48436/32309

Week 03 Browser Files Report

Upload this document as a pdf.

Name: Huynh Lam Student ID: 13264763 Date: 22/08/2021 Activity No.: Cmp1/03

Due Date:

Three days after the lab.

Q1) Chrome Cookie Files – using chrome

A) What is your **complete** chrome version number? 92.0.4515.131. Is it 32 or 64 bit? 64 bit

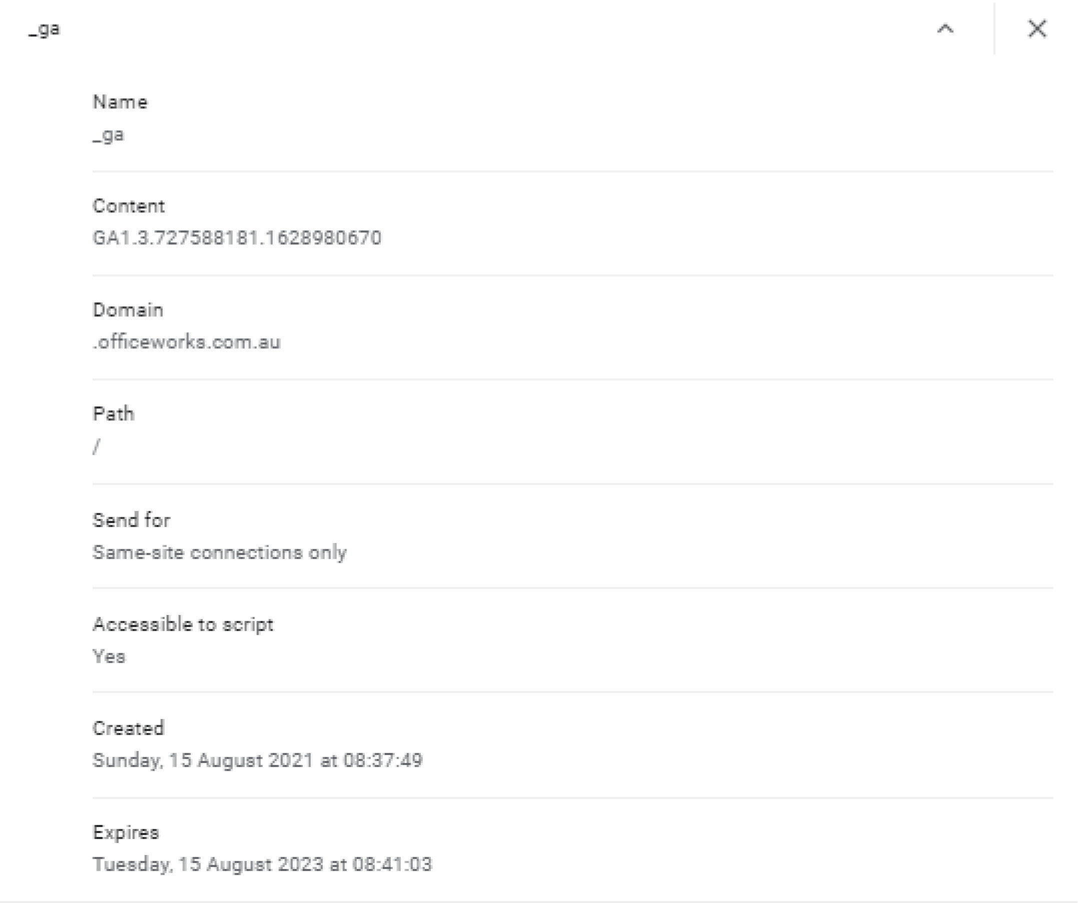
C) Note the 64GB SanDisk micro SDHC Product Code. SDSQUA464

D1) Cookie analysis 1

officeworks.com.au cookies.

