NAME: \_\_\_Coleton Sanheim\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



Lab 8:   
Forensic Analysis – File Analysis

ITSC 306: Computer Forensics

Table of Contents

[Lab Outcome 2](#_Toc494961317)

[Readings 2](#_Toc494961318)

[Introduction 2](#_Toc494961319)

[1.0 Downloading Forensic Tools 3](#_Toc494961320)

[2.0 Registry Analysis 3](#_Toc494961321)

[3.0 Metadata Analysis 7](#_Toc494961322)

[4.0 Log Analysis 10](#_Toc494961323)

[5.0 Shellbags Analysis 14](#_Toc494961324)

[6.0 Keyword Search 15](#_Toc494961325)

[7.0 Timeline Analysis 17](#_Toc494961326)

[References 23](#_Toc494961327)

ITSC 306: Computer Forensics

Lab 6: Forensic Analysis – File Analysis

Lab Outcome

* Create a VMWare image that can be used for the forensic analysis of digital evidence.

Readings

* Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry
  + Chapter 1: Registry Analysis
* EnCase Computer Forensics: The Official EnCase Certified Examiner – Study Guide
  + Chapter 8: File Signature Analysis and Hash Analysis
  + Chapter 9: Windows Operating System Artifacts

Introduction

Once you have collected all of the evidence to be examined and copied it so that you are only working on a copy of the evidence, you can examine the evidence and see what it tells you about the incident.

There are many full forensic suites available, such as EnCase, Forensic Toolkit (FTK), Forensic Explorer and Autopsy. There are also many specialized tools, such as:

* Registry RegRipper
* File Metadata ExifTool
* Log Analysis Highlighter
* Memory Analysis Volatility
* Keyword Search Bstrings
* Imaging FTK Imager

In this unit, you will look at some of these specialized tools.

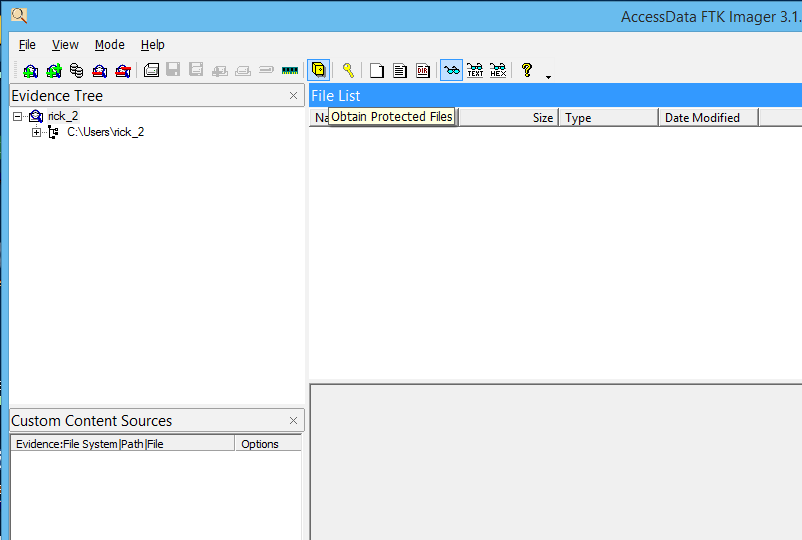
1. Downloading Forensic Tools
2. Create two folders on your desktop called **Tools** and **Week 9 Evidence Files**.
3. Download the following tools and install them in the Tools folder. If you have already downloaded the following tools, move the tools into the Tools folder.

* [FTK Imager Lite](http://accessdata.com/product-download/ftk-imager-lite-version-3.1.1) (http://accessdata.com/product-download/digital-forensics/ftk-imager-lite-version-3.1.1)
* [ExifTool](https://sno.phy.queensu.ca/~phil/exiftool/) (http://www.sno.phy.queensu.ca/~phil/exiftool/)
* [Highlighter](https://www.fireeye.com/services/freeware/highlighter.html) (https://www.fireeye.com/services/freeware/highlighter.html)

Note: Uses an installer and puts a menu option on the Start menu.

* [ShellBags Explorer](https://ericzimmerman.github.io/) (https://ericzimmerman.github.io/)
* [bstrings](https://ericzimmerman.github.io/) (https://ericzimmerman.github.io/)
* [Timeline Explorer](https://ericzimmerman.github.io/) (https://ericzimmerman.github.io/)
* [RegRipper](https://github.com/keydet89/RegRipper2.8) (https://github.com/keydet89/RegRipper2.8)

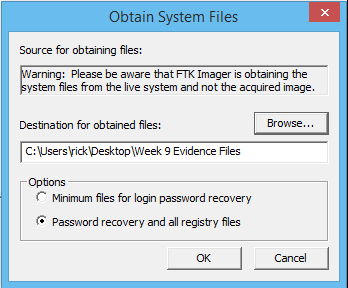
1. Registry Analysis
2. Open FTK Imager Lite and select **Obtain Protected Files**.



**Figure 1:**

Source: FTK Imager. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

1. Select **Password recovery and all registry files**.
2. The *Obtain System Files* window opens.
3. In the *Destination* box, select the path to your **Week 9 Evidence Files** folder, and then click **OK**.

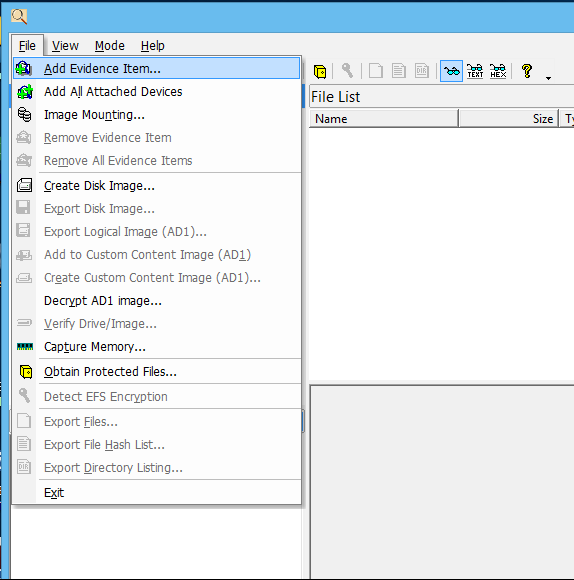


**Figure 2:**

Source: FTK Imager. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

Now you are going to copy an NTUSER.DAT file other than your own, since it is locked by the system.

1. Select **File > Add Evidence Item**.



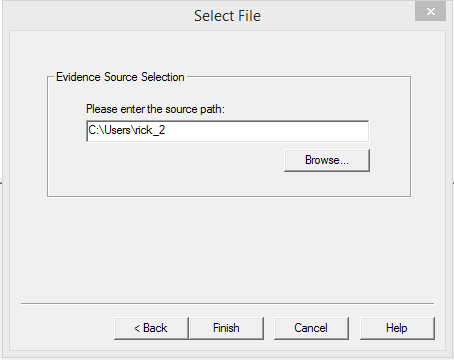
**Figure 3:**

Source: FTK Imager. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

1. Select **Contents of a Folder**, and then click **Next**.

The *Select File* window appears.

