

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

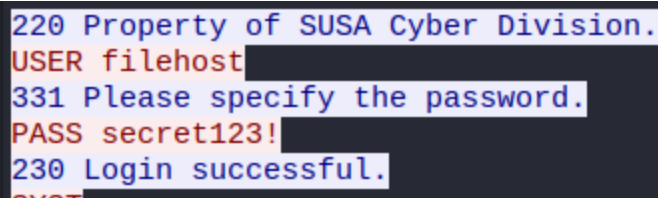
- What is the *Username* and *Password* used to log into the FTP server
- What is the name of the *file* that was downloaded
- In *Bytes* how large is the downloaded file
- What are the contents of the downloaded file
- What is the decrypted message in the downloaded file

FILE

- INTERCEPT_FTP_TRAFFIC.pcapng
-

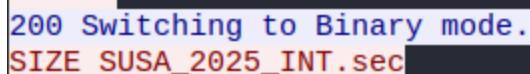
Answers

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

A screenshot of an FTP session showing a successful login. The text is as follows:

```
220 Property of SUSA Cyber Division.  
USER filehost  
331 Please specify the password.  
PASS secret123!  
230 Login successful.
```

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

A screenshot of an FTP session showing the start of a file transfer. The text is as follows:

```
200 Switching to Binary mode.  
SIZE SUSA_2025_INT.sec
```

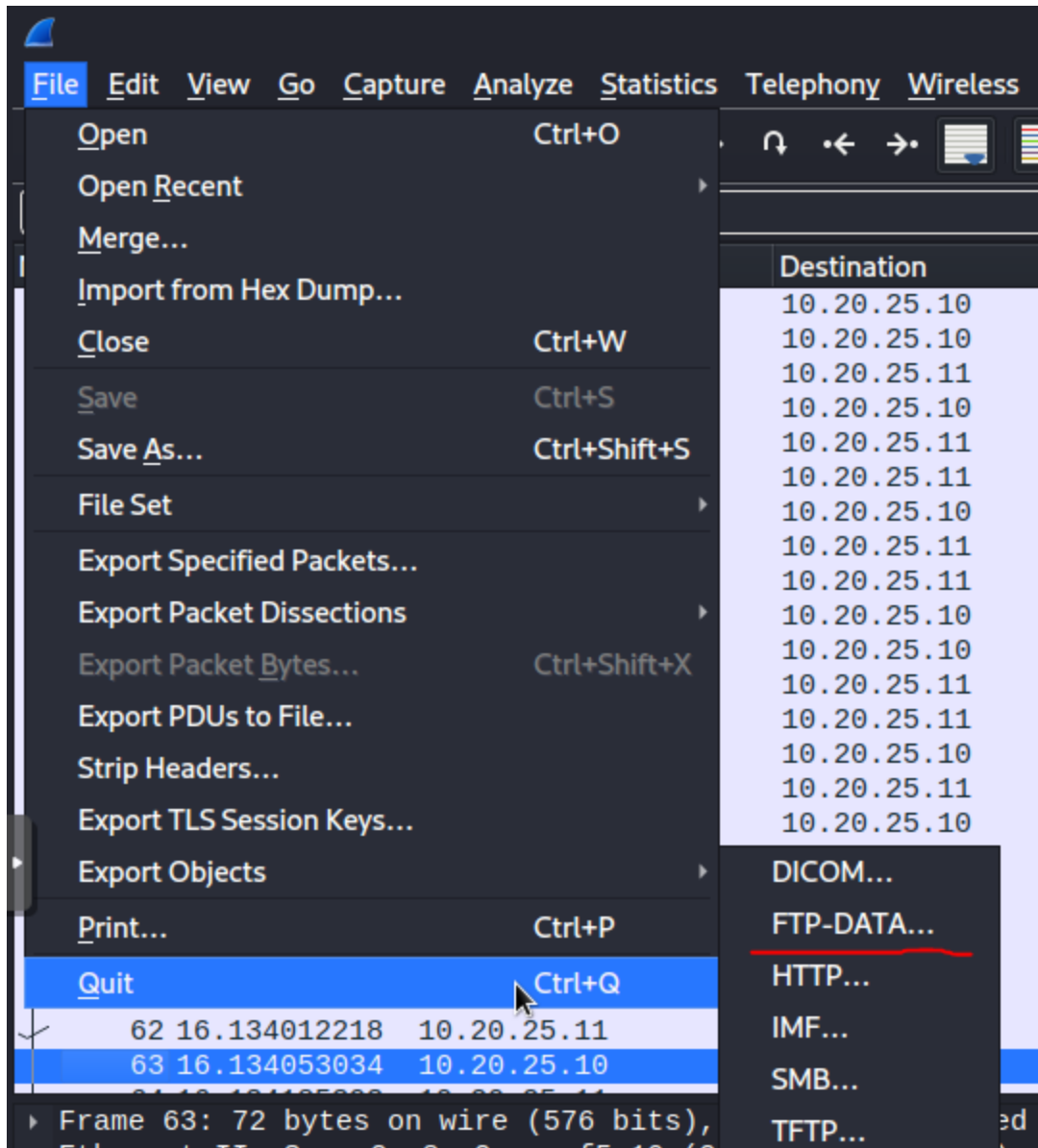
- In *Bytes* how large is the downloaded file

- 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:**

SW50ZWwgQnJpZWZpbmcuDQoNCk5lZWQgdG8gRml4IEZUUCBzZXJ2ZXIsIGNyZWRIbnRpY
WxzIGhhdmUgYmVlbiBsZWFrZWQuLi4NCi0gSVQg

- **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

Need to Fix FTP server, credentials have been leaked...

