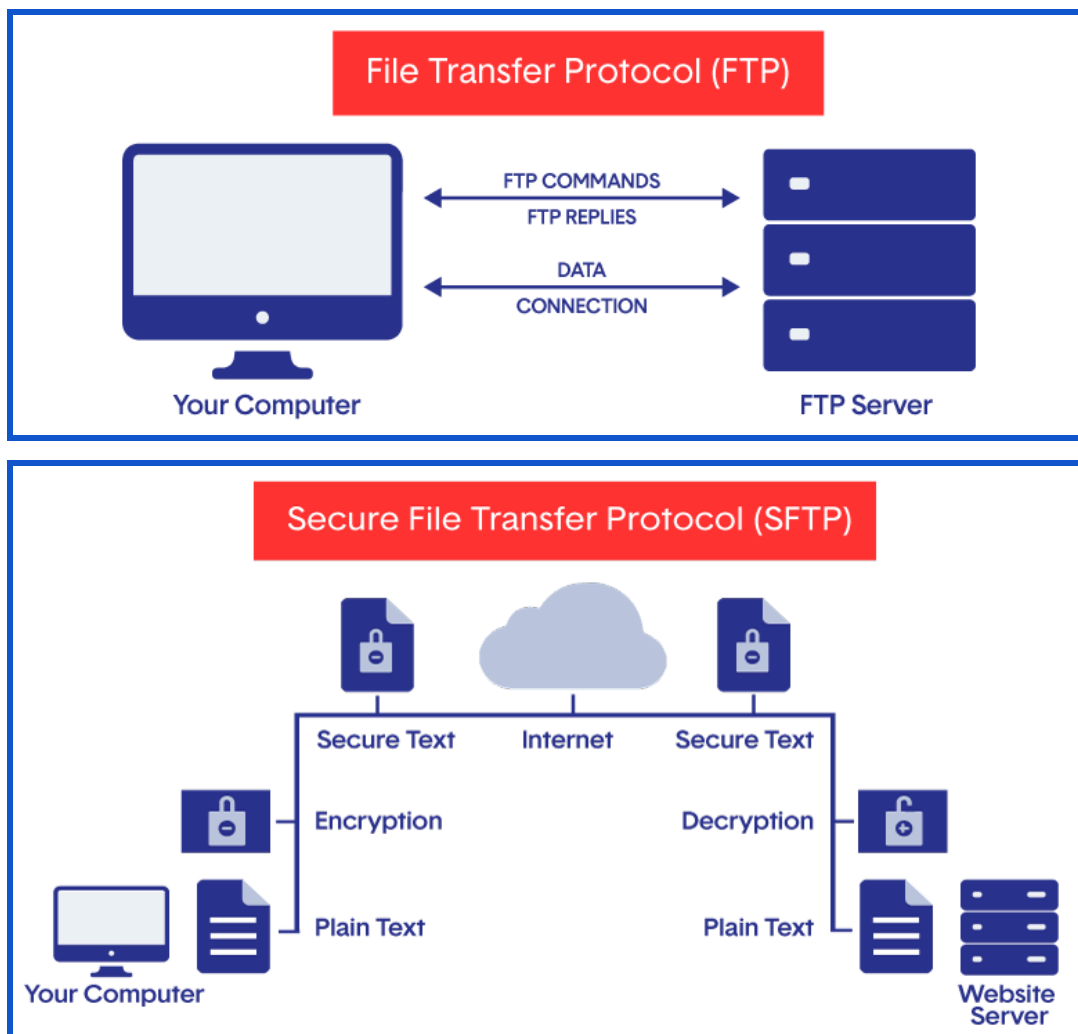


## Wireshark HW 2.0 Analyzing FTP PacketsV(

### OVERVIEW

**File Transfer Protocol (FTP)** is a protocol, or set of rules, used to exchange files over the Internet using an FTP client program. You can copy or move files from a server to a client (laptop, smartphone, etc.), and upload or transfer files from a client to a server. However, using this method is not secure. So your user name, password, and files are not encrypted, which can be intercepted by a threat actor. Instead, other protocols are used, such as **SFTP (FTP over SSH)** and **FTPS (FTP over SSL)** since it is secure and the information is not in plain text.

