2024-08-15 - TRAFFIC ANALYSIS EXERCISE ANSWERS

Link to the exercise:

- https://www.malware-traffic-analysis.net/2024/08/15/index.html

Links to some tutorials I've written that should help with this exercise:

- Wireshark Tutorial: Changing Your Column Display
- Wireshark Tutorial: Identifying Hosts and Users
- Wireshark Tutorial: Display Filter Expressions
- Wireshark Tutorial: Exporting Objects from a Pcap

ENVIRONMENT:

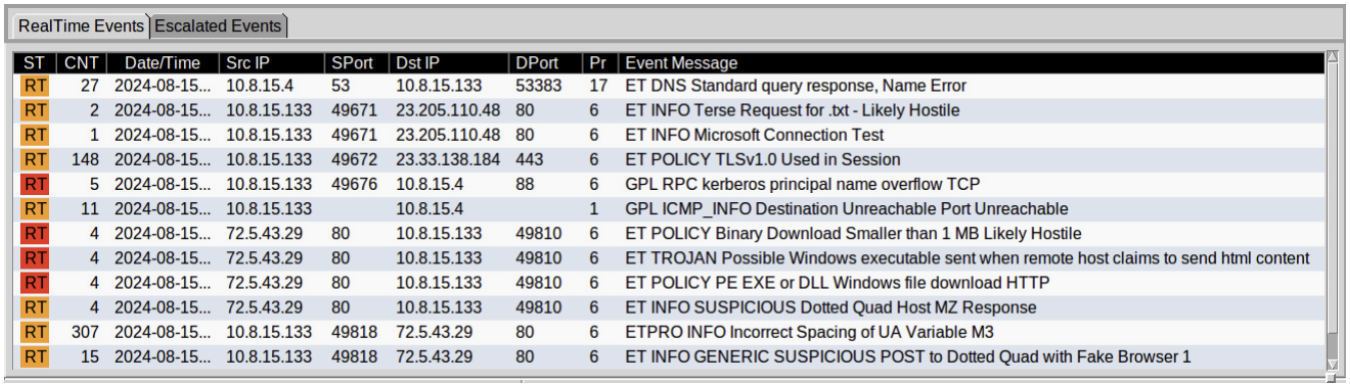
- LAN segment range: `10.8.15.0/24` (`10.8.15.0` through `10.8.15.255`)
- Domain: `lafontainebleu.org`
- AD environment name: `LAFONTAINEBLEU`
- Domain Controller: `10.8.15.4` - `WIN-JEGJIX7Q9RS`
- LAN segment gateway: `10.8.15.1`
- LAN segment broadcast address: `10.8.15.255`

BACKGROUND:

- A Windows host was infected, and it seems to be from WarmCookie malware.

TASK:

- Write an incident report based on traffic from the packet capture (pcap) and the alerts. Extract any malware from the pcap and provide files hashes in the report.



RealTime Events | Escalated Events

ST	CNT	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	27	2024-08-15...	10.8.15.4	53	10.8.15.133	53383	17	ET DNS Standard query response, Name Error
RT	2	2024-08-15...	10.8.15.133	49671	23.205.110.48	80	6	ET INFO Terse Request for .txt - Likely Hostile
RT	1	2024-08-15...	10.8.15.133	49671	23.205.110.48	80	6	ET INFO Microsoft Connection Test
RT	148	2024-08-15...	10.8.15.133	49672	23.33.138.184	443	6	ET POLICY TLSv1.0 Used in Session
RT	5	2024-08-15...	10.8.15.133	49676	10.8.15.4	88	6	GPL RPC kerberos principal name overflow TCP
RT	11	2024-08-15...	10.8.15.133		10.8.15.4		1	GPL ICMP_INFO Destination Unreachable Port Unreachable
RT	4	2024-08-15...	72.5.43.29	80	10.8.15.133	49810	6	ET POLICY Binary Download Smaller than 1 MB Likely Hostile
RT	4	2024-08-15...	72.5.43.29	80	10.8.15.133	49810	6	ET TROJAN Possible Windows executable sent when remote host claims to send html content
RT	4	2024-08-15...	72.5.43.29	80	10.8.15.133	49810	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	4	2024-08-15...	72.5.43.29	80	10.8.15.133	49810	6	ET INFO SUSPICIOUS Dotted Quad Host MZ Response
RT	307	2024-08-15...	10.8.15.133	49818	72.5.43.29	80	6	ETPRO INFO Incorrect Spacing of UA Variable M3
RT	15	2024-08-15...	10.8.15.133	49818	72.5.43.29	80	6	ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1

Shown above: Screenshot of alerts from the infection.

2024-08-15 - TRAFFIC ANALYSIS EXERCISE ANSWERS

ANSWER (EXAMPLE OF AN INCIDENT REPORT):

Executive Summary:

- On Thursday 2024-08-15 at approximately 00:11 UTC, a Windows host used by Pierce Lucero was infected with WarmCookie malware.

