FORENSIC REPORT: A Review of an Alleged Security Breach of Iridium Electronics’ Network

Case Number: RA-2019

Evidence Number(s): RA-2019-001
RA-2019-002
RA-2019-003
RA-2019-004
RA-2019-005
RA-2019-006
RA-2019-007

Examiner: Michael Fernez
Iridium Electronics, Inc
899 10th Ave, New York, NY
P: (516) 643 1730
E: mjfernez@gmail.com

Table of Contents

Request

The examiner, an employee of Iridium Electronics' corporate security office, was requested to investigate a former employee by the name of Richmond Avenal. Iridium Electronics was alerted to a potential security breach by Jen Barber, a financial analyst, who alleges that Mr. Avenal operated her computer remotely in order to view and steal confidential financial information belonging to Iridium Electronics.

To direct my investigation, I was requested to:

- Collect and verify a copy of the recovered evidence in a forensically sound manner
- Examine the devices for any evidence that support or deny Ms. Barber's claims that Mr. Avenal had accessed her computer via Team Viewer
- Examine Mr. Avenal's devices for any evidence that he accessed, copied, or transmitted information which was confidential or he was otherwise unauthorized to access
- Examine all devices for any other potential unlawful activities Mr. Avenal might have committed during the course of his employment

Executive Summary

I received a total of 4 EnCase format images [1] (two broken into three fragments) containing the contents of both Avenal's and Barber's computers and USB drives. These will be referred to in this document by their device labels: RICHMOND-PC, BARBER-PC, CRUZER_2GB, and JETFHLASH USB. I also received two snapshots and copies of the volatile or RAM memory [2] which were taken at the time the computers were seized. The IT security staff also granted me permission to view and extract messages from their email server and utilize Avenal's decryption keys.

After taking steps to secure and verify each image, I utilized FTK Imager and Autopsy to search for and extract files of interest. I examined and extracted folders and files associated with each user including documents, shortcut files (a.k.a. link files), program files, Team Viewer log files, registry files, web history and deleted files in the Recycle Bin. On the basis of these analyses, I also inspected each computer for shellbag keys, jump lists, prefetch files, and system restore points (or volume shadow copies) to find more detailed information on the files and programs accessed by the user and to recover deleted files [3-4]. From the examination, I was able to determine:

1. RICHMOND-PC was connected to BARBER-PC via TeamViewer at the time of seizure on October 14th, 2015 at 12:45 PM. RICHMOND-PC was also used to access confidential files on BARBER-PC belonging to Iridium Electronics. (Exhibit A)

2. Richmond Avenal was given notice by Jen Barber on October 9th, 2015 via email that her work documents were confidential after he had referenced them in a previous email (Exhibit B)

3. RICHMOND-PC was also connected to and accessed confidential files on BARBER-PC on October 8th, 2015. However, the files were not stored or recoverable from Avenal's devices. (Exhibit C).

4. There is some evidence to suggest more Teamviewer sessions were launched between October 8th and October 14th on each PC in log files which were recovered from system backups.

5. CRUZER_2GB from the suspect's drawer contained installers for the programs Sdelete and Eraser secure deletion software as well as Team Viewer. There is evidence that same drive was connected to RICHMOND-PC multiple times

6. RICHMOND-PC contains references to another external drive labeled "VHD" which contained folders labeled "Quotes Downloaded October 8th, 2015" and "Quotes Downloaded October 14th, 2015"

Collection Summary

This examination was performed on an Encase Image File [4], created under the direction of Iridium Electronics by Johnny Imager. Upon receiving the image from Google Drive, I verified the drive’s hash value in FTK Imager and recorded its properties. The suspected stolen documents were provided from the same and verified by the same process. The computer image was stored on an external USB drive and mounted as read-only [5].

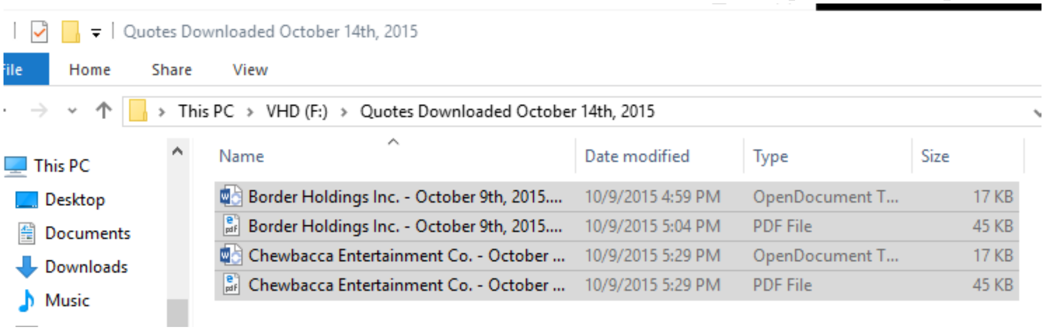
Evidence File	Size (bytes)	Description
IRIDIUM-AVENAL.E01	64,424,509,440	RICHMOND-PC
AVENAL SanDisk Cruzer Micro.E01	2,055,021,056	CRUZER_2GB USB Drive
IRRIDUM-AVENAL Memory.bin	2,147,483,648	RICHMOND-PC RAM memory
IRRIDIUM-BARBER.E01	64,424,509,440	BARBER-PC
BARBER JetFlash 1GB.E01	1,022,361,600	JETFLASH USB drive
IRRIDUM-BARBER Memory.bin	2,147,483,648	BARBER-PC RAM memory
IRRIDIUM-DC Logical Acq.L01	9,374,505	IRRIDIUM-DC