What JavaScript library is dropping these cookies? analytics.jsdrops

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



_ga

Name
_ga

Content
GA1.3.727588181.1628980670

Domain
.officeworks.com.au

Path
/

Send for
Same-site connections only

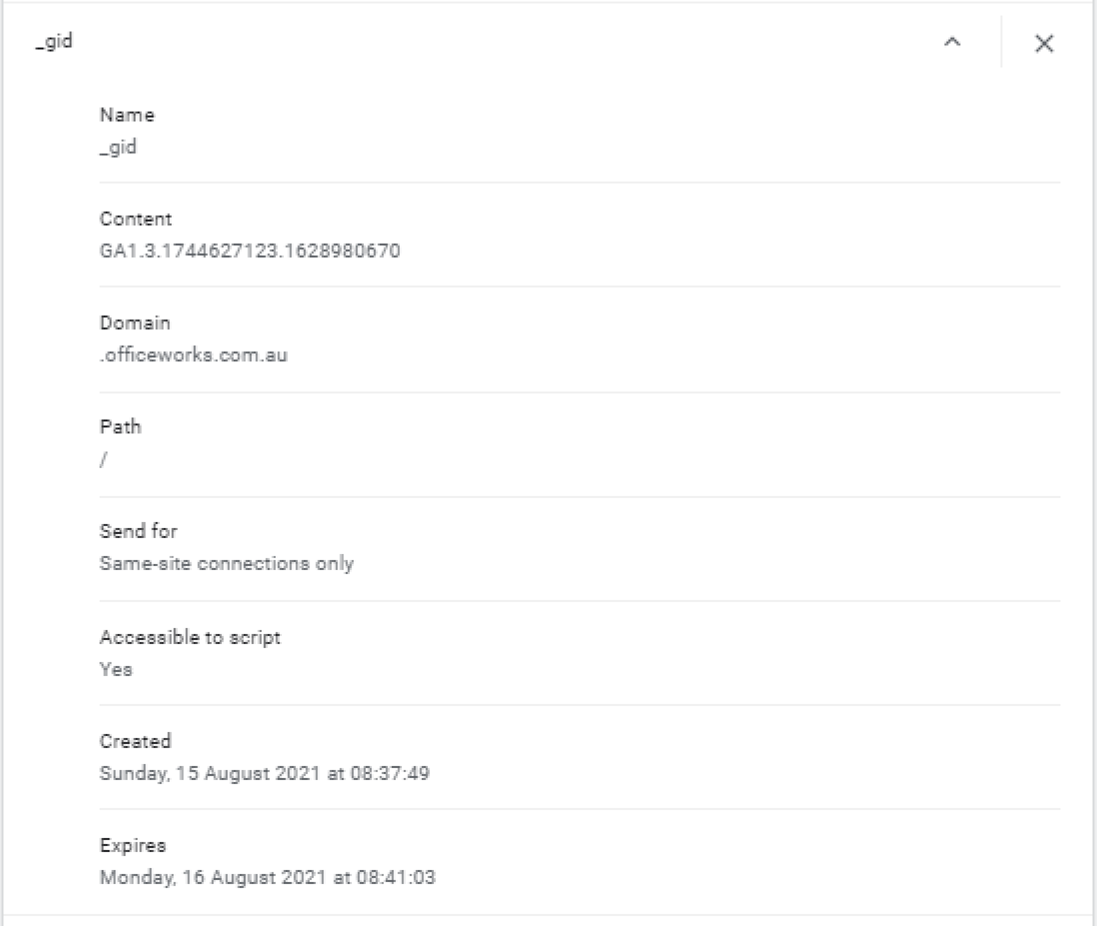
Accessible to script
Yes

Created
Sunday, 15 August 2021 at 08:37:49

Expires
Tuesday, 15 August 2023 at 08:41:03

What is the cookie lifetime? Lifetime starts on 15th August 2021 08:37:49 and ends on 15th August 2023 08:41:03 (2 years)

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



_gid

Name
_gid

Content
GA1.3.1744627123.1628980670

Domain
.officeworks.com.au

Path
/

Send for
Same-site connections only

Accessible to script
Yes

Created
Sunday, 15 August 2021 at 08:37:49

Expires
Monday, 16 August 2021 at 08:41:03

What is the cookie lifetime?

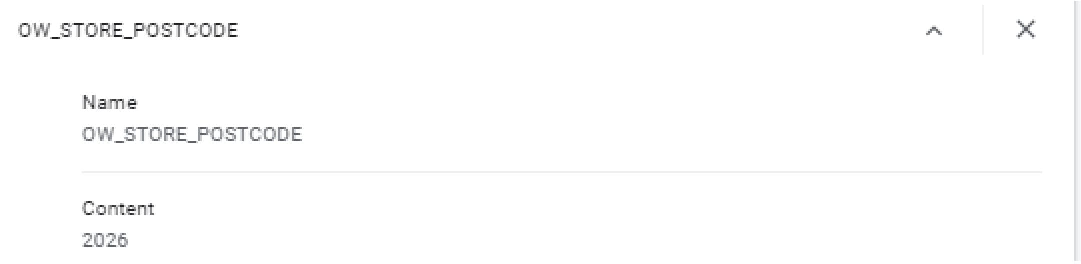
Lifetime starts on 15th August 2021 08:37:49 and ends on 16th August 2021 08:41:03 (1 day)

D2) Cookie analysis 2

www.officeworks.com.au cookies.