Victim Details:

- Host name: `DESKTOP-H8ALZBV`
- IP address: `10.8.15.133`
- MAC address: `00:1c:bf:03:54:82`
- Windows user account name: `plucero`

Indicators of Compromise (IOCs):

ZIP download:

`104.21.55.70:80 – **quote.checkfedexexp.com** – GET /managements?16553a25e45250a41fd5&endeds=MIGpq&JStx=59bf050d37df88a9-ade43358-eaa1220b-0571422b-0f33e6aa150e86bafd0ed4&Ld=9d7502d88d752a27b1d00587309184b5a215`

Follow-up download (unknown content):

`172.67.170.169:443 – https://**business.checkfedexexp.com**/data-privacy?zj=ZzqRKxVRQ&pOd=GEokiOXFwH&sourcedp=tQMQJlIo&Tfocontent=IxGTZjXqxJ&Jr_cid=9464552&L=8174388`

DLL download:

`http://**72.5.43.29**/data/0f60a3e7baecf2748b1c8183ed37d1e4`

POST-infection traffic:

`72.5.43.29:80 – **72.5.43.29** – POST /`
`72.5.43.29:80 – **72.5.43.29** – GET /`

2024-08-15 - TRAFFIC ANALYSIS EXERCISE ANSWERS

Downloaded ZIP archive SHA256 hash:

`798563fcf7600f7ef1a35996291a9dfb5f9902733404dd499e2e736ea1dc6fc5`
File size: 2,767,804 bytes
File name: `Invoice 876597035_003.zip`

Extracted JS file SHA256 hash:

`dab98819d1d7677a60f5d06be210d45b74ae5fd8cf0c24ec1b3766e25ce6dc2c`
File size: 6,990,020 bytes
File name: `Invoice-876597035-003-8331775-8334138.js`

Downloaded DLL file SHA256 hash:

`b7aec5f73d2a6bbd8cd920edb4760e2edadc98c3a45bf4fa994d47ca9cbd02f6`
File size: 159,232 bytes
File type: PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Run method: `rundll32` *[filename]*`,Start`
Reference DLL run method: https://www.elastic.co/security-labs/dipping-into-danger
Any.Run analysis: https://app.any.run/tasks/5d1f09a9-dc83-4070-bd8b-4c9a593fc572

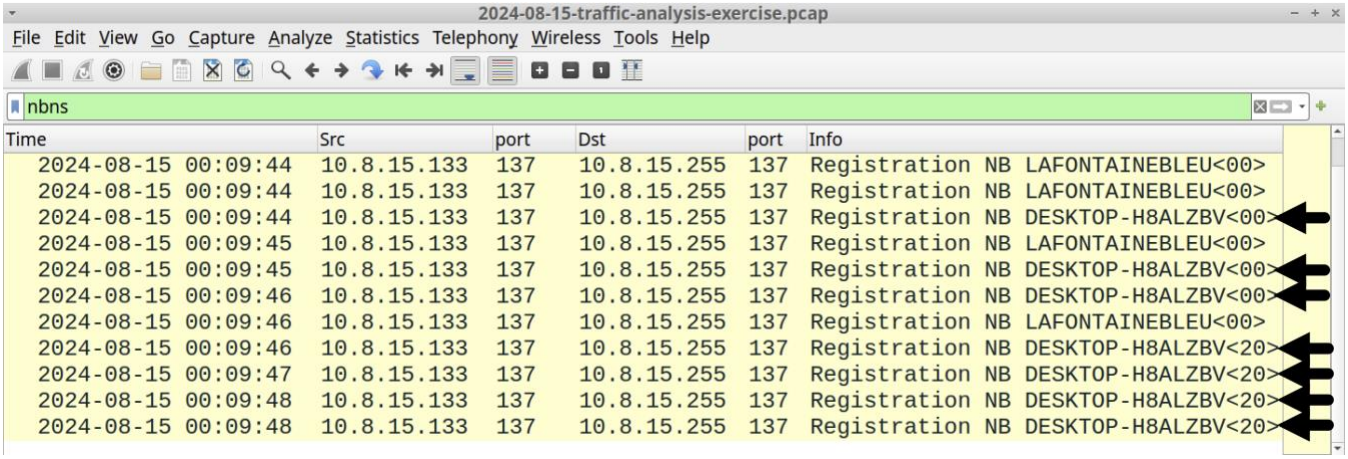
HINTS:

Note: These hints assume you've set up Wireshark according to the tutorials listed at the beginning of this document.

Of note, the common internal, non-routable IPv4 address for all of the alerts is `10.8.15.133`. To find further victim information, use the Identifying Hosts and Users Wireshark tutorial I wrote.