Evidence File	MD5 hash
IRIDIUM-AVENAL.E01	f9bb6e91a4efa64aa178e054672409ef
AVENAL SanDisk Cruzer Micro.E01	518dd322f8a532b688ac52fc238a8f76
IRRIDUM-AVENAL Memory.bin	45fa8429d76ea2a78f2e5906359a39d8
IRRIDIUM-BARBER.E01	4f9b30ba64f69731cebbfbf4fda4bd51
BARBER JetFlash 1GB.E01	83b9882d79e96f3b4a21b3a81b2e61cd
IRRIDUM-BARBER Memory.bin	ef102186924e7fed24bc6d3bbbea4ec1
IRRIDIUM-DC Logical Acq.L01	64ab92437fc03a28519cf93c9e983c15

Investigation Report

Preliminary Investigation

The Iridium IT security staff documented the seizure of RICHMOND-PC and BARBER-PC in the form of screen shots, presented as **Exhibit A**. The screen shot of BARBER-PC shows a Chrome browser in incognito mode sending an email to a contact labeled “Vince Black” with four documents labeled “Border Holdings Inc. - October 9th.pdf” and similar. Also evident in the bottom-right corner is a Team Viewer dialog labeled with “RICHMOND-PC.” In the corresponding screen shot of RICHMOND-PC, a file viewer windows is present and is open to a network drive belonging to BARBER-PC (\\irridium.barber\c$\Users\jen.barber\Documents\Quotes\”) with four documents of the same name highlighted. The same four documents are also highlighted in a file viewer window viewing the path “F:\Quotes Downloaded October 14th, 2015.” The four files in question are presented below.


Quotes Downloaded October 14th, 2015
ile
Home
Share
View
This PC › VHD (F:) › Quotes Downloaded October 14th, 2015
This PC
Desktop
Documents
Downloads
Music

Name	Date modified	Type	Size
Border Holdings Inc. - October 9th, 2015....	10/9/2015 4:59 PM	OpenDocument T...	17 KB
Border Holdings Inc. - October 9th, 2015....	10/9/2015 5:04 PM	PDF File	45 KB
Chewbacca Entertainment Co. - October ...	10/9/2015 5:29 PM	OpenDocument T...	17 KB
Chewbacca Entertainment Co. - October ...	10/9/2015 5:29 PM	PDF File	45 KB

Figure 1. Four quotes from Iridium Electronics as viewed from RICHMOND-PC

Iridium Mail Server

The Iridium Mail Server was provided as a logical image, simply a directory of folders from the server. It contained all correspondence among Iridium employees Avenal, Barber, Reynholm, and Trenneman. I browsed these email files manually using Mozilla Thunderbird as an email client. Among these messages, a particular email chain was recovered between Jen Barber and Richmond Avenal concerning quotes Mr. Avenal noticed on Ms. Barber’s screen. Ms. Barber replies firm that the files are "supposed to be confidential" and that Mr. Avenal was "taking too much of an unhealthy interest" in her work. This email chain is presented separately as **Exhibit B**.

Recovered USB Drives

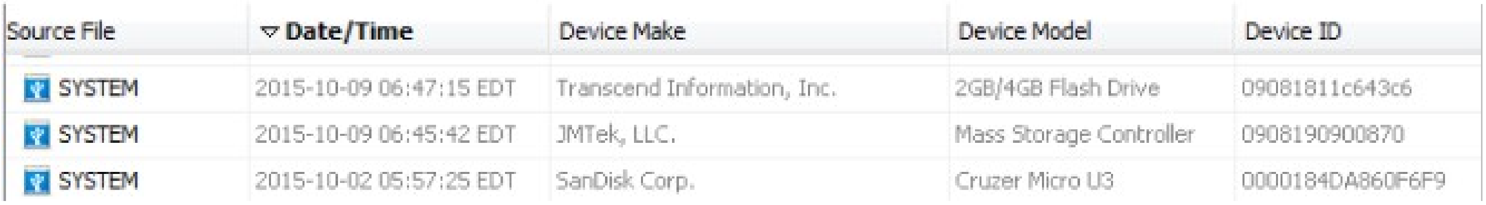
Two USB drives were recovered from Iridium Electronics, one turned over from Ms. Barber and one found locked inside Mr. Avenal's drive. Ms. Barber's drive was searched for abnormalities and file damage, but none appeared evident. The drive contains Vacation Photos that Ms. Barber had shared with work colleagues.