Select the OW_STORE_POSTCODE cookie.

Explain which details might be of forensic interest. The details of the content would be of forensic interest as this is where the user has set their store which gives information on the postcode of the Officeworks store. As you can see the image below this person has set their cookies to location of 2026 which corresponds to the Glebe store.



OW_STORE_POSTCODE

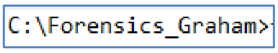
Name
OW_STORE_POSTCODE

Content
2026

Q2) Chrome Cookie Files – using the cmd line

Copy the Cookies file to C:\Forensics_YourName

On your laptop open a cmd window and CD to your C:\forensics folder.

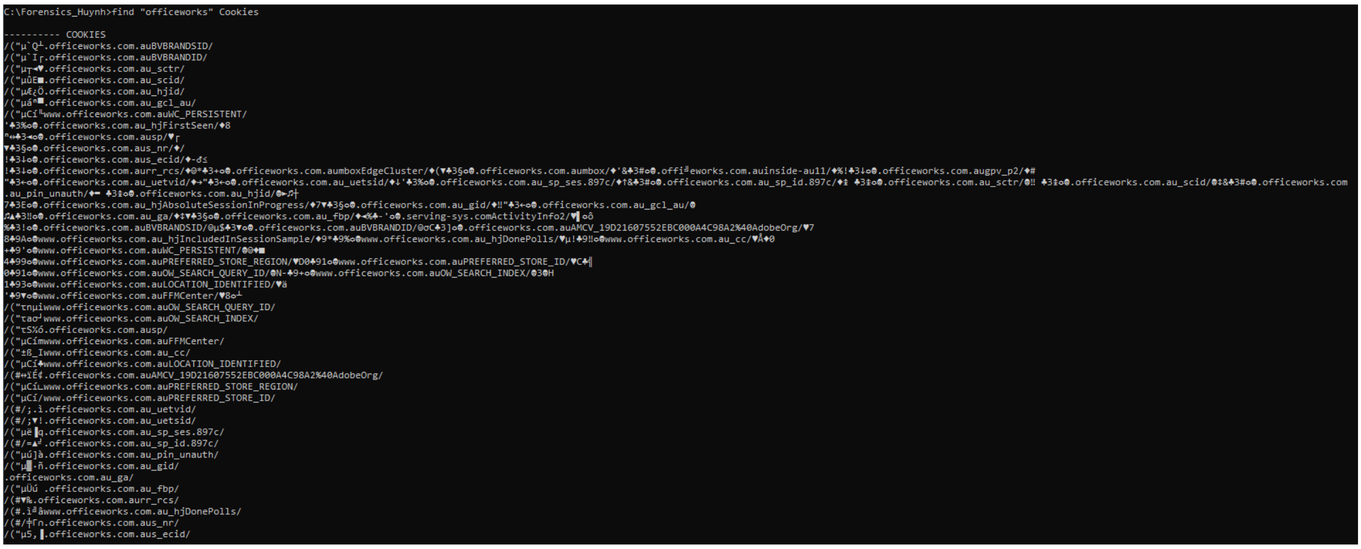


```
C:\Forensics_Graham>
```

Run find on the term Officeworks in the Cookies file again, this time ignore case and count the number of hits.

