48436/32309 Week 04 Network Packets and Wireshark

This week we will examine network servers and network packets for forensic evidence.

Q1) Web Server Forensics

A) See what Builtwith.com does in the Lecture slides week 3.

Run Builtwith against the Officeworks website.

Name two Analytics and Tracking tools detected that have usage that is still growing strongly (has not peaked).

_____

Two Content Delivery platforms are Akamai and CloudFront. Compare and contrast these two platforms.

Describe any growth peaks.

_____

One Content Management System used is Atlassian Cloud. What do you know about Atlassian?

_____

B) See what w3techs.com does in the Lecture slides week 3.

Run w3techs against the Officeworks website. (Click the Sites Tab.)

What is the Server side programming language used? _____

What is the Client side programming language used? _ __

What is the Web Server engine? _____

Who hosts this website? _____

C) IP details for Officeworks.

What is the IPv4 address? _ _____ What cmd line tool did you use? _____

Who owns this address? _____ What website did you use? _ _____ Where

is it located? _____

48436/32309 Week 04 Network Packets and Wireshark

Q2) DNS

Find a website that displays public dns servers in Australia.

_____

List here two public dns servers supplied by ISPs in the state of NSW.

List the owner, ip address, suburb and AS number. _____

8.8.8.8 is the dns for Google. Show here a cmd line lookup tool to name this IP. _____

What is the registered name of 8.8.8.8?_ ___

List two more dns with single digit IP addresses. List their registered name and the IPv4 number.

1)____ and 2)___

Q3) Network cookie collection

Here we will use Wireshark to capture evidence of a suspect visiting a website.

This is of limited value with **SSL** (encrypted) packets.

(Optional Advanced: To see more find an old website still using http or use an intercepting proxy such as Burp Suite.)

You need Wireshark installed on your laptop. If you would like a reminder on using Wireshark, look at the Wireshark warmup Lab in Canvas Readings for Week 4.

Part 1: Setup

Step 1: Set Cookies

Open the Chrome Web Browser. From the Chrome menu, select Settings.

Under Privacy and Security select Clear Browsing Data.

Select everything. Click Clear Data. This will force the server to send new cookies for Wireshark to capture.

Under Privacy and Security select Site Settings. Select Cookies and site data, Select Allow all cookies.

Now select See all cookies and site data.

Search for officeworks. There should be none. If there is, delete all data.

Return to your home page.

Step 2: Collect cookies

Note here the current date and time. _____ (Wireshark time stamps each packet collected.)

Start Wireshark. From the menu, select Capture, Options.

Select the active Interface to the internet. Click the Start Button, (a blue fin icon upper left). Minimise Wireshark.

In Chrome, repeat the Week 3 Lab Q1-B) Check cookie settings and Google search for USB Pen Drive.

Repeat the Week 3 Lab Q1-C) Add Chrome cookies

In Officeworks Search for SanDisk Ultra.

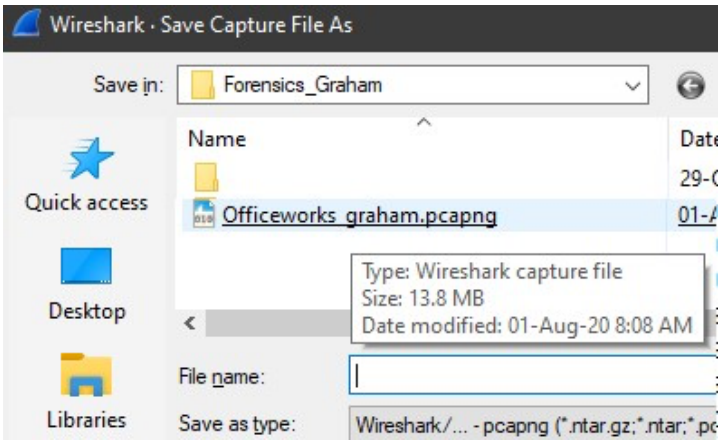
Add your item to your Officeworks Cart and Checkout. Confirm your item and Your Store is Glebe.

Stop Wireshark capture.

In Chrome, check that you have the same officeworks (lower case o) cookies as in Week 3.

Part 2: Evidence Acquisition

We have been asked to find details of the suspect's visits to Officeworks in the captured network packets.



Step 1: Collect the evidence and the analysis files.

