48436/32309 Week 04 Network Packets and Wireshark Report

Upload this document as a pdf.

Name: Huynh Lam Student ID: 13264763 Date: 28/08/2021
Activity No.: Cmp1/03

Due Date:

Three days after the lab.

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).

- Adobe Dynamic Tag Management Usage Statistics
- LinkedIn Insights Usage Statistics

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

Describe any growth peaks.

- Both companies have a declining graph after hitting their peeks. However, CloudFront had a bit more stable decline than Akamai which had 2 declines. CloudFront revenue is performing better than Akamai and in Australia, CloudFront is the 5th most popular in content delivery platforms

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

- Atlassian is one of the big leading technology companies in Australia and their cloud usage statistics have been soaring.

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? PHP

What is the Client side programming language used? JavaScript

What is the Web Server engine? Nginx

48436/32309 Week 04 Network Packets and Wireshark Report

Who hosts this website? Amazon

C) IP details for Officeworks.

What is the IPv4 address? 13.239.126.216 or 52.65.120.234 What cmd line tool did you use? nslookup

Who owns this address? Amazon Technologies What website did you use? https://dnschecker.org/ip-whois-lookup.php

Where is it located?

Address: 410 Terry Ave N.

City: Seattle

StateProv: WA

PostalCode: 98109

Country: US

Q2) DNS

Find a website that displays public dns servers in Australia.

https://public-dns.info/nameserver/au.html

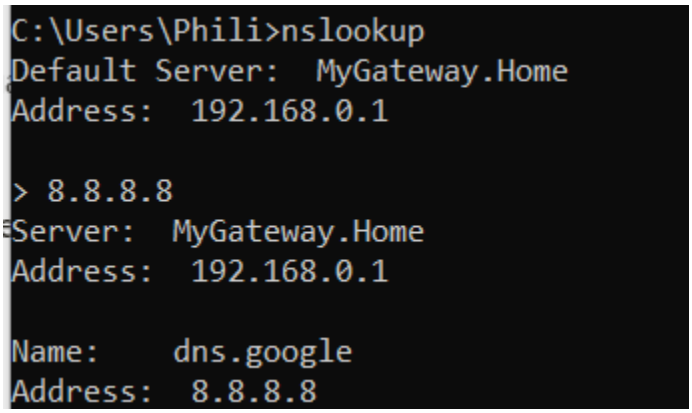
List here two public dns servers supplied by ISPs in the state of NSW.

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

- Mammoth Media Pty Ltd, 43.229.62.192, Macquarie Park, 133159
- TEFINCOM S.A, 103.86.96.100, Sydney, 136787

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

48436/32309 Week 04 Network Packets and Wireshark Report



What is the registered name of 8.8.8.8? dns.google

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

- 1.1.1.1 CloudFlareNet
- 1.0.0.3 CloudFlareNet

Q3) Network cookie collection

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

Part 1: Setup

Clear cookies, Set Cookies, Collect cookies. Do all this.

Part 2: Acquisition

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**.

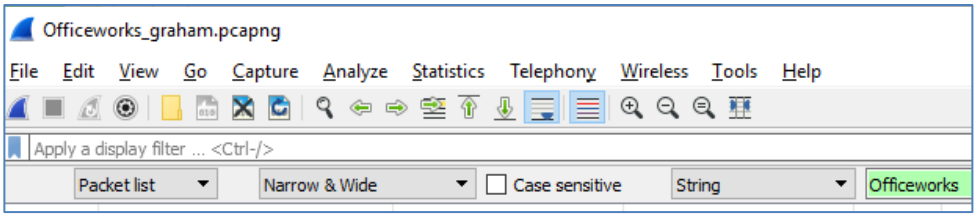
From the menu, select View, Time Display Format. Select Date and Time of Day.

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

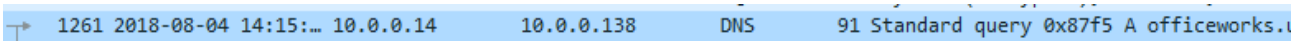
48436/32309 # Week 04 Network Packets and Wireshark Report

Select String and Packet List.