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

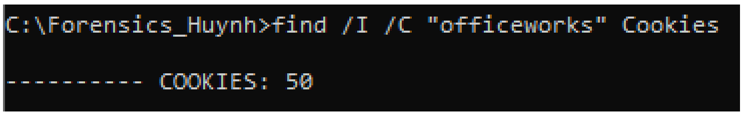
Command: find "officeworks" Cookies



```
C:\Forensics_Huynh>find "officeworks" Cookies

---------- COOKIES
/("µ`Q┴.officeworks.com.auBVBRANDSID/
/("µ`I┌.officeworks.com.auBVBRANDID/
/("µ┬◄♥.officeworks.com.au_sctr/
/("µûE■.officeworks.com.au_scid/
/("µÆ¿Ö.officeworks.com.au_hjid/
/("µáⁿ▀.officeworks.com.au_gcl_au/
/("µCí╙www.officeworks.com.auWC_PERSISTENT/
'♣3%☼●.officeworks.com.au_hjFirstSeen/♦8
ⁿ↔♣3◄☼●.officeworks.com.ausp/♥┌
▼♣3§☼●.officeworks.com.aus_nr/♦/
!♣3↓☼●.officeworks.com.aus_ecid/♦-δ≤
!♣3↓☼●.officeworks.com.aurr_rcs/♦◎*♣3+☼●.officeworks.com.aumboxEdgeCluster/♦(▼♣3§☼●.officeworks.com.aumbox/♦'&♣3#☼●.offi╝eworks.com.auinside-au11/♦%!♣3↓☼●.officeworks.com.augpv_p2/♦#
"♣3←☼●.officeworks.com.au_uetvid/♦→"♣3←☼●.officeworks.com.au_uetsid/♦↓'♣3%☼●.officeworks.com.au_sp_ses.897c/♦↑&♣3#☼●.officeworks.com.au_sp_id.897c/♦↨ ♣3↨☼●.officeworks.com.au_sctr/●‼ ♣3↨☼●.officeworks.com.au_scid/●↨&♣3#☼●.officeworks.com
.au_pin_unauth/♦═ ♣3↨☼●.officeworks.com.au_hjid/●►♫┼
7♣3E☼●.officeworks.com.au_hjAbsoluteSessionInProgress/♦7▼♣3§☼●.officeworks.com.au_gid/♦‼"♣3←☼●.officeworks.com.au_gcl_au/●
♫▲♣3‼☼●.officeworks.com.au_ga/♦↕▼♣3§☼●.officeworks.com.au_fbp/♦◄%♣-'☼●.serving-sys.comActivityInfo2/♥▌☼ô
%♣3!☼●.officeworks.com.auBVBRANDSID/◎µ$♣3▼☼●.officeworks.com.auBVBRANDID/◎σC♣3]☼●.officeworks.com.auAMCV_19D21607552EBC000A4C98A2%40AdobeOrg/♥7
8♣9A☼●www.officeworks.com.au_hjIncludedInSessionSample/♦9*♣9%☼●www.officeworks.com.au_hjDonePolls/♥µ!♣9‼☼●www.officeworks.com.au_cc/♥Å♦0
+♣9'☼●www.officeworks.com.auWC_PERSISTENT/●◎♦■
4♣99☼●www.officeworks.com.auPREFERRED_STORE_REGION/♥D0♣91☼●www.officeworks.com.auPREFERRED_STORE_ID/♥C♣╣
0♣91☼●www.officeworks.com.auOW_SEARCH_QUERY_ID/●N-♣9+☼●www.officeworks.com.auOW_SEARCH_INDEX/●3●H
1♣93☼●www.officeworks.com.auLOCATION_IDENTIFIED/♥ä
'♣9▼☼●www.officeworks.com.auFFMCenter/♥8☼┴
/("τnµiwww.officeworks.com.auOW_SEARCH_QUERY_ID/
/("τaσ┘www.officeworks.com.auOW_SEARCH_INDEX/
/("τS%ó.officeworks.com.ausp/
/("µCímwww.officeworks.com.auFFMCenter/
/("±ß_Iwww.officeworks.com.au_cc/
/("µCí♣www.officeworks.com.auLOCATION_IDENTIFIED/
/(#↔ïÉ¢.officeworks.com.auAMCV_19D21607552EBC000A4C98A2%40AdobeOrg/
/("µCíLwww.officeworks.com.auPREFERRED_STORE_REGION/
/("µCí/www.officeworks.com.auPREFERRED_STORE_ID/
/(#/;.ì.officeworks.com.au_uetvid/
/(#/;▼!.officeworks.com.au_uetsid/
/("µë▐q.officeworks.com.au_sp_ses.897c/
/(#/=▲╛.officeworks.com.au_sp_id.897c/
/("µú]à.officeworks.com.au_pin_unauth/
/("µ▓·ñ.officeworks.com.au_gid/
.officeworks.com.au_ga/
/("µÜú .officeworks.com.au_fbp/
/(#▼₧.officeworks.com.aurr_rcs/
/(#.ì╜âwww.officeworks.com.au_hjDonePolls/
/(#/╪Γn.officeworks.com.aus_nr/
/("µ5,▌.officeworks.com.aus_ecid/
```

Command: find /I /C "officeworks" Cookies



```
C:\Forensics_Huynh>find /I /C "officeworks" Cookies

---------- COOKIES: 50
```

Advanced

Copy the Cookies file to your Linux desktop (WSL on Windows 10).