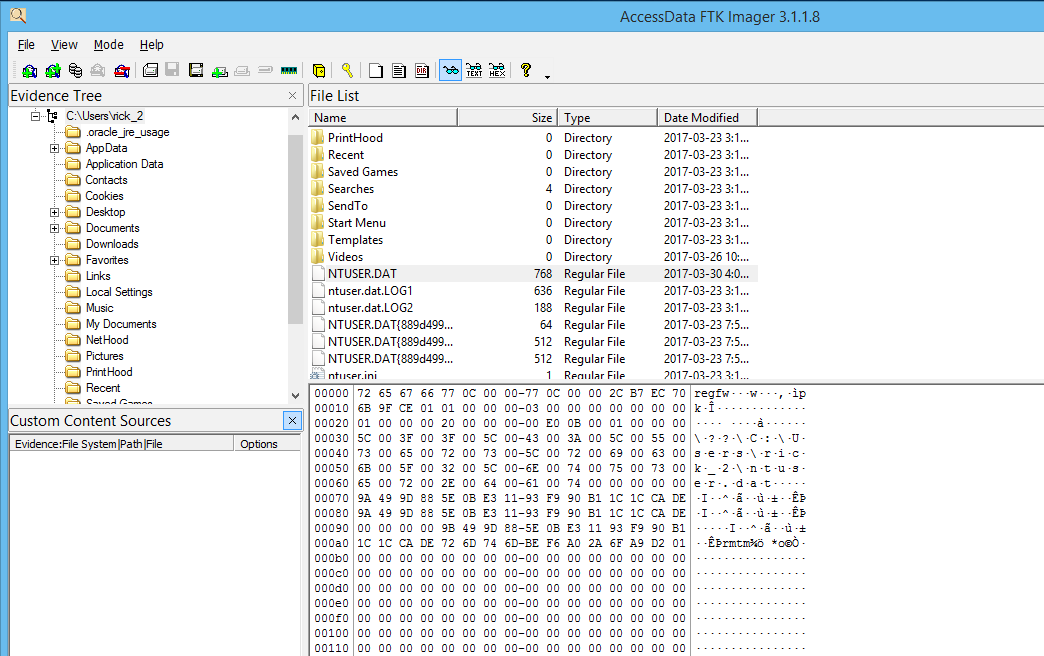
1. Browse to a user profile other than your own, select it and then click **Finish**.



**Figure 4:**

Source: FTK Imager. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

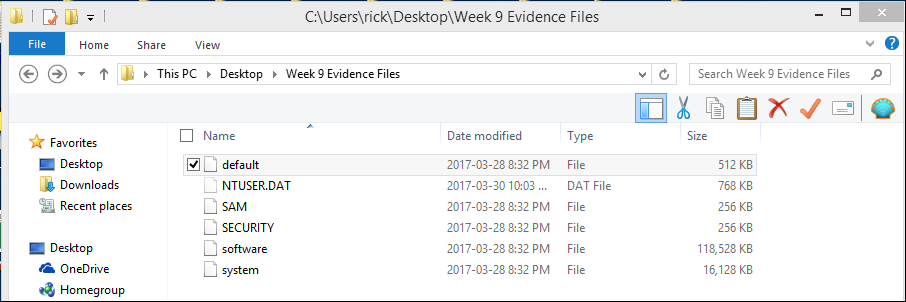
1. Click the root of the user profile in the *Evidence Tree* pane.
2. Select the **NTUSER.DAT** file, then right-click the file and select **Export Files**.
3. Select the destination folder **Week 9 Evidence Files**.



**Figure 5:**

Source: FTK Imager. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

The Week 9 Evidence Files folder should look like Figure 6:

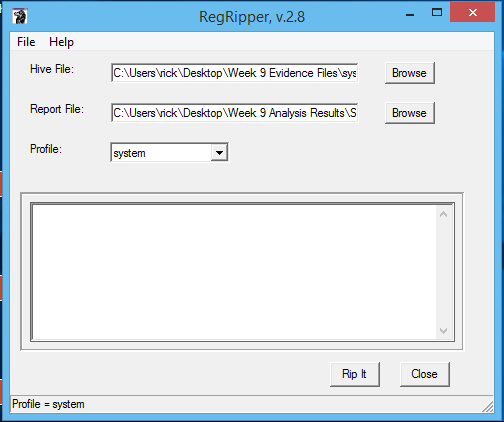


**Figure 6:**

Used with permission from Microsoft.

1. Now that you have evidence to examine, double-click the **Tools** folder and navigate to the RegRipper files.
2. Double-click **rr.exe**.

The following box appears (Figure 7):



**Figure 7:**

Source: RegRipper. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

1. Populate the Hive File, Report File and Profile boxes as shown in Figure 7.

**Note:** The Hive File system is in the Week 9 Evidence File folder and the Report File is in the Week 9 Analysis Results folder.

1. Name the file **system registry.txt** and select **system** as the profile.
2. Once all entries are populated, click **Rip It**.

When completed, a window appears showing how many (if any) plugins completed with errors.

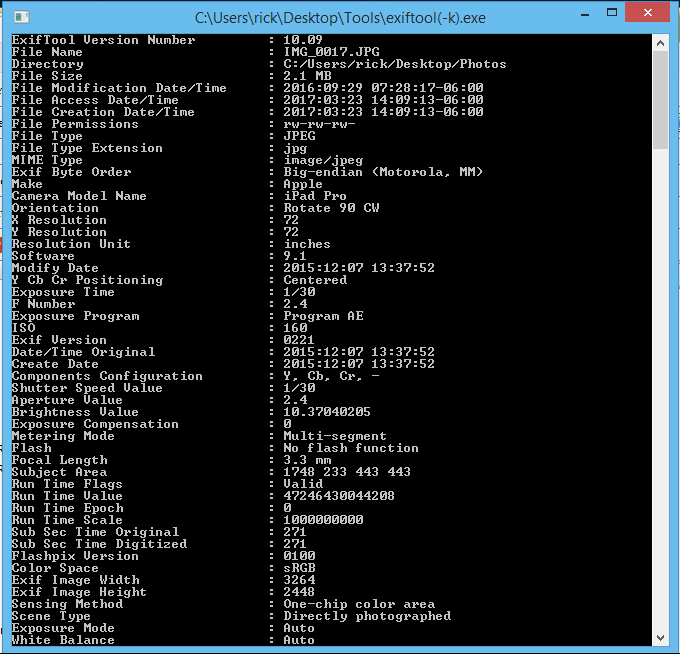
**Note:** A log file with the same name (in this case, **system registry.log**) will appear in the same folder as the report file.

1. Do this for each of the registry files in the Week 9 Evidence Files folder, and then review the results of each registry file to see the type of information that this program can capture.
2. Metadata Analysis

In this section, you will examine metadata from both a document and a picture file.

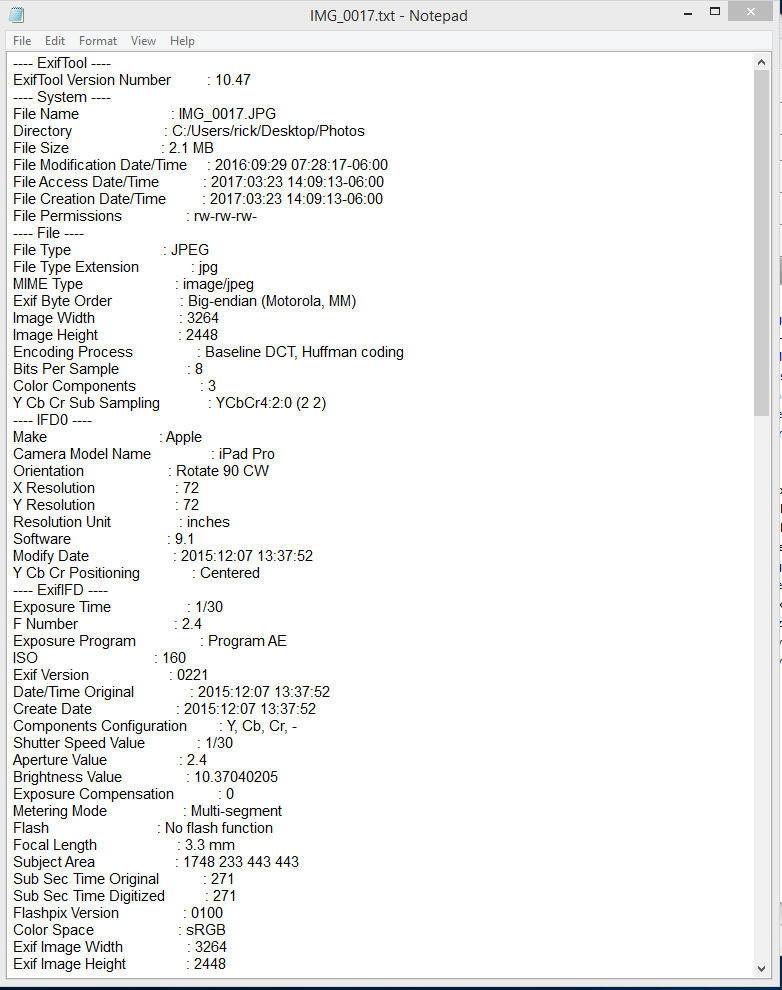
1. Copy the file called **exiftool(-k).exe** (located in the exiftool.zip file) into your Tools folder and rename it **exiftool(-k -a -u -g1 -w txt).exe**.