Mr. Avenal's drive was encrypted with BitLocker. I mounted the image of the USB as a "removable device" using Arsenal Image Mounter and was prompted for the decryption key. The recovery key was provided by the Iridium IT security staff, so I selected "Forgot Password" and unlocked the drive using the recovery key. The drive contains two folders "Installers" and "Private." The "Installers" folder contains installers for TeamViewer, Sdelete, File Date Change, and Eraser. The "Private" folder contained protected documents that appeared to be manuals and more BitLocker decryption keys. I attempted to review the contents of these documents, both with a hex editor and Microsoft Azure Protection Viewer, but no further information could be recovered.

Recovered Computers: Registry Analysis

Using FTK Imager, I located the system registry files in "C:\Windows\System32\config\" for both RICHMOND-PC and BARBER-PC [6]. In this case, I was particularly interested in the SYSTEM and SOFTWARE files which contain information about hardware and software respectively, but also the SAM file which would contain more details about the user accounts [6]. To accomplish this analysis, I used Regripper to load each extracted registry file and write the results to a report file.

Using the results of these reports I determined the respective IP addresses of RICHMOND-PC and BARBER-PC (192.168.0.22 and 21), the computer and network names, and user sids. The reports from Regripper's analysis of the SOFTWARE and SYSTEM registry files also revealed two external storage devices, two USB drives, one SanDisk Cruzer and one Kingston.

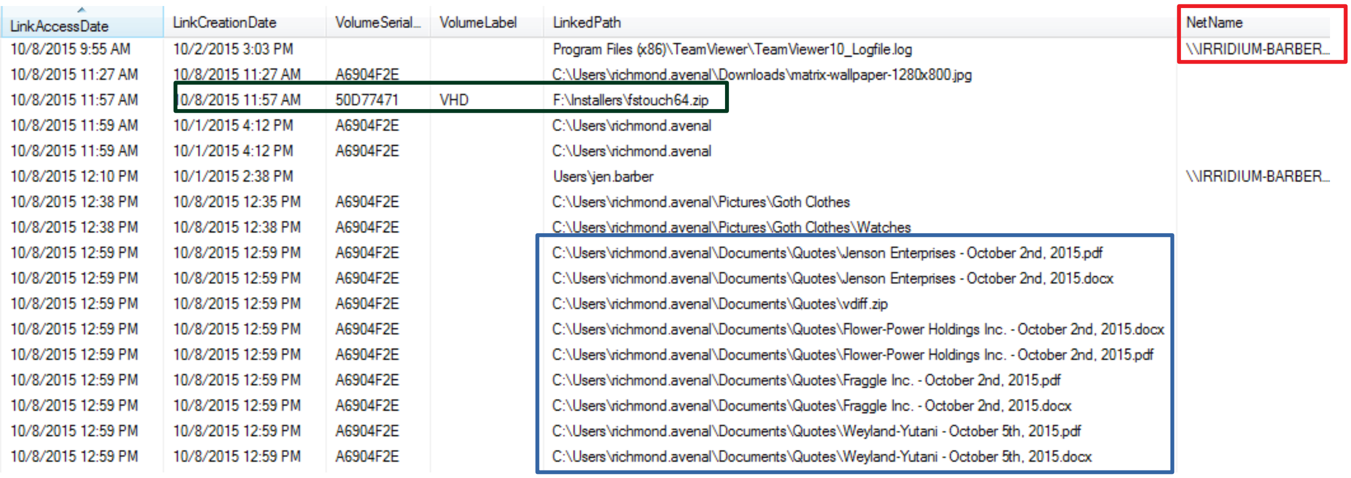


Source File	Date/Time	Device Make	Device Model	Device ID
SYSTEM	2015-10-09 06:47:15 EDT	Transcend Information, Inc.	2GB/4GB Flash Drive	09081811c643c6
SYSTEM	2015-10-09 06:45:42 EDT	JMTek, LLC.	Mass Storage Controller	0908190900870
SYSTEM	2015-10-02 05:57:25 EDT	SanDisk Corp.	Cruzer Micro U3	0000184DA860F6F9

Figure 2. External storage, which was attached to the computer as viewed in Autopsy, showing device models and serial numbers

Recovered Computers: Link File and Jump list Analysis

Continuing with FTK Imager, the folder "C:\Users\richmond.avenal\AppData\Roaming\ Microsoft\Windows\Recent\" was extracted to examine link files and jump lists [3]. In all. 114 link files were recovered. Using the tool Link Parser and JumpListsView, I organized the files by accessed time and browsed them manually. Most notable among these files were linked paths to folders which were not recoverable on RICHMOND-PC, for example "C:\Users\richmond.avenal\Documents\Quotes\" last accessed on October 8th, 2015. Also notable were artifacts pointing to BARBER-PC as the network name and an external drive labeled "VHD" which was not recovered as evidence. The Recent folder of RICHMOND-PC is submitted as **Exhibit C,** snapshot in Figure 3.