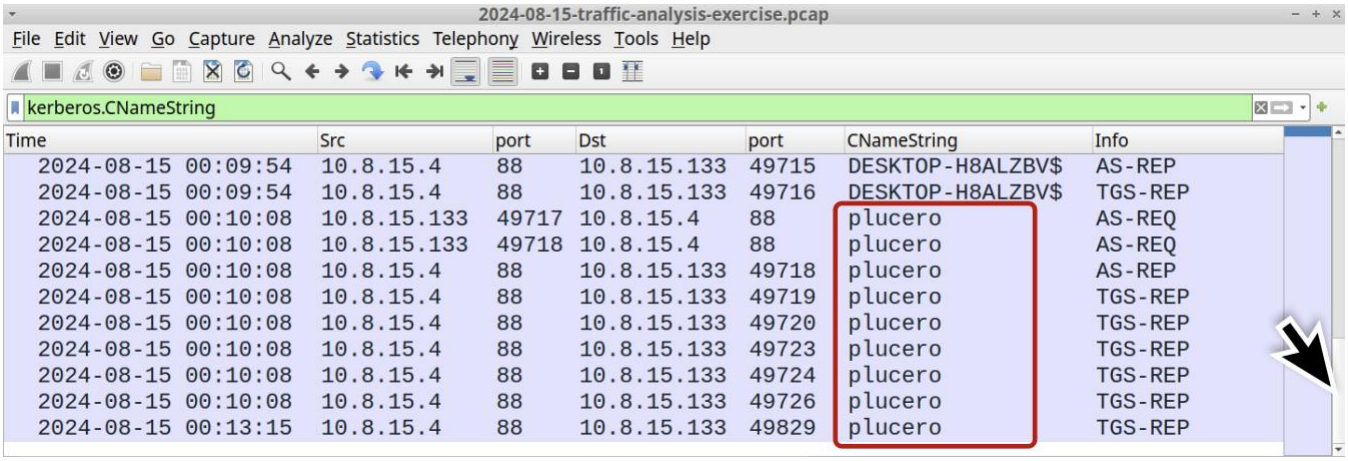
For example, you can filter on `nbns` in Wireshark to quickly find the host name of the infected Windows host at `10.8.15.133`.

2024-08-15 - TRAFFIC ANALYSIS EXERCISE ANSWERS



Shown above: Finding the windows host name by filtering on NBNS traffic.

If you've set up your column display according to my directions in the Identifying Hosts and Users Wireshark tutorial, you can filter on Kerberos.CNameString and find the Windows user account name `plucero` associated with `10.8.15.133`.

