

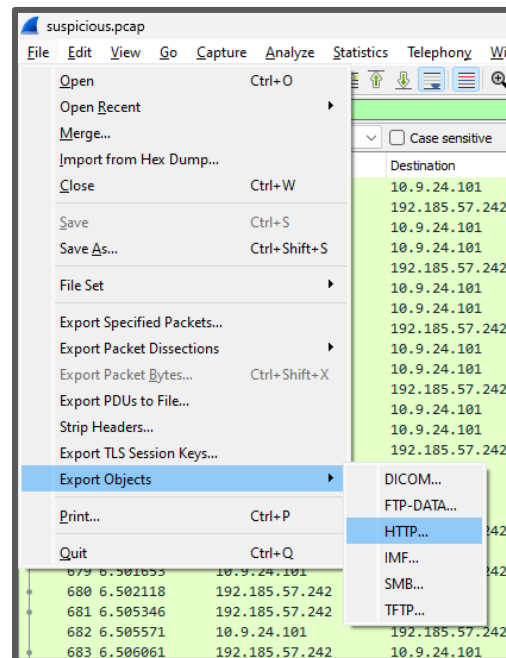
Lab: Wireshark Phishing SANS Holiday Hack 2022

Isaac Falero

IS 401/501

08/29/2023

1. There are objects in the PCAP file that can be exported by Wireshark and/or Tshark. What type of objects can be exported from this PCAP?



Wireshark · Export · HTTP object list

Text Filter:

Packet	Hostname	Content Type	Size	Filename
8	adv.epostoday.uk	text/html	754 bytes	app.php
687	adv.epostoday.uk	text/html	808 kB	app.php
692	adv.epostoday.uk	text/html	1130 bytes	favicon.ico

Answer: HTTP

Explanation: Open the PCAP file in Wireshark. Using the “Export Objects” function, you’ll find that the objects can only be exported to an HTTP object list.

2. What is the file name of the largest file we can export?

Wireshark · Export · HTTP object list

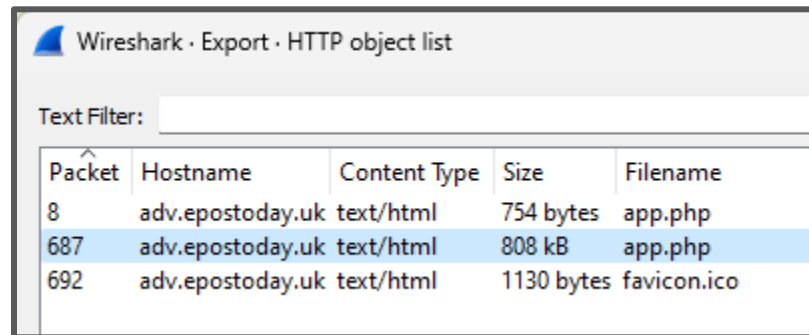
Text Filter:

Packet	Hostname	Content Type	Size	Filename
8	adv.epostoday.uk	text/html	754 bytes	app.php
687	adv.epostoday.uk	text/html	808 kB	app.php
692	adv.epostoday.uk	text/html	1130 bytes	favicon.ico

Answer: app.php

Explanation: In Wireshark, export the objects to an HTTP object list using the “Export Objects” function. The file size is specified in the “Size” column.

3. What packet number starts that app.php file?



Wireshark · Export · HTTP object list

Text Filter:

Packet	Hostname	Content Type	Size	Filename
8	adv.epostoday.uk	text/html	754 bytes	app.php
687	adv.epostoday.uk	text/html	808 kB	app.php
692	adv.epostoday.uk	text/html	1130 bytes	favicon.ico

Answer: 687

Explanation: In Wireshark, export the objects to an HTTP object list using the “Export Objects” function. The packet number is specified in the “Packet” column.

4. What is the IP of the Apache server?



Apply a display filter ... <Ctrl-/>

Packet details ▾ Narrow & Wide ▾ ☐ Case sensitive String ▾ **apache**

No.	Time	Source	Destination
8	0.808778	192.185.57.242	10.9.24.101
9	0.855760	10.9.24.101	192.185.57.242
10	0.862771	10.9.24.101	192.185.57.242

```
Frame 8: 738 bytes on wire (5904 bits), 738 bytes captured (5904 bits)
Ethernet II, Src: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1), Dst: HewlettP_1c:47:ae (00:08:02:1c:47:ae)
Internet Protocol Version 4, Src: 192.185.57.242, Dst: 10.9.24.101
Transmission Control Protocol, Src Port: 80, Dst Port: 60511, Seq: 1, Ack: 448, Len: 684
```

Answer: 192.185.57.242

Explanation: In Wireshark, search for the string “apache” inside the packet details using the “Find” function. The Apache server IP address is found in the “Source” column, or in the packet details at the “Src” IP address.

