2024-07-30 - TRAFFIC ANALYSIS EXERCISE ANSWERS

Link to quiz:

- https://www.malware-traffic-analysis.net/2024/07/30/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: 172.16.1.0/24 (172.16.1.0 through 172.16.1.255)
- Domain: wiresharkworkshop.online
- Domain Controller: 172.16.1.4 - WIRESHARK-WS-DC
- LAN segment gateway: 172.16.1.1
- LAN segment broadcast address: 172.16.1.255

TASK:

- Write an incident report based on traffic from the pcap.

ANSWER (EXAMPLE OF AN INCIDENT REPORT):

Executive Summary:

- On Tuesday 2024-07-30 at approximately 02:40 UTC, a Windows host used by Clark Collier was infected with STRRAT malware.

Victim Details:

- Host name: DESKTOP-SKBR25F
- IP address: 172.16.1.66
- MAC address: 00:1e:64:ec:f3:08
- Windows user account name: ccollier

2024-07-30 - TRAFFIC ANALYSIS EXERCISE ANSWERS

Indicators of Compromise (IOCs):

Suspicious traffic to file sharing domains:

- port 443 - github.com - HTTPS traffic
- port 443 - objects.githubusercontent.com - HTTPS traffic
- port 443 - repo1.maven.org - HTTPS traffic

Post-infection traffic for STRRAT:

- 141.98.10.69 port 12132 - TCP traffic for STRRAT

IP address check by infected Windows host:

- port 80 - ip-api.com - GET /json/

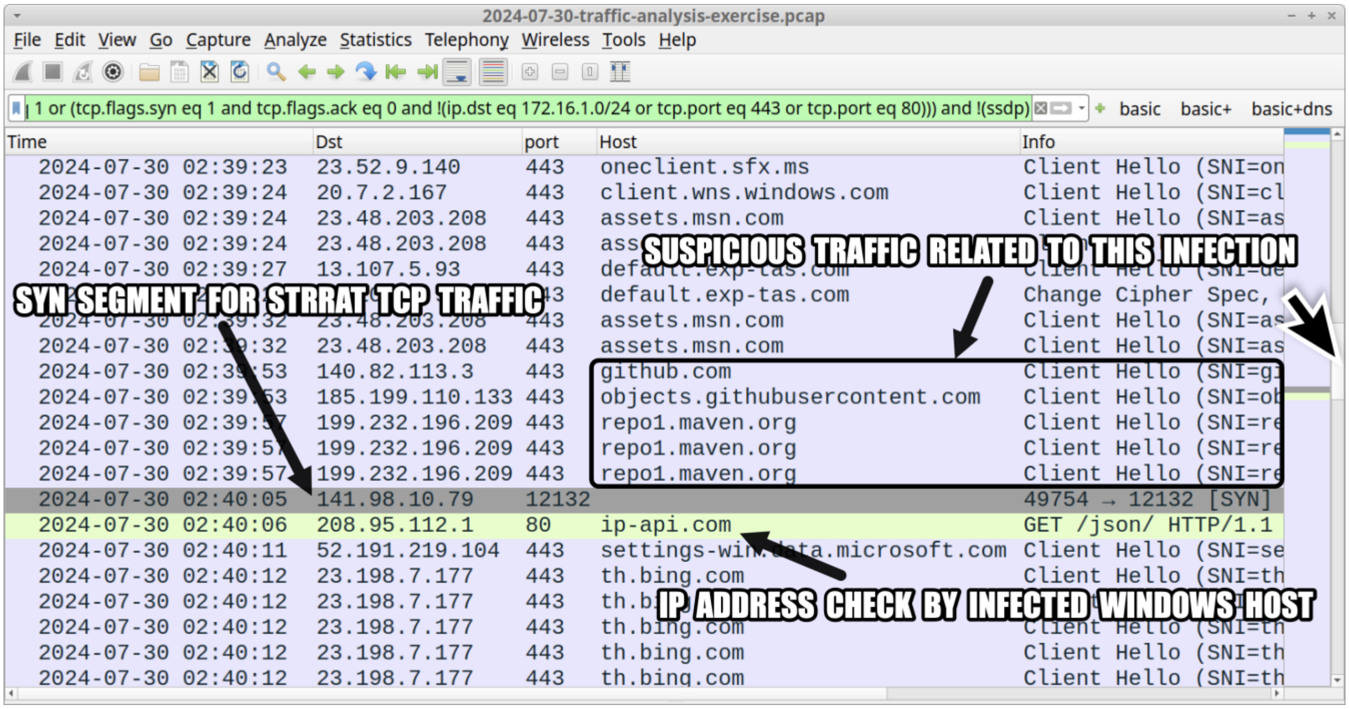
HINTS:

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

Wireshark filter to help find the initial SYN segment for TCP traffic for STRRAT in the pcap:

```
(http.request or tls.handshake.type eq 1 or
(tcp.flags.syn eq 1 and tcp.flags.ack eq 0 and !(ip.dst
eq 172.16.1.0/24 or tcp.port eq 443 or tcp.port eq 80)))
and !(ssdp)
```

2024-07-30 - TRAFFIC ANALYSIS EXERCISE ANSWERS



2024-07-30-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
basic basic+ basic+dns
SYN SEGMENT FOR STRRAT TCP TRAFFIC
SUSPICIOUS TRAFFIC RELATED TO THIS INFECTION
IP ADDRESS CHECK BY INFECTED WINDOWS HOST

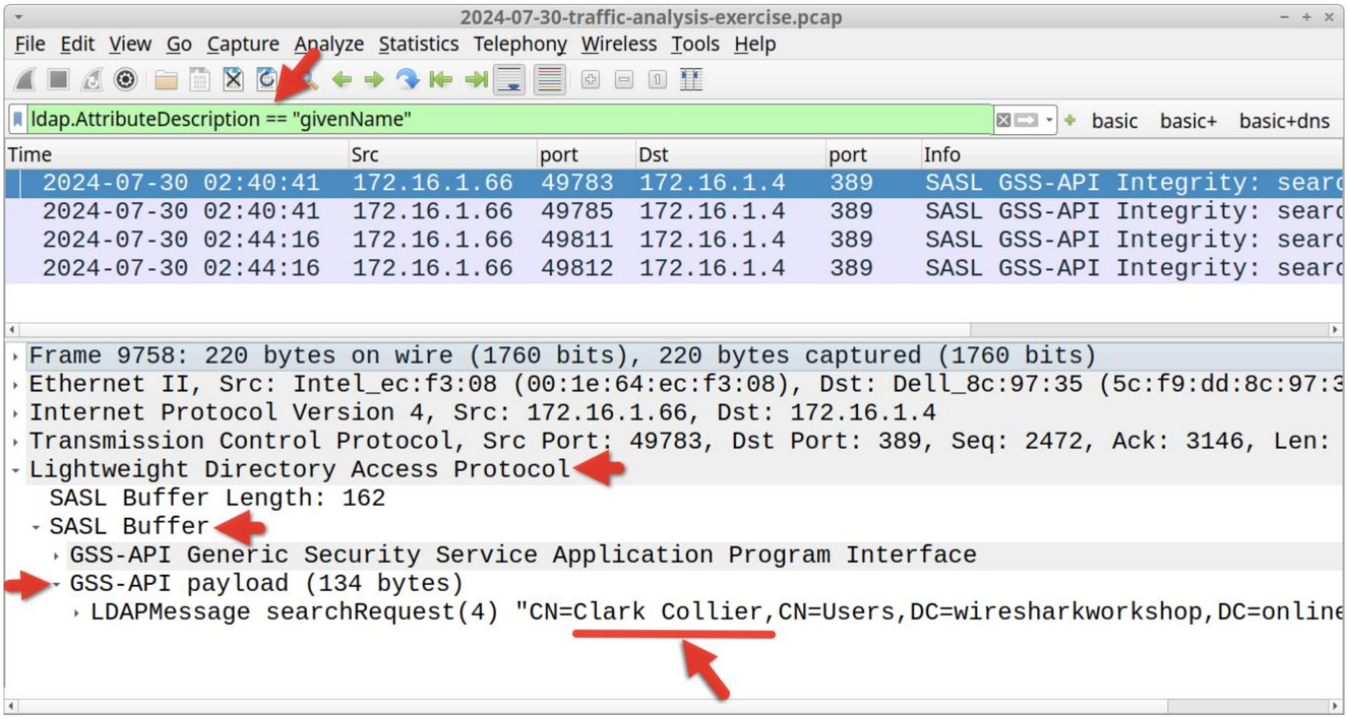
```
1 or (tcp.flags.syn eq 1 and tcp.flags.ack eq 0 and !(ip.dst eq 172.16.1.0/24 or tcp.port eq 443 or tcp.port eq 80))) and !(ssdp)
```

```
Time                 Dst             port  Host                             Info
2024-07-30 02:39:23  23.52.9.140     443   oneclient.sfx.ms                 Client Hello (SNI=on
2024-07-30 02:39:24  20.7.2.167      443   client.wns.windows.com           Client Hello (SNI=cl
2024-07-30 02:39:24  23.48.203.208   443   assets.msn.com                   Client Hello (SNI=as
2024-07-30 02:39:24  23.48.203.208   443   ass[illegible]                   [illegible]
2024-07-30 02:39:27  13.107.5.93     443   default.exp-tas.com              Client Hello (SNI=de
[illegible]          [illegible]     443   default.exp-tas.com              Change Cipher Spec,
2024-07-30 02:39:32  23.48.203.208   443   assets.msn.com                   Client Hello (SNI=as
2024-07-30 02:39:32  23.48.203.208   443   assets.msn.com                   Client Hello (SNI=as
2024-07-30 02:39:53  140.82.113.3    443   github.com                       Client Hello (SNI=gi
2024-07-30 02:39:53  185.199.110.133 443   objects.githubusercontent.com    Client Hello (SNI=ob
2024-07-30 02:39:57  199.232.196.209 443   repo1.maven.org                  Client Hello (SNI=re
2024-07-30 02:39:57  199.232.196.209 443   repo1.maven.org                  Client Hello (SNI=re
2024-07-30 02:39:57  199.232.196.209 443   repo1.maven.org                  Client Hello (SNI=re
2024-07-30 02:40:05  141.98.10.79    12132                                  49754 → 12132 [SYN]
2024-07-30 02:40:06  208.95.112.1    80    ip-api.com                       GET /json/ HTTP/1.1
2024-07-30 02:40:11  52.191.219.104  443   settings-win.data.microsoft.com  Client Hello (SNI=se
2024-07-30 02:40:12  23.198.7.177    443   th.bing.com                      Client Hello (SNI=th
2024-07-30 02:40:12  23.198.7.177    443   th.bing.com                      Client Hello (SNI=th
2024-07-30 02:40:12  23.198.7.177    443   th.bing.com                      Client Hello (SNI=th
2024-07-30 02:40:12  23.198.7.177    443   th.bing.com                      Client Hello (SNI=th
2024-07-30 02:40:12  23.198.7.177    443   th.bing.com                      Client Hello (SNI=th
```

