**3906ICT/7906ICT Digital Forensics**

**Tutorial 4.1 – Mobile Device Forensics**

The aim of this tutorial is to give you some experience with analysing Android based forensic artefacts. We will cover some of the topics raised in the Lecture, but there are many more Android and mobile forensic artefacts 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**

# Mobile Device Scenario

You work as a digital forensics investigator and you have been given a full Android disk image obtained using the Cellebrite UFED data extractor device.

# 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.

Check disk space df -h

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 *tutorial4.1* 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. It is a 5Gb download expanding to 32Gb.

**Answer:**

Check disk space df -h

1. Create a directory in the /cases directory called Android and unzip the file using 7z here.

**Answer:**

$ 7z l Tutorial4.1.7z

1. Check the md5sum of the blk0\_mmcblk0.bin file is 5dafc6668c2c0e6bb3a928f35676d3bd and blk32\_mmcblk0rpmb.bin is a26f0b56848b1bdbb350f70141b58098.

**Answer:**

$ md5sum \*

5dafc6668c2c0e6bb3a928f35676d3bd blk0\_mmcblk0.bin

a26f0b56848b1bdbb350f70141b58098 blk32\_mmcblk0rpmb.bin

11b2b1b8e76a632ae0fcc77749f7ebff Tutorial4.1.7z

1. Use Sleuth kit to examine the image file format status.

**Answer:**

$ img\_stat '/home/sansforensics/Downloads/Tutorial\_4.1/blk0\_mmcblk0.bin'

IMAGE FILE INFORMATION

--------------------------------------------

Image Type: raw

Size in bytes: 31268536320

Sector size: 512

sansforensics@siftworkstation: ~/Downloads/Tutorial\_4.1

$ img\_stat '/home/sansforensics/Downloads/Tutorial\_4.1/blk32\_mmcblk0rpmb.bin'

IMAGE FILE INFORMATION

--------------------------------------------

Image Type: raw

Size in bytes: 4194304

Sector size: 512

1. Which Sleuth kit command will display the layout of the disk? Use it to identify partitions and unallocated space. Take note of the differences between Android and Windows partitions from Tutorial 2.2.

**Answer:**

$ mmls blk0\_mmcblk0.bin

$ mmls blk32\_mmcblk0rpmb.bin

$ mmls -B blk0\_mmcblk0.bin

1. Mount the data partition (the largest one) in blk0\_mmcblk0.bin so you can access it as a disk to the /mnt/e01 mount point. Note you may need to calculate the offset when the partition begins. This time we won’t mount read only as we need to change some things.

**Answer:**

Offset: 0007782400

052: 044 0007782400 0061071323 0053288924 0025G userdata

0007782400 x 512 = 3984588800

$ sudo mount -o loop,offset=3984588800 blk0\_mmcblk0.bin /mnt/e01

$ cd /mnt/e01

ls

1. A lot of information in Android is in SQLite databases. Use apt to install the sqlitebrowser.

**Answer:**

In the Development subdirectory

ls -al

Not all are executable by user

sudo su root

1. Log in as root. Many Android files and directories are restricted to root access only.

**Answer:**

sudo su root

# Available Apps

1. What are the stock and non-stock apps that have been installed on this phone?

**Answer:**

find /mnt/e01 -name \*.apk

1. Apps can provide the identity of the phone owner. What is the owner’s main google email address?

**Answer:**

cd data

root@siftworkstation:/mnt/e01/data# ls -al | grep gm

drwx------. 4 1001 1001 4096 Apr 16 1970 com.android.sdm.plugins.diagmon

drwx------. 11 10084 10084 4096 Dec 1 2018 com.google.android.gm

drwxr-x--x. 29 10020 10020 4096 Dec 6 2018 com.google.android.gms

drwxr-x--x. 8 10019 10019 4096 Dec 7 2018 com.google.android.gms.setup

cd com.google.android.gm

cd shared\_prefs/

ls

cat Gmail.xml > '/home/sansforensics/Downloads/Tutorial\_4.1/Gmail.xml'

<string name="thisisdfir@gmail.com-account-alias">thisisdfir@gmail.com</string>

<string name="thisisdfirtwo@gmail.com-account-alias">[thisisdfirtwo@gmail.com</string](mailto:thisisdfirtwo@gmail.com%3c/string)>

1. What is the phone owner’s Facebook name.

**Answer:**

cd ..

cd databases/

ls

cp mailstore.thisisdfir@gmail.com.db ' /home/sansforensics/Downloads/Tutorial\_4.1/'

cd /home/sansforensics/Downloads/Tutorial\_4.1

ls -al

$ sudo chown sansforensics:sansforensics [mailstore.thisisdfir@gmail.com.db](mailto:mailstore.thisisdfir@gmail.com.db)

root@siftworkstation:/mnt/e01/data# ls -al | grep face

drwx------. 4 10060 10060 4096 Apr 16 1970 com.android.facelock

drwx------. 39 10103 10103 4096 Dec 7 2018 com.facebook.orca

cd com.facebook.orca

ls

cd shared\_prefs/

ls

cat com.facebook.orca\_preferences.xml | less (NOPE)

cd ../databases/

cp threads\_db2 /home/sansforensics/Downloads/Tutorial\_4.1/

$ sudo chown sansforensics:sansforensics threads\_db2

Open DB:

"name":"ThisIs Dfir"

"name":"Josh Hickman"

# SMS and Messages

SMS and Txt Messages can give some record of conversations made with the phone.