### FTP vs. SFTP

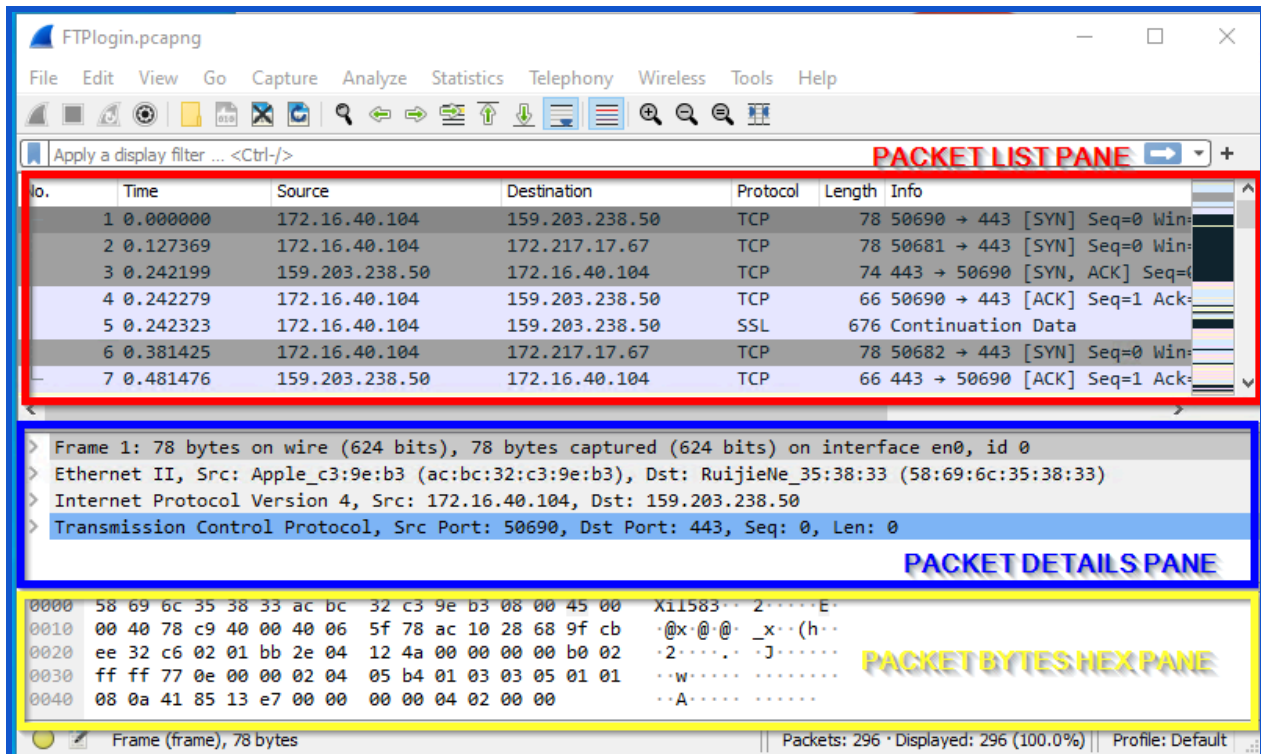


## SCENARIO

At work, Sam has just been assigned a project. Recently, there was some activity on the company's network that was sent over FTP protocol. Knowing that this network is unsafe, it is Sam's job to discover exactly what delicate information was put at risk and then explain this information to the employees so they can keep their information safe moving forward.

## OBJECTIVE

In this lab will take a closer look at the project Sam has been assigned. And use Wireshark to examine what was sent over FTP.