Use File Explorer to use or make a C:\Forensics_Yourname folder.

In Wireshark, select File, Save As and save the capture as **Officeworks_yourname** of type **pcapng** into this C:\Forensics_yourname folder.

Part 3: Viewing Website visits with Wireshark

Open your saved Wireshark session, **Officeworks_yourname.pcapng**

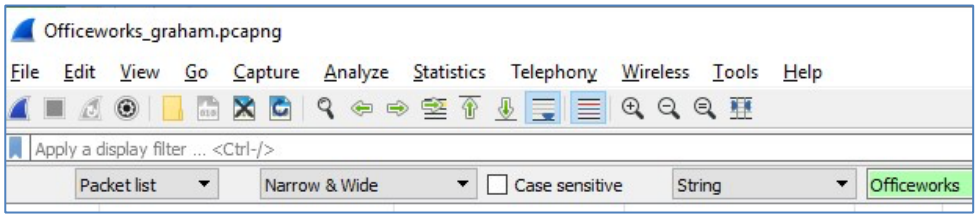
From the menu, select View, Time Display Format. Select Date and Time of Day.

Now search for the visit to the Officeworks web server. From the menu, click Edit, Find Packet.

Select Packet List and String. Enter the search term. Make sure you are at the top of the list of packets. (You can see packet #1).

48436/32309 Week 04 Network Packets and Wireshark

A) Click the Find button at right to search for the string **Officeworks**.



Select the matching packet in the Packet list window pane. (Arrow at left.).

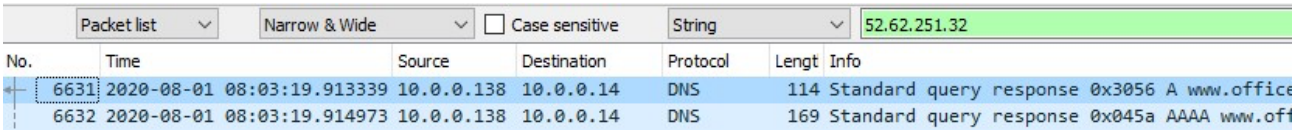
Take a screenshot for your report. Include the date and time and the matching text. (yours will be different.)

B) In your cmd window, use the nslookup tool to find the ipv4 address for officeworks.com.au. Yours may be different.

```
C:\Users\graha>nslookup officeworks.com.au
Server:  mygateway
Address:  10.0.0.138

Non-authoritative answer:
Name:    officeworks.com.au
Addresses:  52.62.251.32
          3.105.41.131
```

Locate the first packet with this ip address. (Search from the top. Packet #1)



Take a screenshot for your report. Include the packet number, date and time, destination address and info. (yours will be different.)

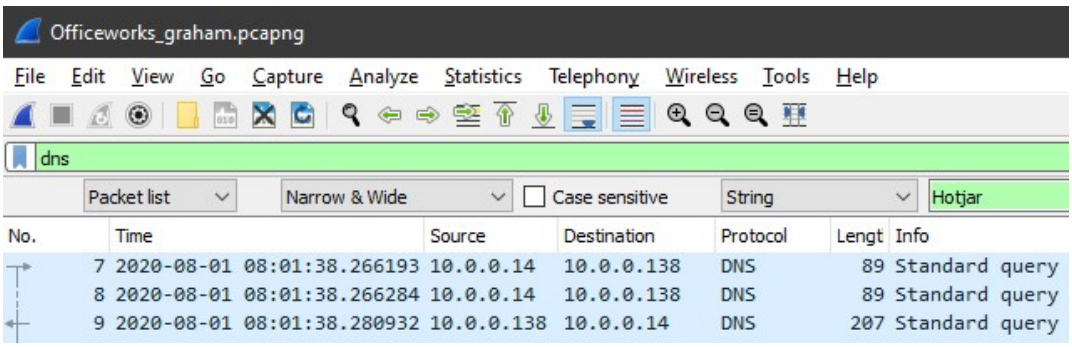
What is the packet protocol? _____

C) Tracking cookies. (refer to Q1A)

We want to find the IPv4 address of the tracking cookie used. We will filter the packets by dns to remove unwanted packets (noise.)

