Machine: 7001
FTP

Premise

- Users are given a pcap file containing data which needs to be used to answer a series of questions
  - NIST: K0491, K0555

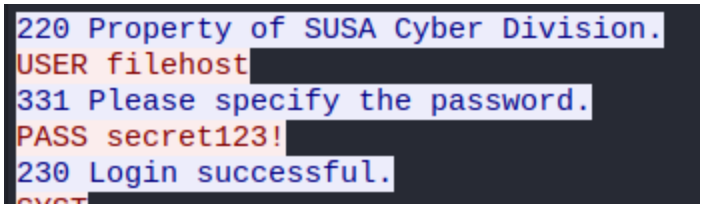
Questions

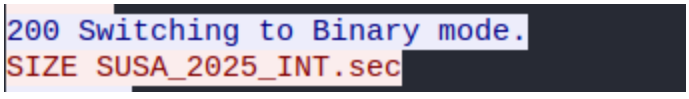
- What is the *Username* and *Password* used to log into the FTP server
- What is the name of the *file* that was downloaded
- In *Bytes* how large is the downloaded file
- What are the contents of the downloaded file
- What is the decrypted message in the downloaded file

FILE

- INTERCEPT_FTP_TRAFFIC.pcapng

Answers

- **What is the *Username* and *Password* used to log into the FTP server**
  - User: filehost
  - PW: secret123!
  - 

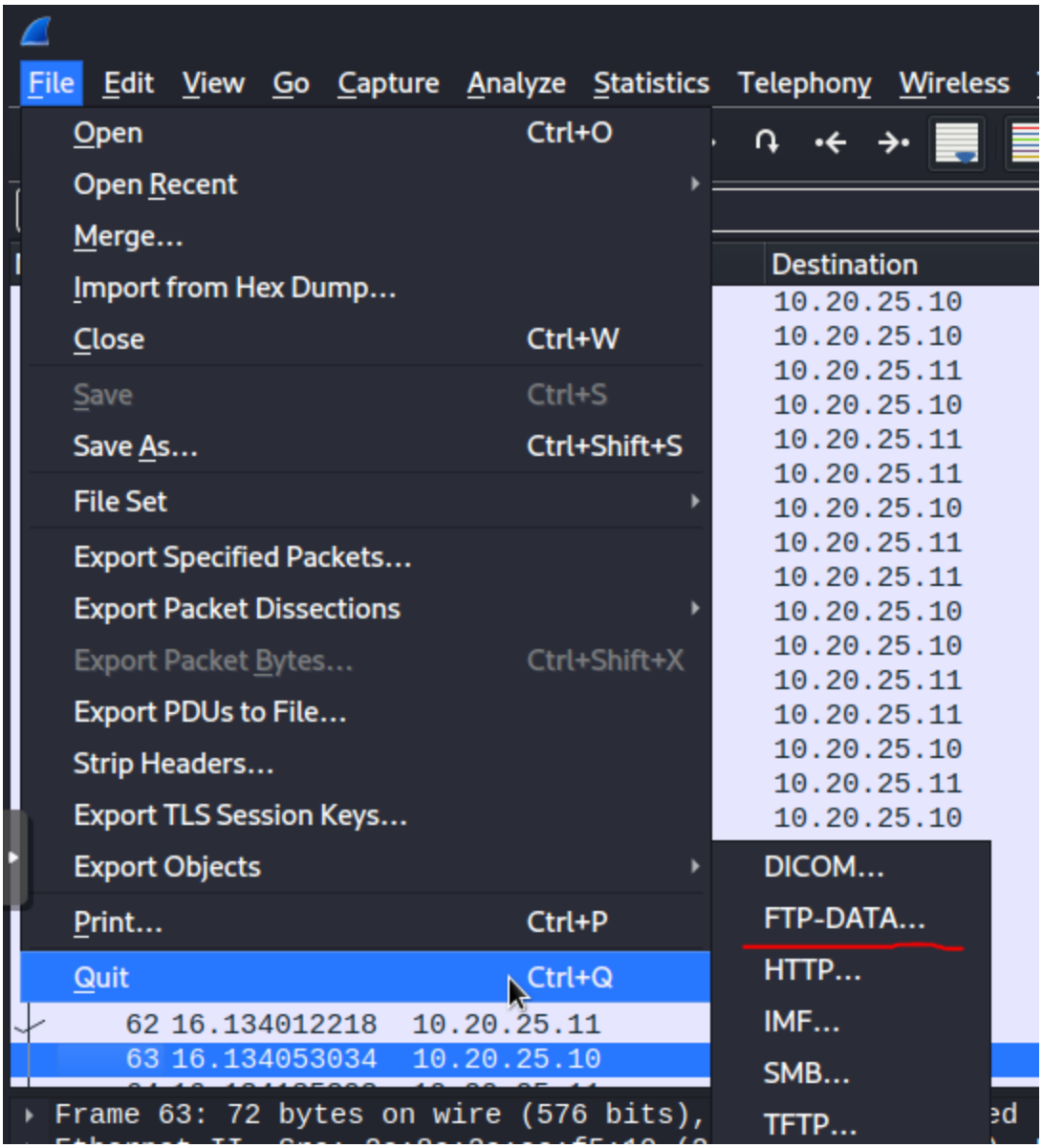
- **What is the name of the *file* that was downloaded**
  - SUSA_2025_INT.sec
  - 