The screenshot shows the Wireshark interface with the file **FTPlogin.pcapng** open. The **PACKET LIST PANE** displays a list of captured packets. The first packet is a SYN packet from 172.16.40.104 to 159.203.238.50 on port 443. The **PACKET DETAILS PANE** shows the structure of the first packet: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The **PACKET BYTES HEX PANE** shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.40.104	159.203.238.50	TCP	78	50690 → 443 [SYN] Seq=0 Win=0
2	0.127369	172.16.40.104	172.217.17.67	TCP	78	50681 → 443 [SYN] Seq=0 Win=0
3	0.242199	159.203.238.50	172.16.40.104	TCP	74	443 → 50690 [SYN, ACK] Seq=0
4	0.242279	172.16.40.104	159.203.238.50	TCP	66	50690 → 443 [ACK] Seq=1 Ack=0
5	0.242323	172.16.40.104	159.203.238.50	SSL	676	Continuation Data
6	0.381425	172.16.40.104	172.217.17.67	TCP	78	50682 → 443 [SYN] Seq=0 Win=0
7	0.481476	159.203.238.50	172.16.40.104	TCP	66	443 → 50690 [ACK] Seq=1 Ack=0

Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface en0, id 0  
Ethernet II, Src: Apple\_c3:9e:b3 (ac:bc:32:c3:9e:b3), Dst: RuijieNe\_35:38:33 (58:69:6c:35:38:33)  
Internet Protocol Version 4, Src: 172.16.40.104, Dst: 159.203.238.50  
Transmission Control Protocol, Src Port: 50690, Dst Port: 443, Seq: 0, Len: 0

0000 58 69 6c 35 38 33 ac bc 32 c3 9e b3 08 00 45 00 X11583... 2.....E..  
0010 00 40 78 c9 40 00 40 06 5f 78 ac 10 28 68 9f cb .@x:@. \_x..(h..  
0020 ee 32 c6 02 01 bb 2e 04 12 4a 00 00 00 00 b0 02 .2..... .J.....  
0030 ff ff 77 0e 00 00 02 04 05 b4 01 03 03 05 01 01 ..w.....  
0040 08 0a 41 85 13 e7 00 00 00 00 04 02 00 00 ..A.....

## Steps

Download this file and double-click it to open it in Wireshark: [FTPlogin.pcapng](#)

## Submission Process

Complete and answer the following questions and activities below. Submit an edited version of this document with the appended answers.

In the image above, we can see 7 packets in the **Packet List Pane**.

- How many different computers are involved in these packets?

*Three*

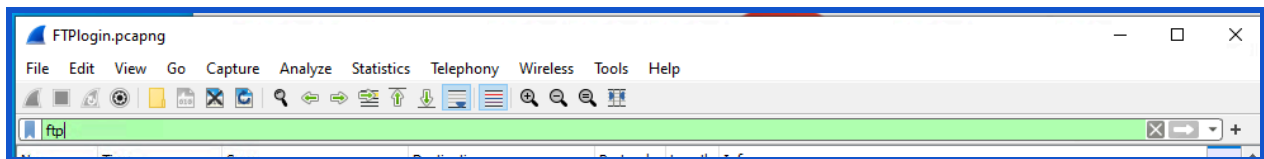
- How can you tell?

*By looking at the IP addresses*

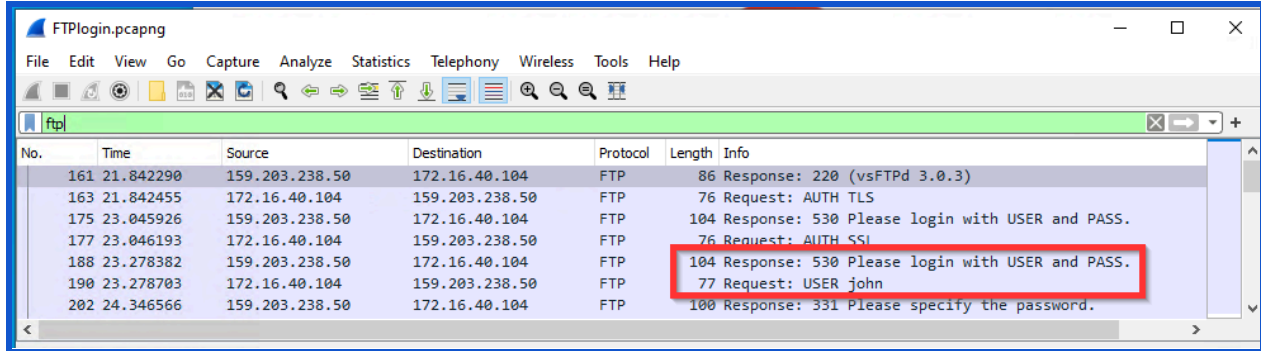
The FTP protocol that Sam's colleagues use is a very unsafe protocol because it sends information over the network without encryption (known as plain or clear text). To find out who used this protocol, we will analyze the PCAP file to find their username and password.