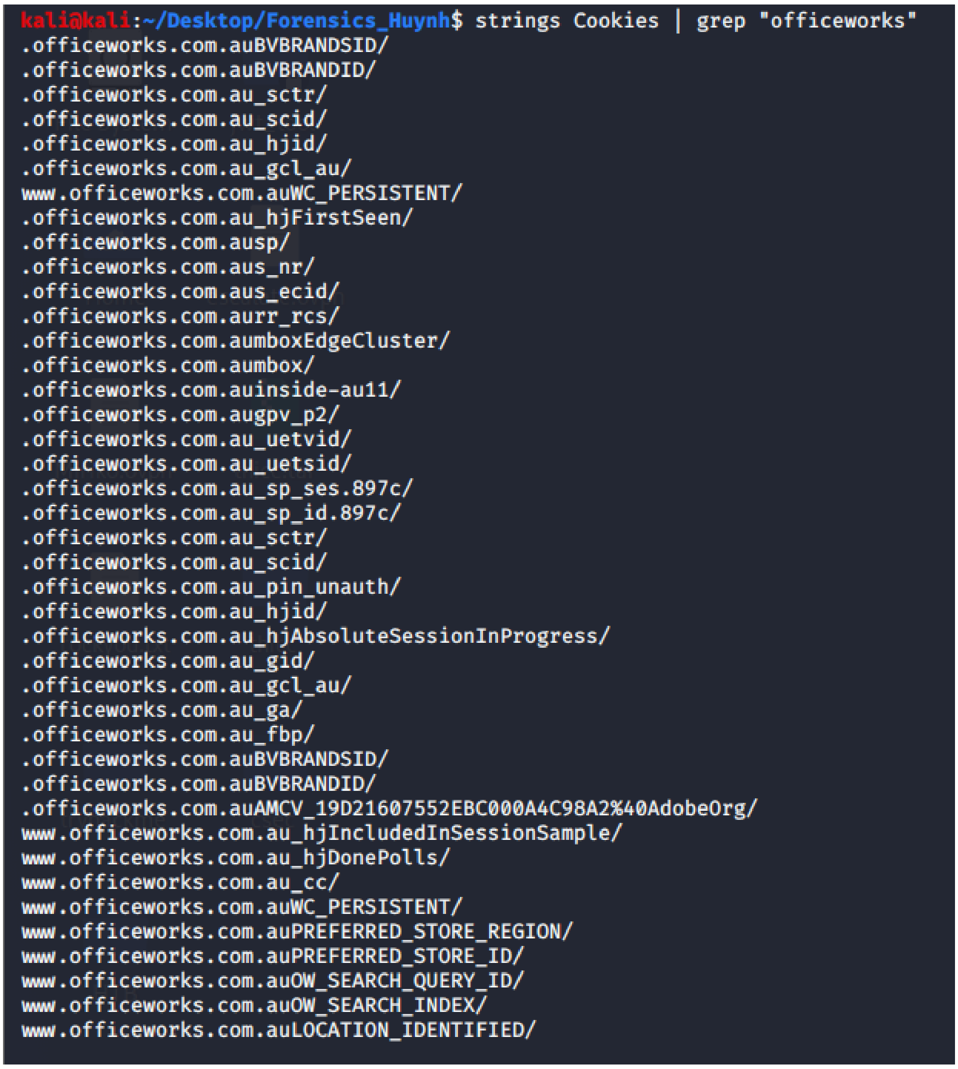
Open a Linux shell window.

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

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

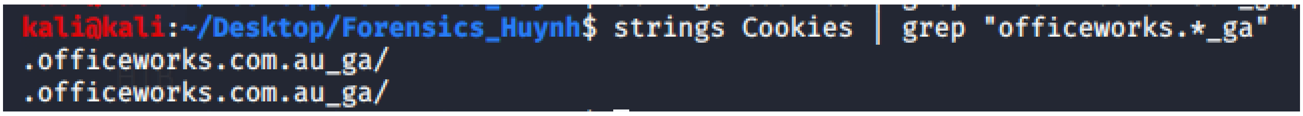
Take a screen shot for your report, showing the command syntax and the result.