LinkAccessDate	LinkCreationDate	VolumeSerial...	VolumeLabel	LinkedPath	NetName
10/8/2015 9:55 AM	10/2/2015 3:03 PM			Program Files (x86)\TeamViewer\TeamViewer10_Logfile.log	\\IRRIDIUM-BARBER...
10/8/2015 11:27 AM	10/8/2015 11:27 AM	A6904F2E		C:\Users\richmond.avenal\Downloads\matrix-wallpaper-1280x800.jpg	
10/8/2015 11:57 AM	10/8/2015 11:57 AM	50D77471	VHD	F:\Installers\fstouch64.zip	
10/8/2015 11:59 AM	10/1/2015 4:12 PM	A6904F2E		C:\Users\richmond.avenal	
10/8/2015 11:59 AM	10/1/2015 4:12 PM	A6904F2E		C:\Users\richmond.avenal	
10/8/2015 12:10 PM	10/1/2015 2:38 PM			Users\jen.barber	\\IRRIDIUM-BARBER...
10/8/2015 12:38 PM	10/8/2015 12:35 PM	A6904F2E		C:\Users\richmond.avenal\Pictures\Goth Clothes	
10/8/2015 12:38 PM	10/8/2015 12:38 PM	A6904F2E		C:\Users\richmond.avenal\Pictures\Goth Clothes\Watches	
10/8/2015 12:59 PM	10/8/2015 12:59 PM	A6904F2E		C:\Users\richmond.avenal\Documents\Quotes\Jenson Enterprises - October 2nd, 2015.pdf	
10/8/2015 12:59 PM	10/8/2015 12:59 PM	A6904F2E		C:\Users\richmond.avenal\Documents\Quotes\Jenson Enterprises - October 2nd, 2015.docx	
10/8/2015 12:59 PM	10/8/2015 12:59 PM	A6904F2E		C:\Users\richmond.avenal\Documents\Quotes\vdiff.zip	
10/8/2015 12:59 PM	10/8/2015 12:59 PM	A6904F2E		C:\Users\richmond.avenal\Documents\Quotes\Flower-Power Holdings Inc. - October 2nd, 2015.docx	
10/8/2015 12:59 PM	10/8/2015 12:59 PM	A6904F2E		C:\Users\richmond.avenal\Documents\Quotes\Flower-Power Holdings Inc. - October 2nd, 2015.pdf	
10/8/2015 12:59 PM	10/8/2015 12:59 PM	A6904F2E		C:\Users\richmond.avenal\Documents\Quotes\Fraggle Inc. - October 2nd, 2015.pdf	
10/8/2015 12:59 PM	10/8/2015 12:59 PM	A6904F2E		C:\Users\richmond.avenal\Documents\Quotes\Fraggle Inc. - October 2nd, 2015.docx	
10/8/2015 12:59 PM	10/8/2015 12:59 PM	A6904F2E		C:\Users\richmond.avenal\Documents\Quotes\Weyland-Yutani - October 5th, 2015.pdf	
10/8/2015 12:59 PM	10/8/2015 12:59 PM	A6904F2E		C:\Users\richmond.avenal\Documents\Quotes\Weyland-Yutani - October 5th, 2015.docx	

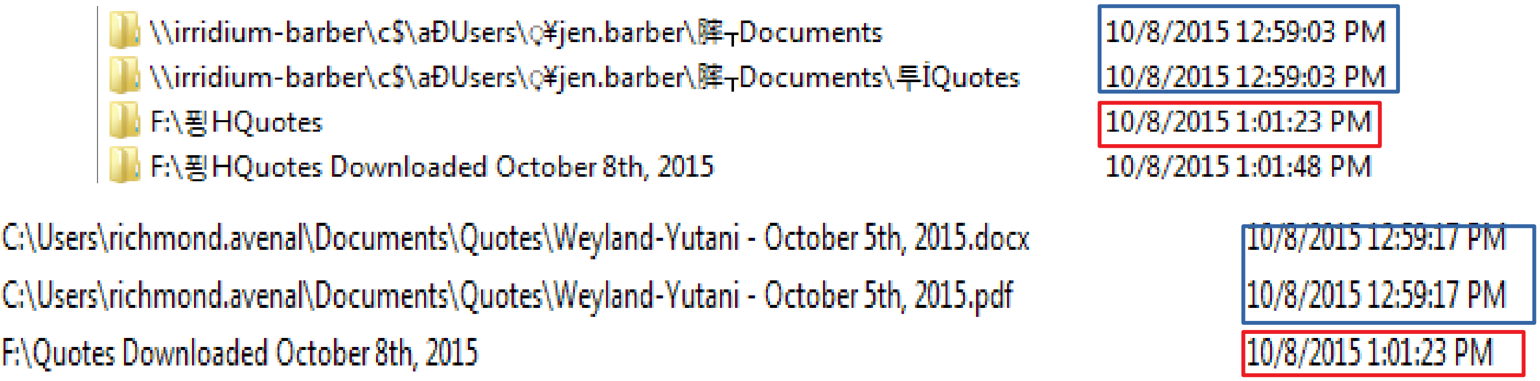
Figure 3. The results of Link Parser, showing files accessed by RICHMOND-PC. Notably, there are artifacts showing work files and TeamViewer log files which were accessed under Jen Barber's network name (red). Corresponding results found in Jump Lists

The same process was repeated for link files on BARBER-PC, but did not reveal abnormalities as indicated above.