**Note:** If you dragged and dropped a file onto the file with the original name, you would see a command shell with the results of the analysis. When you drag and drop a file onto the renamed file (Figure 8), the results are saved to a text file with the same filename as the evidence file and in the same location as the evidence file (Figure 9).



**Figure 8:**

Used with permission from Microsoft.



**Figure 9:**

Used with permission from Microsoft.

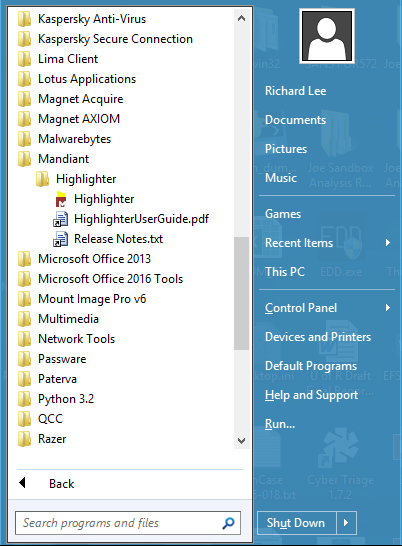
1. Experiment by dragging and dropping various file types on to either exiftool(-k).exe or exiftool(-k -a -u -g1 -w txt).exe and review the results to see the types of information that can be recovered.
2. Log Analysis

This section begins with the analysis of a text-based log file, in this case the eventlog that you converted to a text file with your Live Response Kit in Week 3. The program you will use is called Highlighter.

Read the [Product Review – Mandiant Highlighter](http://brakertech.com/mandiant-highlighter-log-and-text-file-viewer-review/) (http://brakertech.com/mandiant-highlighter-log-and-text-file-viewer-review/)

1. Run Highlighter by navigating to your Windows Start Program list and selecting **Mandiant > Highlighter > Highlighter**.

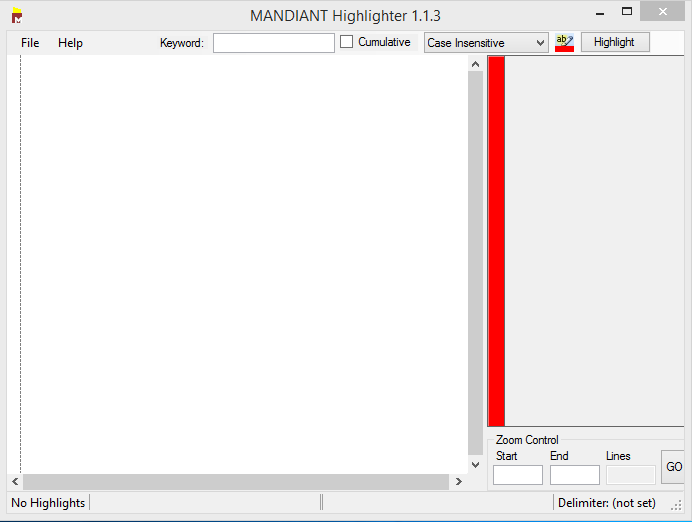
This is the default installation location.



**Figure 10:**

Used with permission from Microsoft.

The following screen appears (Figure 11):



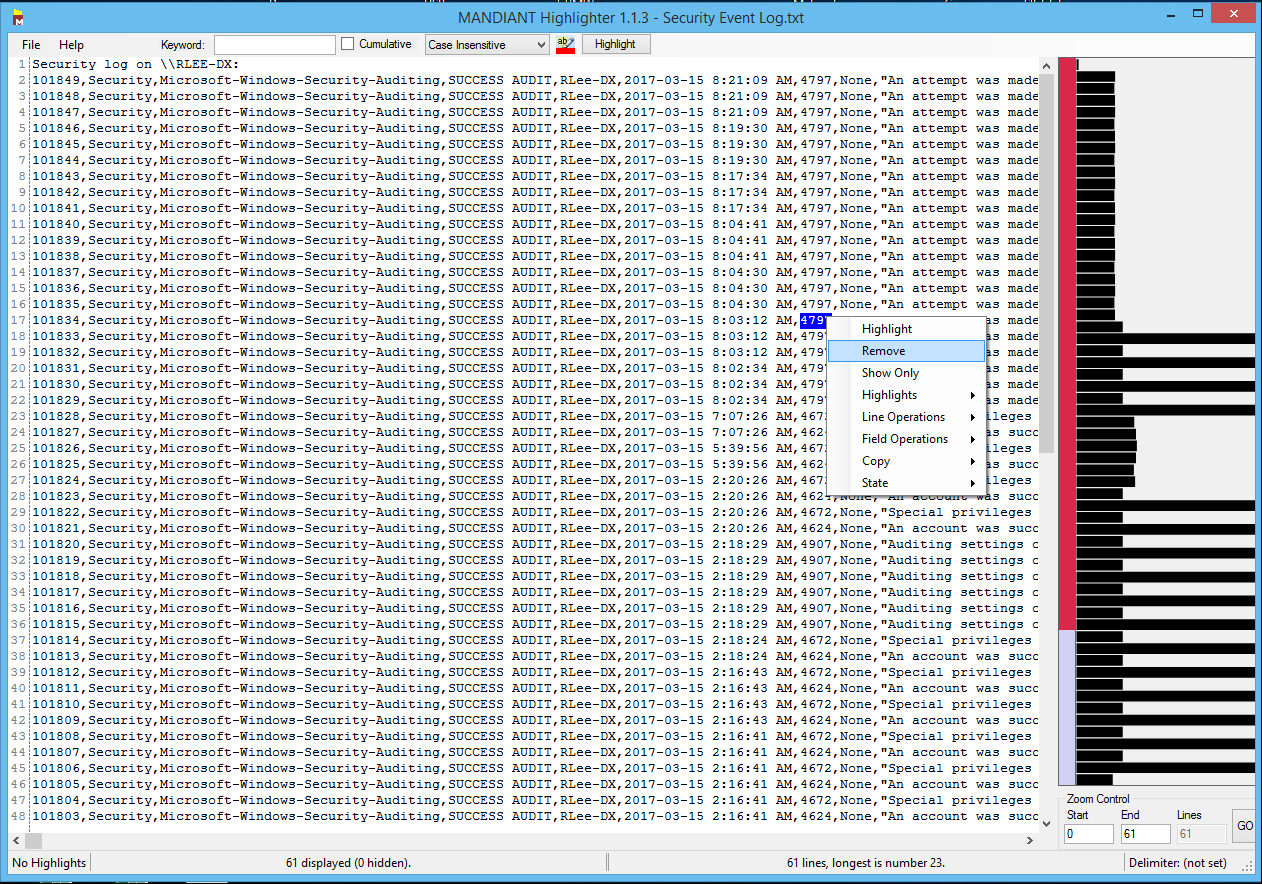
**Figure 11:**

Source: MANDIANT Highlighter. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

1. Create a new text document by right-clicking the desktop and selecting **New > Text document**. Rename the file **Security Eventlog.txt**.
2. Find and open the text file you created by running your Live Response Kit (LRK) in Week 3.
3. Find in the document **psloglist -s -x security** and highlight either the entire log portion or a part of the log, and then paste that text into the new document you have created.
4. In Mandiant Highlighter, click **File > Open > File** and select your new document.