Command: strings Cookies | grep "officeworks"



```
kali@kali:~/Desktop/Forensics_Huynh$ strings Cookies | grep "officeworks"
.officeworks.com.auBVBRANDSID/
.officeworks.com.auBVBRANDID/
.officeworks.com.au_sctr/
.officeworks.com.au_scid/
.officeworks.com.au_hjid/
.officeworks.com.au_gcl_au/
www.officeworks.com.auWC_PERSISTENT/
.officeworks.com.au_hjFirstSeen/
.officeworks.com.ausp/
.officeworks.com.aus_nr/
.officeworks.com.aus_ecid/
.officeworks.com.aurr_rcs/
.officeworks.com.aumboxEdgeCluster/
.officeworks.com.aumbox/
.officeworks.com.auinside-au11/
.officeworks.com.augpv_p2/
.officeworks.com.au_uetvid/
.officeworks.com.au_uetsid/
.officeworks.com.au_sp_ses.897c/
.officeworks.com.au_sp_id.897c/
.officeworks.com.au_sctr/
.officeworks.com.au_scid/
.officeworks.com.au_pin_unauth/
.officeworks.com.au_hjid/
.officeworks.com.au_hjAbsoluteSessionInProgress/
.officeworks.com.au_gid/
.officeworks.com.au_gcl_au/
.officeworks.com.au_ga/
.officeworks.com.au_fbp/
.officeworks.com.auBVBRANDSID/
.officeworks.com.auBVBRANDID/
.officeworks.com.auAMCV_19D21607552EBC000A4C98A2%40AdobeOrg/
www.officeworks.com.au_hjIncludedInSessionSample/
www.officeworks.com.au_hjDonePolls/
www.officeworks.com.au_cc/
www.officeworks.com.auWC_PERSISTENT/
www.officeworks.com.auPREFERRED_STORE_REGION/
www.officeworks.com.auPREFERRED_STORE_ID/
www.officeworks.com.auOW_SEARCH_QUERY_ID/
www.officeworks.com.auOW_SEARCH_INDEX/
www.officeworks.com.auLOCATION_IDENTIFIED/
```

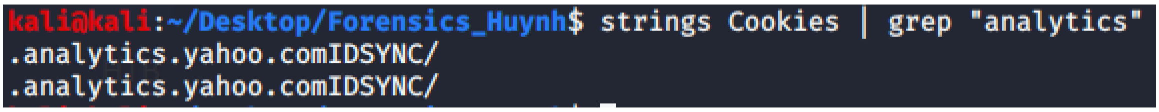
Command: strings Cookies | grep "officeworks.*_ga"



```
kali@kali:~/Desktop/Forensics_Huynh$ strings Cookies | grep "officeworks.*_ga"
.officeworks.com.au_ga/
.officeworks.com.au_ga/
```

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

Command: strings Cookies | grep"analytics"



```
kali@kali:~/Desktop/Forensics_Huynh$ strings Cookies | grep "analytics"
.analytics.yahoo.comIDSYNC/
.analytics.yahoo.comIDSYNC/
```

What analytics website (if any) did you find? There are analytics from There is analytics from yahoo which is Yahoo’s tracker.

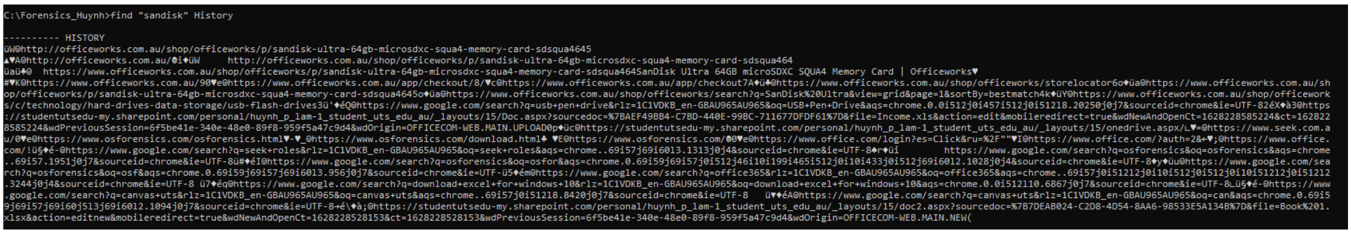
Q3) Chrome history

Copy the History file to C:\Forensics_YourName

Use find to confirm your search for "sandisk"

Take a screen shot for your report.

