48436/32309

Week 03 Browser Files

This week we will examine browser files for forensic evidence and do some fingerprinting.

Warning: If you do this lab twice (or have visited Officeworks) you will get different answers due to caching. To repeat the lab, clear cookies and site data first.

Q1) Chrome cookies – using chrome

Open Chrome. Install if necessary.

A) Check the Browser version is up-to-date.

Select the Menu icon at top right. Select help, about.

Confirm Version 84. If less than 84, then update.

What is your **complete** chrome version number? _____ . Is it 32 or 64 bit? ____

B) Now check the cookie settings.

Select the chrome menu icon at top right and then select settings.

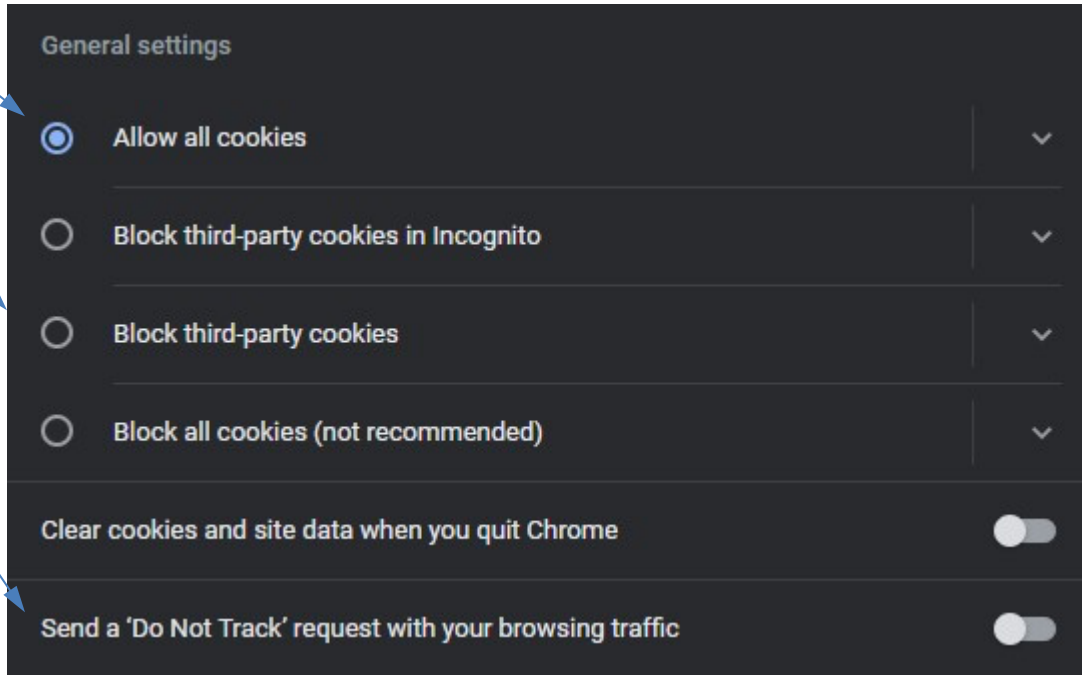
Scroll down to Privacy and Security.
Select Cookies and other site data.

Confirm setting to allow all cookies.

Confirm third-party cookies are not blocked.

Confirm Do Not Track is off.

Return to your home page.



If you have an Add blocker, disable it too.

Go to Google. Search for USB Pen Drive.

Scroll down and Select USB Flash Drives | Officeworks.

C) Now add some cookies

In Officeworks, search for SanDisk Ultra.

In the search results, locate and click a 64GB microSDXC result.

Note the Product Code. _____

Click the green Add to Cart button.

From the top menu select Store Locator.

Enter your location as Glebe 2037.

Confirm Your Store is set to Glebe.

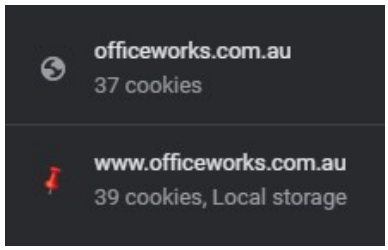
Check you have 1 item in your cart at top right. Click your cart. Confirm Item and Checkout. Confirm your item and Continue Checkout. When you get to Create Account, abandon the Checkout and close the Officeworks tab.

D) Now look at the cookies

Select the Chrome menu icon and then select Cookies and other site data.

D1) Cookie analysis 1

Scroll down to See all Cookies and Site Data. Expand.



Search cookies for officeworks (Lowercase O)

You should see many cookies from officeworks.com.au. Select these.

Note the _ga and _gid cookies.

What java script library is dropping these cookies? _____

Open the _ga cookie. Take a screen shot of the Name, Content, Domain, Created and Expires.

What is the cookie lifetime? _____

Open the _gid cookie. Take a screen shot of the Name, Content, Domain, Created and Expires.

What is the cookie lifetime? _____

D2) Cookie analysis 2

You should see many cookies from www.officeworks.com.au. Select these.

Select the OW_STORE_POSTCODE cookie.

Explain which details might be of forensic interest.

Use your browser to go back to Officeworks and Set your preferred store to Bondi Junction.

Return to the cookies. Check that the postcode cookie updated.

Q2) Chrome Cookie Files – using the cmd line

If you are doing a post mortem analysis you do not want to use chrome as it will alter the cookie files.