Recovered Computers: Shellbag Analysis

Since I was able to recover link files, I chose to look for any evidence in the system shellbag keys pointing to these files since shellbags are used by Windows File Explorer to keep track of file information [10]. The UserClass.dat and NTUSER.DAT files were extracted from "C:\Users\richmond.avenal\AppData\Local\Microsoft\Windows\" and "C:\Users\richmond.avenal\" and loaded into ShellBagsView to be analyzed.

A comparative result of both jump lists and shellbags recovered from October 8th, 2015 are presented as **Exhibit C**. As figure 4 shows, the timestamps paint a clear picture that quotes were accessed by RICHMOND-PC through the network drive first, then on RICHMOND-PC locally, and then on an external device.



```
\\irridium-barber\c$\aĐUsers\ç¥jen.barber\降┬Documents                      10/8/2015 12:59:03 PM
\\irridium-barber\c$\aĐUsers\ç¥jen.barber\降┬Documents\투İQuotes            10/8/2015 12:59:03 PM
F:\횡HQuotes                                                                 10/8/2015 1:01:23 PM
F:\횡HQuotes Downloaded October 8th, 2015                                    10/8/2015 1:01:48 PM

C:\Users\richmond.avenal\Documents\Quotes\Weyland-Yutani - October 5th, 2015.docx     10/8/2015 12:59:17 PM
C:\Users\richmond.avenal\Documents\Quotes\Weyland-Yutani - October 5th, 2015.pdf      10/8/2015 12:59:17 PM
F:\Quotes Downloaded October 8th, 2015                                                10/8/2015 1:01:23 PM
```

Figure 4. A comparison of shellbags (top) versus jump lists (bottom) recovered early 10/8/2015. PC accesses Jen Barber's documents through the network folder at 1:59 PM (local time), and new files appear in Richmond's document at 1:59:17. A USB device is accessed at 2:01 PM

Recovered Computers: Program Files and Prefetch Analysis

Knowing TeamViewer was installed on both machines, I researched the tool to see if it keeps logs of users connecting through the software. TeamViewer keeps logs in both “C:\Program Files (x86)\” and “ C:\Users\jen.barber\AppData\Roaming\TeamViewer\” and according to a Senior Support Engineer at Team Viewer, the logs keep times in local time [10-11].

On RICHMOND-PC the log files in the Program Files folder indicated numerous sessions from 10/8/2015 to 10/14/2015, however no files could be recovered from the cache folder. Notably, RICHMOND-PC logged a TeamViewer session 10/8/15 at 1:48:25 PM, 10 minutes before accessing the folder on BARBER-PC in Figure 4. RICHMOND-PC also logged a session on 10/14/15 at 12:25:08 PM, 20 minutes before the device was seized. On BARBER-PC, the log file recovered from Program Files indicated only a single session for 10/14/2015 at 12:22:06 PM. A backup log file labeled “OLD” indicated one more session on 10/10/2015 at 4:00 AM. However, the TeamViewer folder was missing from the cache folder altogether.

Both PCs were also analyzed for any abnormal processes. The Windows Prefetch folder [12] was extracted and viewed in WinPreftechView. Other than TeamViewer, no other processes stood out as relevant to this investigation.