Figure 1. Finding the malicious and suspicious traffic in this pcap using the above Wireshark filter.

Wireshark filter to help find the victim’s first and last names in the pcap:

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



2024-07-30-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
basic basic+ basic+dns

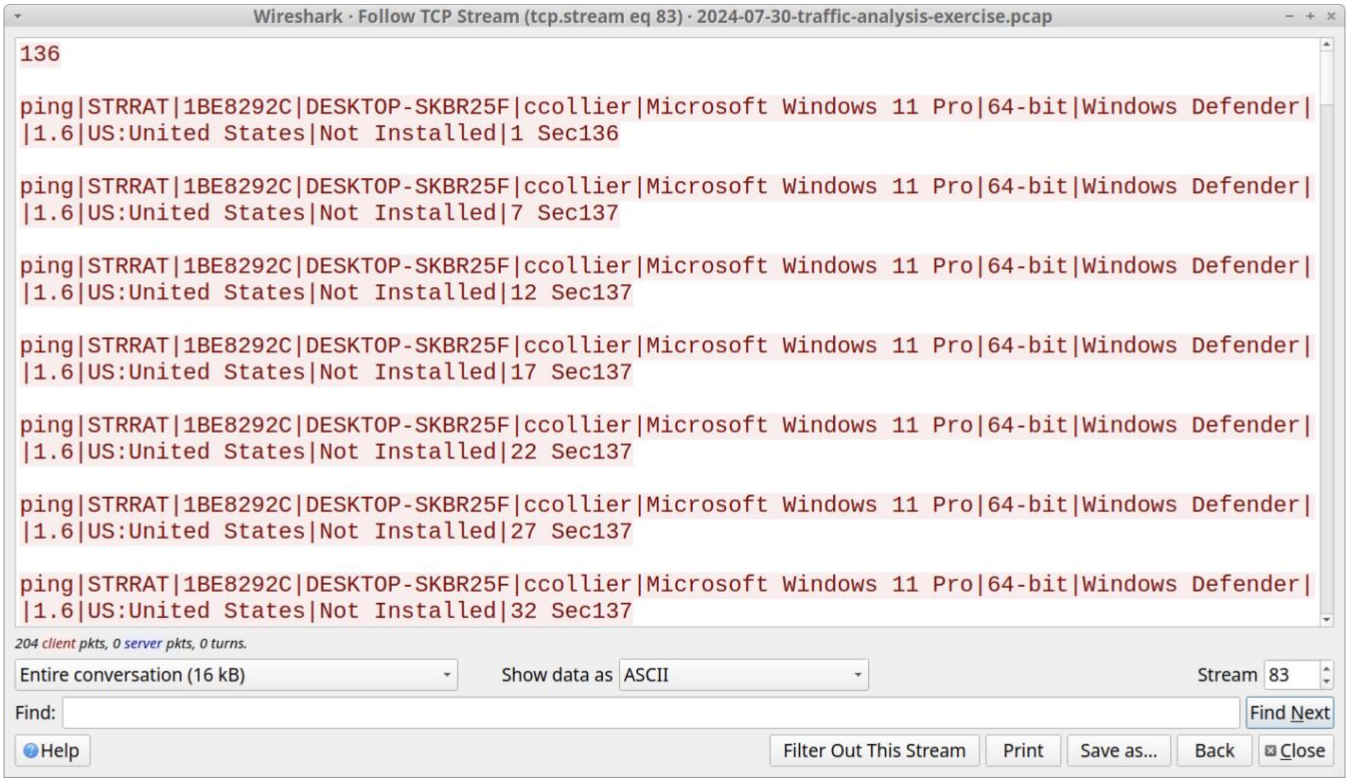
```
ldap.AttributeDescription == "givenName"
```

```
Time                 Src          port   Dst         port  Info
2024-07-30 02:40:41  172.16.1.66  49783  172.16.1.4  389   SASL GSS-API Integrity: searc
2024-07-30 02:40:41  172.16.1.66  49785  172.16.1.4  389   SASL GSS-API Integrity: searc
2024-07-30 02:44:16  172.16.1.66  49811  172.16.1.4  389   SASL GSS-API Integrity: searc
2024-07-30 02:44:16  172.16.1.66  49812  172.16.1.4  389   SASL GSS-API Integrity: searc
```

```
› Frame 9758: 220 bytes on wire (1760 bits), 220 bytes captured (1760 bits)
› Ethernet II, Src: Intel_ec:f3:08 (00:1e:64:ec:f3:08), Dst: Dell_8c:97:35 (5c:f9:dd:8c:97:3
› Internet Protocol Version 4, Src: 172.16.1.66, Dst: 172.16.1.4
› Transmission Control Protocol, Src Port: 49783, Dst Port: 389, Seq: 2472, Ack: 3146, Len:
⌄ Lightweight Directory Access Protocol
    SASL Buffer Length: 162
  ⌄ SASL Buffer
    › GSS-API Generic Security Service Application Program Interface
    ⌄ GSS-API payload (134 bytes)
      › LDAPMessage searchRequest(4) "CN=Clark Collier,CN=Users,DC=wiresharkworkshop,DC=online
```

