

Aim:

To introduce Forensic concepts around evidence.

To open a Forensic case, collect evidence and draw a conclusion.

Method:

We **strongly** recommend you create a **Windows 10 virtual machine** and perform all the tutorials of this course on the virtual machine. You can create a snapshot of the virtual machine when the virtual machine is created so that you can roll back if needed.

Perform this lab and answer the questions below. Use the Lab **Report** document to create a **Forensics Report** for your Tutor. Do NOT upload these instructions.

Due Date:

Three days after the lab.

Assessment:

1% and Feedback will be given.

Q1) Digital Evidence ISO 27037.

Read the document in **Readings – Week 1** and answer these questions, you may need to use Google to find all the answers.

- a) Explain the four processes used to handle **Digital Evidence**.
- b) What is a **Digital Evidence First Responder**?
- c) A Standard computer workstation with network connections may contain digital evidence. Name four more **types of devices** that may contain digital evidence.
- d) What is **spoliation** in regards to Digital Evidence?

Q2) Evidence Collection – rfc3227.

Read the document in **Readings – Week 1** and answer these questions, you may need to use Google to find all the answers.

- a) From a legal point of view, why is it important to collect evidence correctly?
- b) Give an example of the **order of volatility** for a typical system, shortest first.
- c) Describe what needs to be documented in a **Chain of Custody form**.
- d) Name a command line program available on both Windows and Linux used to generate and compare **hashes** of files on a disk.

Q3) OSForensics

First generate some evidence. Open your **Chrome** Browser (Firefox will do as well.)

Go to Google and search for **Seek Roles**. Select **seek.com.au** in the hits found.

Confirm the Seek home page appears. Close Chrome.

Use notepad to save a text file called **Contacts** on your desktop. Include the name **Tony** in your contacts file. See (1)

Close notepad.

We will later search for **evidence** of your interaction with Tony

Now we will see how an investigator uses OSForensics to manage his/her investigation.

Download the program.

For Win 10 use <https://www.osforensics.com/download.html>

Version 7 is the current version (or use the link in canvas).

Right click the downloaded **osf.exe** file and run as administrator to Install OSForensics on a Windows Laptop, Windows Workstation or Windows Virtual Machine (VM). Accept the defaults.

If you have problems at any stage, ask your group for help. If the problem cannot be resolved, do not worry.

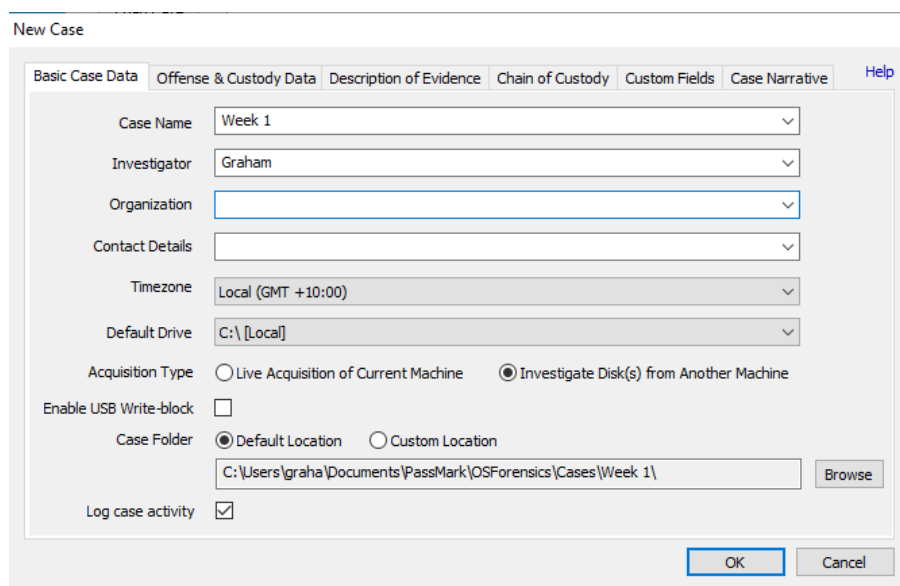
Just document what happened and include a snapshot of any error messages to discuss with your tutor.

Run OSForensics. Click the **Continue Using Free Version** button. Note you have 30 days left (we just try OSForensics this week).

a) **Add a Forensics Case.**

Select **Manage Case** from the Menu Bar at left. Select the **New Case** button.