Recovered Computers: Volume Shadow Copy Analysis

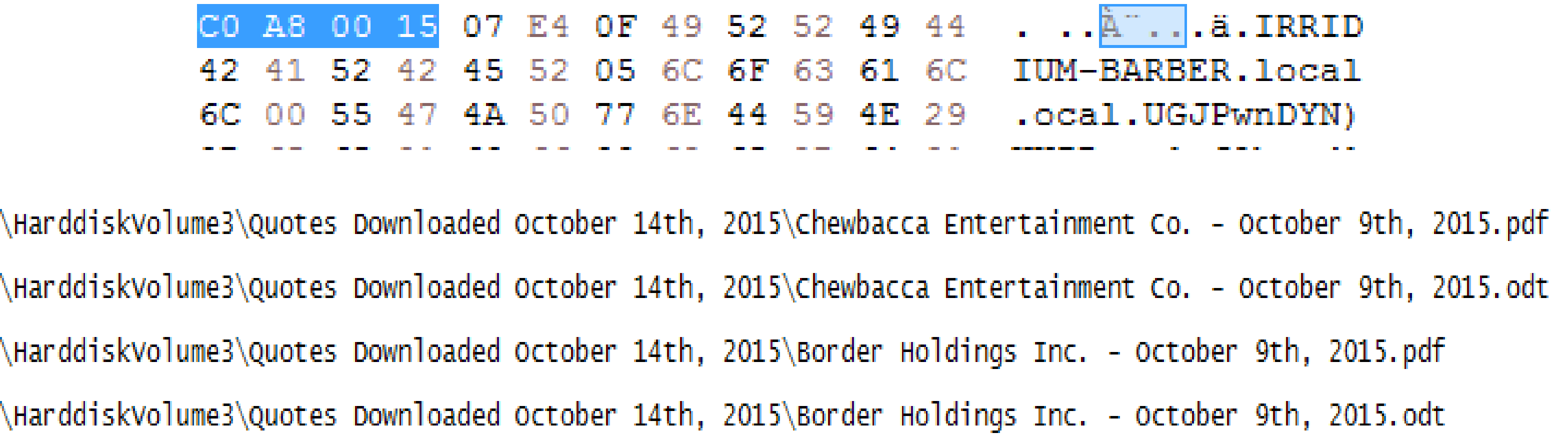
Noting from the previous analysis that a log folder was missing on BARBER-PC and also that certain files were once linked to on RICHMOND-PC, I analyzed both PCs for system backups using the Volume Shadow Toolset. After mounting each computer using Arsenal Image Mounter, four VSCs were recovered from each drive. On RICHMOND-PC’s backups dated October 8th and October 10th, I was specifically looking for recoverable evidence of the quotes referenced in the Jump List analysis, however, the paths were not available on either backup. On BARBER-PC backups dated October 8th, 9th and 10th were examined for potential missing log files. In all, evidence of four new TeamViewer sessions were recovered from these old log files (included in **Exhibit D**).

Recovered Computers: Web History Analysis

The web history for all installed browsers on both BARBER-PC and AVENAL-PC was extracted and viewed using Autopsy. The web history did not contain any artifacts or references to Team Viewer or any additional files accessed by RICHMOND-PC. The web history did not indicate any unlawful behavior or behavior which would violate the Iridium Electronics employee contract.

Recovered Computers: RAM Analysis

I conducted an analysis of the volatile memory captured the date of seizure using the tool volatility [2]. In addition to confirming the time zone and operating system information, I determined all running processes on both systems at the time of seizure, noting the process numbers for TeamViewer_Des.exe and TeamViewer_Ser.exe. I then dumped the memory of each process to a file and extracted any words or characters located in memory to another file using the "strings" tool from SysInternals [**Exhibit E**]. Using both a text editor and a hex editor, I searched for any results for "RICHMOND-PC," "BARBER-PC," "AVENAL," "BARBER," "jen.barber," "iridium-barber," and the IP address of each computer in hexadecimal. All search terms returned hits and revealed full paths to the files accessed in Exhibit A [Figure 5]. In processes recovered from RICHMOND-PC I found 13 and 15 references to BARBER-PC's IP address in each ("Des" and "Ser") respectively . In processes recovered from BARBER-PC I found 29 and 28 references to RICHMOND-PC's IP address in each ("Des" and "Ser") respectively.



```
C0 A8 00 15 07 E4 0F 49 52 52 49 44   . ..À¨...ä.IRRID
42 41 52 42 45 52 05 6C 6F 63 61 6C   IUM-BARBER.local
6C 00 55 47 4A 50 77 6E 44 59 4E 29   .ocal.UGJPwnDYN)
```

```
\HarddiskVolume3\Quotes Downloaded October 14th, 2015\Chewbacca Entertainment Co. - October 9th, 2015.pdf
\HarddiskVolume3\Quotes Downloaded October 14th, 2015\Chewbacca Entertainment Co. - October 9th, 2015.odt
\HarddiskVolume3\Quotes Downloaded October 14th, 2015\Border Holdings Inc. - October 9th, 2015.pdf
\HarddiskVolume3\Quotes Downloaded October 14th, 2015\Border Holdings Inc. - October 9th, 2015.odt
```

Figure 5. (top) artifacts of BARBER-PC's IP address (192.168.0.21) in TeamViewer process (bottom) artifacts of files accessed during the session

Conclusion

I conclude, based on the examination outlined in previous sections, that the suspect's Windows computer does contain evidence that the user of RICHMOND-PC had access to and attempted to transmit confidential documents belonging to Iridium Electronics. The user accomplished this through accessing a co-workers' PC, BARBER-PC, using Windows File Viewer and Team Viewer to remotely monitor and control it. This conclusion was met following the example of official forensic reports and recommended guidelines to preserve data accuracy and integrity. I certify all the contents of this report are true to the best of my knowledge.