Command: find "sandisk" history



```
C:\Forensics_Huynh>find "sandisk" History

---------- HISTORY
üW@http://officeworks.com.au/shop/officeworks/p/sandisk-ultra-64gb-microsdxc-squa4-memory-card-sdsqua4645
▲♥A@http://officeworks.com.au/☻i♦üW     http://officeworks.com.au/shop/officeworks/p/sandisk-ultra-64gb-microsdxc-squa4-memory-card-sdsqua464
üaü♣@  https://www.officeworks.com.au/shop/officeworks/p/sandisk-ultra-64gb-microsdxc-squa4-memory-card-sdsqua464SanDisk Ultra 64GB microSDXC SQUA4 Memory Card | Officeworks♥
#♥K@https://www.officeworks.com.au/90♥e@https://www.officeworks.com.au/app/checkout/8/♥c@https://www.officeworks.com.au/app/checkout7A♦ü♣@https://www.officeworks.com.au/shop/officeworks/storelocator6o♦üa@https://www.officeworks.com.au/sh
op/officeworks/p/sandisk-ultra-64gb-microsdxc-squa4-memory-card-sdsqua4645o♦üa@https://www.officeworks.com.au/shop/officeworks/search?q=SanDisk%20Ultra&view=grid&page=1&sortBy=bestmatch4k♦üY@https://www.officeworks.com.au/shop/officework
s/c/technology/hard-drives-data-storage/usb-flash-drives3ü'♦éQ@https://www.google.com/search?q=usb+pen+drive&rlz=1C1VDKB_en-GBAU965AU965&oq=USB+Pen+Drive&aqs=chrome.0.0i512j0i457i512j0i512l8.20250j0j7&sourceid=chrome&ie=UTF-82éX♦à3@https
://studentutsedu-my.sharepoint.com/personal/huynh_p_lam-1_student_uts_edu_au/_layouts/15/Doc.aspx?sourcedoc=%7BAEF49BB4-C7BD-440E-99BC-711677DFDF61%7D&file=Income.xls&action=edit&mobileredirect=true&wdNewAndOpenCt=1628228585224&ct=162822
8585224&wdPreviousSession=6f5be41e-340e-48e0-89f8-959f5a47c9d4&wdOrigin=OFFICECOM-WEB.MAIN.UPLOAD0p♦üc@https://studentutsedu-my.sharepoint.com/personal/huynh_p_lam-1_student_uts_edu_au/_layouts/15/onedrive.aspx/∟♥=@https://www.seek.com.a
u/0♥e@https://www.osforensics.com/osforensics.html♥-♥_@https://www.osforensics.com/download.html♣ ♥E@https://www.osforensics.com/☻0♥e@https://www.office.com/login?es=Click&ru=%2F""♥I@https://www.office.com/?auth=2&←♥;@https://www.office.
com/!ü§♦é-@https://www.google.com/search?q=seek+roles&rlz=1C1VDKB_en-GBAU965AU965&oq=seek+roles&aqs=chrome..69i57j69i60l3.1313j0j4&sourceid=chrome&ie=UTF-8♠r♦üi        https://www.google.com/search?q=osforensics&oq=osforensics&aqs=chrome
..69i57.1951j0j7&sourceid=chrome&ie=UTF-8ü#♦éI@https://www.google.com/search?q=osforensics&oq=osfor&aqs=chrome.0.69i59j69i57j0i512j46i10i199i465i512j0i10i433j0i512j69i60l2.1028j0j4&sourceid=chrome&ie=UTF-8♦y♦üu@https://www.google.com/sea
rch?q=osforensics&oq=osf&aqs=chrome.0.69i59j69i57j69i60l3.956j0j7&sourceid=chrome&ie=UTF-ü5♦ém@https://www.google.com/search?q=office365&rlz=1C1VDKB_en-GBAU965AU965&oq=office365&aqs=chrome..69i57j0i512l2j0i10i512j0i512j0i10i512l2j0i512l2
.3244j0j4&sourceid=chrome&ie=UTF-8 ü7♦éq@https://www.google.com/search?q=download+excel+for+windows+10&rlz=1C1VDKB_en-GBAU965AU965&oq=download+excel+for+windows+10&aqs=chrome.0.0i512l10.6867j0j7&sourceid=chrome&ie=UTF-8∟ü§♦é-@https://www
.google.com/search?q=canvas+uts&rlz=1C1VDKB_en-GBAU965AU965&oq=canvas+uts&aqs=chrome..69i57j0i512l8.8420j0j7&sourceid=chrome&ie=UTF-8   ü▼♦éA@https://www.google.com/search?q=canvas+uts&rlz=1C1VDKB_en-GBAU965AU965&oq=can&aqs=chrome.0.69i5
9j69i57j69i60j5l3j69i60l2.1094j0j7&sourceid=chrome&ie=UTF-8→é\♦à;@https://studentutsedu-my.sharepoint.com/personal/huynh_p_lam-1_student_uts_edu_au/_layouts/15/doc2.aspx?sourcedoc=%7B7DEAB024-C2D8-4D54-8AA6-98533E5A134B%7D&file=Book%201.
xlsx&action=editnew&mobileredirect=true&wdNewAndOpenCt=1628228528153&ct=1628228528153&wdPreviousSession=6f5be41e-340e-48e0-89f8-959f5a47c9d4&wdOrigin=OFFICECOM-WEB.MAIN.NEW(
```