- **In *Bytes* how large is the downloaded file**

- 109 Bytes

```
RETR SUSA_2025_INT.sec
150 Opening BINARY mode data connection for SUSA_2025_INT.sec (109 bytes).
226 Transfer complete.
```

- **What are the contents of the downloaded file**
  - Students will need to Export the data from the pcap using
  - **File > Export Objects > FTP-DATA**



  - **Contents:**
    SW50ZWwgQnJpZWZpbmcuDQoNCk5lZWQgdG8gRml4IEZUUCBzZXJ2ZXIsIGNyZWRlbnRpYWxzIGhhdmUgYmVlbiBsZWFrZWQuLi4NCi0gSVQg

- **What is the decrypted message in the downloaded file**
  - Students will need to recognize that the file is encoded in Base64, and then either use cyberchef, or an online decoder to get the manifest

```
Intel Briefing.
```

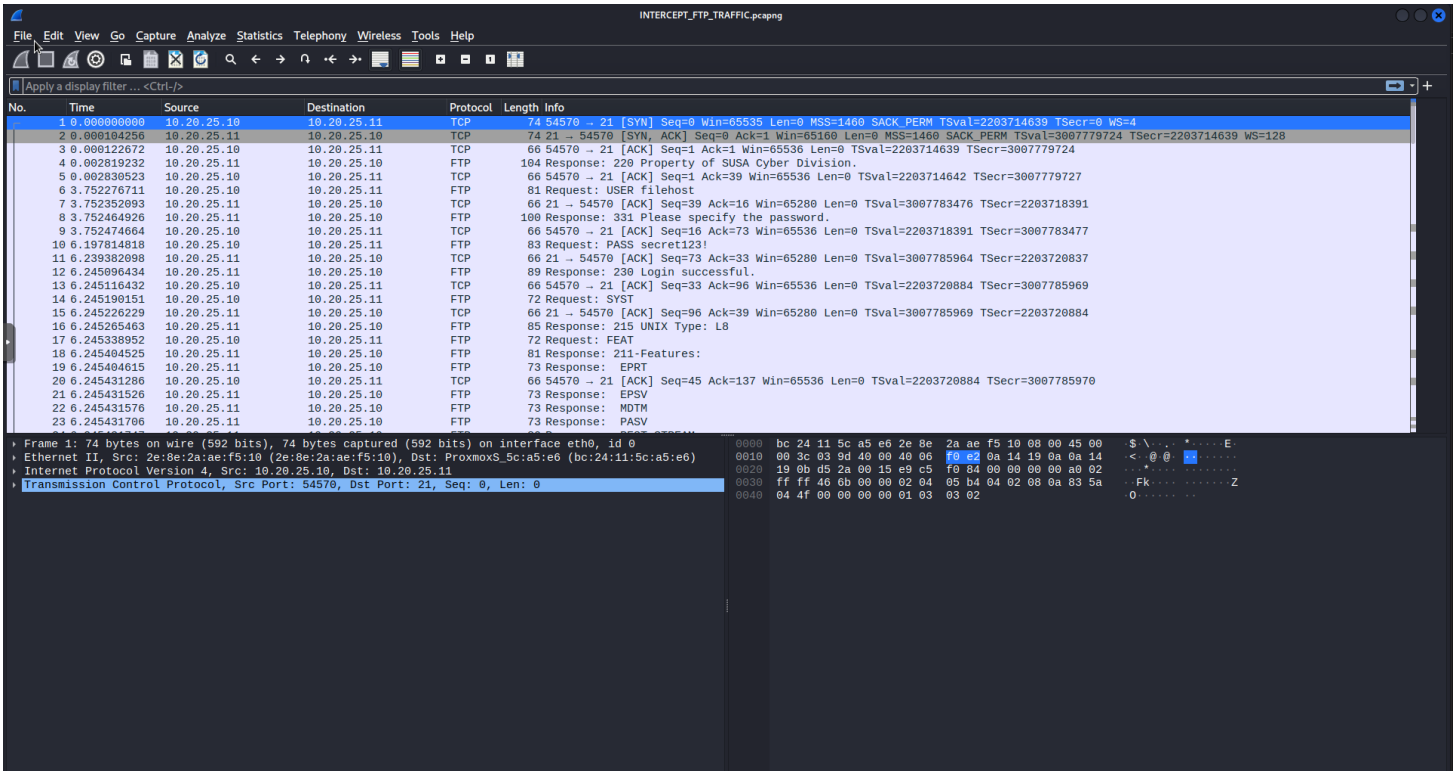
```
Need to Fix FTP server, credentials have been leaked...
- IT
```