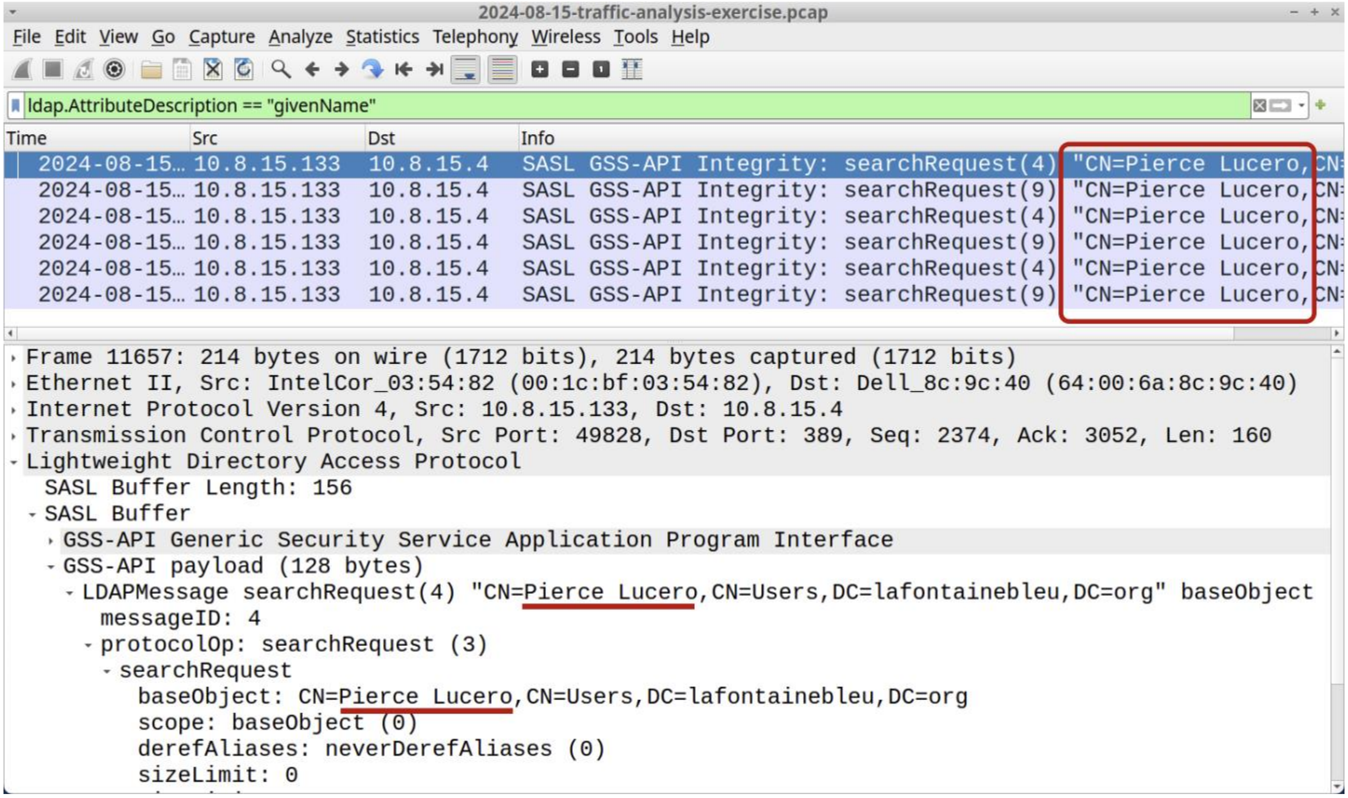


Shown above: Finding the windows user account name by filtering on Kerberos traffic.

This is slightly different than what I have in my Wireshark tutorial, but you can use the following Wireshark filter to help find the victim's first and last names in the pcap:

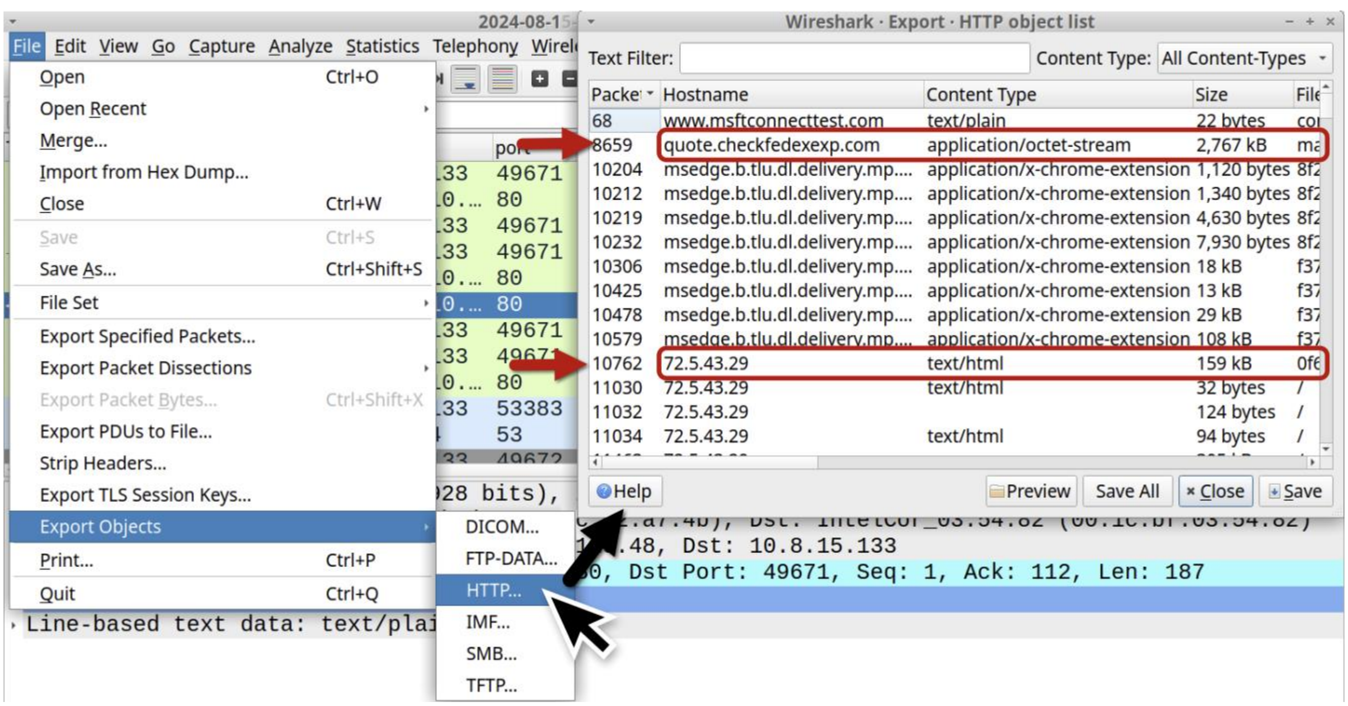
```
ldap.AttributeDescription == "givenName"
```

2024-08-15 - TRAFFIC ANALYSIS EXERCISE ANSWERS



Shown above: Finding the victim's first & last name in the pcap using above Wireshark filter for LDAP.