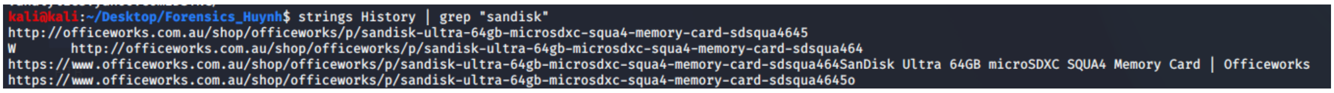
Q3b) Advanced

Copy the History file to your Linux desktop.

Use strings to extract the text and grep to search for ‘sandisk’.

Take a screenshot for your report.

Command: strings History | grep “sandisk”



```
kali@kali:~/Desktop/Forensics_Huynh$ strings History | grep "sandisk"
http://officeworks.com.au/shop/officeworks/p/sandisk-ultra-64gb-microsdxc-squa4-memory-card-sdsqua4645
W       http://officeworks.com.au/shop/officeworks/p/sandisk-ultra-64gb-microsdxc-squa4-memory-card-sdsqua464
https://www.officeworks.com.au/shop/officeworks/p/sandisk-ultra-64gb-microsdxc-squa4-memory-card-sdsqua464SanDisk Ultra 64GB microSDXC SQUA4 Memory Card | Officeworks
https://www.officeworks.com.au/shop/officeworks/p/sandisk-ultra-64gb-microsdxc-squa4-memory-card-sdsqua4645o
```

Q4) Fingerprinting

Note here your Chrome Browser version __ (see Q1)

4A) BrowserLeaks

Using your Laptop, open the Browserleaks website in Chrome.

a) Perform Ip Address detection.
What is your public ip address? 1.40.13.119

What is your AS Number? AS4804

What does ASN mean? Autonomous System Number (ASN) is a globally unique identifier that defines a group of one or more IP prefixes run by one or more network operators that maintain a single, clearly defined routing policy. These groups of IP prefixes are known as autonomous systems

Note TCP/IP Fingerprinting.
What is your OS? Windows (NT kernel)

Where is your IP? Blacktown

What is your _ga cookie date code? 1628983984 What is your _ga date? Your time zone: Sunday, August 15, 2021 9:33:04 AM GMT+10:00

b) Return to the Home Page. Perform Canvas Fingerprinting

Include the probability ratios in your answers.

What is your OS platform and version? Windows 3145/3252, Windows 10 2972/3252

What is your chrome browser version? Chromium 1910/3252

Comment on how accurate is BrowserLeaks in determining your fingerprint. BrowserLeaks is quite accurate in guessing the Operating system/version running and as well as the browser version which they don't have a specific option but the other category is accurate for my version. Their ratio rating for the OS seems very accurate, while the browser ratios are a bit far off each other.

4B) Panopticlick

Using your Laptop, open the Panopticlick website in Chrome.

Click the TEST YOUR BROWSER button.

List any tests your browser passed. Protecting you from fingerprinting, Your browser has a unique fingerprint

Click Show full results.

What is your OS platform and Version? Windows NT 10.0; Win64; x64

What is your Chrome browser Version? Chrome/92.0.4515.131

Week 03 Browser Files Report

What is your Time zone? TIME ZONE: Australia/Sydney

Comment on how accurate is Panopticlick in determining your fingerprint. Panopticlick accuracy is much higher than browser leaks. This is only based on the fact they have guessed my Operating system and exact browser version. There are no ratio checks shown, but has a more accurate output than browser leaks.

Upload Save this report as a pdf and upload.