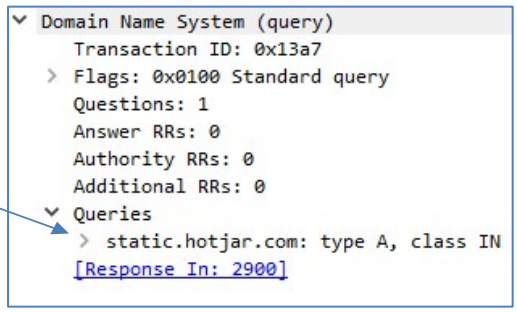
Enter dns as the display filter top left. Click the find arrow top right. Confirm you only see dns packets.

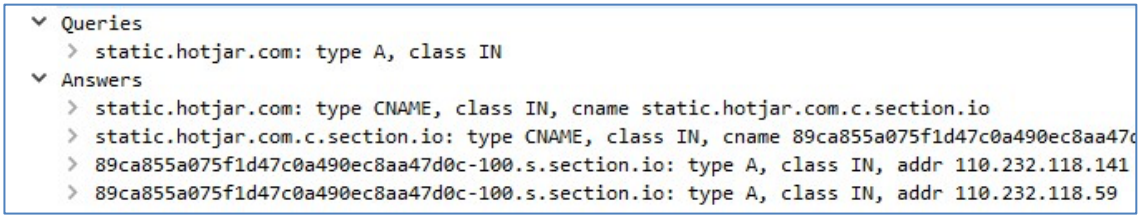
48436/32309 Week 04 Network Packets and Wireshark



Use a Packet list String search to find the DNS type A request for the following Analytics and Tracking (A&T) tools. Search from the top each time.

Expand the packet detail window. Expand the dns request. Click the link to see the dns response.





Include the packet number and the IPv4 address. One address each is sufficient. (If the response is static write static with the ip address returned.)

- Hotjar ___static_____
- Bazaarvoice _____

Find two more A&T cookies.

- _____ _____
- _____ _____

Can you find evidence of A Content Delivery Network (CDN) hosting? ____ If so which?

_____

Can you find evidence of a Content Management System (CMS) cookie? ___ If so which?

_____

Would you still see these cookies in wireshark while using the Incognito browser?

Close Wireshark.

Q4) Tcpdump filters

In Q3, we saw how to use Wireshark to analyse a Wireshark pcap dump file.

We can also dump packets with a command line tool.

This allows us to watch a suspect remotely and start capturing packets without the suspect's knowledge.

We can use the packet capture tool that comes with wireshark called dumpcap.exe.

(You need some wireshark dlls as well, see https://www.winpcap.org/install/)

The capture tool that comes with Linux is called tcpdump. You do not have rights to capture in the UTS Lab or WSL but you can run tcpdump on your own Linux or MacOS box.

Here we use the Windows version called Windump.
Copy Windump from Canvas to your C:\Forensics_yourname folder.

Run your Windows 10 cmd as administrator. Cd to your C:\Forensics_yourname

folder. Check your interfaces with windump -D

```
C:\Forensics_graham>WinDump.exe -D
1.\Device\NPF_{531346A2-CC55-4A62-94BD-560F5B207B1F} (Intel(R) PRO/1000 MT Network
```

Note the Ethernet interface, here number 1. We set the interface using the -i flag.

a) Run windump with the right interface (-i1 perhaps) and confirm you see packets.

   Stop the capture with Ctrl +C.

b) Set the filter to capture only icmp (-i1 icmp) and then in another shell, ping your gateway.

   Take a screen shot of the 8 icmp packets for your report. You may have to extend your shell window to stop word wrap. Stop the capture again.

c) Set the filter to **capture dns**.

We want to prove or deny that the suspect searched for or was referred to Officeworks, so we capture 20 packets to see where the browser goes. Start Windump.

windump –i1 –n -c20 udp port 53

Now open a Windows 10 browser and go to Officeworks.com.au Take

a screen shot of the Officeworks dns packets for your report.

Explain the extra websites in the list.

Q5) Optional Extra – whois – no upload

Open your shell terminal on your Linux Box (Either UTS workstation or Windows 10 WSL.)

Enter the following:

whois $(curl -s ifconfig.me/ip) (You may need to install whois)

Wait several seconds for a reply.

Explain the command line. _____

What is the purpose of the ip address that is used here? Hint see the Startup module labs.

_____

Upload

Upload your report as a pdf.