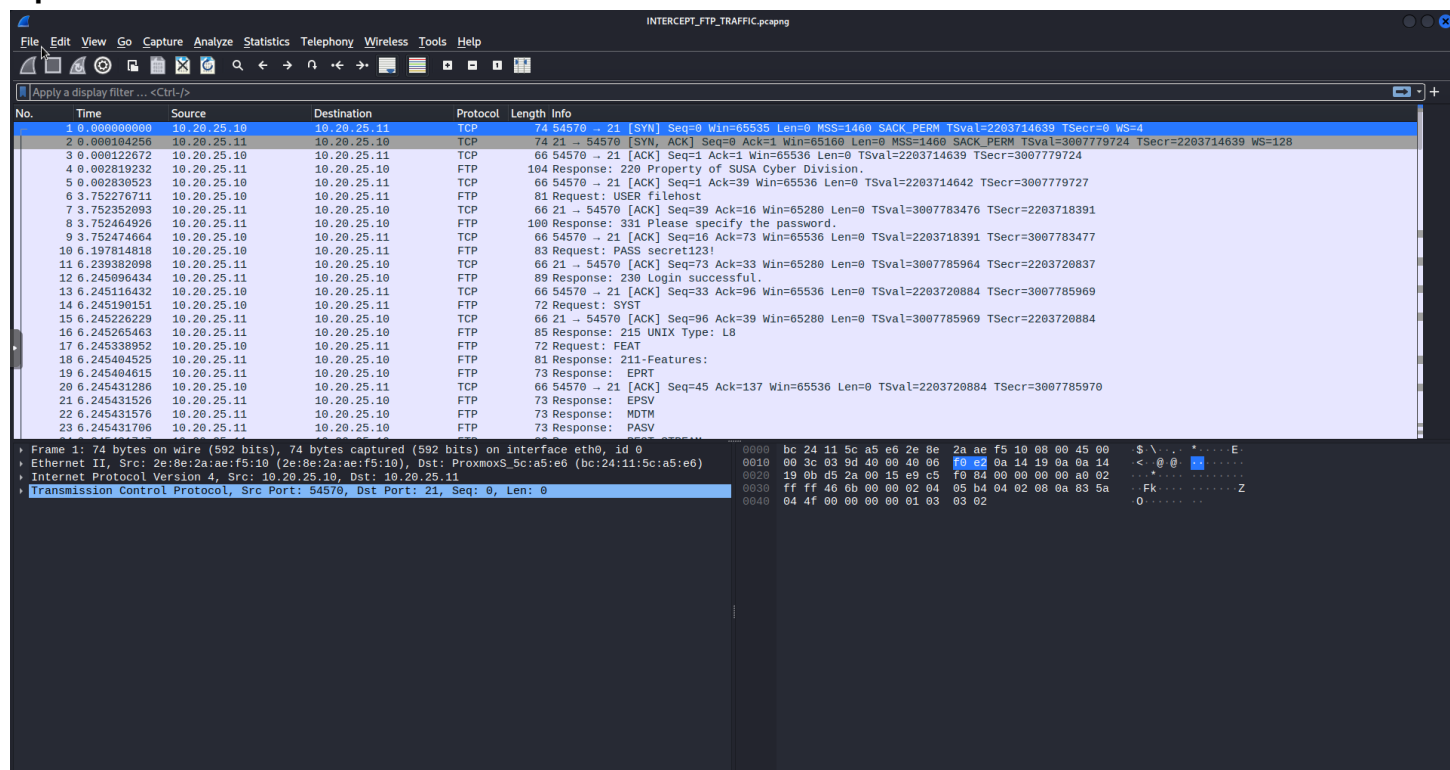
- IT

Recommended Tools

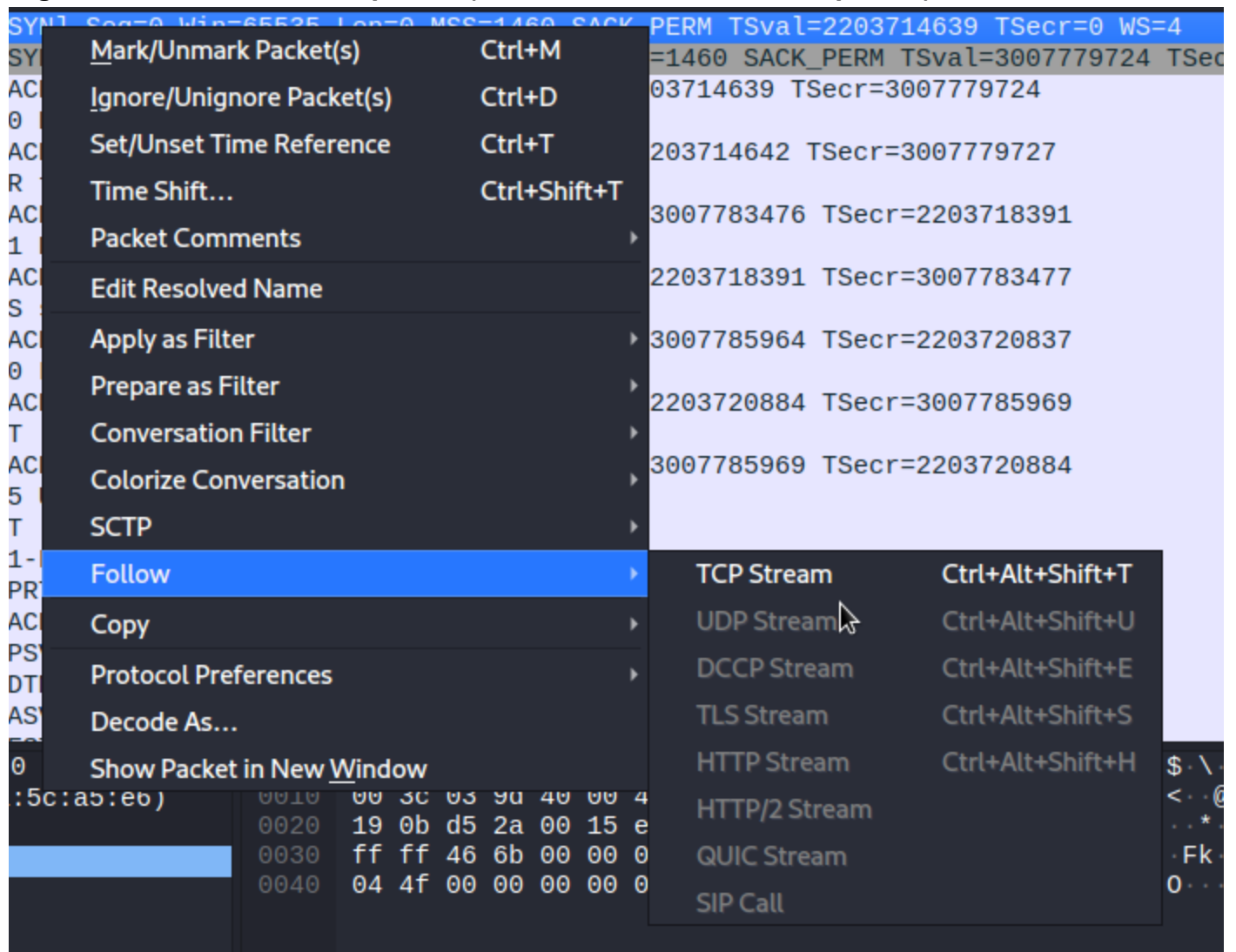
- Wireshark
- Cyberchef/Online Base64 Decoder

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

```

220 Property of SUSANA Cyber Division.
USER filehost
331 Please specify the password.
PASS secret123!
230 Login successful.
SYST
215 UNIX Type: L8
FEAT
211-Features:
EPRT
EPSV
MDTM
PASV
REST STREAM
SIZE
TVFS
211 End
EPSV
229 Entering Extended Passive Mode (|||31300|)
LIST
150 Here comes the directory listing.
226 Directory send OK.
EPSV
229 Entering Extended Passive Mode (|||60004|)
NLST
150 Here comes the directory listing.
226 Directory send OK.
TYPE I
200 Switching to Binary mode.
SIZE SUSANA_2025_INT.sec
213 109
EPSV
229 Entering Extended Passive Mode (|||49532|)
RETR SUSANA_2025_INT.sec
150 Opening BINARY mode data connection for SUSANA_2025_INT.sec (109 bytes).
226 Transfer complete.
MDTM SUSANA_2025_INT.sec
213 20250408202541
QUIT
221 Goodbye.

```

14 client pkt(s), 26 server pkt(s), 28 turn(s).

Entire conversation (798 bytes)

Show data as ASCII

Stream 0

Find:

Find Next

Filter Out This Stream

Print

Save as...

Back

Close

Help

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**

```

220 Property of SUSANA Cyber Division.
USER filehost

