**7906ICT Digital Forensics**

**Tutorial 3.1 – Network Forensics**

The aim of this tutorial is to give you some experience with the network forensic analysis with pcap files. We will cover some of the topics raised in the Lecture, but there are many more techniques you are open to explore. The tutorial this week has two parts. The first part will revisit the scenario from last week and the second part will investigate well-known network forensics training scenarios.

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**

# Part 1 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. Note we will be using the same evidence as the last tutorial. You may skip this step if the evidence is on your virtual machine from last time.

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 *tutorial2.2* 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 2.5Gb download.

1. Create a directory in the /cases directory called schardt and unzip the file here.
2. Concatenate the DD image files into one file using the cat command.

**Answer:**

cat SCHARDT.001 SCHARDT.002 SCHARDT.003 SCHARDT.004 SCHARDT.005 SCHARDT.006 SCHARDT.007 SCHARDT.008 > schardt.dd

sudo mount -o ro,loop,offset=32256 /cases/schardt/schardt.dd /mnt/windows\_mount

cd /mnt/windows\_mount

1. Check the image hash.

# Investigate Web Behaviour

Now we will investigate the web browsing behaviour of Greg Schardt, Mr. Evil.

1. Check that the pasco application is installed on the SIFT workstation.

**Answer:**

pasco

1. Read the man page for pasco.
2. Use pasco to view Mr. Evil’s web history in the mounted file system. Has he accessed suspicious web pages and when?

**Answer:**

cd Documents\ and\ Settings/

cd Mr.\ Evil/

cd Local\ Settings/

cd History/

cd History.IE5/

pasco index.dat > /cases/schardt/IEHistory.csv

cd /cases/schardt/

1. Use pasco to view Mr. Evil’s browser cache in the mounted file system. Does this cache confirm web page access? What is the difference between these two sources of evidence?

**Answer:**

cd Documents\ and\ Settings/

cd Mr.\ Evil/

cd Local\ Settings/

cd Temporary\ Internet\ Files/

cd Content.IE5/

pasco index.dat > /cases/schardt/Cache.csv

Cache contains access to webpages (URL) and not files (as well) unlike the history

# Part 2 Evidence

Now we will investigate packet capture data.

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 *tutorial3.1* 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.

1. Unzip the downloaded files. Create a directory in the /cases directory for each scenario and move the appropriate file to each case directory.
2. Check the image hash for each file?
   * The Scenario 1 evidence file is evidence01.pcap
   * MD5 (evidence.pcap) = d187d77e18c84f6d72f5845edca833f5
   * The Scenario 2 evidence file is evidence02.pcap.
   * MD5 (evidence02.pcap) = cfac149a49175ac8e89d5b5b5d69bad3
   * The Scenario 3 evidence file is suspect.pcap.
   * MD5 (suspect.pcap) = 7121691c5be717562c0cbcf056f365ef

**Answer:**

md5sum \*.pcap

md5sum -c <<<"d187d77e18c84f6d72f5845edca833f5 \*evidence01.pcap"

md5sum -c <<<"cfac149a49175ac8e89d5b5b5d69bad3 \*evidence02.pcap"

md5sum -c <<<"7121691c5be717562c0cbcf056f365ef \*suspect.pcap"

Use Wireshark and Network Miner to help you to answer the following network forensic questions. To start Wireshark you can type “wireshark &” from a terminal in the virtual machine.

To use Network Miner, first download it from Blackboard. You can install it on your Windows host or install it on your SiftWorkstationGU virtual machine. Unzip the file and run the NetworkMiner.exe file in the extracted folder. If you are running the program on a Linux machine, it will use the Wine application to run. The Z:\ drive will be the Linux file system root.

Most answers for this tutorial can be easily found using Network Miner. See how much information you can confirm using Wireshark also.

# Scenario 1

Anarchy-R-Us, Inc. suspects that one of their employees, Ann Dercover, is really a secret agent working for their competitor. Ann has access to the company’s prize asset, the secret recipe. Security staff are worried that Ann may try to leak the company’s secret recipe.

Security staff have been monitoring Ann’s activity for some time, but haven’t found anything suspicious– until now. Today an unexpected laptop briefly appeared on the company wireless network. Staff hypothesize it may have been someone in the parking lot, because no strangers were seen in the building. Ann’s computer, (192.168.1.158) sent IMs over the wireless network to this computer. The rogue laptop disappeared shortly thereafter.