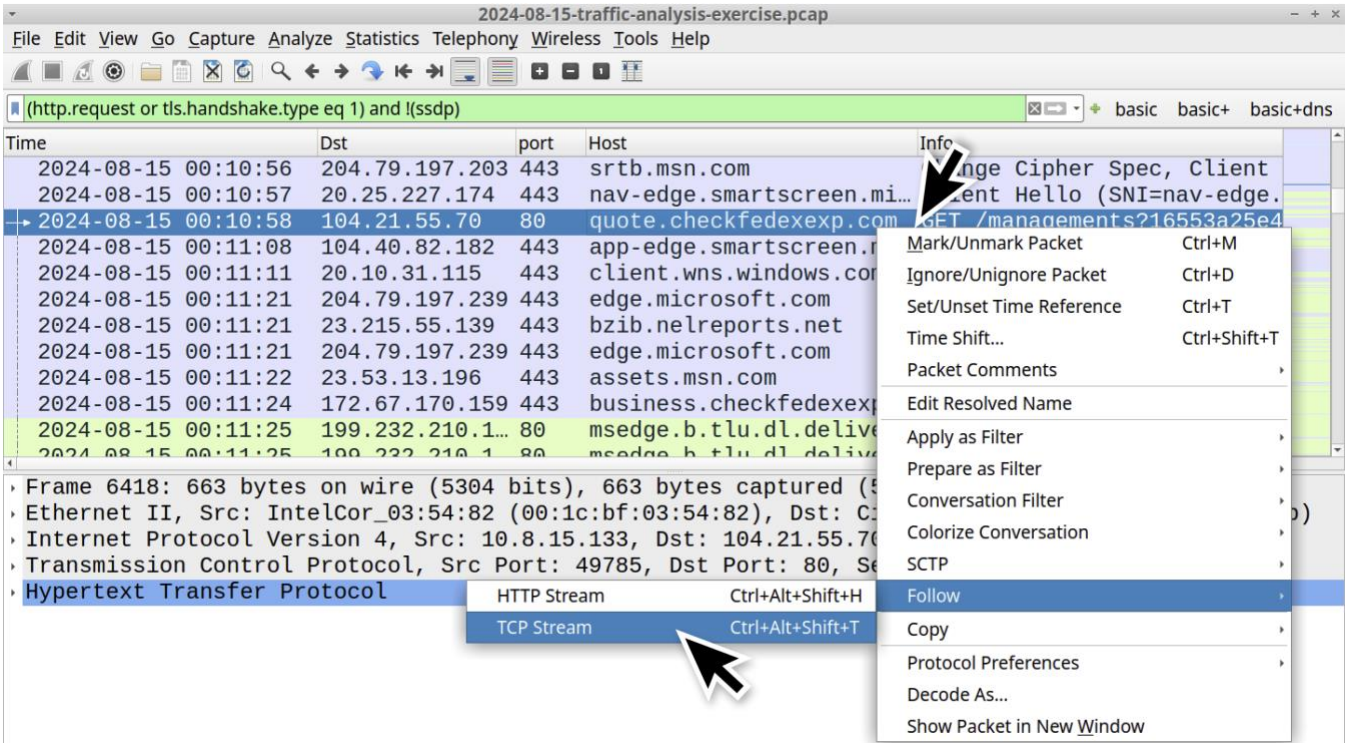
We can export the zip archive from `quote.checkfedexexp.com` and the DLL from `72.5.43.29` by using the File → Export Object → HTTP… menu path.