```

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

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|-------------|-------------|----------|--------|---|
| 1 | 0.000000000 | 10.20.25.10 | 10.20.25.11 | TCP | 74 | 54570 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=2203714639 TSecr=0 WS=4 |
| 2 | 0.000104256 | 10.20.25.11 | 10.20.25.10 | TCP | 74 | 21 → 54570 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3007779724 TSecr=2203714639 WS=128 |
| 3 | 0.000122672 | 10.20.25.10 | 10.20.25.11 | TCP | 66 | 54570 → 21 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=2203714639 TSecr=3007779724 |
| 4 | 0.002819232 | 10.20.25.11 | 10.20.25.10 | FTP | 104 | Response: 220 Property of SUSANA Cyber Division. |
| 5 | 0.002830523 | 10.20.25.10 | 10.20.25.11 | TCP | 66 | 54570 → 21 [ACK] Seq=1 Ack=39 Win=65536 Len=0 TSval=2203714642 TSecr=3007779727 |
| 6 | 0.002970741 | 10.20.25.10 | 10.20.25.11 | FTP | 66 | Request: USER filehost |
| 7 | 0.782352093 | 10.20.25.11 | 10.20.25.10 | TCP | 66 | 21 → 54570 [ACK] Seq=39 Ack=16 Win=65280 Len=0 TSval=3007783476 TSecr=2203718391 |
| 8 | 0.752464926 | 10.20.25.11 | 10.20.25.10 | FTP | 100 | Response: 331 Please specify the password. |
| 9 | 0.752474664 | 10.20.25.10 | 10.20.25.11 | TCP | 66 | 54570 → 21 [ACK] Seq=16 Ack=73 Win=65536 Len=0 TSval=2203718391 TSecr=3007783477 |
| 10 | 6.197814818 | 10.20.25.10 | 10.20.25.11 | FTP | 83 | Request: PASS secret123! |
| 11 | 6.239382098 | 10.20.25.11 | 10.20.25.10 | TCP | 66 | 21 → 54570 [ACK] Seq=73 Ack=33 Win=65280 Len=0 TSval=3007785964 TSecr=2203720837 |
| 12 | 6.245096434 | 10.20.25.11 | 10.20.25.10 | FTP | 89 | Response: 230 Login successful. |
| 13 | 6.245116432 | 10.20.25.10 | 10.20.25.11 | TCP | 66 | 54570 → 21 [ACK] Seq=33 Ack=96 Win=65536 Len=0 TSval=2203720884 TSecr=3007785969 |
| 14 | 6.245190151 | 10.20.25.10 | 10.20.25.11 | FTP | 72 | Request: SYST |
| 15 | 6.245226229 | 10.20.25.11 | 10.20.25.10 | TCP | 66 | 21 → 54570 [ACK] Seq=96 Ack=39 Win=65280 Len=0 TSval=3007785969 TSecr=2203720884 |
| 16 | 6.245265463 | 10.20.25.11 | 10.20.25.10 | FTP | 85 | Response: 215 UNIX Type: L8 |
| 17 | 6.245338952 | 10.20.25.10 | 10.20.25.11 | FTP | 72 | Request: FEAT |
| 18 | 6.245404525 | 10.20.25.11 | 10.20.25.10 | FTP | 81 | Response: 211-Features: |
| 19 | 6.245404615 | 10.20.25.11 | 10.20.25.10 | FTP | 73 | Response: EPRT |
| 20 | 6.245431286 | 10.20.25.10 | 10.20.25.11 | TCP | 66 | 54570 → 21 [ACK] Seq=45 Ack=137 Win=65536 Len=0 TSval=2203720884 TSecr=3007785970 |
| 21 | 6.245431526 | 10.20.25.11 | 10.20.25.10 | FTP | 73 | Response: EPSV |
| 22 | 6.245431570 | 10.20.25.11 | 10.20.25.10 | FTP | 73 | Response: MDTM |
| 23 | 6.245431706 | 10.20.25.11 | 10.20.25.10 | FTP | 73 | Response: PASV |

| | | | |
|---|------|---|------------------------|
| Frame 6: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface eth0, id 0 | 0000 | bc 24 11 5c a5 e6 2e 8e 2a ae f5 10 08 00 45 10 | \$ \ E |
| Ethernet II, Src: 2e:8e:2a:ae:f5:10 (2e:8e:2a:ae:f5:10), Dst: ProxmoxS_5c:a5:e6 (bc:24:11:5c:a5:e6) | 0010 | 00 43 03 a0 40 00 40 06 f0 c8 0a 14 19 0a 0a 14 | . C @ @ |
| Internet Protocol Version 4, Src: 10.20.25.10, Dst: 10.20.25.11 | 0020 | 19 0b d5 2a 00 15 e9 c5 f0 85 50 3b 47 0d 00 18 | . * P : 0 |