Each entry takes one line and there is a graphical representation on the right-hand side of the window.

1. You can easily remove lines that you know are not pertinent to your investigation. For example, highlight eventid **4797**, right-click it and select **Remove** (Figure 12).



**Figure 12:**

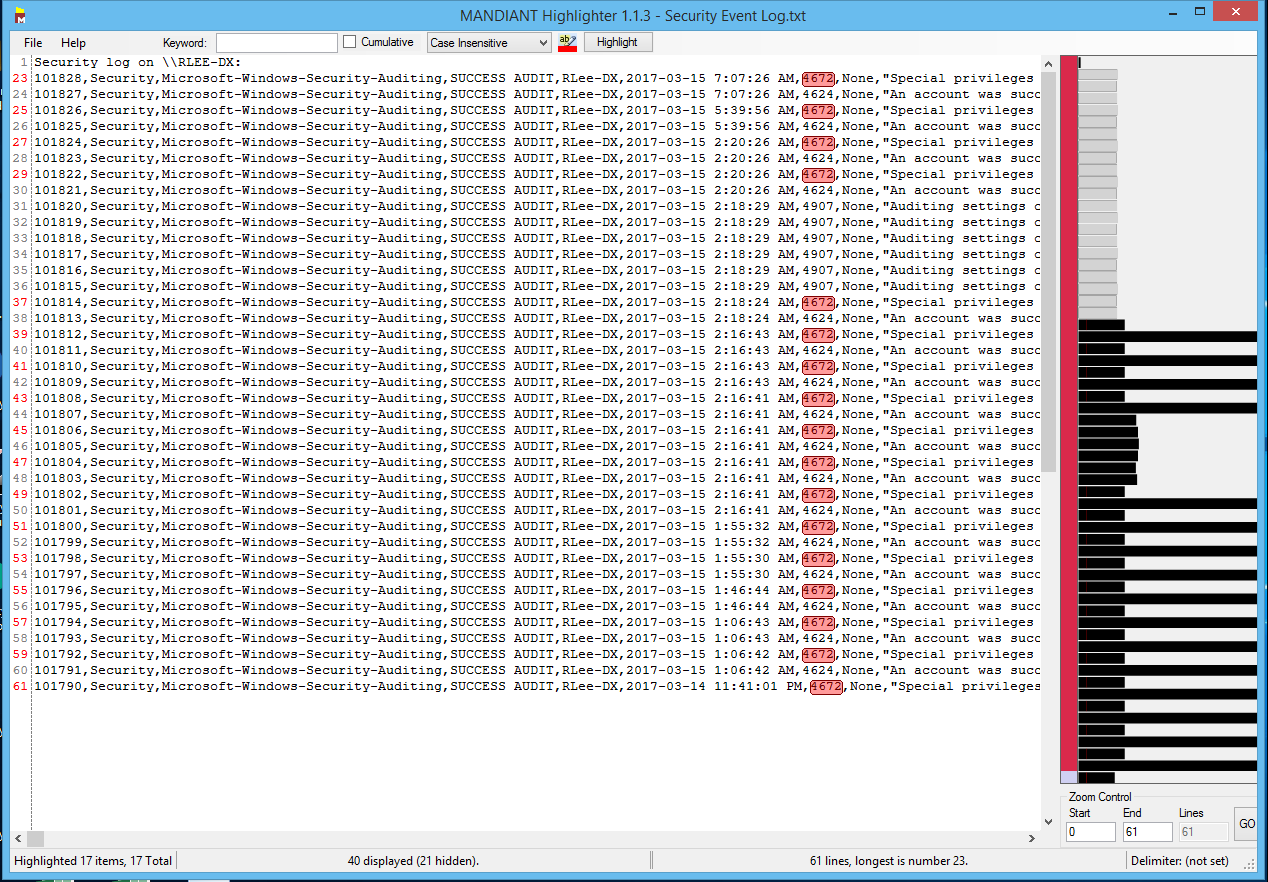
Source: MANDIANT Highlighter. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

1. Replace the lines by right-clicking in the text window and selecting **Reclaim Lines Previously Removed**.

**Notes:**

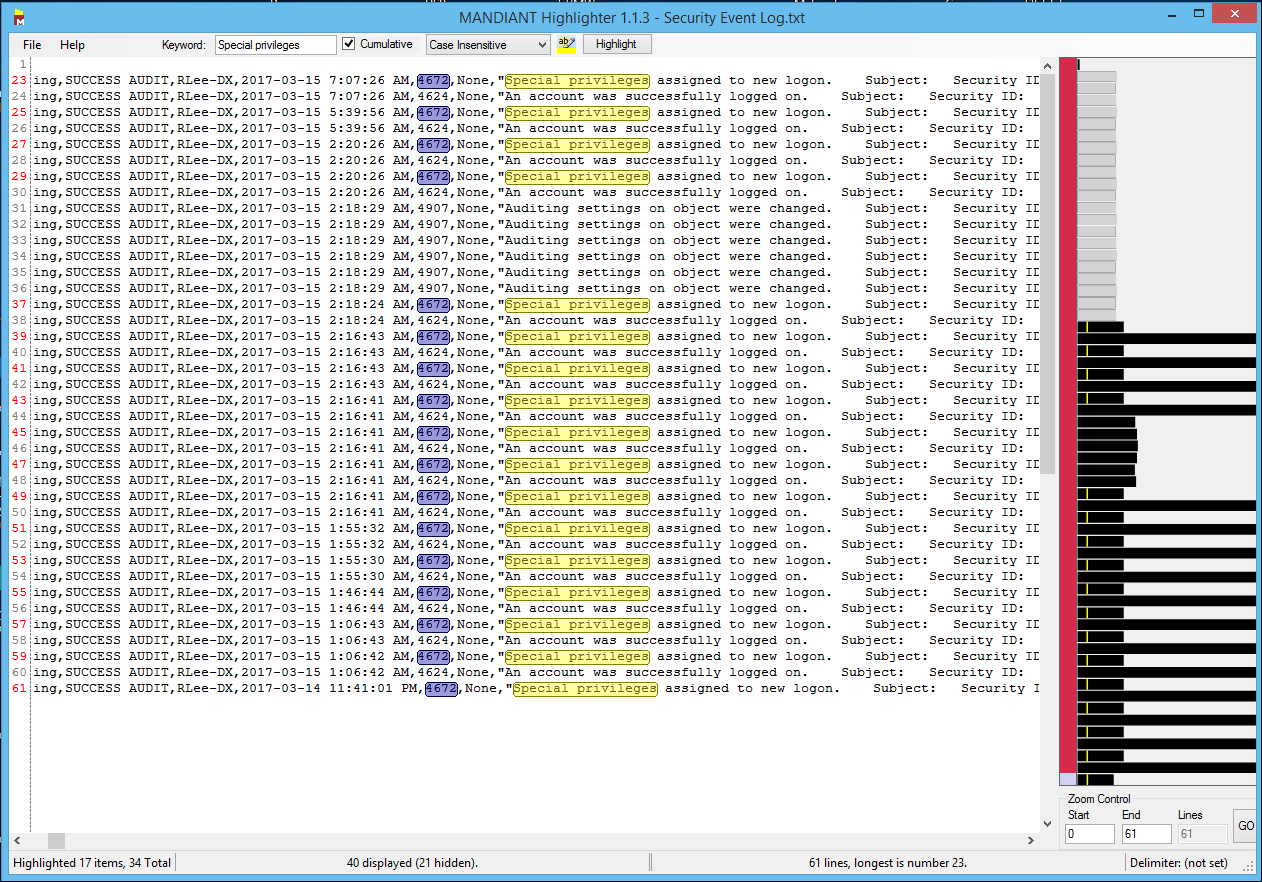
* It is useful to have a good knowledge of Windows eventids or have access to a list of common eventids used during investigations.
* You can also search using IP addresses, dates and eventids, and then right-click and select **Highlight**.
* You can also conduct keyword searches using the bar on the top of the screen, which will highlight the text with the colour you choose (Figure 13). You can then perform another keyword search and select the **Cumulative** box to choose another colour, and both results will be displayed (Figure 14). This is an easier way to review information than reading a very large text file in Wordpad.