**Follow the steps below to find this information:**

1. In Wireshark, at the top, in the "Apply a display filter" box, type ftp and press the "Enter" key. Wireshark filters the packets, showing only the packets that use File Transfer Protocol (FTP).



2. On the right side, under the **"Info"** column, you can see the login process for a user named "john".



No.	Time	Source	Destination	Protocol	Length	Info
161	21.842290	159.203.238.50	172.16.40.104	FTP	86	Response: 220 (vsFTPd 3.0.3)
163	21.842455	172.16.40.104	159.203.238.50	FTP	76	Request: AUTH TLS
175	23.045926	159.203.238.50	172.16.40.104	FTP	104	Response: 530 Please login with USER and PASS.
177	23.046193	172.16.40.104	159.203.238.50	FTP	76	Request: AUTH SSI
188	23.278382	159.203.238.50	172.16.40.104	FTP	104	Response: 530 Please login with USER and PASS.
190	23.278703	172.16.40.104	159.203.238.50	FTP	77	Request: USER john
202	24.346566	159.203.238.50	172.16.40.104	FTP	100	Response: 331 Please specify the password.

## John's Password

Now that we know the username "John" by looking in the info category of these packets.

- Can you find the Password too?

Yes

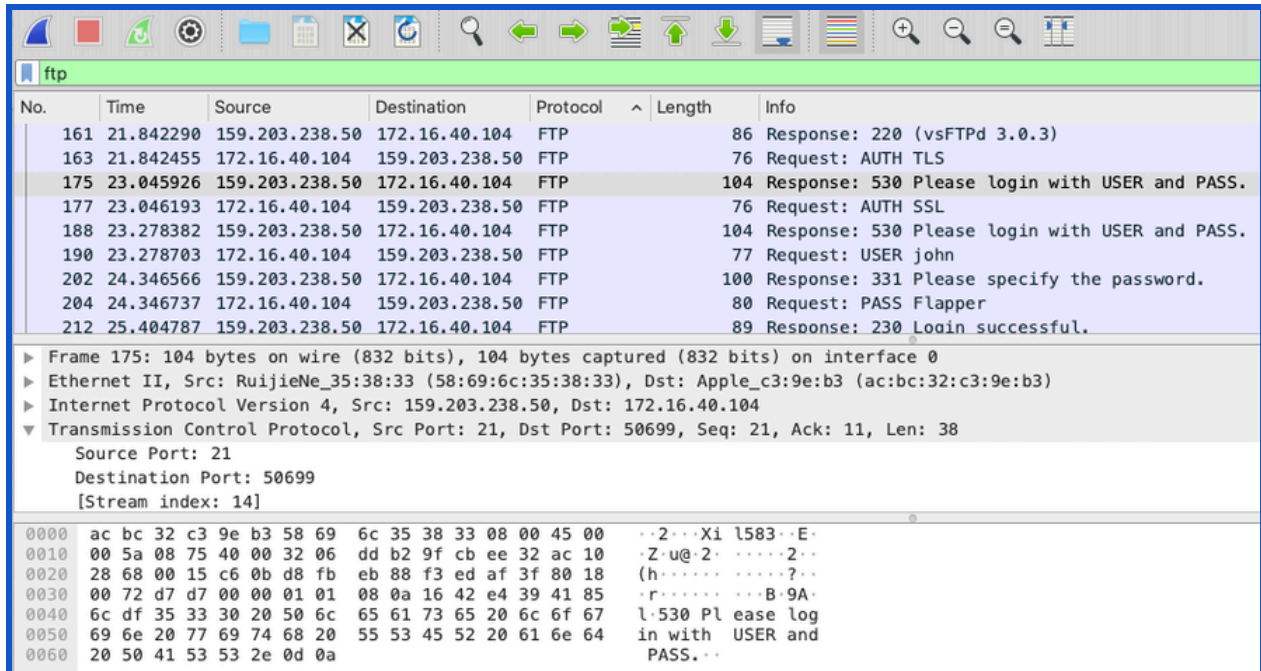
- What is John's password ?