| Transmission Control Protocol, Src Port: 54570, Dst Port: 21, Seq: 1, Ack: 39, Len: 15 | 0030 | 40 00 46 72 00 00 01 01 08 0a 83 5a 12 f7 b3 47 | @ Fr Z . . G |
| File Transfer Protocol (FTP) | 0040 | 13 8f 55 53 45 52 20 66 69 6c 65 68 6f 73 74 0d | . USER f ilehost . |
| Request command: USER | 0050 | | |
| Request arg: filehost | | | |
| [Current working directory:] | | | |

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

| | | | | | | | |
|----|--------------|-------------|-------------|-----|-----|---|--|
| 1 | 0.000000000 | 10.20.25.10 | 10.20.25.11 | TCP | 74 | 54570 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=2203714639 TSecr=0 WS=4 | |
| 2 | 0.000104256 | 10.20.25.11 | 10.20.25.10 | TCP | 74 | 21 → 54570 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3007779724 TSecr=2203714639 WS=128 | |
| 3 | 0.000122672 | 10.20.25.10 | 10.20.25.11 | TCP | 66 | 54570 → 21 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=2203714639 TSecr=3007779724 | |
| 4 | 0.0002819232 | 10.20.25.11 | 10.20.25.10 | FTP | 104 | Response: 220 Property of SUSA Cyber Division. | |
| 5 | 0.0002830523 | 10.20.25.10 | 10.20.25.11 | TCP | 66 | 54570 → 21 [ACK] Seq=1 Ack=39 Win=65536 Len=0 TSval=2203714642 TSecr=3007779727 | |
| 6 | 3.752276711 | 10.20.25.10 | 10.20.25.11 | FTP | 81 | Request: USER filehost | |
| 7 | 3.752352693 | 10.20.25.11 | 10.20.25.10 | TCP | 66 | 21 → 54570 [ACK] Seq=39 Ack=16 Win=65280 Len=0 TSval=3007783476 TSecr=2203718391 | |
| 8 | 3.752464926 | 10.20.25.11 | 10.20.25.10 | FTP | 100 | Response: 331 Please specify the password. | |
| 9 | 3.752474664 | 10.20.25.10 | 10.20.25.11 | TCP | 66 | 54570 → 21 [ACK] Seq=16 Ack=73 Win=65536 Len=0 TSval=2203718391 TSecr=3007783477 | |
| 10 | 6.197814818 | 10.20.25.10 | 10.20.25.11 | FTP | 83 | Request: PASS secret123! | |
| 11 | 6.239382098 | 10.20.25.11 | 10.20.25.10 | TCP | 66 | 21 → 54570 [ACK] Seq=73 Ack=33 Win=65280 Len=0 TSval=3007785964 TSecr=2203720837 | |
| 12 | 6.245096434 | 10.20.25.11 | 10.20.25.10 | FTP | 89 | Response: 230 Login successful. | |
| 13 | 6.245116432 | 10.20.25.10 | 10.20.25.11 | TCP | 66 | 54570 → 21 [ACK] Seq=33 Ack=96 Win=65536 Len=0 TSval=2203720884 TSecr=3007785969 | |
| 14 | 6.245190151 | 10.20.25.10 | 10.20.25.11 | FTP | 72 | Request: SYST | |
| 15 | 6.245226229 | 10.20.25.11 | 10.20.25.10 | TCP | 66 | 21 → 54570 [ACK] Seq=96 Ack=39 Win=65280 Len=0 TSval=3007785969 TSecr=2203720884 | |
| 16 | 6.245265463 | 10.20.25.11 | 10.20.25.10 | FTP | 85 | Response: 215 UNIX Type: L8 | |
| 17 | 6.245338952 | 10.20.25.10 | 10.20.25.11 | FTP | 72 | Request: FEAT | |
| 18 | 6.245404525 | 10.20.25.11 | 10.20.25.10 | FTP | 81 | Response: 211-Features: | |
| 19 | 6.245404615 | 10.20.25.11 | 10.20.25.10 | FTP | 73 | Response: EPRT | |
| 20 | 6.245431286 | 10.20.25.10 | 10.20.25.11 | TCP | 66 | 54570 → 21 [ACK] Seq=45 Ack=137 Win=65536 Len=0 TSval=2203720884 TSecr=3007785970 | |
| 21 | 6.245431526 | 10.20.25.11 | 10.20.25.10 | FTP | 73 | Response: EPSV | |
| 22 | 6.245431576 | 10.20.25.11 | 10.20.25.10 | FTP | 73 | Response: MDTM | |
| 23 | 6.245431706 | 10.20.25.11 | 10.20.25.10 | FTP | 73 | Response: PASV | |