1. Experiment with using Highlighter with the other log files from your LRK.



**Figure 13:**

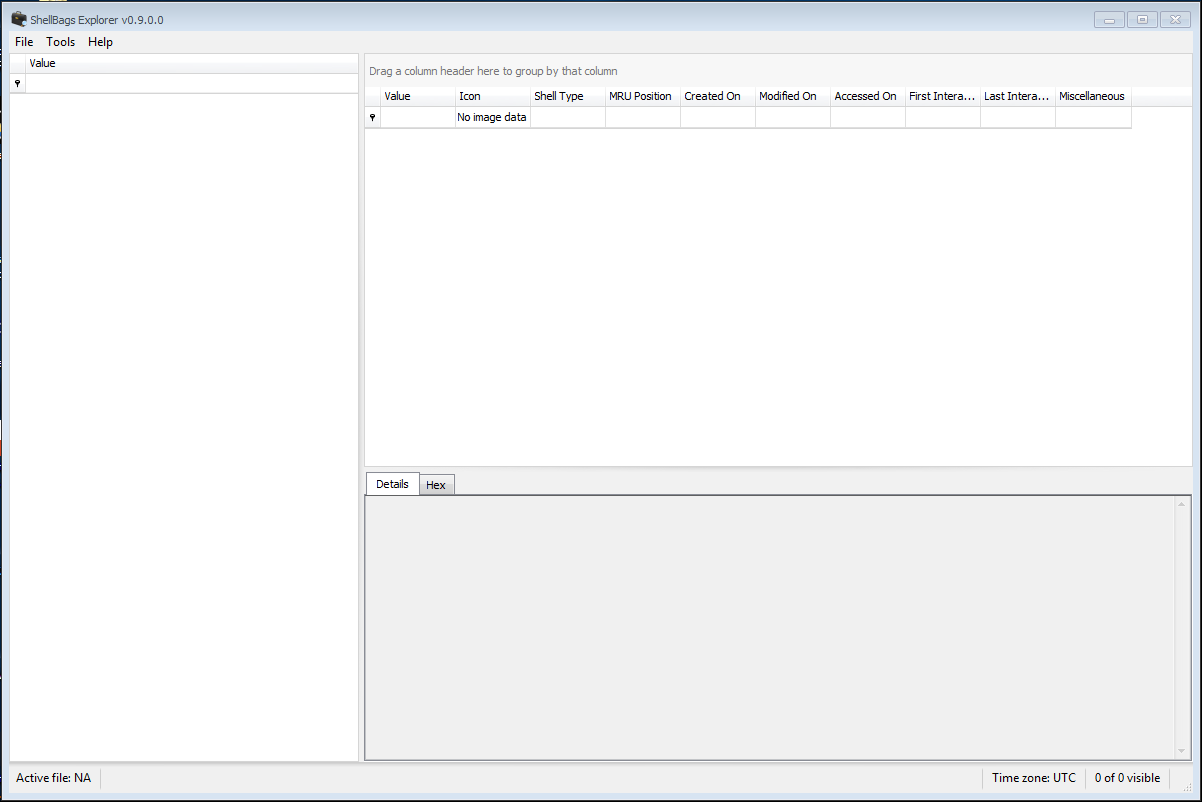
Source: MANDIANT Highlighter. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.



**Figure 14:**

Source: MANDIANT Highlighter. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

1. Shellbags Analysis
2. Open **ShellBagsExplorer.exe**.



**Figure 15:**

Source: Shellbags Explorer. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

1. Click **File > Load Active Registry**.

Once the parsing is complete, a window appears displaying the results of the parse.

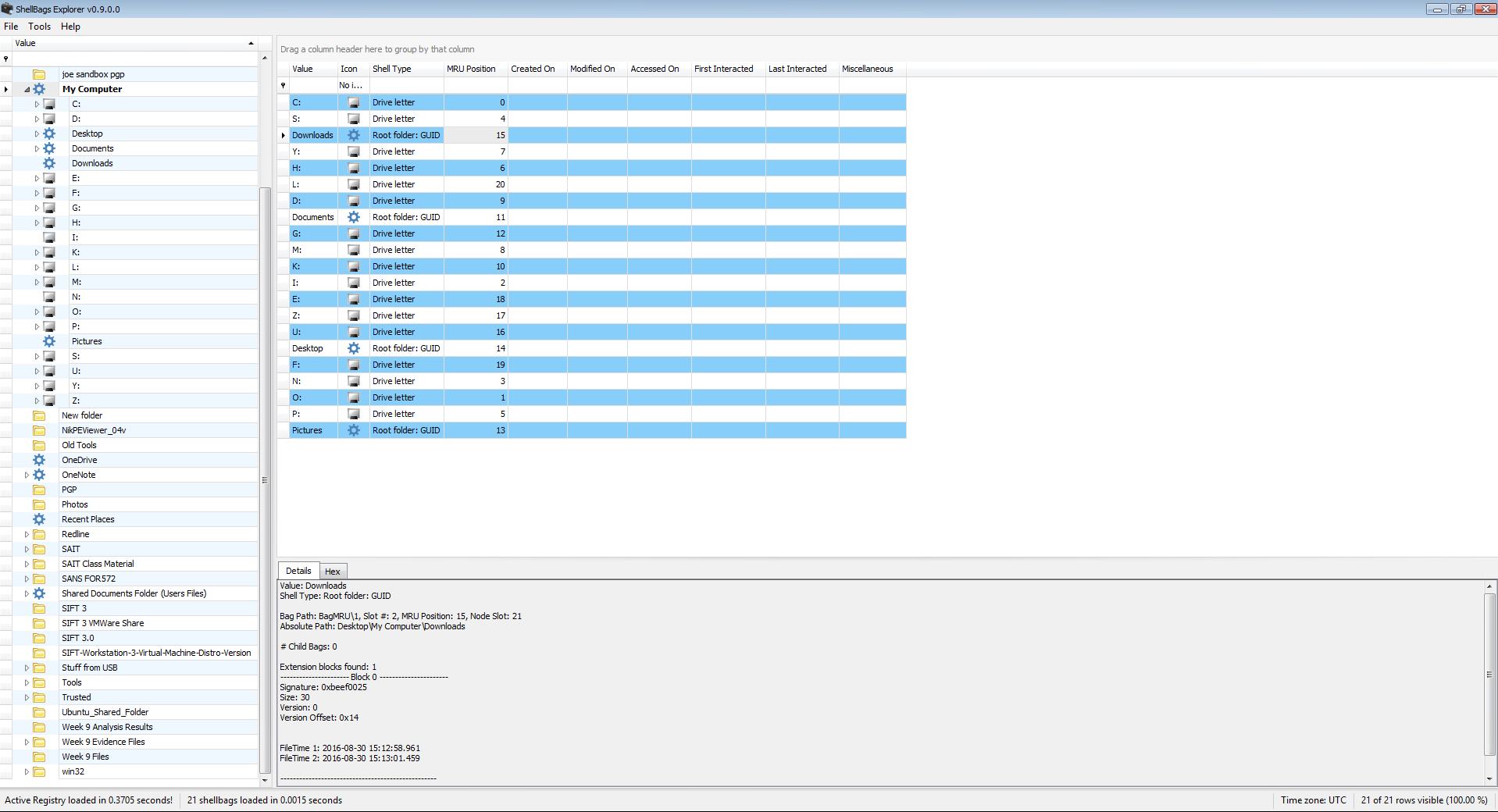
Machine generated alternative text:
Parsing complete 
Parse time: O. 37 seconds 
She118ags found: 923 
Shellaags processed: 923 (100.00 %) 
Totals by bag type 
Variable: Users property view: 12 
GLIID: Control panel: 14 
Control Panel Category: 6 
Root folder: GUID: 10 
Directory: 848 
File: 4 
Drive letter: 17 
CDSurn: 4 
Zip fie contents: I 
Variable: HTTP URI: 6 
Variable: I 

**Figure 16:**

Source: Shellbags Explorer. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

1. Click **OK**.

The data appears in the main Shellbags window.