Figure 2. Finding the victim’s first and last name in this pcap using the above Wireshark filter for LDAP.

2024-07-30 - TRAFFIC ANALYSIS EXERCISE ANSWERS



Wireshark · Follow TCP Stream (tcp.stream eq 83) · 2024-07-30-traffic-analysis-exercise.pcap

```
136

ping|STRRAT|1BE8292C|DESKTOP-SKBR25F|ccollier|Microsoft Windows 11 Pro|64-bit|Windows Defender|
|1.6|US:United States|Not Installed|1 Sec136

ping|STRRAT|1BE8292C|DESKTOP-SKBR25F|ccollier|Microsoft Windows 11 Pro|64-bit|Windows Defender|
|1.6|US:United States|Not Installed|7 Sec137

ping|STRRAT|1BE8292C|DESKTOP-SKBR25F|ccollier|Microsoft Windows 11 Pro|64-bit|Windows Defender|
|1.6|US:United States|Not Installed|12 Sec137

ping|STRRAT|1BE8292C|DESKTOP-SKBR25F|ccollier|Microsoft Windows 11 Pro|64-bit|Windows Defender|
|1.6|US:United States|Not Installed|17 Sec137

ping|STRRAT|1BE8292C|DESKTOP-SKBR25F|ccollier|Microsoft Windows 11 Pro|64-bit|Windows Defender|
|1.6|US:United States|Not Installed|22 Sec137

ping|STRRAT|1BE8292C|DESKTOP-SKBR25F|ccollier|Microsoft Windows 11 Pro|64-bit|Windows Defender|
|1.6|US:United States|Not Installed|27 Sec137

ping|STRRAT|1BE8292C|DESKTOP-SKBR25F|ccollier|Microsoft Windows 11 Pro|64-bit|Windows Defender|
|1.6|US:United States|Not Installed|32 Sec137
```

204 client pkts, 0 server pkts, 0 turns.

Entire conversation (16 kB)

Show data as: ASCII

Stream: 83

Figure 3. TCP stream of the STRRAT post-infection traffic. Note the `STRAAT` string in each line starting with `ping`.

To find the victim information, use the Identifying Hosts and Users Wireshark tutorial I wrote.

I used the following Java archive (.jar) file to generate the infection for this exercise:

- SHA256 hash: `4c249b325125235b50d9690560c4197a28fd62901b5e02d9eba7436b29447cdd`
- File size: 409,654 bytes
- File name: `PL#40704.jar`
- Delivery method: email attachment