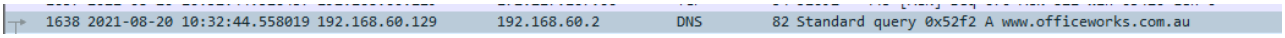
A) Search for the string **Officeworks**.



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.)

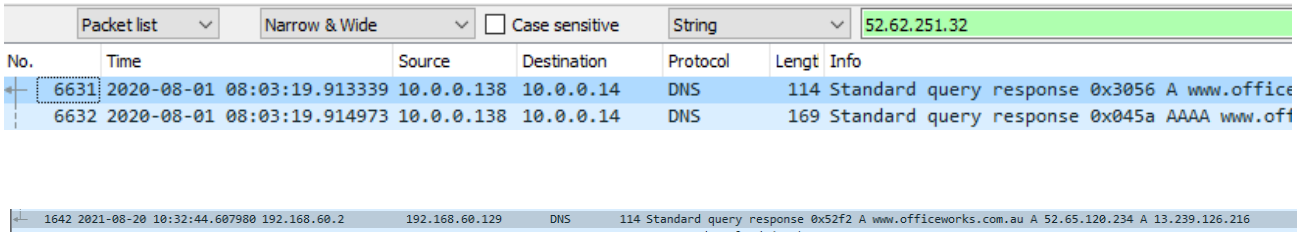


B) In your cmd window, use the nslookup tool to find the ipv4 address for officeworks.com.au

Name: officeworks.com.au Address: 52.62.251.32 or similar.

Locate the first packet with this ip address. (Search from the start).

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



What is the packet TCP/IP protocol? DNS

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.

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 Packet Number: 5764 static: 99.86.212.40
- Bazaarvoice Packet Number: 7663 Address: 13.226.107.40
  Find two more A&T cookies.
- EveresTech Packet Number: 2739 Address 13.229.0.102
- Inside-graph Packet Number: 3816 Address: 104.18.30.173

Can you find evidence of a Content Delivery Network (CDN) hosting? Yes

If so which? Akamai

Can you find evidence of A Content Management System (CMS) cookie? Yes

If so which? Contentful

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

Yes, because incognito mode only removes the activity's history traces rather than deleting incoming and outgoing traffic.

Close Wireshark.

Q4) Tcpdump filters

Check your interfaces with windump -D

a) Run windump with the right interface and confirm you see packets.

b) Set the filter to **capture only icmp** and then in another window, ping your gateway.

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

```
C:\Forensics_Huynh>windump -i1 icmp
windump: listening on \Device\NPF_{D72799D2-FCDF-4FB3-AD41-CD5FA3A4BF2A}
11:28:27.153630 IP DESKTOP-LD37IOO.localdomain > 192.168.60.2: ICMP echo request, id 1, seq 5, length 40
11:28:27.153887 IP 192.168.60.2 > DESKTOP-LD37IOO.localdomain: ICMP echo reply, id 1, seq 5, length 40
11:28:28.174887 IP DESKTOP-LD37IOO.localdomain > 192.168.60.2: ICMP echo request, id 1, seq 6, length 40
11:28:28.175502 IP 192.168.60.2 > DESKTOP-LD37IOO.localdomain: ICMP echo reply, id 1, seq 6, length 40
11:28:29.219872 IP DESKTOP-LD37IOO.localdomain > 192.168.60.2: ICMP echo request, id 1, seq 7, length 40
11:28:29.220481 IP 192.168.60.2 > DESKTOP-LD37IOO.localdomain: ICMP echo reply, id 1, seq 7, length 40
11:28:30.252258 IP DESKTOP-LD37IOO.localdomain > 192.168.60.2: ICMP echo request, id 1, seq 8, length 40
11:28:30.252810 IP 192.168.60.2 > DESKTOP-LD37IOO.localdomain: ICMP echo reply, id 1, seq 8, length 40
```