**Figure 17:**

Source: Shellbags Explorer. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

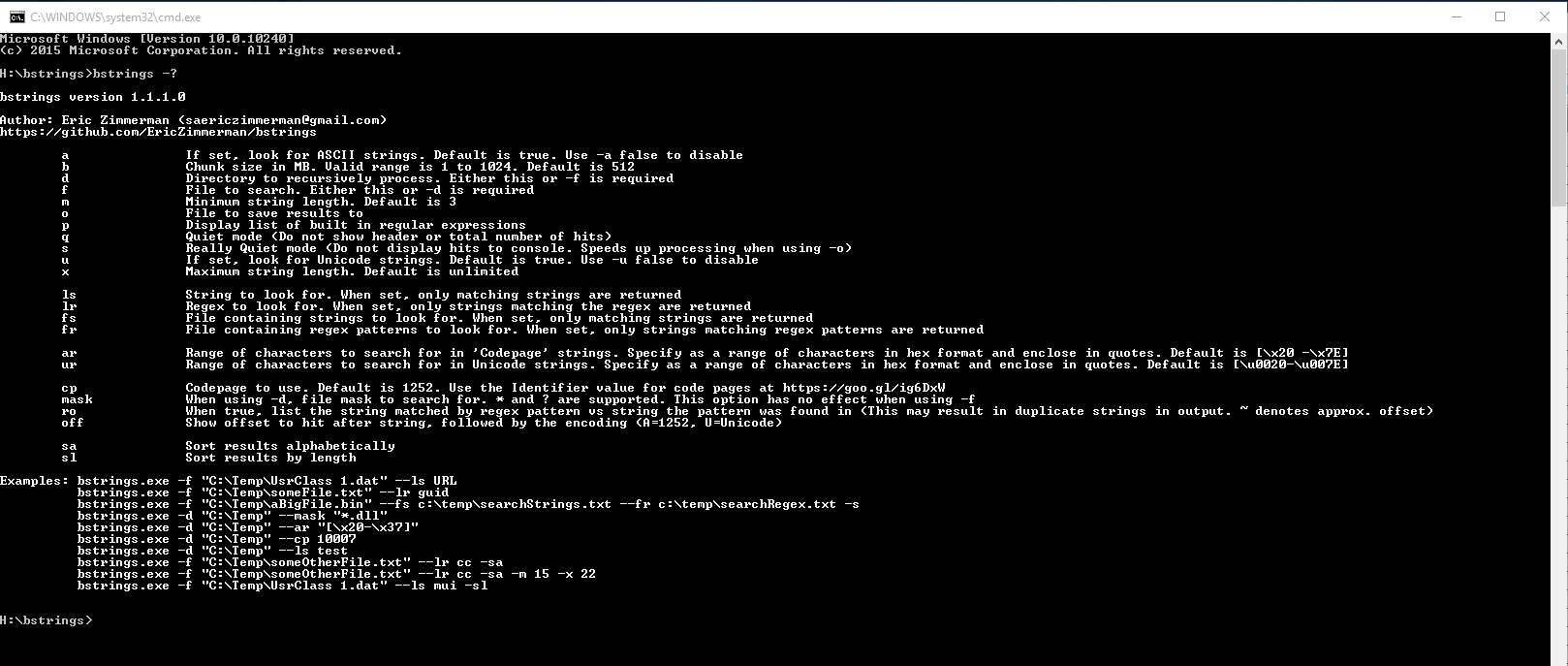
1. Keyword Search

More information is available at:

* https://binaryforay.blogspot.ca/2016/04/bstrings-v11-released.html
* https://binaryforay.blogspot.ca/2016/02/bstrings-10-released.html

1. Open a command prompt as an administrator.
2. In your command shell, change directories to your Tools folder on your desktop.
3. Run the command bstrings.exe -?

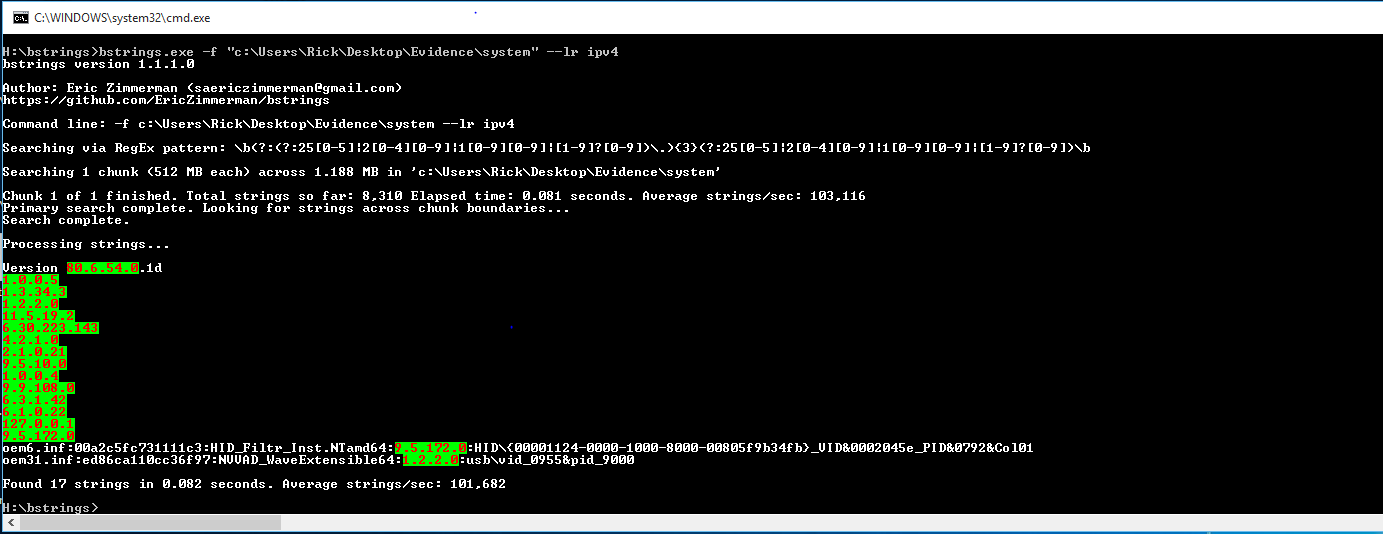
The help screen appears showing the different switches you can use, what they do, some example command lines and what the results should be.



**Figure 18:**

Used with permission from Microsoft.

1. Run the command bstrings.exe -f C:\ path to your (Week 9 Evidence Files)\system –lr ipv4. This searches the system file for any Version 4 IP addresses and highlights them.