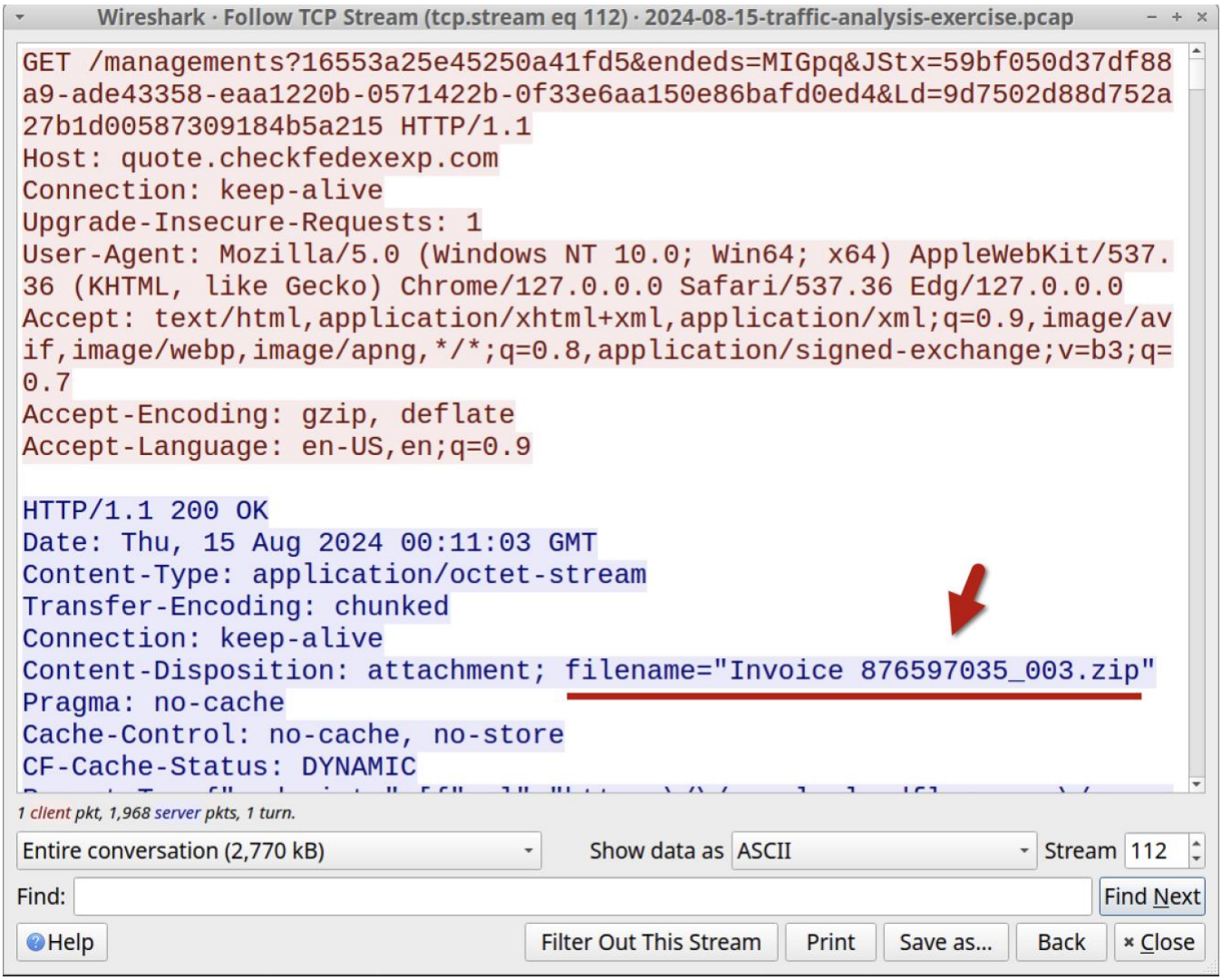
Shown above: Using Wireshark to export the zip archive and the DLL from the pcap.

2024-08-15 - TRAFFIC ANALYSIS EXERCISE ANSWERS

The name of the zip archive is contained in the HTTP response headers, which you can see by following the TCP stream or HTTP stream of that particular HTTP GET request.



Shown above: Following the TCP stream for the HTTP GET request to `quote.checkfedexexp.com`.

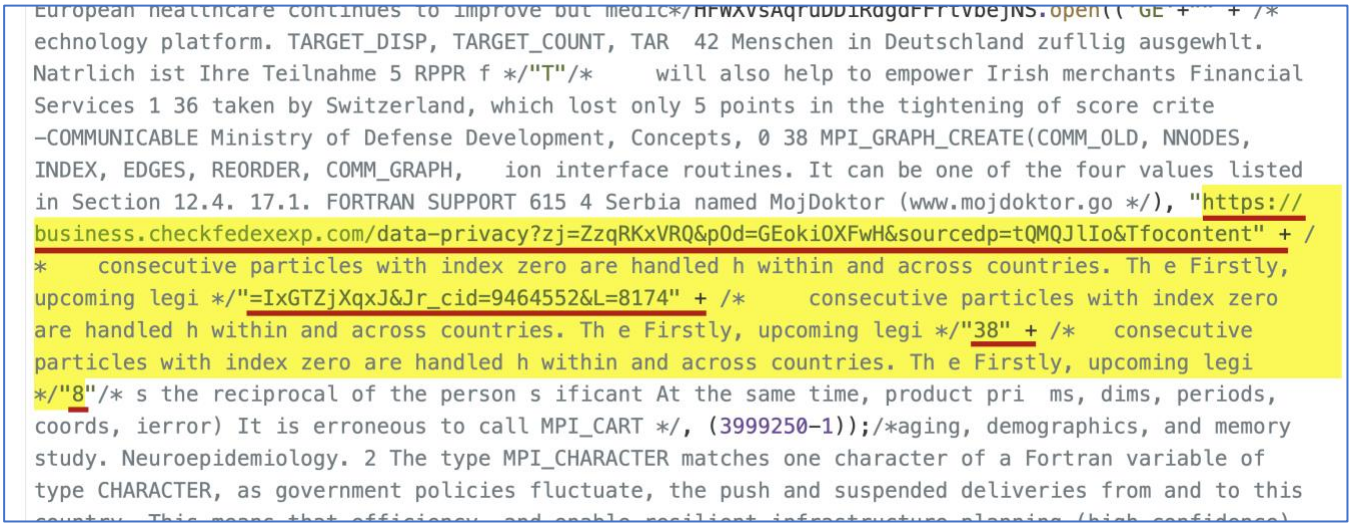


Shown above: Finding the zip archive file name in the TCP stream window.

