**3906ICT/7906ICT Digital Forensics**

**Tutorial 4.2 – Timeline Analysis**

The aim of this tutorial is to give you some experience with generating and analysing a timeline of digital events. We will cover some of the topics raised in the Lecture, but there are many more techniques and tools that you are open to explore.

Please note that this tutorial is not a step by step guide. The expectations are that if you are not sure of how to do something, you should find out via internet search or by asking your tutor.

# Preliminaries

There are two options for doing the practical component of this tutorial. You can do this tutorial by logging into the Griffith Cyber Range which is an Internet isolated set of virtual machines that has been set up on the Griffith network. The other is to download and install the software on your local PC.

## Set Up Option 1 – Griffith Cyber Range

If you are not on a Griffith University campus need to VPN into the Griffith Network. Details of how to VPN into the Griffith Network can be found here: https://intranet.secure.griffith.edu.au/computing/remote-access/virtual-private-network. Go to the bottom of the page and find the instructions for your device.

Once you have set up your VPN to the Griffith network, you can use your browser to go to the following page:

https://cyber.ict.griffith.edu.au/

The credentials for the Griffith Cyber Range Server are:

**Username: sXXXXXXX**

**Password: changeme**

sXXXXXXX is your Griffith username. When you log in for the first time change your password (which you will need to remember). To do this go to your username menu on the top right corner of the web page and select the Settings item. The Settings page will allow you to reset your password. Once you have reset the password, use your new password for subsequent logins. For this tutorial we will be using the SIFT workstation. Click on the SIFT link and you will be connected to a virtual machine running the SANS SIFT workstation Linux distribution.

When you have finished your tutorial simply close the browser tab with the connection to the virtual machine. Or press Shift-Ctrl-Alt to access the web menu and disconnect from the Griffith Cyber Range.

## Set Up Option 2 – Install on your local PC

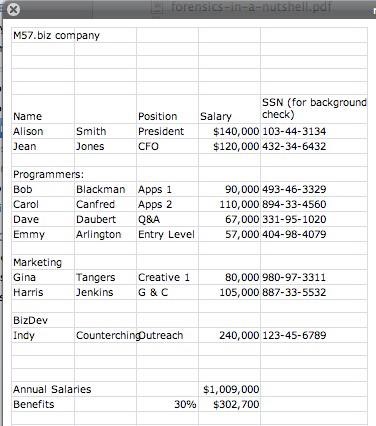
The other option is to install the SIFT workstation on your local PC. Links to the virtual machine OVA file for download are found on the Learning@Griffith web site. **Note:** The SIFT workstation is a 15GB download. You will need to install VirtualBox and select File->Import Appliance to install the SIFT workstation Virtual machine. Start the Virtual Machine and log in.

The login credentials for the SIFT workstation are:

**Username: sansforensics**

**Password: forensics**

# Timeline Scenario

 A document is leaked on the Internet which contains confidential information about M57′s employees such as SSN, salaries and positions in the company. This sensitive Excel sheet has mysteriously appeared on a competitor’s website. Jean, the CFO, is believed to be involved since she had access to this file. She claims that the president Alison Smith asked explicitly for this information. However, Alison denies having asked for it or having received it.

The spreadsheet came from CFO Jean's computer. You are given a copy of the spreadsheet, "m57biz.xls".

Questions to answer:

* How did the documents get on the competitor's website?
* When did Jean create this spreadsheet?
* How did it get from her computer to competitor's website?

# Evidence

Assuming that the correct evidence has been identified and collected, the next step is to download the disk image onto the SIFT workstation virtual machine.

1. If you are using the Griffith Cyber Range, your virtual machines are isolated from the Internet but you can download the evidence for this tutorial from [http://forensic-tutorials.griffith.internal](http://forensic-tutorials.griffith.internal/) in the *tutorial4.2* directory. If you are using your own local SIFT workstation you can download the evidence from the link provided in the

Learning@Griffith page for this tutorial. It is a 4Gb download.