Recommended Tools

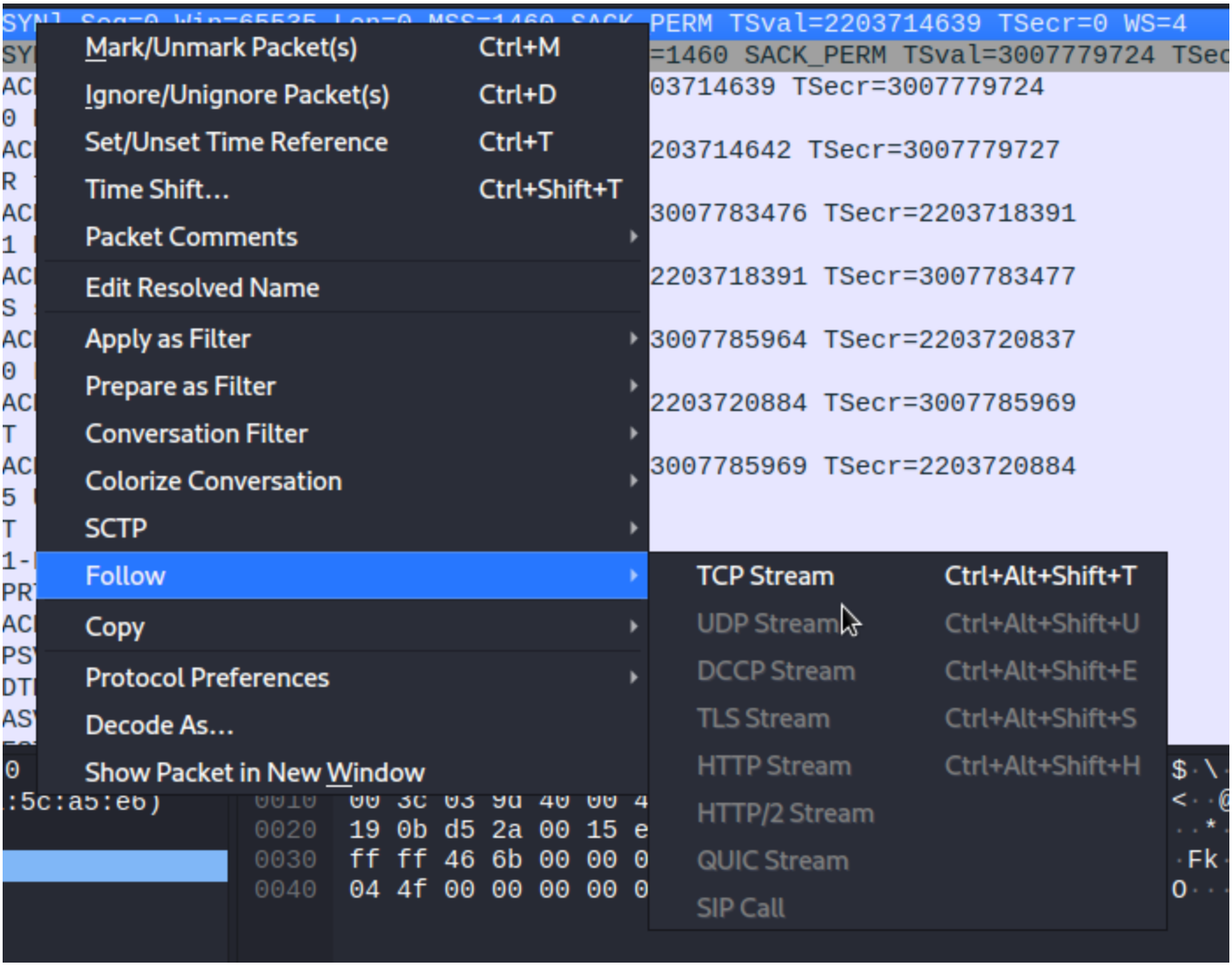
- Wireshark
- Cyberchef/Online Base64 Decoder