**Figure 19:**

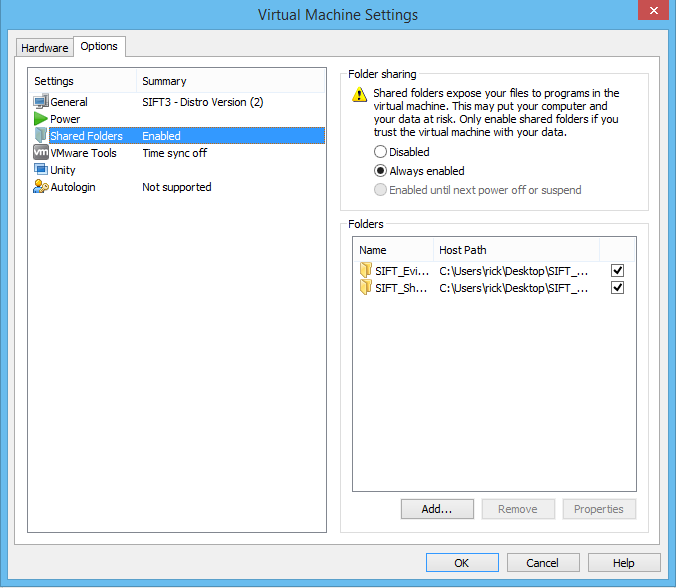
Used with permission from Microsoft.

1. Timeline Analysis

In this section you will use your SIFT VMWare Forensic Workstation for the analysis. You may want to review the YouTube video [SANS DFIR Webcast -- DFIR using SIFT Workstation](https://www.youtube.com/watch?v=w1ygCP2TeCY) (https://www.youtube.com/watch?v=w1ygCP2TeCY).

1. Create two shared folders (both always enabled):

* SIFT\_Shared (Read, Write)
* SIFT\_Evidence (Read Only)



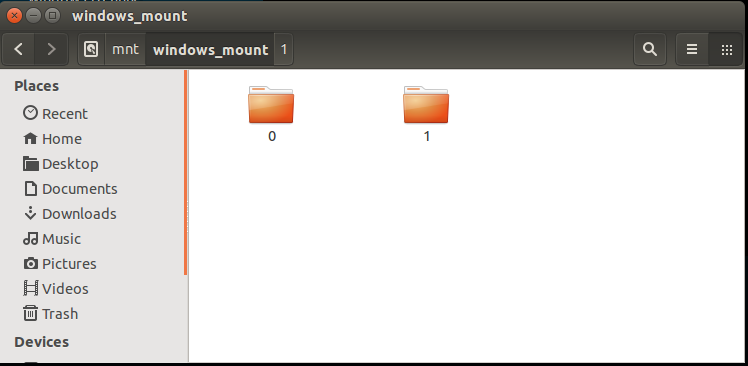
**Figure 20:**

Source: SANS Institute. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

1. Mount your image **cfreds2015\_data\_leakage\_pc.dd** from the terminal to the **windows\_mount** mount point with the following command:

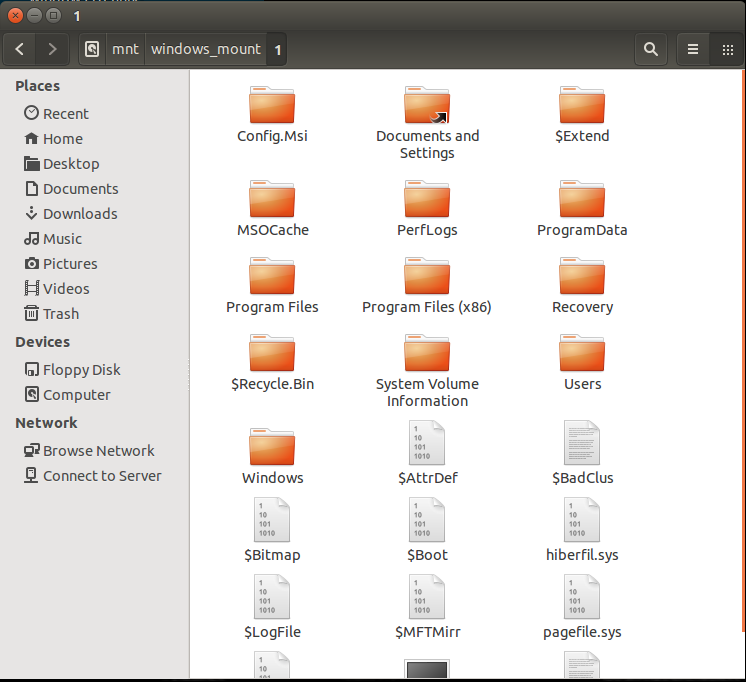
sudo imageMounter.py /mnt/hgfs/SIFT\_Evidence/cfreds\_2015\_data\_leakage\_pc.dd /mnt/windows\_mount/

Two folders named **0** and **1** appear in the **windows\_mount** folder (Figure 21). The 0 folder is a non-bootable partition and folder 1 is the C/: drive from the image (Figure 22).



**Figure 21:**

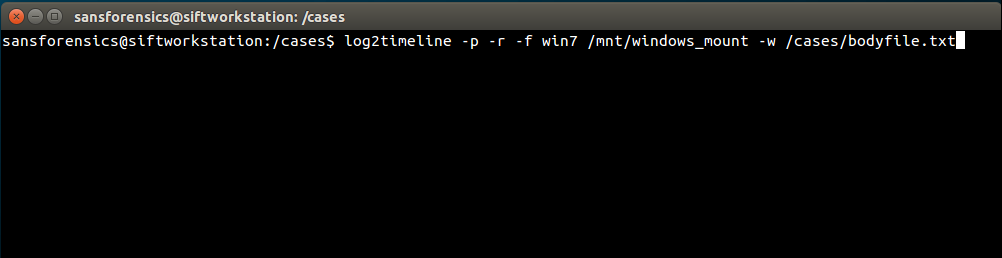
Source: SANS Institute. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.



**Figure 22:**

Source: SANS Institute. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

1. Run the installed tools to examine either the image file or the individual files in the windows\_mount folder.

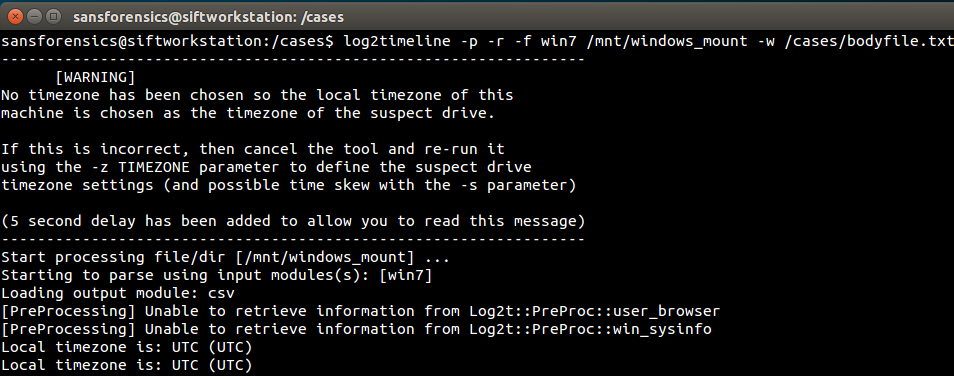


**Figure 23:**

Source: SANS Institute. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

1. The command log2timeline -p -r -f win7 /mnt/windows\_mount -w /cases/bodyfile.txt creates **bodyfile.txt** in the Cases folder on the desktop.

