**23rd Aug ‘23**

**(IS 401/501-01 MERGED) (FA23) CYBERSECURITY PRINCIPLES**

**Pod 6**

**Challenge 2 (Wireshark Phishing)**

**Amogh Patel**

**Collaborator:** [**Hackerman**](https://www.youtube.com/watch?v=TjLsnhg18Pw&ab_channel=Hackerman)



**Objective:** Investigate the file provided (suspicious pcap) for malicious network traffic using Wireshark or Tshark.

**Prompt 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?

**Answer:** DICOM, FTP-DATA, HTTP, IMF, SMB, TFTP.

**Explanation:** When exporting these objects from a PCAP file using Wireshark or Tshark, one can extract and save the specific content related to each of these protocols for further analysis or archival purposes.

**A screenshot of a computer

Description automatically generated**

**Prompt 2:** What is the file name of the largest file we can export?

**Answer:** app.php.

**Explanation:** Amongst the available files app.hpp is the largest file with a file size of 808kb.

A screenshot of a computer

Description automatically generated

**Prompt 3: What packet number starts that app.php file?**

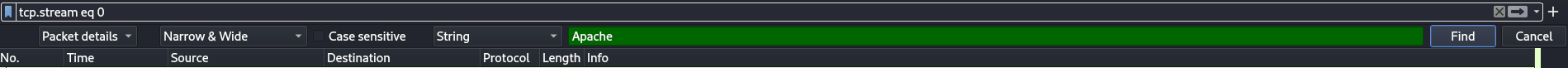
**Answer:** 687.

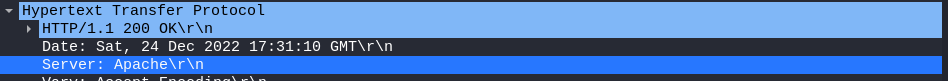
**Explanation:** The corresponding packet number for app.php is 687.

**Prompt 4:** What is the IP of the Apache server?

**Answer:** 192.185.57.242

**Explanation:** For the corresponding packet number (687) used the ‘find packet’ function to search for ‘Apache’ as the keywork. Once found, note the IP address of the Apache server.





**Prompt 5:** What file is saved to the infected host?

**Help used:** [**Hackerman**](https://www.youtube.com/watch?v=TjLsnhg18Pw&ab_channel=Hackerman)(accessed 08/23/2023)

**Answer:** Ref\_Sept24-2020.zip.

**Explanation:** Using the hints we are told check the HTTP stream and look for a .zip file pertaining to the Apache server.

A screen shot of a computer

Description automatically generated

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

**Help used:** [**Hackerman**](https://www.youtube.com/watch?v=TjLsnhg18Pw&ab_channel=Hackerman)(accessed 08/23/2023)

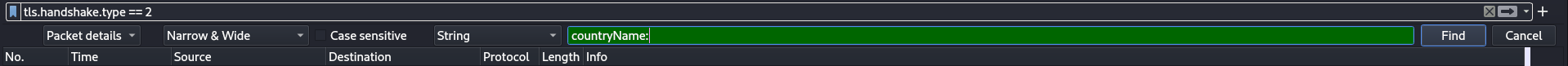
**Answer:** Israel, South Sudan, United States.

**Explanation:**

1) Used the TLS handshake type filter in Wireshark to find the server hello (Where client hello is a value of 1 and server hello which is a value of 2). tls.handshake.type == 2.

2) Once the TLS filter was applied, used the find packet function to look for country.

3) Looked up the found country codes to their corresponding countries using ssl.com.

A computer screen with white text

Description automatically generated

**Prompt 7:** Is the host infected?

**Answer:** Yes.