“We have a packet capture of the activity,” said security staff, “but we can’t figure out what’s going on. Can you help?”

Your task is to figure out who Ann was IM-ing, what she sent, and recover evidence including:

1. What is the name of Ann’s IM buddy?

**Answer:**

Buddy: Sec558user1

1. What was the first comment in the captured IM conversation?

**Answer:**

Here's the secret recipe... I just downloaded it from the file server. Just copy to a thumb drive and you're good to go

1. What is the name of the file Ann transferred?

**Answer:**

recipe.docx

1. What is the magic number of the file you want to extract (first four bytes)?

**Answer:**

<https://asecuritysite.com/forensics/magic>

[50 4B 03 04 [PK]](https://asecuritysite.com/forensics/docx)

1. What was the MD5sum of the file?

**Answer:**

$ md5sum SecretRecipe.docx

8350582774e1d4dbe1d61d64c89e0ea1 SecretRecipe.docx

1. What is the secret recipe?

# Scenario 2

As a result of the Anarchy-R-Us affair Ann Dercover has been arrested. After being released on bail, Ann disappears! Fortunately, investigators were carefully monitoring her network activity before she skipped town.

“We believe Ann may have communicated with her secret lover, Mr. X, before she left,” says the police chief. “The packet capture may contain clues to her whereabouts.”

Your task is to figure out what Ann emailed, where she went, and recover evidence including:

1. What is Ann’s email address?

**Answer:**

Ann - [sneakyg33k@aol.com](mailto:sneakyg33k@aol.com)

Other - sec558@gmail.com

1. What is Ann’s email password?

**Answer:**

NTU4cjAwbHo=

558r00lz

1. What is Ann’s secret lover’s email address?

**Answer:**

mistersecretx@aol.com

1. What two items did Ann tell her secret lover to bring?

**Answer:**

Hi sweetheart! Bring your fake passport and a bathing suit. Address =

attached. love, Ann

1. What is the NAME of the attachment Ann sent to her secret lover?

**Answer:**

secretrendezvous.docx

1. What is the MD5sum of the attachment Ann sent to her secret lover?

**Answer:**

$ md5sum secretrendesvous.docx

9e423e11db88f01bbff81172839e1923 secretrendesvous.docx

1. In what CITY and COUNTRY is their rendezvous point?

**Answer:**

Playa del Carmen

Mexico

1. What is the MD5sum of the image embedded in the document?

**Answer:**

$ md5sum image.png

aadeace50997b1ba24b09ac2ef1940b7 image.png

# Scenario 3

Your organization has become aware of external attempts to gain access to sensitive proprietary information on its computer systems and has stepped up its monitoring in response. Data from this monitoring, in addition to interviews with employees, has focused attention on a single user, who is suspected of collaborating with an outside party.

It's your task to analyze this data and determine what can be established about the activity of the user.

1. What is the identity of the suspect? What is their email address?

**Answer:**

steve.vogon@gmail.com

1. What IP address and hostname does the suspect's Linux computer have?

**Answer:**

192.168.151.130

192.168.151.130 [goldfinger] (Linux)

1. What evidence do you have to assume that this computer is running Linux?

**Answer:**

p0f (NetSA): Linux 2.6 (older, 6) (possibly Mandriva 2010.x, Ubuntu 7.x) [Linux] (100.00 %)

Satori DHCP: Linux - Linux 2.6 (100.00 %)

Satori TCP: Linux - Linux 2.6 (100.00 %)

Web Browser User-Agent 1 : Mozilla/5.0 (X11; U; Linux i686; en-US) Gecko/20071126

Web Browser User-Agent 2 : Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.0.12) Gecko/20071020 CentOS/1.5.0.12-6.el5.centos Firefox/1.5.0.12

1. What Google searches did the suspect perform?

**Answer:**

overseas credit card payments

hurricane

1. What message did the email contain that the suspect sent from his Gmail account?

**Answer:**

Hello,<br><br>Can you please tell me what the minimum balance requirement is for opening an overseas account at your bank<br>

Hello,<br><br>Can you please tell me what the minimum balance requirement is for opening an overseas account at your bank?<br><br>Thank you,<br><br>Steve K. Vogon<br><br>

1. One web page opened by the suspect contains a map, what region does the map show?

**Answer:**

caribbean

# Tutorial Quiz

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