| | | | |
|---|------|---|-----------------------|
| Frame 10: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface eth0, id 0 | 0000 | bc 24 11 5c a5 e6 2e 8e 2a ae f5 10 08 00 45 10 | \$ \ E |
| Ethernet II, Src: 2e:8e:2a:ae:f5:10 (2e:8e:2a:ae:f5:10), Dst: ProxmoxS_5c:a5:e6 (bc:24:11:5c:a5:e6) | 0010 | 00 45 03 a2 40 00 40 06 f0 c4 0a 14 19 0a 0a 14 | E _ @ _ |
| Internet Protocol Version 4, Src: 10.20.25.10, Dst: 10.20.25.11 | 0020 | 19 0b d5 2a 00 15 e9 c5 f0 94 50 3b 47 2f 80 18 | P;G/ |
| Transmission Control Protocol, Src Port: 54570, Dst Port: 21, Seq: 16, Ack: 73, Len: 17 | 0030 | 40 00 46 74 00 00 01 01 08 0a 83 5a 1c 85 b3 47 | @ F Z . . G |
| File Transfer Protocol (FTP) | 0040 | 22 35 50 41 53 53 20 73 65 63 72 65 74 31 32 33 | "5PASS s ecret123 |
| Request command: PASS | 0050 | 21 0d 0a | ! |
| Request arg: secret123! | | | |
| [Current working directory:] | | | |

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

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|-------------|-------------|----------|--------|--|
| 31 | 7.946260871 | 10.20.25.11 | 10.20.25.10 | FTP | 114 | Response: 229 Entering Extended Passive Mode (31300) |
| 32 | 7.946275009 | 10.20.25.10 | 10.20.25.11 | TCP | 66 | 54570 → 21 [ACK] Seq=51 Ack=243 Win=65536 Len=0 TSval=2203722585 TSecr=3007787670 |
| 36 | 7.946460377 | 10.20.25.10 | 10.20.25.11 | FTP | 72 | Request: LIST |
| 37 | 7.946650506 | 10.20.25.11 | 10.20.25.10 | FTP | 105 | Response: 150 Here comes the directory listing. |
| 43 | 7.946832850 | 10.20.25.11 | 10.20.25.10 | FTP | 90 | Response: 226 Directory send OK. |
| 44 | 7.946855482 | 10.20.25.10 | 10.20.25.11 | TCP | 66 | 54570 → 21 [ACK] Seq=57 Ack=306 Win=65536 Len=0 TSval=2203722586 TSecr=3007787671 |
| 45 | 15.321627367 | 10.20.25.10 | 10.20.25.11 | FTP | 72 | Request: EPSV |
| 46 | 15.321904429 | 10.20.25.11 | 10.20.25.10 | FTP | 114 | Response: 229 Entering Extended Passive Mode (60004) |
| 50 | 15.322080801 | 10.20.25.10 | 10.20.25.11 | FTP | 72 | Request: NLST |
| 51 | 15.322271621 | 10.20.25.11 | 10.20.25.10 | FTP | 105 | Response: 150 Here comes the directory listing. |
| 57 | 15.322553732 | 10.20.25.11 | 10.20.25.10 | FTP | 90 | Response: 226 Directory send OK. |
| 58 | 15.322573780 | 10.20.25.10 | 10.20.25.11 | TCP | 66 | 54570 → 21 [ACK] Seq=69 Ack=417 Win=65536 Len=0 TSval=2203729961 TSecr=3007795046 |
| 59 | 16.133754652 | 10.20.25.10 | 10.20.25.11 | FTP | 74 | Request: TYPE I |
| 60 | 16.133882042 | 10.20.25.11 | 10.20.25.10 | FTP | 97 | Response: 200 Switching to Binary mode. |
| 61 | 16.133933749 | 10.20.25.10 | 10.20.25.11 | FTP | 90 | Request: SIZE SUSA_2025_INT.sec |
| 62 | 16.134012218 | 10.20.25.11 | 10.20.25.10 | FTP | 75 | Response: 213 109 |
| 63 | 16.134053034 | 10.20.25.10 | 10.20.25.11 | FTP | 72 | Request: EPSV |
| 64 | 16.134185393 | 10.20.25.11 | 10.20.25.10 | FTP | 114 | Response: 229 Entering Extended Passive Mode (49532) |
| 68 | 16.134337560 | 10.20.25.10 | 10.20.25.11 | FTP | 90 | Request: RETR SUSA_2025_INT.sec |
| 69 | 16.134526736 | 10.20.25.11 | 10.20.25.10 | FTP | 142 | Response: 150 Opening BINARY mode data connection for SUSA_2025_INT.sec (109 bytes). |
| 75 | 16.134818436 | 10.20.25.11 | 10.20.25.10 | FTP | 90 | Response: 226 Transfer complete. |
| 76 | 16.135066240 | 10.20.25.10 | 10.20.25.11 | TCP | 66 | 54570 → 21 [ACK] Seq=131 Ack=605 Win=65536 Len=0 TSval=2203730774 TSecr=3007795859 |
| 77 | 16.135637469 | 10.20.25.10 | 10.20.25.11 | FTP | 90 | Request: MDTM SUSA_2025_INT.sec |