Walkthrough

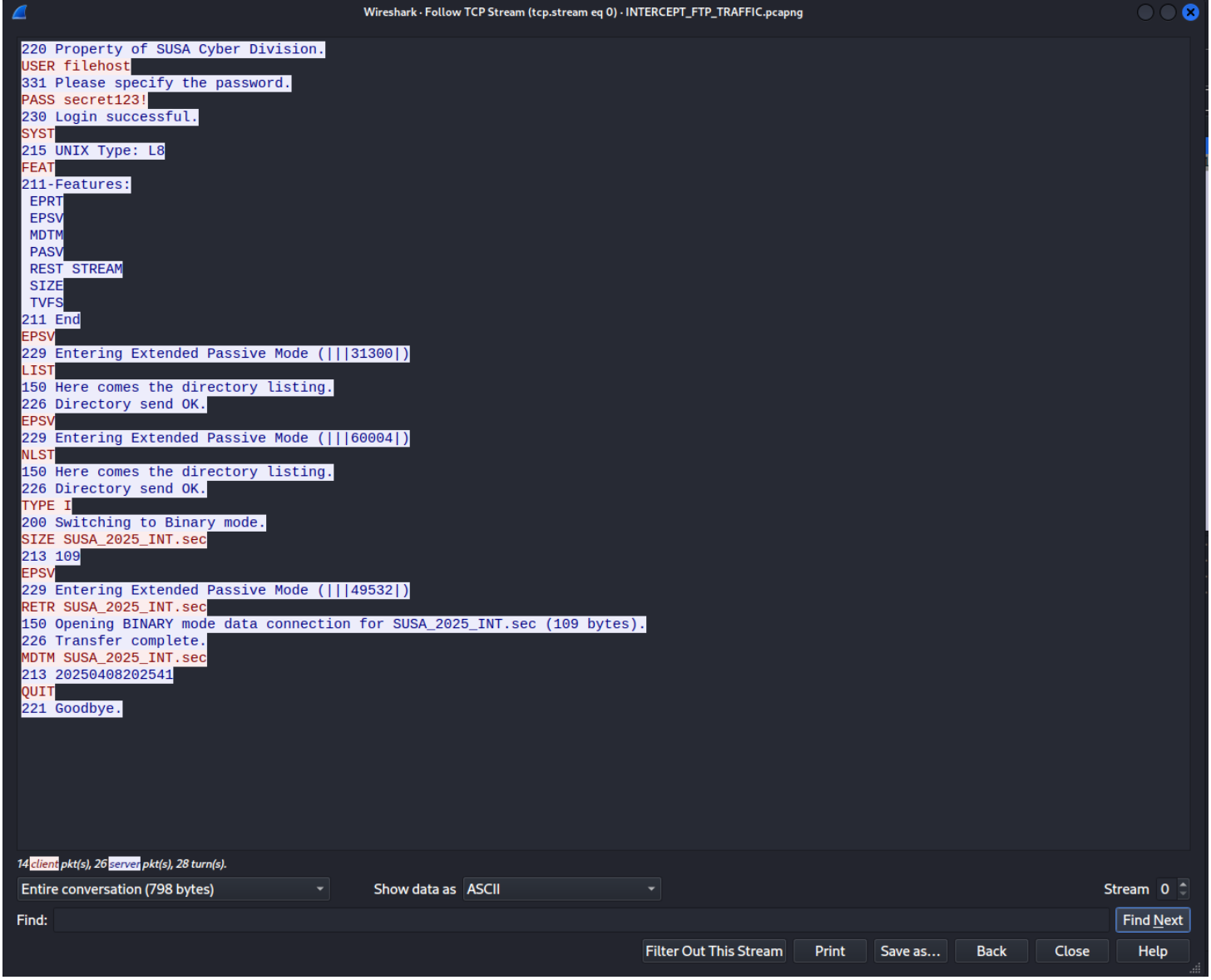
1. **Open the Wireshark Packet**



2. **Right click on the first TCP packet (In this case that is the first packet)**

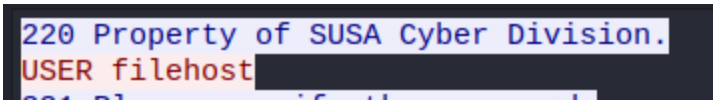


3. **This will show the first TCP stream of the packet capture. In this example there was only one tcp stream which handled the FTP traffic**