Signature:

Date: 5/13/2019

Timeline

*Times are local times UTC +0100

October 8th, 2015

9:44:37 AM RICHMOND-PC accesses ("\\irridium-barber\c$\Users\jen.barber\Documents\")

10:55:34 AM BARBER-PC logs a TeamViewer session

RICHMOND-PC accesses the log file in the Program Files folder on BARBER-PC through file viewer ("\\irridium-barber\c$\Program Files (x86)\TeamViewer\")

11:34:05 AM BARBER-PC logs a TeamViewer session

1:48:25 PM RICHMOND-PC logs a TeamViewer session

1:58:57 PM RICHMOND-PC accesses the Quotes folder on BARBER-PC ("\\irridium-barber\Users\richmond.avenal\Documents\Quotes\")

1:59:17 PM RICHMOND-PC accesses the local Quotes folder in Avenal's Documents ("\Users\richmond.avenal\Documents\Quotes\")

2:01:23 PM RICHMOND-PC accesses storage "F:\Quotes", "F:\Quotes Downloaded October 8th, 2015"

October 9th, 2015

07:24:25 AM BARBER-PC logs a TeamViewer session

11:17:58 AM RICHMOND-PC logs a TeamViewer session

12:24:52 PM RICHMOND-PC logs a TeamViewer session

5:42 PM - 5:46 PM Barber and Avenal have a conversation regarding confidential information, Exhibit

6:23:37 PM Teamviewer session initiates on AVENAL-PC

October 10th, 2015

Several Teamviewer sessions logged on each PC, but no accessed files are logged by either system

October 14th, 2015

12:22:06 PM BARBER-PC logs a TeamViewer session

12:25:08 PM RICHMOND-PC logs a TeamViewer session

12:39:32 PM RICHMOND-PC accesses storage path "F:\Quotes Downloaded October 14th, 2015"

12:45:40 PM - Avenal's system is seized and imaged by Iridium IT security staff

Tools Used

AccessData® FTK® Imager v3.4.3.3 – imaging and verification tool for digital evidence, https://accessdata.com/product-download

Arsenal Image Mounter – tool for mounting forensic images, https://arsenalrecon.com/#products/

Autopsy v. 4.4.1 – File carving, data extraction, and case management tool, https://www.sleuthkit.org/autopsy/

Browsing History View v2.17 – tool for examining web history artifacts, http://www.nirsoft.net/utils/browsing_history_view.html

Diskpart v 6.2.9200 – Windows utility for managing disks and drives, https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/diskpart

Jump Lists View v1.16 – View jump list information stored by Windows, http://www.nirsoft.net/utils/jump_lists_view.html

Link Parser v1.3 – tool for extracting information from .lnk files, https://4discovery.com/link-parser/

Microsoft Azure Protection Viewer v. 2.0.779,1.48.204 – tol for viewing “PFILE” type protected documents, https://www.microsoft.com/en-us/download/details.aspx?id=54536

Mozilla Thunderbird v 60.6.1 – email client tool, https://www.thunderbird.net/en-US/

OpenSSL v 1.1.0g – all purpose encryption and hashing tool https://www.openssl.org/

Regripper v 2.8 – tool for reading registry information on offline systems, https://github.com/keydet89/RegRipper2.8

Shellbags View v 1.21 – tool for viewing shellbag keys and artifacts http://nirsoft.net/utils/shell_bags_view.html

Strings v2.53 – tool for parsing ascii strings in binary files, https://docs.microsoft.com/en-us/sysinternals/downloads/strings

VSCToolset v6.0.1 – tool for exploring volume shadow copies, https://df-stream.com/vsc-toolset/

Win-Prefetch-View v 1.35 – tool for viewing contents and details of a Windows Prefetch folder https://www.nirsoft.net/utils/win_prefetch_view.html

Windows Snipping Tool – for screenshots, https://support.microsoft.com/en-us/help/13776/windows-use-snipping-tool-to-capture-screenshots

WinRAR Archiving Tool v5.60 – for extracting and managing archives https://www.rarlab.com/

Glossary

Acquisition: the process of discovering and forensically copying a file

Encase File Format (E01): a disk image file format specifically designed to store data securely with a built in mechanism to check for data tampering (see [7] and “Hashing” for more details)

File system: the basic software for controlling how data is restored and retrieved on a computer. Examples include FAT file systems (often on USB drives), NTFS (Windows drives), and EXT (Linux drives)

File Allocation Table: a file system structure which utilizes an indexed table for identifying and retrieving files. Prominently the default file system on USB drives and older computer hardware

Footer: a string of characters which indicates the end of a file when viewed in raw format

Forensic Container: a family of file formats (.AD1 and .L01 for example), which are used to store and verify copies of disk images. They are analogous to a physical evidence locker

Hash: the result of a one-way cryptographic function (known as a hash function), which generates a fixed message unique to the input it was fed (a word, a file, etc). Colloquially, it is often referred to as a “digital fingerprint,” as fingerprints identify people, the hash value can identify a file. The hash is most often used to prove a file has not been changed.