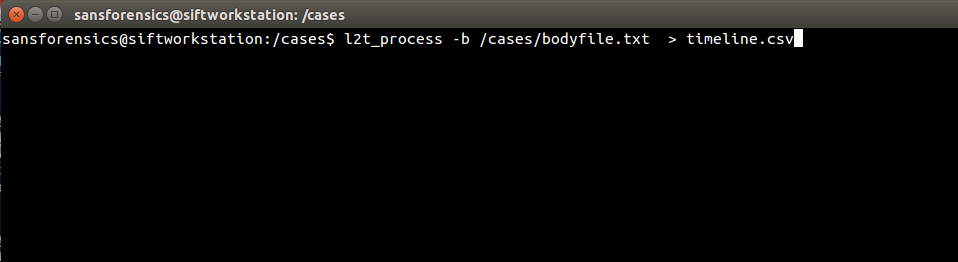
**Note:** If no timezone is selected, the timezone of the analysis system is used.



**Figure 24:**

Source: SANS Institute. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

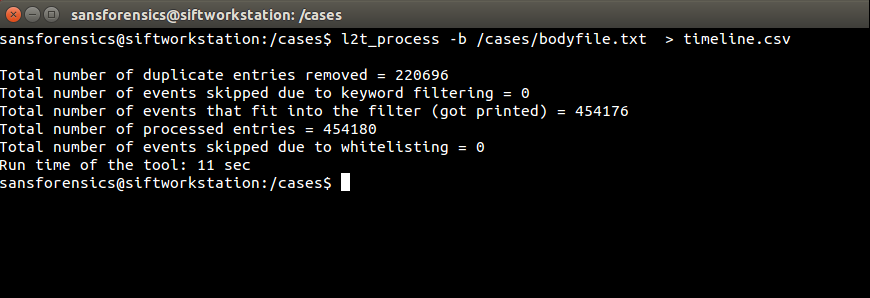
1. Once the **bodyfile.txt** file has been created, convert it into a comma separated file so that you can open it in a spreadsheet program such as Excel. Use the command l2t\_process -b /cases/bodyfile.txt > timeline.csv.



**Figure 25:**

Source: SANS Institute. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

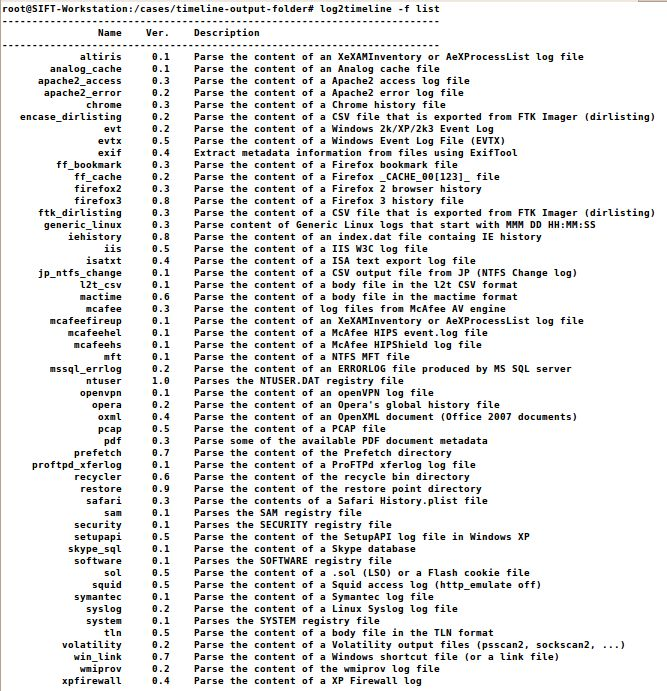
The following screen appears (Figure 26):



**Figure 26:**

Source: SANS Institute. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

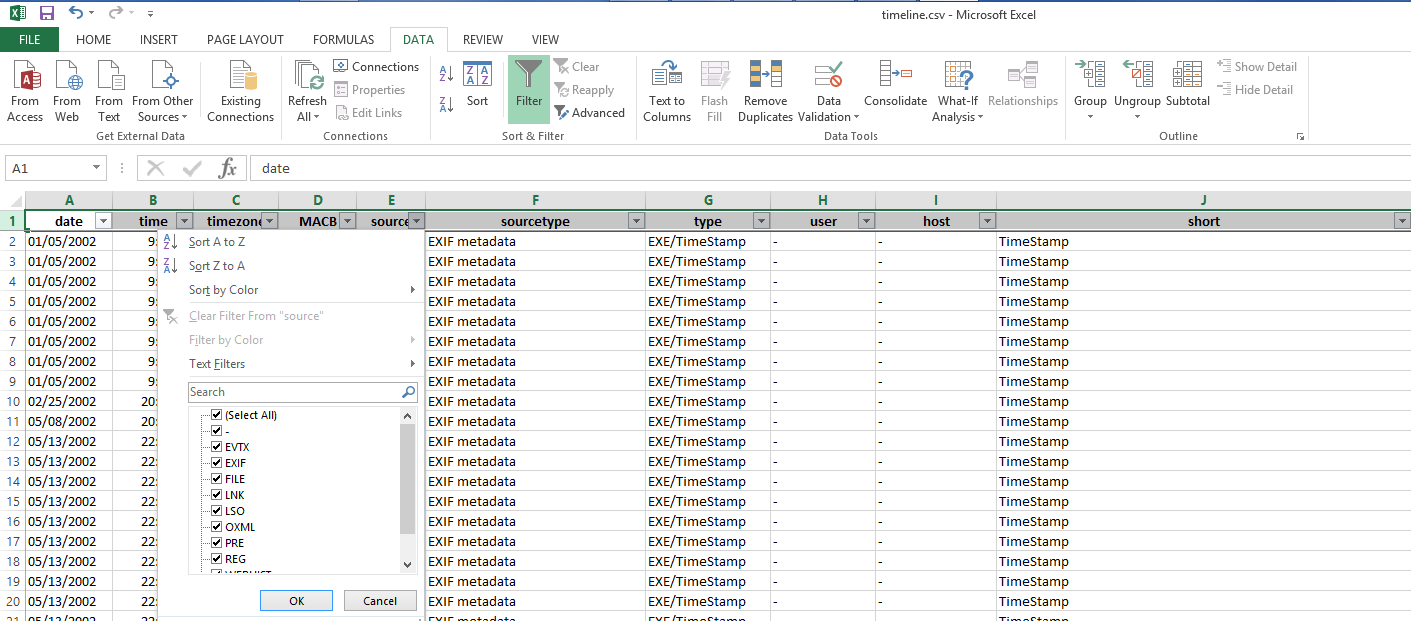
1. In the SIFT workstation, copy the file timeline.csv into the **/mnt/hgfs/SIFT\_Shared** folder.
2. Run the command log2timeline –f list to see what is parsed by log2timeline (Figure 27).



**Figure 27:**

Source: ???.

1. On your Windows system, open the **timeline.csv** file in the Users/[your Profile Name]/Desktop/SIFT\_Shared folder in Excel or other spreadsheet program.
2. Once open, freeze the top row and format the column names so that they are bold and centered.
3. If you’re using Excel, highlight the top row and select **Data > Filter** to easily filter your data. In this case, you can select All, EVTX, EXIF, File, LNK, FSO, etc. from the Source column (Figure 28).



**Figure 28:**

Used with permission from Microsoft.

1. Review the output to see the types of data available in the timeline.csv file.

References

AccessData. (2010). FTK IMager Lite (Version 3.1.1) [Computer software]. Retrieved from http://accessdata.com/product-download/ftk-imager-lite-version-3.1.1

FireEye, Inc. (2011). MANDIANT Highlighter (Version 1.1.3) [Computer software]. Retrieved from https://www.fireeye.com/services/freeware/highlighter.html

RegRipper (Version 2.8) [Computer software]. Retrieved from <https://github.com/keydet89/RegRipper2.8>

SANS Institute (2017). SIFT Workstation [VMware Appliance]. Retrieved from https://digital-forensics.sans.org/community/downloads

Zimmerman, E. (n.d.). Shellbags (Version 0.9.5.0) [Computer software]. Retrieved from https://ericzimmerman.github.io/