Name the Case **Week 1**. Enter your name as the Investigator. Click OK.



New Case

Basic Case Data | Offense & Custody Data | Description of Evidence | Chain of Custody | Custom Fields | Case Narrative | Help

Case Name: Week 1

Investigator: Graham

Organization:

Contact Details:

Timezone: Local (GMT +10:00)

Default Drive: C:\ [Local]

Acquisition Type: ☐ Live Acquisition of Current Machine ☒ Investigate Disk(s) from Another Machine

Enable USB Write-block: ☐

Case Folder: ☒ Default Location ☐ Custom Location

Case Folder Path: C:\Users\graha\Documents\PassMark\OSForensics\Cases\Week 1

Log case activity: ☒

OK Cancel



(1)

b) Search for recent activity.

Select **User Activity** from the menu bar at left.

Click the Scan button at right. Click Yes and OK to add the disk.

Wait a few minutes until your device is scanned. Ignore errors.

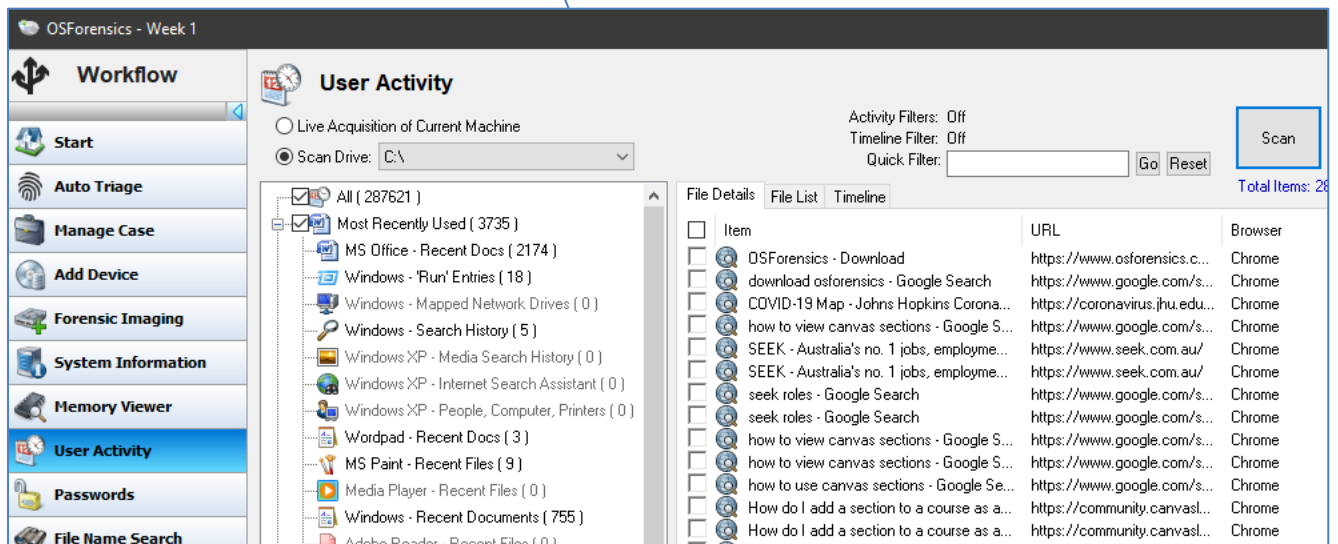
A summary window appears. Click OK.

You should have a list of User Activity.

Sort by Access Time descending.

Confirm you have evidence of your visit to Seek.

You should see **Seek** in Chrome Browser history.



Take a **screenshot** for your Report.

c) Index your text files and then search them.

Select **Create Index** from the menu bar at left. Tick only **Plain Text Files** and then click the **Next** button.

