Week 1 Activity

Objective

The objective of this activity is to perform a simple computer forensic process and then write a report that is understood by a lay reader (e.g. manager, lawyer, jury, etc) and is persuasive enough to demonstrate your competence. A secondary objective is getting familiar with the Win10 and Kali Linux Virtual Machines provided as part of the course material and some of the tools on them.

The activity comprises three parts:

- Part A – to be done in tomorrow's tutorial/lab;
- Part B – to be done at home as an individual assessment task;
- Part C – is preparation for a later activity;
- Part D – is optional.

Scenario (will be used across multiple activities)

You have been engaged by a lawyer acting for Ms Moneypenny and are briefed with the following (some of this is important now and others later):

- The client has been codocile[1] with Mr Bond for about 10 years living together in a grand estate owned by Mr Bond;
- The client has suspected that Mr Bond has been having an affair and is seeking to maximise any windfall from a separation;
- The client has an external hard disk drive that is relevant to the case;
- The client says that she is sure there used to be more pictures on the external hard disk drive than are showing now. The following are especially relevant:
  - two identical pictures of a wall in the room where Mr Bond and his lover used to meet;
  - two different pictures of Mr Bond's Land Rover car;
  - a picture of a sports car that is she says is that of Mr Bond's lover.
- You are to assume that you have been provided with the requisite formalities for an expert's report, which will get to later in the course.

Instructions for week 1 activity

Part A (to be done in the tutorial/lab)

When a lawyer formally asks you to do something for a case, this is called then "giving instructions" or you "receiving instructions".

[1] "Codocile" is the legal term for living together and is typically used as a precursor to be claiming a de-facto relationship

You instructed that the external hard disk drive should copied onto DVD-rom drives so it can be sent Mr Bond's lawyer. This should be done early so both sides have access to the evidence.

For the sake of the activity, we will use a small USB key (circa 256Mb) instead of the said external hard disk drive. We are doing this so that the technical process of copying and later analysis activities will be fast. We will pretend that the 256Mb USB key is a larger storage device and that needs to be split into portions that are 50Mb to fit onto the DVD-roms.

For the sake of the exercise, you are to:

1. Make the copy and a hash of the copy i.e. make a forensic copy;
2. Compress the copy;
3. Split the compressed copy into 50Mb pieces (normally you would also hash the pieces, but we won't for the exercise);
4. Put it back together;
5. Demonstrate that the re-constructed image is a reliable copy of the forensic copy

A sample solution is provided for this part of the activity and you can check your results against files provided. Make sure to documents what you do using contemporaneous notes and where appropriate you might also use pictures/screenshots.

If you finish early you should start of the Optional Part D.

(**Note**: in later weeks you will be provided with further instructions relating to this scenario for analysis activities. Although most of the exercise material relating to the scenario is already on the VMs, the weekly activities have been sequenced to match the course so please don't skip ahead).

Part B (to be done at home)

This part is in two parts:

1. Prepare a report on what you have done in Part A. At this stage of the course, it is not expected to be presented as an expert's report and a short essay style will suffice (maximum 4 pages, not including pictures). For each step, you will need to provide commentary on:
    a. What you are doing;
    b. Why you are doing it;
    c. The outcome of the process;
    d. Why you know the outcome is reliable (this may not apply for every step)
2. Get a non-technical person (e.g. partner, friend, parent, sibling, etc) to read the above report and provide feedback. Can they readily follow it without your explanations? Prepare a 1-2 page reflection (maximum 2 pages) on how you found the writing of the report and some of the things you could improve after getting the feedback from the lay reader. They may relate to how you approached Part A, how you recorded Part A or how you approached Part B.

NOTE: your submission is to be a single PDF file, clearly marked with you name and student number on every page.

Part C (to be done at home)

This part is preparation for a later activity. It is not part of the Week 1 assessment task.

You are aware that Mr Bond and Ms Moneypenny are celebrities of some notoriety. Although you know that professional conduct is that you are expected not to make any enquires beyond those that are relevant to your answering your instructions, your curiosity gets the better of you.

Log into your Google account and search for the following:

1. Where does James Bond live?
2. What is Moneypenny's first name?
3. Three other things you think are important. Record:
    a. the search term(s) that you used;
    b. the day/time of your search.
4. Also records:
    a. the browser type;
    b. your visible IP address (from https://whatismyipaddress.com/);
    c. your real-world location i.e. street address.
5. Go incognito and then repeat the first two searches.

Part D (optional)

1. Get a USB key (the smaller the faster the activity);
2. Use dcfldd on Kali Linux to make a forensic copy. Record the hash;
3. Use Guymager on Kali Linux to make a forensic copy. Is the copy the same as (2)?
4. Use a commercial imager to make a forensic copy in the dd format. Is the copy the same as (2) and (3)?

You may want to use the following:

- Getdata forensic imager comes with Forensic Explorer (on the supplied Win10 VM) or you can download a standalone version here: http://www.forensicimager.com/
- You can download FTK Imager Lite here: https://accessdata.com/product-download/ftk-imager-lite-version-3-1-1 (this is the one I normally choose)

Sample solution for Part 1

Tools

Forensic Workstation #1: A Kali Linux workstation
(Optional) Forensic Workstation #2: A Windows 10 workstation with Forensic Explorer[2] installed.

An image of the USB key is installed in the Documents folder on each workstation (both Win10 and Kali Linux) and is called USBkey.img as well as outputs for each step.

Ensure you have enough free space – you will need at least 2Gb free space - on the VM to store the multiple copies that you will be making as part of the activity.

Process

Step 1 – hash of original

```
md5sum USBkey.img > USBkey.md5
```

The output is a file called USBkey.md5 that contains the MD5 hash of the image.

Step 2 – compress image

```
gzip -k USBkey.img
```

The output is a file called USBkey.img.gz

Step 3 – split compressed image

```
split -b 50M -d USBkey.img.gz USBkey.0

-b = size in bytes, M = Mb
-d = numeric suffix i.e. 01,02,03,etc
```

The output is a series of files USBkey.001, USBkey.002, etc which can be copied to DVD as per instructions.

Step 4 – put back together and decompress

The following steps demonstrate the reliability of the split files i.e. that they produce a file which is identical to the original image.

```
cat USBkey.??? > USBkey2.gz
```

The output is a file called USBkey2.gz

[2] This is installed in the Win10 VM that is supplied

```
gunzip -k USBkey2.gz
```

The output is a file called USBkey2

```
md5sum USBkey2 > USBkey2.md5
```

The output is a file called USBkey2.md5. Compare this with USBkey.md5 (created at Step 1)

Step 5 – demonstrating that the files are indeed the same

```
diff USBkey*.md5
```

There will be some output from the diff as the filenames are different, but the md5 should be the same.