5. What file is saved to the infected host?

```

let byteNumbers = new Array(byteCharacters.length);
for (let i = 0; i < byteCharacters.length; i++) {
    byteNumbers[i] = byteCharacters.charCodeAt(i);
}
let byteArray = new Uint8Array(byteNumbers);

// now that we have the byte array, construct the blob from it
let blob1 = new Blob([byteArray], {type: 'application/octet-stream'});

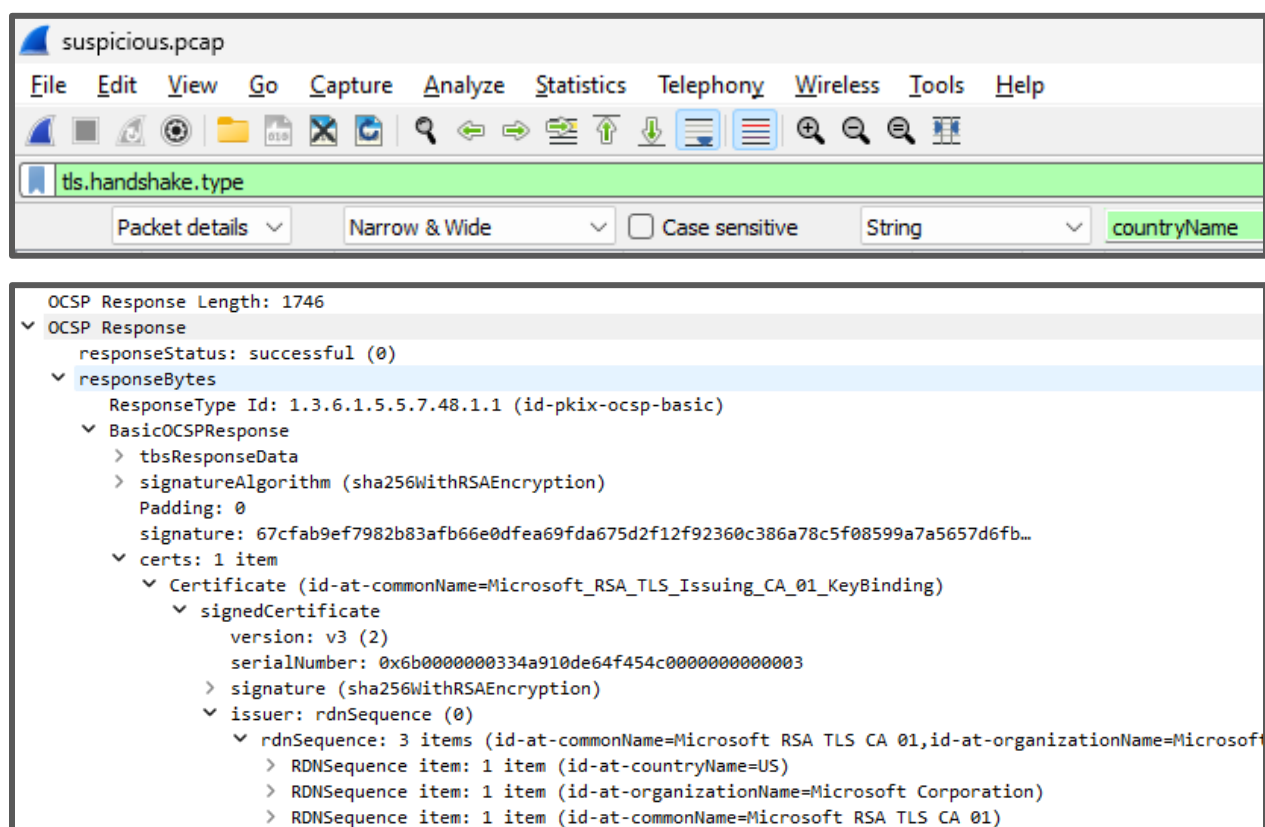
saveAs(blob1, 'Ref_Sept24-2020.zip');

```

Answer: Ref_Sept24-2020.zip

Explanation: In Wireshark, export the objects to an HTTP object list using the “Export Objects” function. Save the exported file named “app.php” and open it in Notepad. Scrolling to the bottom of the file, you’ll find that blob1 is saved as “Ref_Sept24-2020.zip.”

- 6. Attackers used bad TLS certificates in this traffic. Which countries were they registered to? Submit the name of the countries in alphabetical order separated by commas (Ex: Norway, South Korea).**



The image shows the Wireshark network protocol analyzer interface. The top pane displays a packet list with the selected packet being 'tls.handshake.type'. The bottom pane shows the packet details for this type of packet. The 'OCSP Response' section is expanded, showing a 'successful (0)' status. The 'responseBytes' section is also expanded, revealing a 'BasicOCSPResponse' with a 'signatureAlgorithm' of 'sha256WithRSAEncryption'. The 'certs' section is expanded, showing a single 'Certificate' with a 'signedCertificate' containing a 'version' of 'v3 (2)', a 'serialNumber', and a 'signature'. The 'issuer' is identified as 'rdnSequence (0)', which contains three items: 'id-at-commonName=Microsoft RSA TLS Issuing CA 01', 'id-at-organizationName=Microsoft Corporation', and 'id-at-countryName=US'. The 'countryName' field is highlighted in green, indicating the country of registration.

Answer: Ireland, Israel, South Sudan, United States

Explanation: In Wireshark, filter for TLS handshake certificates using “tls.handshake.type == 11.” Then, search for the string “countryName” in the packet details using the “Find” function. Cycling through the results will eventually show you four country codes: IE, IL, SS, and US – which correspond to the following countries: Ireland, Israel, South Sudan, and United States.

7. Is the host infected (Yes/No)?

Answer: Yes

Explanation: Unfortunately, all evidence points to “Yes.”

Collaborators

Patrick Doolin

Aaron Thammavongsa

Isaac Vaillancourt

References

Hakerman. (2022, December 8). *KringleCon 2022 Walkthrough - Wireshark Practice* [Video]. YouTube. <https://www.youtube.com/watch?v=TjLsnhg18Pw>

Wireshark TLS client Hello Filter. W3schools. (2022, December 3). <https://www.w3schools.blog/wireshark-tls-client-hello-filter>