1. Where in the disk image is the stock SMS and messaging information kept?

**Answer:**

root@siftworkstation:/mnt/e01# find . -name \*telephony\*

root@siftworkstation:/mnt/e01# find . -name \*providers.telephony\*

./misc/profiles/cur/0/com.android.providers.telephony

./misc/profiles/ref/com.android.providers.telephony

./data/com.android.providers.telephony

find: ??./data/com.whatsapp/files/.trash/81419edf-1cc3-4943-852f-34df6d188b2c??: Structure needs cleaning

./user\_de/0/com.android.providers.telephony

./media/0/Android/data/com.android.providers.telephony

/user\_de/0/com.android.providers.telephony/databases/telephony.db

cd user\_de/0/com.android.providers.telephony/databases/telephony.db

ls

cp mmssms.db /home/sansforensics/Downloads/Tutorial\_4.1/

$ sudo chown sansforensics:sansforensics mmssms.db

cp telephony.db /home/sansforensics/Downloads/Tutorial\_4.1/

$ sudo chown sansforensics:sansforensics telephony.db

\*look into carriers\*

1. Open the SQLite database that holds the SMS messages. What was the first received message?

**Answer:**

Welcome to TracFone! Your number is: 9197580276, your Last Day of Service is 01/28/2019. For self-help options, text 'HELP' to 611611.

1. Who sent the message and what was it about?

**Answer:**

From “TracFone”

# Network Connections

Network connections can give some information as to where the phone has been located and thus the owner of the phone’s locations.

1. Where in the disk image is the wireless network information kept?

**Answer:**

cd /mnt/e01

root@siftworkstation:/mnt/e01# find /mnt/e01 -name 'wifi'

/mnt/e01/misc/wifi

find: ??/mnt/e01/data/com.whatsapp/files/.trash/81419edf-1cc3-4943-852f-34df6d188b2c??: Structure needs cleaning

cd /mnt/e01/misc/wifi

ls

cat wpa\_supplicant.conf

1. How many wireless networks has this phone connected to?

**Answer:**

Answer

1. Is there any other interesting information kept about these networks?

**Answer:**

cat wpa\_supplicant.conf -- shows passwords

# Phone Calls

Phone calls made by the suspect can add a lot of weight to a case.

1. Where in the disk image is the phone call information kept?

**Answer:**

cd /mnt/e01

find . -name "\*calllog\*" OR find /mnt/e01 -name "\*calllog\*"

cd data/com.android.providers.contacts/databases/

cp calllog.db '/home/sansforensics/Downloads/Tutorial\_4.1/'

cp contacts2.db '/home/sansforensics/Downloads/Tutorial\_4.1/'

$ sudo chown sansforensics:sansforensics calllog.db

$ sudo chown sansforensics:sansforensics contacts2.db

1. How many phone calls were made?

**Answer:**

See calls in calllog.db

1. When was the last call made?

**Answer:**

Copy “1544033627703”

date -d @1544033627703

Mon 23 Jun 50898 01:55:03 PM UTC

date -d @1544033627.703

Wed 05 Dec 2018 06:13:47 PM UTC

# Photos Taken

Photos and other media that are generated on the phone camera may often hold information that is important to a case.

1. Where in the disk image is the phone camera photo information kept?

**Answer:**

cd ../../..

root@siftworkstation:/mnt/e01#

find /mnt/e01 -name "\*camera\*"

find /mnt/e01 -name "\*jpg\*"

/mnt/e01/media/0/DCIM/Camera/IMG\_20181129\_162642.jpg

/mnt/e01/media/0/DCIM/Camera/IMG\_20181129\_165144.jpg

/mnt/e01/media/0/DCIM/Camera/IMG\_20181129\_165213.jpg

/mnt/e01/media/0/DCIM/Camera/IMG\_20181130\_082525.jpg

/mnt/e01/media/0/DCIM/Camera/IMG\_20181130\_082856.jpg

/mnt/e01/media/0/DCIM/Camera/IMG\_20181130\_083324.jpg

1. How many photos were taken? When was the first photo taken?

**Answer:**

cp -r /mnt/e01/media/0/DCIM/Camera/ /home/sansforensics/Downloads/Tutorial\_4.1/

ls -al (here its wrong)

cd /mnt/e01/media/0/DCIM/Camera/

ls -al (Here the dates are accurate in the source)

1. Can you view the photos?

**Answer:**

Definitely

# Tutorial Quiz

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