This 6+ MB zip archive contains a 9+ MB .js file. If you double-click on the .js file on a vulnerable Windows host, Windows executes the .js file using `wscript.exe`.

That massive .js file has a lot of garbage/comment-style text, but I found a follow-up HTTPS URL at line 256 in the file.

2024-08-15 - TRAFFIC ANALYSIS EXERCISE ANSWERS

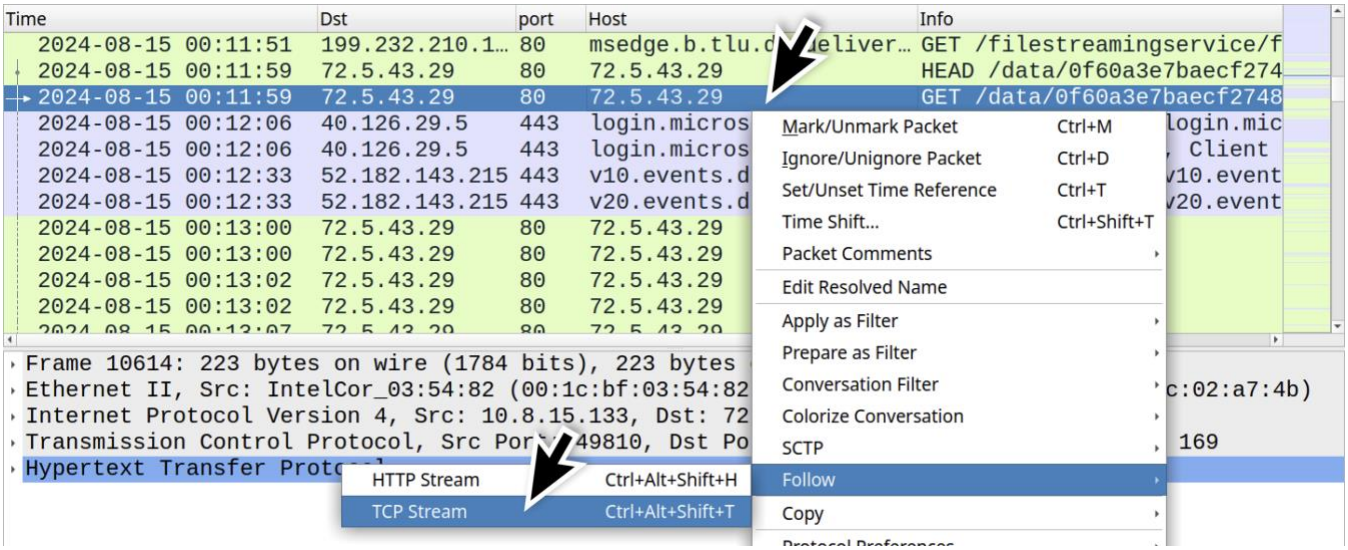


Shown above: Finding the HTTPS URL in the .js file that downloads further malicious content.

Of note, there is HTTPS traffic in the pcap to `business.checkfedexexp.com`, so the .js file did retrieve something, even if we cannot get it from the pcap.