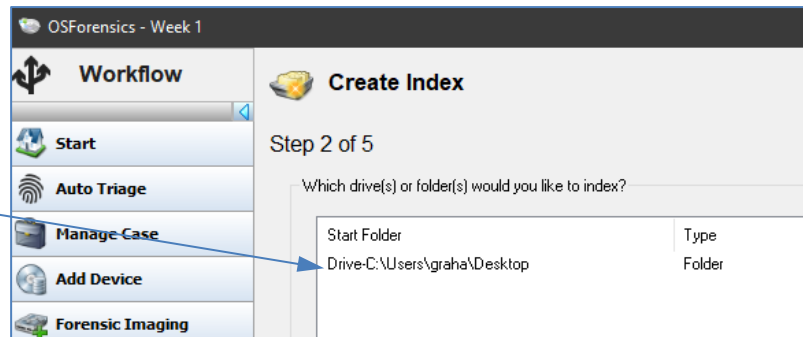
Click **Add** and select specific folder. Search for C:\Users\yourname\Desktop.

Click Ok and OK.

Confirm your result is similar to that shown.

Click Next.

Click **Small**. Click Next.



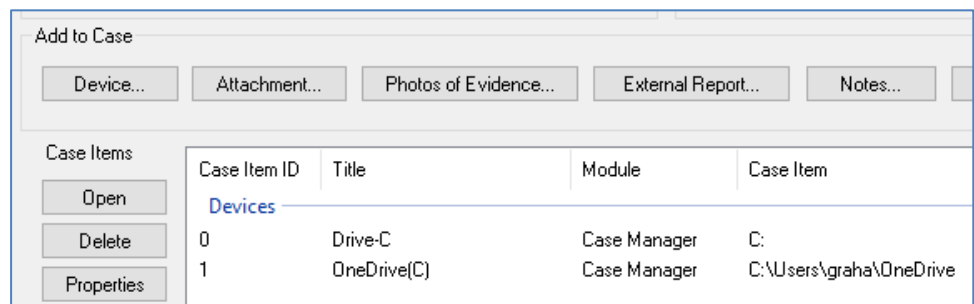
Click the **Start Indexing** button. This may take a few minutes.

If your conacts.txt file was not found, Windows may have moved your desktop to **OneDrive**.

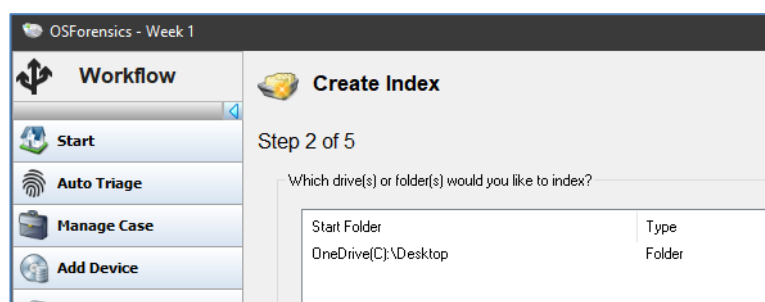
Select Manage Case. Under **Add to Case** Select Device.

Select Folder/Network Path. Browse to OneDrive. Click OK.

Check your Case looks like that shown.

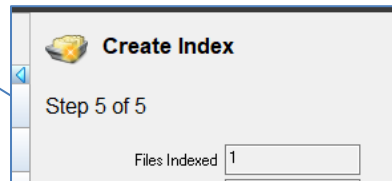


Redo the Create Index using the OneDrive desktop. (*Using 1 thread search in step 3 to reduce memory consumption.*)



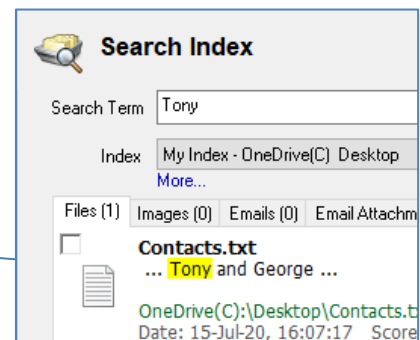
Click the **Start Indexing** button. This may take a few minutes.

At least one file should be indexed.



Select **Search Index** from the menu bar at left.

Enter **Tony** as the search word. Click the **Search** button.



Confirm you see a match to your contacts file.

Take a screen shot for your Report.

Now we have evidence that the suspect knows Tony.

Close OSForensics.

Conclusion

Have a think and draw a conclusion about using Windows 10 data for Forensics.

Consider the amount of data stored and the use of a tool such as OSForensics in finding evidence.

Submission.

Save your document as a **single pdf**.

Upload your pdf using the **Submit Assignment** button on Canvas **Week 1 tutorial**.