| | | | |
|---|------|---|---------------------|
| Frame 61: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface eth0, id 0 | 0000 | bc 24 11 5c a5 e6 2e 8e 2a ae f5 10 08 00 45 10 | \$ \ E |
| Ethernet II, Src: 2e:8e:2a:ae:f5:10 (2e:8e:2a:ae:f5:10), Dst: ProxmoxS_5c:a5:e6 (bc:24:11:5c:a5:e6) | 0010 | 00 4c 03 b1 40 00 40 06 f0 ae 0a 14 19 0a 0a 14 | L _ @ _ |
| Internet Protocol Version 4, Src: 10.20.25.10, Dst: 10.20.25.11 | 0020 | 19 0b d5 2a 00 15 e9 c5 f0 d1 50 3b 48 a6 80 18 | P;H |
| Transmission Control Protocol, Src Port: 54570, Dst Port: 21, Seq: 77, Ack: 448, Len: 24 | 0030 | 40 00 46 7b 00 00 01 01 08 0a 83 5a 43 55 b3 47 | @ F ZCU.G |
| File Transfer Protocol (FTP) | 0040 | 52 92 53 49 5a 45 20 53 55 53 41 5f 32 30 32 35 | R SIZE S USA 2025 |
| Request command: SIZE | 0050 | 5f 49 4e 54 2e 73 65 63 0d 0a | INT.sec |
| Request arg: SUSA_2025_INT.sec | | | |
| [Current working directory:] | | | |

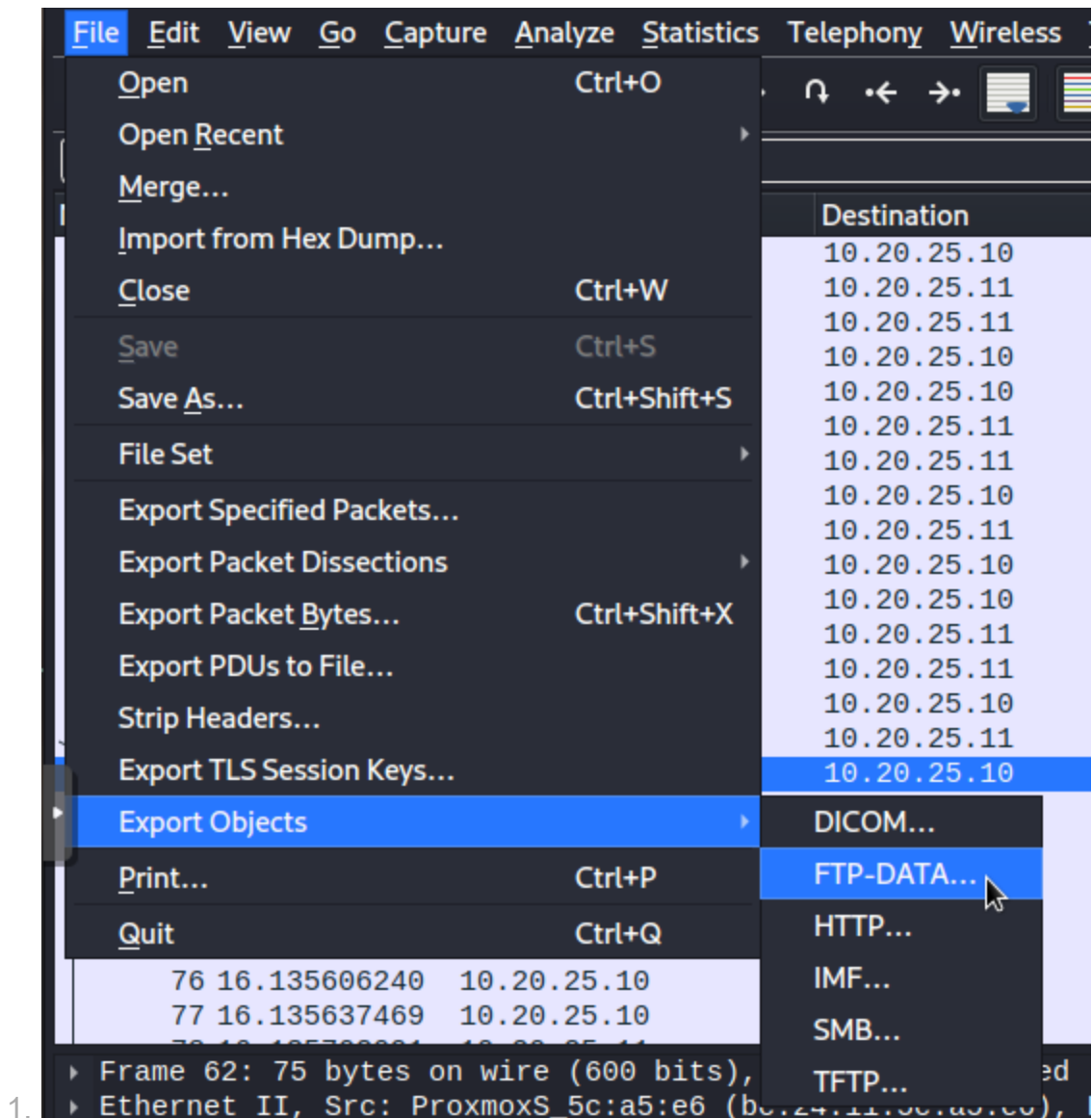
7. To find the size in Bytes , Check either the TCP stream or the raw packet capture