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

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

Now open a browser and go to Officeworks.com.au

Take a screen shot of the Officeworks dns packets for your report. Yours will be different.

```
C:\Forensics_Huynh>windump -i1 -n -c20 udp port 53
windump: listening on \Device\NPF_{D72799D2-FCDF-4FB3-AD41-CD5FA3A4BF2A}
11:31:41.168091 IP 192.168.60.129.52920 > 192.168.60.2.53:  51240+ A? officeworks.com.au. (36)
11:31:41.196272 IP 192.168.60.2.53 > 192.168.60.129.52920:  51240 2/0/0 A 13.239.126.216, (68)
11:31:41.344713 IP 192.168.60.129.55678 > 192.168.60.2.53:  56433+ A? www.officeworks.com.au. (40)
11:31:41.360522 IP 192.168.60.2.53 > 192.168.60.129.55678:  56433 2/0/0 A[|domain]
11:31:41.523470 IP 192.168.60.129.59967 > 192.168.60.2.53:  22715+ A? cdnjs.cloudflare.com. (38)
11:31:41.543858 IP 192.168.60.2.53 > 192.168.60.129.59967:  22715 2/0/0 A 104.16.18.94[|domain]
11:31:41.597410 IP 192.168.60.129.53568 > 192.168.60.2.53:  48300+ A? images.officeworks.com.au. (43)
11:31:41.614684 IP 192.168.60.2.53 > 192.168.60.129.53568:  48300 2/0/0[|domain]
11:31:41.632579 IP 192.168.60.129.55924 > 192.168.60.2.53:  56177+ A? polyfill.io. (29)
11:31:41.651381 IP 192.168.60.2.53 > 192.168.60.129.55924:  56177 4/0/0 A 151.101.1.26,[|domain]
11:31:41.889196 IP 192.168.60.129.61417 > 192.168.60.2.53:  30592+ A? images.ctfassets.net. (38)
11:31:41.935747 IP 192.168.60.2.53 > 192.168.60.129.61417:  30592 6/0/0 CNAME[|domain]
11:31:42.454635 IP 192.168.60.129.64959 > 192.168.60.2.53:  15451+ A? content-autofill.googleapis.com. (49)
11:31:42.475377 IP 192.168.60.2.53 > 192.168.60.129.64959:  15451 1/0/0 (65)
11:31:42.942937 IP 192.168.60.129.61331 > 192.168.60.2.53:  41085+ A? officeworks.tt.omtrdc.net. (43)
11:31:42.959564 IP 192.168.60.2.53 > 192.168.60.129.61331:  41085 4/0/0[|domain]
11:31:43.343640 IP 192.168.60.129.57456 > 192.168.60.2.53:  29637+ A? mboxedge36.tt.omtrdc.net. (42)
11:31:43.364034 IP 192.168.60.2.53 > 192.168.60.129.57456:  29637 4/0/0 A[|domain]
11:31:43.693017 IP 192.168.60.129.52606 > 192.168.60.2.53:  58524+ A? au11-tracker.inside-graph.com. (47)
11:31:43.716480 IP 192.168.60.2.53 > 192.168.60.129.52606:  58524 3/0/0[|domain]
20 packets captured
2173 packets received by filter
0 packets dropped by kernel
```

Explain the extra websites in the list.

- The Cloudflare website is a free and open-source CDN service which make it faster and easier to load library files on your websites
- polyfill.io is a piece of code (usually JavaScript on the Web) used to provide modern functionality on older browsers that do not natively support it.
- mboxedge36tt.omtrdc.net marketing box, which is an area on a web page used by Adobe Target to show different content to visitors in a campaign.
- au11-tracker.inside-graph.com is a tracking tool

--------- ----------

Q5) whois

Explain the command line.

- whois: WHOIS is a query and response protocol that is widely used for querying databases that store the registered users of an Internet resource, such as a domain name or an IP address block
- curl: CURL is a command-line tool to transfer data to or from a server, using any of the supported protocols (HTTP, FTP, IMAP, POP3, SCP, SFTP, SMTP, TFTP, TELNET, LDAP or FILE)
- ifconfig.me/ip: ifconfig.me is a web service that displays information about your connection, including your public IP address, hostname and User-Agent string

48436/32309 # Week 04 Network Packets and Wireshark Report

When combining the commands (curl -s ifconfig.me/ip) together they will get your remote return your remote IP address and Host as seen by other users online. An addition of whois before this command will search and identify who owns a domain of the IP address and how to get in contact with them.

What is the return ip address of ifconfig.me/ip?

This returns my public IP address which is 1.40.13.119

Upload

Upload your report as a pdf.