**Answer:**

Answer

1. Create a directory in the /cases directory called M57jean and unzip the file here.

**Answer:**

cd/home/sansforensics/Downloads/Tutorial\_4.2/

unzip /home/sansforensics/Downloads/Tutorial\_4.2/Tutorial4.2.zip

1. Check the md5sum of the nps-2008-jean.E01 is 647f22836426e071d8e1ccac6da54baf and nps-2008-jean.E02 files is e8845c20bdd2c24e734b7c0bcd1a8eab.

**Answer:**

$ md5sum nps-2008-jean.E01

647f22836426e071d8e1ccac6da54baf nps-2008-jean.E01

$ md5sum nps-2008-jean.E02

e8845c20bdd2c24e734b7c0bcd1a8eab nps-2008-jean.E02

1. These files are using the EWF Encase standard and we should know how to convert this format to a raw dd image. Mount the ewf partition nps-2008-jean.E01 using ewfmount to create a second ewf1 mount point as a raw image on /mnt/ewf/.

**Answer:**

Ewfmount –help

Man ewfmount

Cd /mnt

Ls

$ sudo ewfmount nps-2008-jean.E01 /mnt/ewf

1. Use mmls to view the partition on the new /mnt/ewf/ewf1 mountpoint. You can also mount the ewf1 image to the /mnt/windows\_mount directory so you can access it as you did for the disk image in Tutorial 4.

**Answer:**

$ sudo ls /mnt/ewf

ewf1

$ sudo ls -l /mnt/ewf

total 0

-r--r--r-- 1 root root 10737418240 Oct 2 14:54 ewf1

$ sudo mmls /mnt/ewf/ewf1

DOS Partition Table

Offset Sector: 0

Units are in 512-byte sectors

Slot Start End Length Description

000: Meta 0000000000 0000000000 0000000001 Primary Table (#0)

001: ------- 0000000000 0000000062 0000000063 Unallocated

002: 000:000 0000000063 0020948759 0020948697 NTFS / exFAT (0x07)

003: ------- 0020948760 0020971519 0000022760 Unallocated

(63 x 512 = 32257)

$ sudo mount -o loop,ro,show\_sys\_file,streams\_interface=windows,offset=32256 /mnt/ewf/ewf1 /mnt/windows\_mount

$ cd /mnt/windows\_mount

$ ls

# Timelines with the Sleuth Kit

1. Use the Sleuth kit fls command to create a body file in the /cases/m57jean directory.

**Answer:**

$ sudo fls -o 63 /mnt/ewf/ewf1

$ cd /home/sansforensics/Downloads/Tutorial\_4.2/

$ sudo fls -m "C:" -r -p -o 63 /mnt/ewf/ewf1 > m57bodyfile.txt

$ ls -al

$ head m57bodyfile.txt

1. Examine the body file and note the format of the information stored. Does it match the documentation?

**Answer:**

Absolutely

$ head m57bodyfile.txt

0|C:/$AttrDef ($FILE\_NAME)|4-48-2|r/rr-xr-xr-x|48|0|82|1210717123|1210717123|1210717123|1210717123

0|C:/$AttrDef|4-128-4|r/rr-xr-xr-x|48|0|2560|1210717123|1210717123|1210717123|1210717123

0|C:/$BadClus ($FILE\_NAME)|8-48-3|r/rr-xr-xr-x|0|0|82|1210717123|1210717123|1210717123|1210717123

0|C:/$BadClus|8-128-2|r/rr-xr-xr-x|0|0|0|1210717123|1210717123|1210717123|1210717123

0|C:/$BadClus:$Bad|8-128-1|r/rr-xr-xr-x|0|0|10725732352|1210717123|1210717123|1210717123|1210717123

0|C:/$Bitmap ($FILE\_NAME)|6-48-2|r/rr-xr-xr-x|0|0|80|1210717123|1210717123|1210717123|1210717123

0|C:/$Bitmap|6-128-1|r/rr-xr-xr-x|0|0|327328|1210717123|1210717123|1210717123|1210717123