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

~or~ Look at line 62 of the packet capture

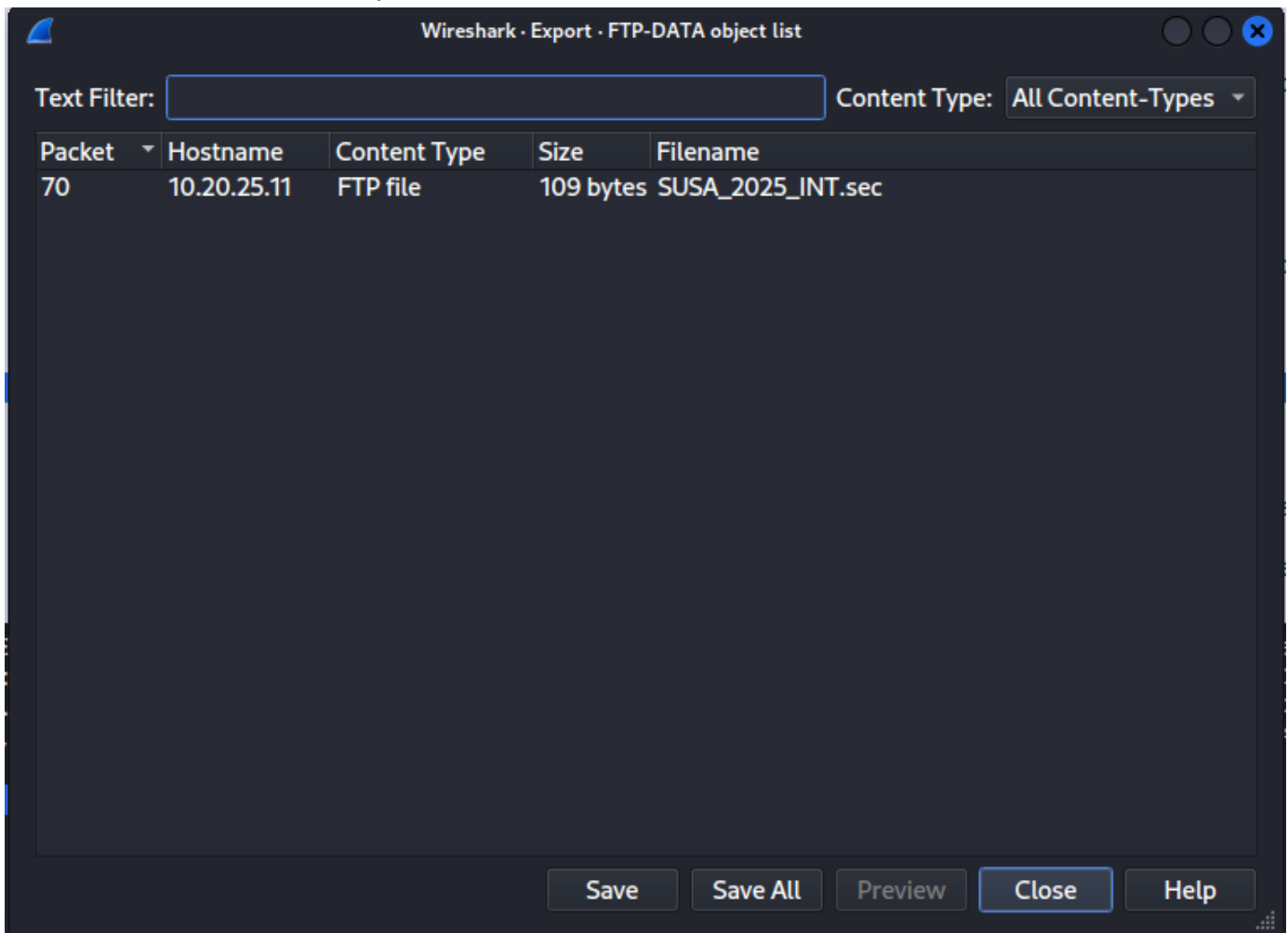

```
31 7.946260871 10.20.25.11 10.20.25.10 FTP 114 Response: 229 Entering Extended Passive Mode (|||31300|)
32 7.946275009 10.20.25.10 10.20.25.11 TCP 66 54570 -> 21 [ACK] Seq=51 Ack=243 Win=65536 Len=0 TSval=2203722585 TSecr=3007787670
36 7.946460377 10.20.25.10 10.20.25.11 FTP 72 Request: LIST
37 7.946650506 10.20.25.11 10.20.25.10 FTP 105 Response: 150 Here comes the directory listing.
43 7.946832850 10.20.25.11 10.20.25.10 FTP 90 Response: 226 Directory send OK.
44 7.946855482 10.20.25.10 10.20.25.11 TCP 66 54570 -> 21 [ACK] Seq=57 Ack=306 Win=65536 Len=0 TSval=2203722586 TSecr=3007787671
45 15.321627367 10.20.25.10 10.20.25.11 FTP 72 Request: EPSV
46 15.321904429 10.20.25.11 10.20.25.10 FTP 114 Response: 229 Entering Extended Passive Mode (|||60004|)
50 15.322080801 10.20.25.10 10.20.25.11 FTP 72 Request: NLST
51 15.322271621 10.20.25.11 10.20.25.10 FTP 105 Response: 150 Here comes the directory listing.
57 15.322553732 10.20.25.11 10.20.25.10 FTP 90 Response: 226 Directory send OK.
58 15.322573780 10.20.25.10 10.20.25.11 TCP 66 54570 -> 21 [ACK] Seq=69 Ack=417 Win=65536 Len=0 TSval=2203729961 TSecr=3007795046
59 16.133754652 10.20.25.10 10.20.25.11 FTP 74 Request: TYPE I
60 16.133882042 10.20.25.11 10.20.25.10 FTP 97 Response: 200 Switching to Binary mode.
61 16.133933749 10.20.25.10 10.20.25.11 FTP 90 Request: SIZE SUSA_2025_INT.sec
62 16.134012210 10.20.25.11 10.20.25.10 FTP 75 Response: 213 109
63 16.134053034 10.20.25.10 10.20.25.11 FTP 72 Request: EPSV
64 16.134185393 10.20.25.11 10.20.25.10 FTP 114 Response: 229 Entering Extended Passive Mode (|||49532|)
68 16.134337560 10.20.25.10 10.20.25.11 FTP 90 Request: RETR SUSA_2025_INT.sec
69 16.134526736 10.20.25.11 10.20.25.10 FTP 142 Response: 150 Opening BINARY mode data connection for SUSA_2025_INT.sec (109 bytes).