We need to use cmd line tools instead. Here we use a built-in Windows (and Linux) tool called find.

On your Laptop, open File Explorer, select C:\. Set your file explorer to see hidden and system files.

(Click View, Folder and Search options. Select the View Tab. Change the settings for hidden and system files.)

Locate your chrome cookie file under C:\User. See Lecture slides. It should be large (MB).

Copy the Cookies file to C:\Forensics_YourName.

```
C:\Forensics_Graham>
```

Each student uses their own username.

You will need to create this folder.

Open a cmd window and CD to your C:\forensics_yourname folder.

Use find to search the strings in the Cookies file for Officeworks

Run find /? to see options.

Run find on Officeworks again, this time ignore case and count the number of hits. This number tells us two things. 1) The suspect visited the site and 2) a big number indicates lots of evidence.

Take a screen shot for your report, showing the command syntax and the count.

Advanced

We cannot see dates and data inside the cookies using find. If you think the website visit is of forensic interest, then switch to Linux.

Copy the Cookie file to your Linux desktop. (Or WSL on Windows 10 – see Readings.)

Open a Linux shell window.

Use the strings command to extract text from the Cookie file. Pipe this into grep and search for Officeworks.

Repeat, but this time display only the _ga cookie matches for Officeworks.

Take a screen shot for your report, showing the command syntax and the result.

Now search the cookie file for analytics using strings then grep.

What analytics website (if any) did you find? _____

Q3) Chrome history

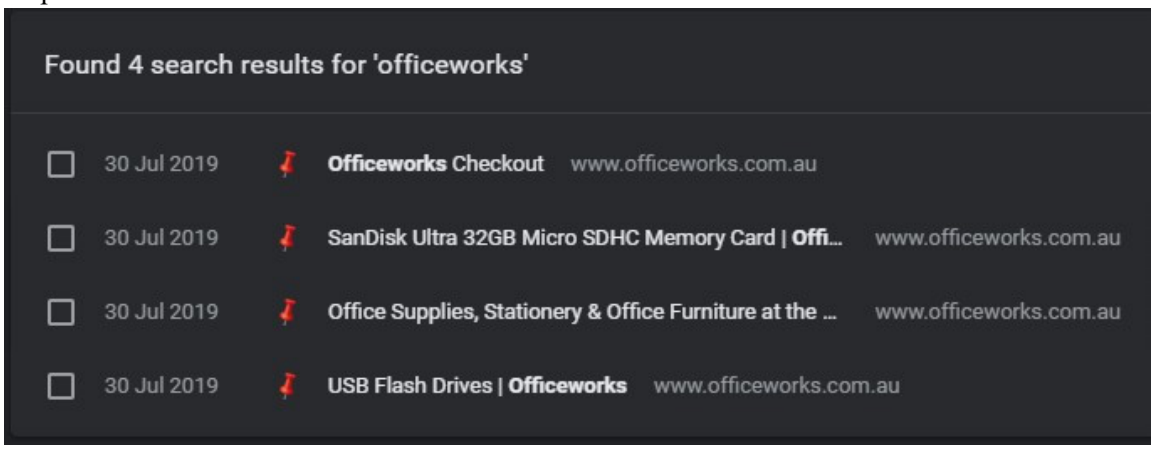
Select the chrome menu icon and then select history.

Note the forensic goldmine here.

Use Ctrl + F to search.

Search for Officeworks.

Note the http requests sorted by date and time, latest first. This is one way you can reconstruct the suspect's timeline



The history file is in the same disk location as the Cookies file. It is also a large file.

Copy this file to C:\Forensics_YourName

Use find to confirm your visit to "Officeworks"

Confirm your search for "sandisk"

Take a screen shot for your report.

Q3b) - Advanced. Copy the History file to your Linux Desktop. Open a shell window.

You can also use Windows 10 Subsystem for Linux, see Readings.

Use strings to extract the text from the History file and grep to search for 'sandisk'

Take a screenshot for your report.

Q4) Fingerprinting

Note here your Chrome Browser version __ (see Q1)

48436/32309

Week 03 Browser Files

4A) BrowserLeaks

Using your Laptop, open the Browserleaks website(https://browserleaks.com/) in Chrome.

a) Perform Ip Address detection.

What is your public ip address? _____

What is your ASN Number? _____

What does ASN mean? _____

Note TCP/IP Fingerprinting.

What is your OS? _____

Where is my IP? _____

What is your _ga cookie date code? _____ What is your _ga date? _____

b) Return to the https://browserleaks.com/ . Perform Canvas Fingerprinting

Include the probability ratios in your answers.

What is your OS platform and Version? _____

What is your Chrome browser Version? _____

Comment on how accurate is BrowserLeaks in determining your fingerprint.

_____

4B) Panopticlick

Using your Laptop, open the Panopticlick website(https://coveryourtracks.eff.org/) in Chrome.

Click the TEST YOUR BROWSER button.

48436/32309

Week 03 Browser Files

List any tests your browser passed. _____

Click Show full results.

What is your OS platform and Version? _____

What is your Chrome browser Version? _____

What is your Time zone? _____

Comment on how accurate is Panopticlick in determining your fingerprint.

_____

Upload.

Save the report as a pdf and upload.