two different sets of shots. The first set was the comparison from before TeamViewer was installed and after it was uninstalled with the "Remove Settings" box unchecked. The second set of RegShots were from before installing TeamViewer and after uninstalling TeamViewer with the "Remove Settings" box checked. We were able to compare the different uninstall options by taking a snapshot of the VM before uninstall, then by uninstalling TeamViewer with one of the options, and then reverting back to the snapshot and choosing the second uninstall option.

The first set gave 80 hits of changed or added values to the registry. Only a number of the results have been shown to save on space.

3.11.1 RegShot Comparison

Fresh Install VS Uninstall with "Remove Settings" Unchecked (80 Total, 30 Shown)
HKLM\SOFTWARE\TeamViewer
HKLM\SOFTWARE\TeamViewer\Version8
HKLM\SOFTWARE\TeamViewer\Version8\AccessControl
HKLM\SOFTWARE\TeamViewer\Version8\DefaultSettings
HKLM\SYSTEM\ControlSet002\services\TeamViewer8
HKU\S-1-5-21-4184274577-1583660518-1765458396-1000\Software\TeamViewer
HKU\S-1-5-21-4184274577-1583660518-1765458396-1000\Software\TeamViewer\Version8
HKU\S-1-5-21-4184274577-1583660518-1765458396-1000\Software\TeamViewer\Version8\MsgBoxDontShow

HKU\S-1-5-21-4184274577-1583660518-1765458396-1000\Software\TeamViewer\Version8\MultiMedia
HKLM\SOFTWARE\TeamViewer\Version8\DefaultSettings\Autostart_GUI: 0x00000001
HKLM\SOFTWARE\TeamViewer\Version8\InstallationDate: "2013-01-23"
HKLM\SOFTWARE\TeamViewer\Version8\Always_Online: 0x00000001
HKLM\SOFTWARE\TeamViewer\Version8\Security_ActivateDirectIn: 0x00000000
HKLM\SOFTWARE\TeamViewer\Version8\Version: "8.0.16642"
HKLM\SOFTWARE\TeamViewer\Version8\LastMACUsed: 00 30 30 30 43 32 39 45 43 38 37 43 32 00 00
HKLM\SOFTWARE\TeamViewer\Version8\LastUpdateCheck: 0x51152533
HKLM\SOFTWARE\TeamViewer\Version8\MIDInitiativeGUID: "{ba332aa9-276c-4c50-af30-46382f8bb4eb}"
HKLM\SOFTWARE\TeamViewer\Version8\MIDVersion: 0x00000001
HKLM\SOFTWARE\TeamViewer\Version8\ClientID: 0x19BCAF03
HKLM\SOFTWARE\TeamViewer\Version8\UsageEnvironmentBackup: 0x00000002
HKLM\SOFTWARE\TeamViewer\Version8\LicenseType: 0x00002710
HKLM\SOFTWARE\TeamViewer\Version8\UpdateVersion: 00
HKLM\SOFTWARE\TeamViewer\Version8\ConnectionHistory: 75 F1 2A C2 D2 5D 3D 35 E6 6C 7B 62 98 CA 6C 62
HKLM\SOFTWARE\TeamViewer\Version8\Security_PasswordStrength: 0x00000001
HKLM\SOFTWARE\TeamViewer\Version8\SecurityPasswordAES: F2 5C 41 A7 21 A8 84 E7 F9 25 CC 3E A6 4E 16 38 B9 9B CF 39 1D B6 55 10 6E 6D E3 C5 14 98 4C 54
HKLM\SOFTWARE\TeamViewer\Version8\LastKeepalivePerformance: "178.238.46.115:1"
HKLM\SYSTEM\ControlSet002\services\TeamViewer8\Type: 0x00000010
HKLM\SYSTEM\ControlSet002\services\TeamViewer8\Start: 0x00000002
HKLM\SYSTEM\ControlSet002\services\TeamViewer8\ErrorControl: 0x00000001
HKLM\SYSTEM\ControlSet002\services\TeamViewer8\ImagePath: ""C:\Program Files (x86)\TeamViewer\Version8\TeamViewer_Service.exe""

The second set only gave 36 changes or additions to the registry. By checking the “Remove Settings” box when uninstalling TeamViewer, the user removed more than half of the entries or changes that would otherwise exist without the box being checked.