75 16.134818436 10.20.25.11 10.20.25.10 FTP 90 Response: 226 Transfer complete.
76 16.135606240 10.20.25.10 10.20.25.11 TCP 66 54570 -> 21 [ACK] Seq=131 Ack=605 Win=65536 Len=0 TSval=2203730774 TSecr=3007795059
77 16.135637469 10.20.25.10 10.20.25.11 FTP 90 Request: MDTM SUSA_2025_INT.sec
78 16.135653001 10.20.25.11 10.20.25.10 FTP 90 Response: 213 109
> Frame 62: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface eth0, id 0
> Ethernet II, Src: ProxmoxS_5c:a5:e6 (bc:24:11:5c:a5:e6), Dst: 2e:8e:2a:ae:f5:10 (2e:8e:2a:ae:f5:10)
> Internet Protocol Version 4, Src: 10.20.25.11, Dst: 10.20.25.10
> Transmission Control Protocol, Src Port: 21, Dst Port: 54570, Seq: 448, Ack: 101, Len: 9
> File Transfer Protocol (FTP)
  * 213 109\r\n
    Response code: File status (213)
    Response arg: 109
    [Current working directory: ]
0000 2e 8e 2a ae f5 10 bc 24 11 5c a5 e6 08 00 45 00  . . . . $ \ . . . E
0010 00 3d df 91 40 00 40 06 14 ed 0a 14 19 0b 0a 14  . . . . @ @ . . . .
0020 19 0a 00 15 d5 2a 59 3b 48 a6 e9 c5 f0 e9 80 18  . . . . * P ; H . . . .
0030 01 fe 40 6c 00 00 01 01 00 0a b3 47 52 92 83 5a  . . . . f l . . . P ; H . . . .
0040 43 55 32 31 33 20 31 30 39 0d 00                CU213 10 9\r\n
```

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

Version 10.5.2 - Sponsored by DEF24.com

Last build: 2 years ago - Version 10 is here! Read about the new features here

Options About / Support

Operations

Search...

Favourites

To Base64

From Base64

To Hex

From Hex

To Hexdump

From Hexdump

URL Decode

Regular expression

Entropy

Fork

Magic

Data format

Encryption / Encoding

Public Key

Arithmetic / Logic

Networking

Language

Utils

Date / Time

Extractors

Compression

Hashing

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars

☐ Strict mode

STEP

BAKE!

☒ Auto Bake

Input

Sa5R2MaG0n3p2dZpbmcu0Q9NCKs12Mqg08lge141E20UCBz2X22X1s108y2aL1bnRPhcz10HhdagYnW1b1B6zHf r2aQuL14NC1dg5Vqj

Output

Intel Briefing.
Need to fix FTP server, credentials have been leaked...
- IT