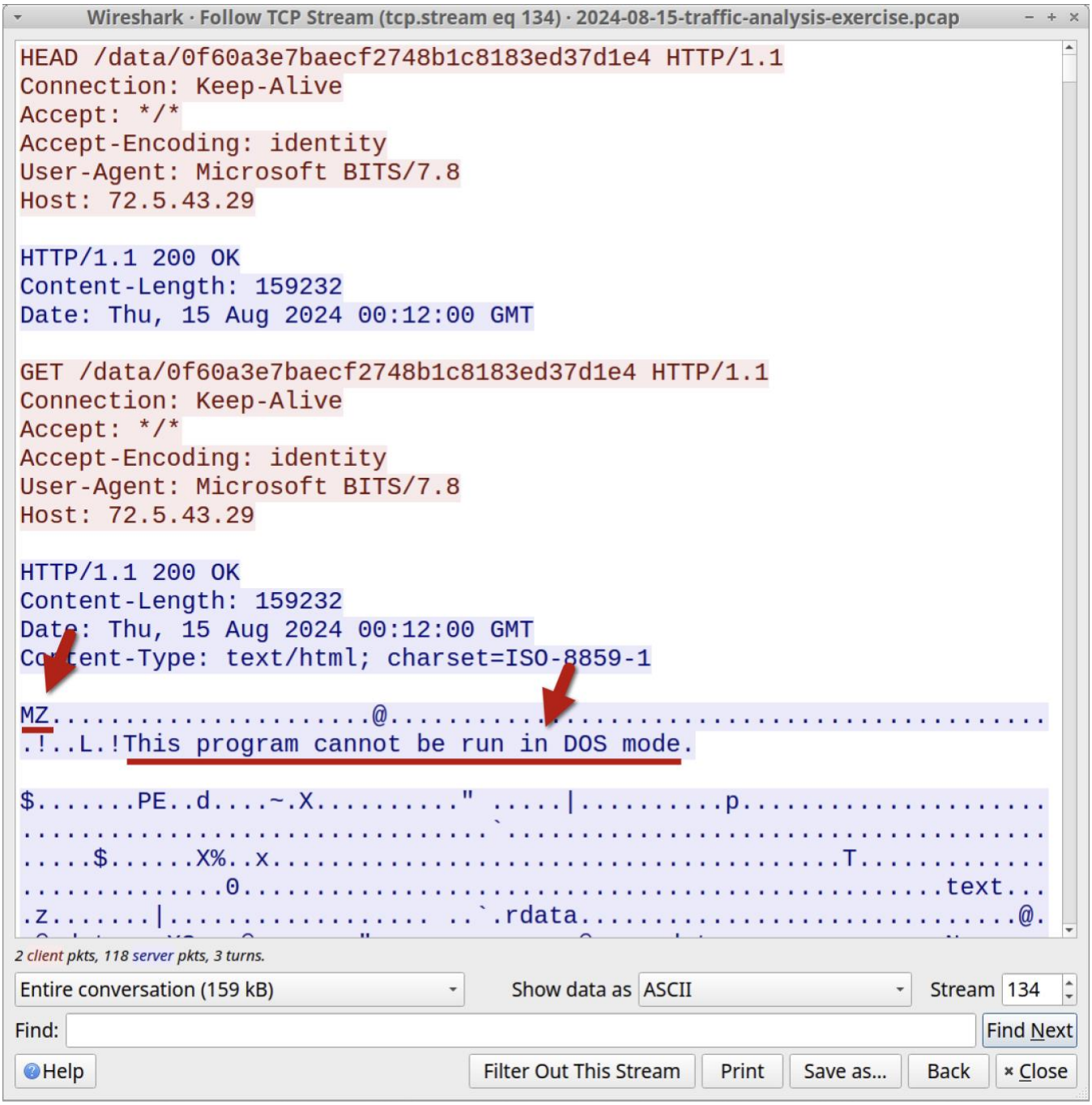
Of note, I recognize the `104.21.0.0/16` and `172.67.0.0/16` IP addresses used by both `.checkfedexexp.com` domains as Cloudflare IP addresses.

If we follow the TCP stream for the first HTTP GET request to `72.5.43.29`, we can see indicators it returned an EXE or DLL file.



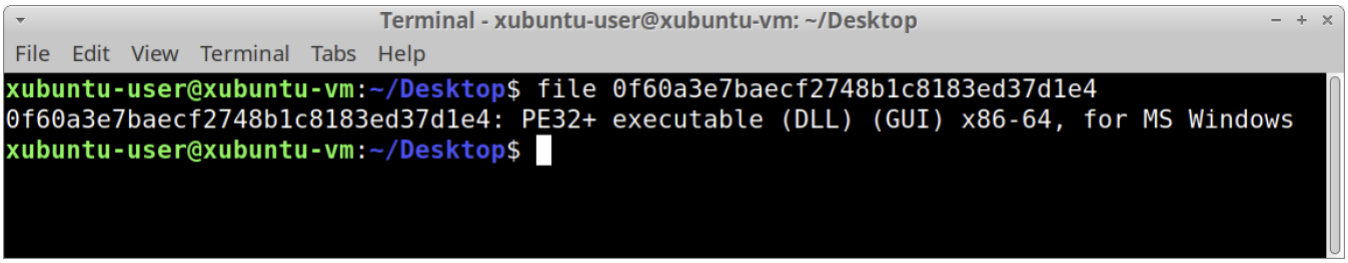
Shown above: Following the TCP stream for the GET request that returned the DLL.

2024-08-15 - TRAFFIC ANALYSIS EXERCISE ANSWERS



Shown above: TCP stream showing an EXE or DLL file returned from `72.5.43.29`.

To determine if this is an EXE or a DLL, you can use the `file` command from a terminal window in macOS or a Linux distro.



Shown above: Finding the exported file is a 64-bit DLL file.

The VirusTotal entry for this DLL indicates a crowd-sourced YARA rule identifies this as WarmCookie. The Any.Run analysis of this file also identifies it as WarmCookie.

Unfortunately, none of the alerts on the network traffic identify the traffic to `72.5.43.29` as WarmCookie, even though the alerts indicate it is malicious or suspicious.

Of note, when I generated the alerts, I set all possible ET signatures in my ruleset to trigger. The results have a lot of informational alerts among the more serious alerts. I hope this can help people learn to sort through alerts and find the actual malicious or suspicious activity.