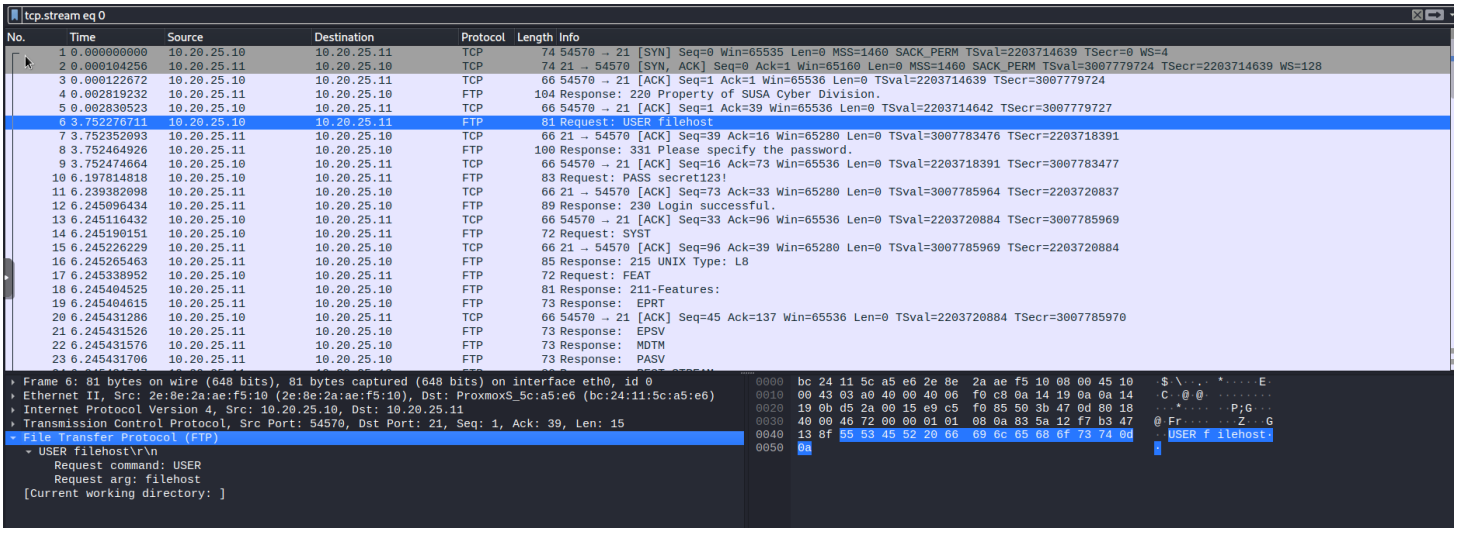


1. This stream shows the entire conversation between the server and the host.

4. **To find the either look at the *TCP* stream output and find the line that says *USER***



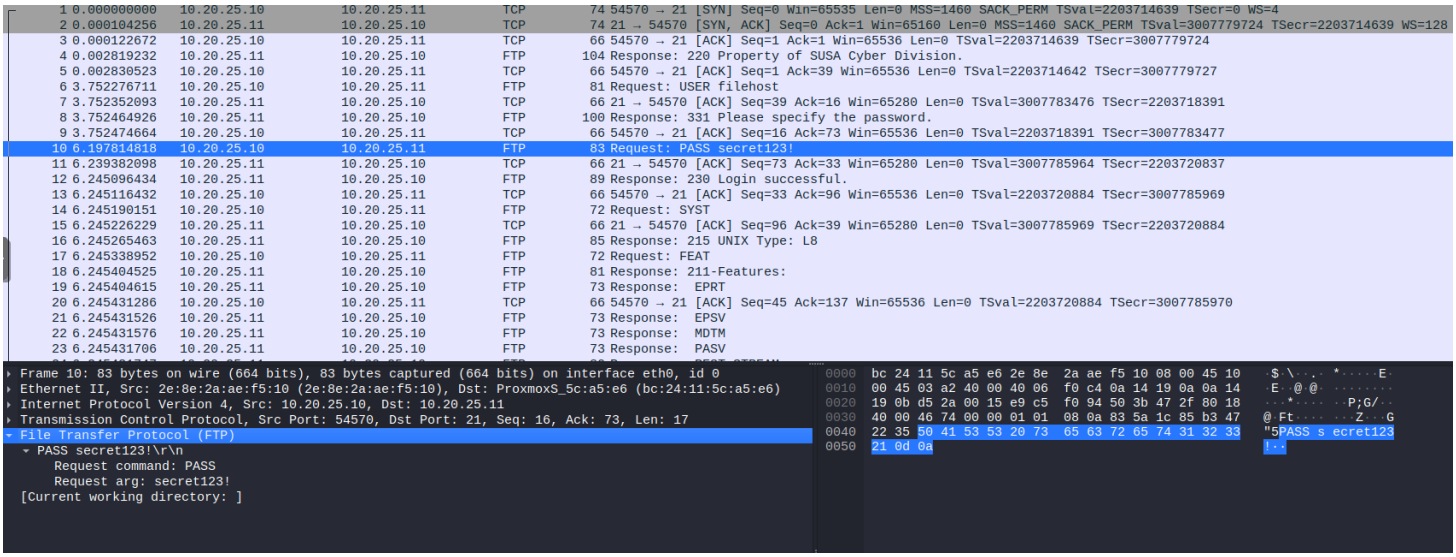
~*or*~ Look at the 6th packet in the capture