0|C:/$Boot ($FILE\_NAME)|7-48-2|r/rr-xr-xr-x|48|0|76|1210717123|1210717123|1210717123|1210717123

0|C:/$Boot|7-128-1|r/rr-xr-xr-x|48|0|8192|1210717123|1210717123|1210717123|1210717123

0|C:/$Extend ($FILE\_NAME)|11-48-3|d/dr-xr-xr-x|0|0|80|1210717123|1210717123|1210717123|1210717123

1. Use the mactime command to create the timeline in CSV format.

**Answer:**

$ mactime -b m57bodyfile.txt > m57timeline.csv

head m57timeline.csv

1. Examine the CSV output using a spreadsheet.

**Answer:**

Answer

1. When were programs installed on the machine? How can you find this out by looking at this timeline?

**Answer:**

The later part of June in 2007

1. It may be that Jean used email to communicate. Search or use grep to look for outlook.pst and m57biz.xls files in the timeline.

**Answer:**

Answer

1. Extract the outlook.pst file and use the readpst command to export emails from the outlook.pst file and check that the emails match the timeline.

**Answer:**

$ cd /mnt/windows\_mount/Documents\ and\ Settings/Jean/Local\ Settings/Application\ Data/Microsoft/Outlook

ls

$ cp outlook.pst /home/sansforensics/Downloads/Tutorial\_4.2/

Readpst [Enter]

\*see options\*

$ readpst outlook.pst

nano Inbox.mbox

vi Inbox.mbox

vi Sent\ Items.mbox

/.xls \*inside vim\*

# Timelines with Plaso and Log2timeline

1. Read the plaso help messages and man page.

**Answer:**

log2timeline --info

1. Use the info option to list the installed plaso parsers. Identify possible parsers for the outlook file and Microsoft office as well as general windows items of interest.

**Answer:**

log2timeline --info

$ sudo log2timeline.py m57log2timeline.plaso /mnt/ewf/ewf1

1. If you have time, run the default log2timeline.py call to create a plaso storage file from the ewf1 mounted image. Otherwise try just the parsers for Outlook and Office. Get a coffee. This might be as far as you get for the workshop.

**Answer:**

sudo log2timeline.py m57log2timeline.plaso /mnt/ewf/ewf1

1. Run the pinfo.py command on the generated plaso storage file. What does it tell you?

**Answer:**

$ sudo pinfo.py m57log2timeline.plaso

$ sudo log2timeline.py --parser "winreg" winreg.plaso /mnt/ewf/ewf1

1. Run psort.py for the date identified in the Sleuth Kit timeline and output the command to a CSV file.

**Answer:**

See options – sudo psort.py

sudo psort.py -o l2tcsv -w m57log2timeline.csv m57log2timeline.plaso

sudo psort.py -w m57log2timeline.csv -o l2tcsv m57log2timeline.plaso (trying the alternate arrangement)

1. Examine the CSV. How does it compare to the Sleuth Kit timeline.

**Answer:**

Open csv file, or

$ grep m57biz.xls m57log2timeline.csv

We see the 1;28am from the email.

# Timelines with Autopsy (Optional)

Autopsy is a graphical front end for the Sleuth Kit. The windows version has been included in the Tutorial4.2.zip file. If you have time, install the Autopsy on a windows system and compare it with the Linux command line version.

1. Unzip the Tutorial4.2.zip file on your windows host along with the nps-2008-jean.E01 and nps-2008-jean.E02 files.

**Answer:**

Answer

1. Install Autopsy using the msi file.

**Answer:**

Answer

1. Start a new case filling in minimal appropriate settings. Add a new data source and open nps-2008-jean.E01. Autopsy should automatically start analysing the image.

**Answer:**

Answer

1. Click on the Timeline button. How does the timeline generated using Autopsy compare with the command line Sleuth Kit timeline?

**Answer:**

Answer

# Tutorial Quiz

You have now completed the exercises for this tutorial. You can now attempt the quiz for this tutorial.