3.11.2 RegShot Comparison

Fresh Install VS Uninstall with “Remove Settings” Checked (36 Total, 20 Shown)
HKLM\SYSTEM\ControlSet002\services\TeamViewer8
HKU\S-1-5-21-4184274577-1583660518-1765458396-1000\Software\TeamViewer
HKLM\SYSTEM\ControlSet002\services\TeamViewer8\Type: 0x00000010
HKLM\SYSTEM\ControlSet002\services\TeamViewer8\Start: 0x00000002
HKLM\SYSTEM\ControlSet002\services\TeamViewer8\ErrorControl: 0x00000001
HKLM\SYSTEM\ControlSet002\services\TeamViewer8\ImagePath: ""C:\Program Files(x86)\TeamViewer\Version8\TeamViewer_Service.exe""
HKLM\SYSTEM\ControlSet002\services\TeamViewer8\DisplayName: "TeamViewer 8"
HKLM\SYSTEM\ControlSet002\services\TeamViewer8\WOW64: 0x00000001
HKLM\SYSTEM\ControlSet002\services\TeamViewer8\ObjectName: "LocalSystem"
HKLM\SYSTEM\ControlSet002\services\TeamViewer8\Description: "TeamViewer Remote Software"
HKLM\SYSTEM\ControlSet002\services\TeamViewer8\FailureActions: 80 51 01 00 00 00 00 00 00 00 00 00 03 00 00 00 14 00 00 00 01 00 00 00 D0 07 00 00 01 00 00 00 D0 07 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-4184274577-1583660518-1765458396-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage\NewShortcuts\C:\Users\Host\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\TeamViewer 8.lnk: 0x00000001
HKU\S-1-5-21-4184274577-1583660518-1765458396-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage\NewShortcuts\C:\ProgramData\Microsoft\Windows\Start Menu\Programs\TeamViewer 8.lnk: 0x00000001
HKU\S-1-5-21-4184274577-1583660518-1765458396-1000\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Persisted\C:\Users\Host\Desktop\TeamViewer_Setup_en-ckj.exe: 0x00000001
HKU\S-1-5-21-4184274577-1583660518-1765458396-1000\Software\Microsoft\Direct3D\MostRecentApplication\Name: "TeamViewer_Service.exe"
HKU\S-1-5-21-4184274577-1583660518-1765458396-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Program Files (x86)\TeamViewer\Version8\tv_x64.exe: "TeamViewer 8"
HKU\S-1-5-21-4184274577-1583660518-1765458396-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Program Files (x86)\TeamViewer\Version8\tv_w32.exe: "TeamViewer 8"
HKU\S-1-5-21-4184274577-1583660518-1765458396-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Program Files (x86)\TeamViewer\Version8\TeamViewer_Service.exe: "TeamViewer 8"

HKU\.DEFAULT\Software\Microsoft\Direct3D\MostRecentApplication\Name: "TeamViewer_Desktop.exe"
HKU\S-1-5-18\Software\Microsoft\Direct3D\MostRecentApplication\Name: "TeamViewer_Desktop.exe"

4 Conclusion

When a victim's system is being accessed by TeamViewer, depending upon their settings, they may have no alerts to the other user's actions, or they may be asked to allow access to their machine. When a system is being controlled by TeamViewer, the mouse movements and clicks will be visible on the system being controlled. As with any program, the Task Manager will always show the service or process that is running behind the program, therefore if a victim's system is running TeamViewer or is being accessed by TeamViewer, evidence of this can be found in the Task Manager. The process will be listed under Processes, and there will be a small amount of CPU and Memory usage from this process.

In TeamViewer, there is a built in session recorder. This allows suspects to record their sessions while they are in a meeting or accessing a remote system; however, the remote system has to allow the session to be recorded. At the same time, even if the remote system does not allow the suspect to record the session, any screen capture program can be used outside of TeamViewer to record the session without the knowledge of the remote system.

There are two methods that can be used to transfer files in TeamViewer: the File Box and the File Transfer service. The File Box only allows for files up to 25 MB in size to be transferred, while the File Transfer service allows for files of any size as well as any amount of files to be transferred at one time. Through both methods, the remote system user must allow the transfers to occur, and they also have the ability to monitor any file being transferred and the ability to cancel files from being transferred. After files are transferred they show up in the log files. Some files on the remote system are restricted from file transfer to the connecting system, such as system files.

When uninstalling TeamViewer, the user is prompted to either remove settings or to retain the settings after the program is uninstalled. For a suspect to remove all traces of evidence, he or she would have to physically access the victim's computer, as you are unable to uninstall TeamViewer while remotely accessing the computer. Generally, the reason that a user would keep his or her settings is if they intend to reinstall the program again, to update it for instance. When a user does not remove the settings there are more artifacts left behind, which can be found in most of the default saved locations mentioned in the report above, versus if they chose to remove all settings. Using the registry as an example, when the program was uninstalled without removing the settings, there were about 80 entries and changes, but when the settings were removed, only 36 entries and changes remained. Other than registry changes, few artifacts are left behind by TeamViewer. The install folder itself remains as well, but nothing else; everything is deleted, including the log file.

The log files left by TeamViewer hold the most data and show a large portion of what has happened during a session, including every file transfer and information about the members in the session. The log file is named

"TeamViewer8_Logfile.log" in Version 8. These log files are all stored in the TeamViewer install folder, which by default is "C:\Program Files (x86)\TeamViewer\Version8" for TeamViewer Version 8.

5 Further Work

Due to the numerous features that exist within TeamViewer, the amount of further work that can be done with TeamViewer is immense. The fact that TeamViewer exists in over 5 different versions, such as the standard version, the host version, and mobile versions, leads to even more information and data that could be gathered and analyzed.

TeamViewer Host version is one version that is particularly interesting and could use more research. This version could be used maliciously against another person if the remote system user was unaware that the program was installed on their system, as it does not need any human interaction and can only be found running in the Task Manager.

More work could also be done with the images from the VMs. Keyword searches and other examination techniques could be used to find more artifacts that TeamViewer leaves behind.

A more thorough search could also be done to find more artifacts and to do more analysis of those artifacts to find out whether or not important data could be found in them. A thorough look through the log files to find more information that is logged by the program could also be beneficial, as this is the largest source of information about previous sessions.

6 References

Nelson, M. (2012, December 22). *TeamViewer 8.* Retrieved February 5, 2013, from ForensicArtifacts.com: http://forensicartifacts.com/

TeamViewer. (2013). *TeamViewer Download for Windows.* Retrieved January 29, 2013, from TeamViewer: http://www.teamviewer.com/en/download/windows.aspx