5. **To find the password again look at either the *TCP* stream or the raw packet capture**

```
331 Please specify the password.
PASS secret123!
230 Login successful.
```

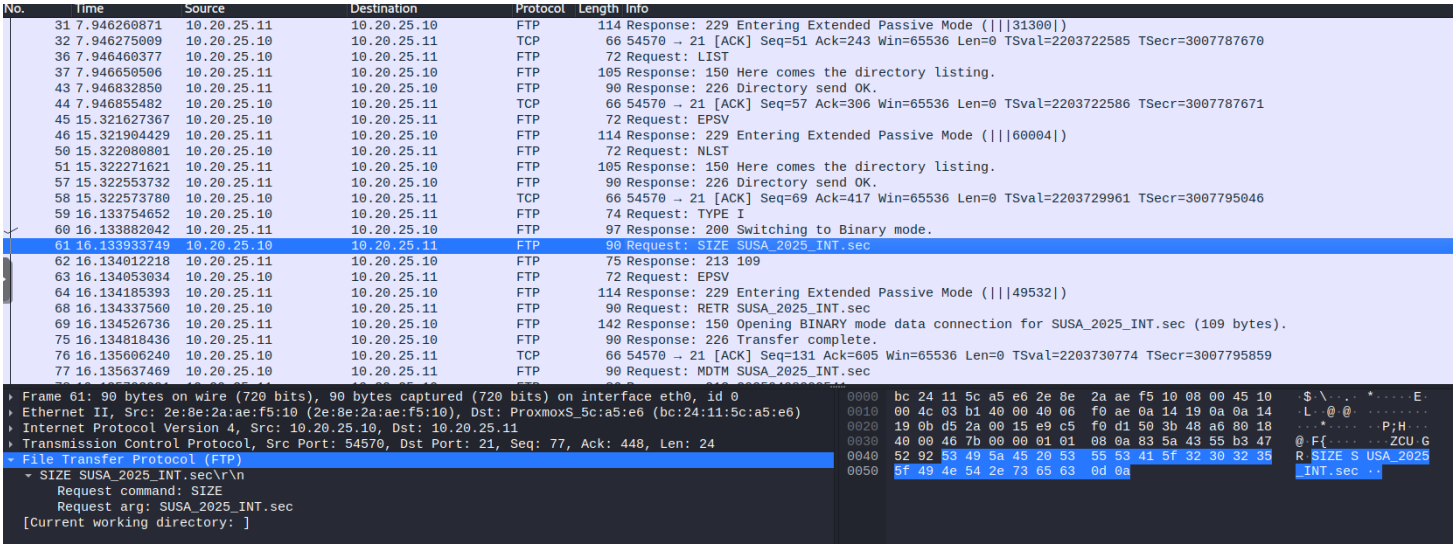
~*or*~ Look at the 10th packet in the capture



6. **To find the name of the file, Check either the TCP stream or the raw packet capture**

```
TYPE I
200 Switching to Binary mode.
SIZE SUSA_2025_INT.sec
213 109
EPSV
```

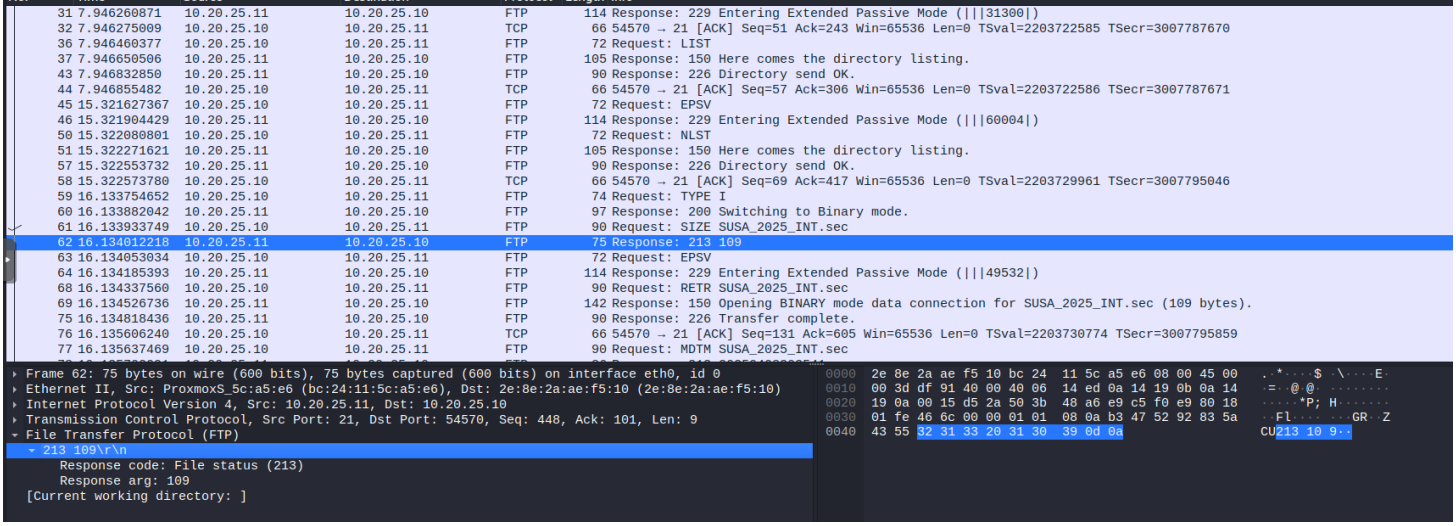
~*or*~ Look at line 61 of the packet capture