Header: a string of characters which indicates the beginning of a file when viewed in raw format

Hexadecimal Number: a number composed using powers of 16 rather than the traditional 10. For example 16 is 10 in hexadecimal since it has 1 sixteen and 0 ones (as opposed to 1 ten and 6 ones)

Hex Editor: a software tool which allows the user to edit bytes of information. This is different from a text editor which allows a user to manipulate characters and strings

Image: in computing, a type of file which stores the raw contents of a hard disk or other storage device. The process of imaging refers to creating an exact copy of the raw contents on a disk

Jump List: shortcut files which are created for the Windows start menu to allow a user easy access to their most recent documents

Link Files: files that link to a particular directory or file. colloquially a “Shortcut”

Metadata: literally “data about the data.” Data which describes a particular digital file. For example, the creation date, file size, and user created information can all be found in metadata

Prefetch: files which are created by Windows when an application is run for the first time.

Shellbags: Key files which contain details about files accessed in Windows File Explorer including size, location, and access times

Windows Registry: a Windows archive which stores all configuration settings for the operating system including settings related to hardware, software, system security, and more. For a detailed look into the Registry see [G5]

Volatile Memory: also called ‘RAM’ or process memory, this is memory which is not typically stored when the computer shuts down, only while a process is still running

Volume Shadow Copy: also known as “system restore point” these are backups stored by Windows so a user can restore their system to an earlier date in the event of failure or data loss.

References

Data Acquisition References:

1. Forensicsware. (n.d.). E01 (Encase Image File Format). Retrieved March 4, 2019, from http://www.forensicsware.com/blog/e01-file-format.html

2. Wade, M. (2016, June 14). Memory Forensics: Where to Start. Retrieved May 12, 2019, from https://www.forensicmag.com/article/2011/06/memory-forensics-where-start

3. Mare, A. L. (2014, April 14). Windows Forensics and Security. Retrieved March 4, 2019, from https://articles.forensicfocus.com/2014/04/14/windows-forensics-and-security/

4. J. McQuaid. (2014, August 6). Forensic Analysis of LNK files. Retrieved March 4, 2019, from https://www.magnetforensics.com/computer-forensics/forensic-analysis-of-lnk-files/

5. How to enable and disable write-protection on a USB flash drive. (2018, May 21). Retrieved March 4, 2019, from https://www.computerhope.com/issues/ch001617.htm

6. Nelson, B., & Phillips, A. (2016). *Guide to computer forensics and investigations: Processing digital evidence*. Chapter 5: Understanding the Windows Registry Australia: Cengage Learning.

7. Acquire Forensics, Simon (2015, October 17). Google Chrome Browser Forensics – Analyze Chrome Data. Retrieved March 24, 2019, from https://www.acquireforensics.com/blog/google-chrome-browser-forensics.html

8. DataForensics, John Doe (2017, October 24). Microsoft Edge Forensics – Carve Artifacts Related to Edge Browser. Retrieved March 24, 2019, from https://www.dataforensics.org/microsoft-edge-browser-forensics/

9. Forensic Analysis of Windows Shellbags. (2016, February 19). Retrieved March 4, 2019,from https://www.magnetforensics.com/computer-forensics/forensic-analysis-of-windows-shellbags/

10. TeamViewer Staff, J. (2019, February 14). Security related logs and monitoring. Retrieved May 12, 2019, from https://community.teamviewer.com/t5/TeamViewer-General/security-related-logs-and-monitoring/td-p/5523

11. TeamViewer Staff, J. (2019, March 07). How to find your log files on Windows and Mac and Linux. Retrieved May 12, 2019, from https://community.teamviewer.com/t5/Knowledge-Base/How-to-find-your-log-files-on-Windows-and-Mac-and-Linux/ta-p/4694

12. Forensic Analysis of Prefetch files in Windows. (2016, February 19). Retrieved from https://www.magnetforensics.com/computer-forensics/forensic-analysis-of-prefetch-files-in-windows/

Reporting and Glossary References:

G1. Ashcroft, J., Daniels, D. J., & Hart, S. V. (n.d.). Forensic Examination of Digital Evidence: A Guide for Law Enforcement. *U.S.Department of Justice Office of Justice Programs*. Retrieved February 24, 2019, from https://www.ncjrs.gov/pdffiles1/nij/199408.pdf.

G2. Nelson, B., & Phillips, A. (2016). *Guide to computer forensics and investigations: Processing digital evidence*. Glossary. Australia: Cengage Learning.

G3. Hash function. (2019, February 21). Retrieved from https://en.wikipedia.org/wiki/Hash_function

G4. Forensic Focus. (n.d.). Retrieved from http://www.forensicfocus.com/computer-forensics-reports

G5. Nelson, B., & Phillips, A. (2016). *Guide to computer forensics and investigations: Processing digital evidence*. Chapter 5: Understanding the Windows Registry Australia: Cengage Learning.