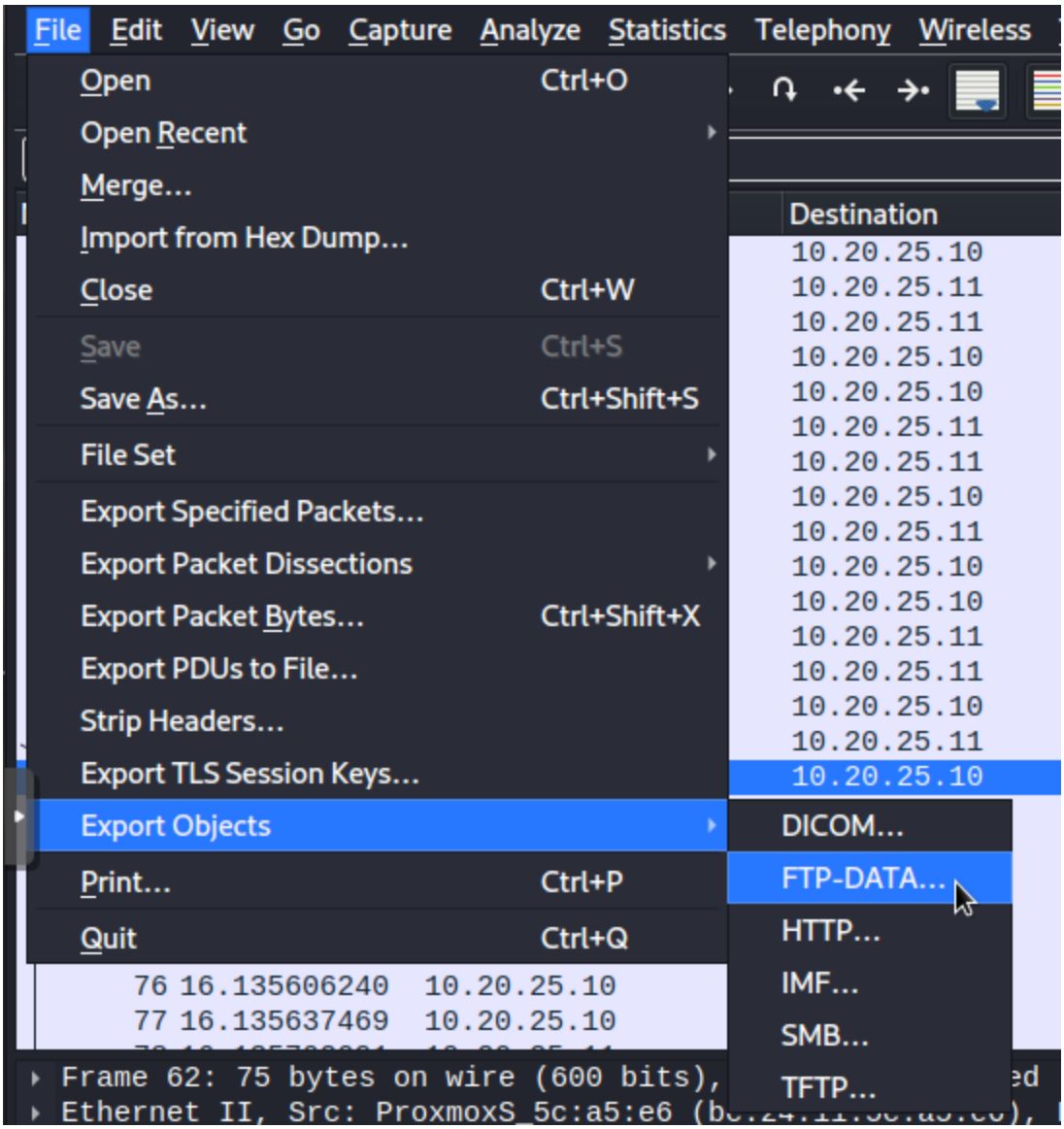
7. **To find the size in Bytes , Check either the TCP stream or the raw packet capture**

```
SIZE SUSA_2025_INT.sec
213 109
EPSV
```

~*or*~ Look at like 62 of the packet capture

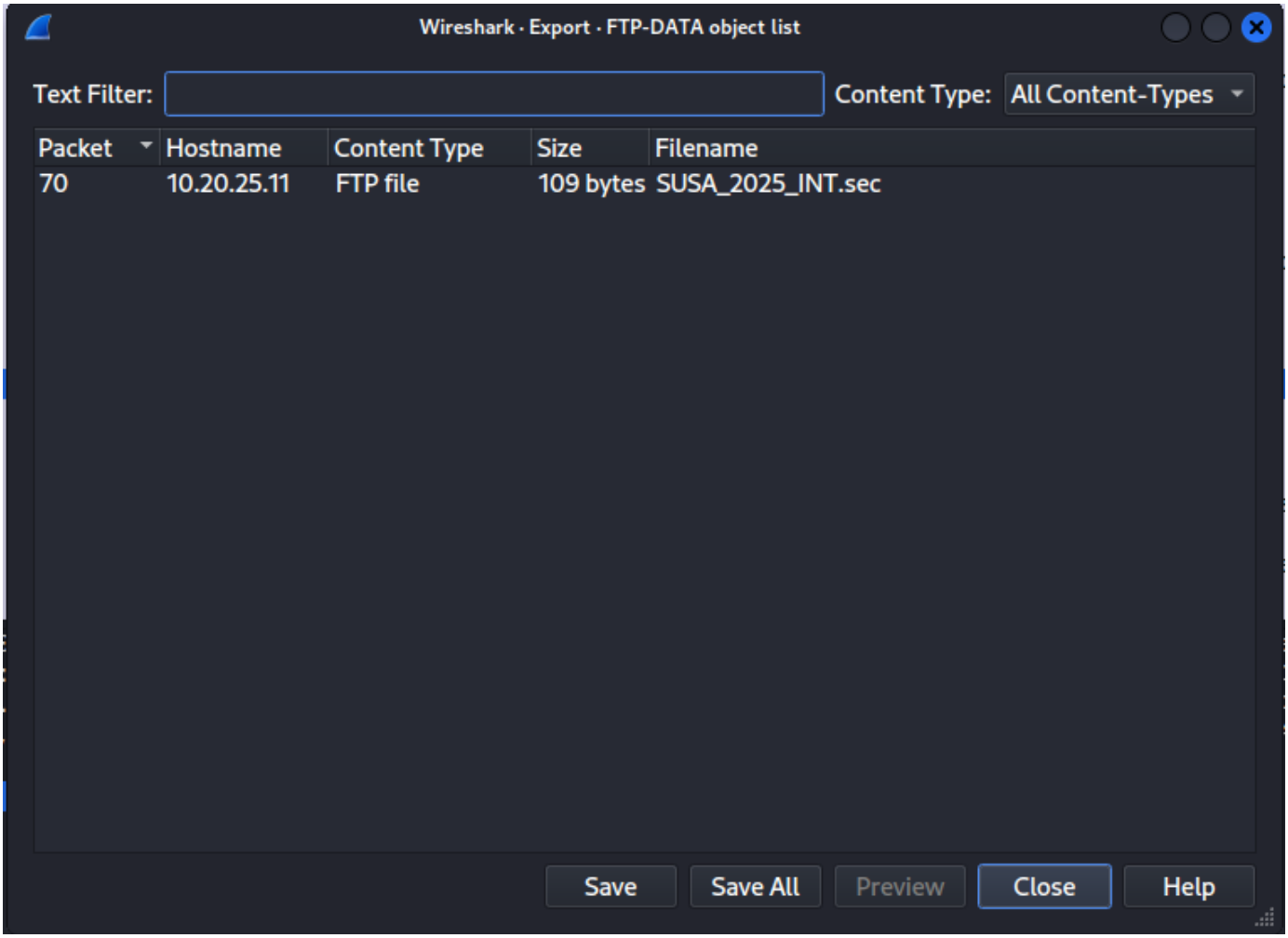


8. **To view the contents of the file, it needs to be saved. That can be done by exporting the FTP data**



1.

2. This will show a file list to export



3. Select the **SUSA_2025_INT.sec** file and then save it
4. Open the file in a text editor and view the contents

9. **The data inside the file is encoded, using base64. Many utilities can be used to decode it**

1. CyberChef.org can be used to decode it