Flapper

Explain, in your own words, why someone should not use an **FTP Server**

FTP was not built to be secure. It is generally considered to be an insecure protocol because it relies on clear-text usernames and passwords for authentication and does not use encryption. Data sent via FTP is vulnerable to sniffing, spoofing, and brute force attacks, among other basic attack methods.

Sam can perform a packet capture to notice that someone used FTP to log into a server to upload and download several files. Knowing how insecure this protocol is, Sam decided to identify who performed this action so they could provide them with feedback on proper cybersecurity procedures and rules. Use the image below to respond to the question regarding this issue.



No.	Time	Source	Destination	Protocol	Length	Info
161	21.842290	159.203.238.50	172.16.40.104	FTP	86	Response: 220 (vsFTPd 3.0.3)
163	21.842455	172.16.40.104	159.203.238.50	FTP	76	Request: AUTH TLS
175	23.045926	159.203.238.50	172.16.40.104	FTP	104	Response: 530 Please login with USER and PASS.
177	23.046193	172.16.40.104	159.203.238.50	FTP	76	Request: AUTH SSL
188	23.278382	159.203.238.50	172.16.40.104	FTP	104	Response: 530 Please login with USER and PASS.
190	23.278703	172.16.40.104	159.203.238.50	FTP	77	Request: USER john
202	24.346566	159.203.238.50	172.16.40.104	FTP	100	Response: 331 Please specify the password.
204	24.346737	172.16.40.104	159.203.238.50	FTP	80	Request: PASS Flapper
212	25.404787	159.203.238.50	172.16.40.104	FTP	89	Response: 230 Login successful.

Frame 175: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface 0		
Ethernet II, Src: RuijieNe_35:38:33 (58:69:6c:35:38:33), Dst: Apple_c3:9e:b3 (ac:bc:32:c3:9e:b3)		
Internet Protocol Version 4, Src: 159.203.238.50, Dst: 172.16.40.104		
Transmission Control Protocol, Src Port: 21, Dst Port: 50699, Seq: 21, Ack: 11, Len: 38		
Source Port: 21		
Destination Port: 50699		
[Stream index: 14]		

0000	ac bc 32 c3 9e b3 58 69	6c 35 38 33 08 00 45 00	..2...Xi 1583..E.
0010	00 5a 08 75 40 00 32 06	dd b2 9f cb ee 32 ac 10	.Z.u@.2. ....2..
0020	28 68 00 15 c6 0b d8 fb	eb 88 f3 ed af 3f 80 18	(h.....?..
0030	00 72 d7 d7 00 00 01 01	08 0a 16 42 e4 39 41 85	.r.....B.9A.
0040	6c df 35 33 30 20 50 6c	65 61 73 65 20 6c 6f 67	l.530 Pl ease log
0050	69 6e 20 77 69 74 68 20	55 53 45 52 20 61 6e 64	in with USER and
0060	20 50 41 53 53 2e 0d 0a		PASS...

FTP, like all other protocols, has a port number that belongs to it. A port number identifies the process or service running on a system.

Using the image above, identify the port number for the FTP protocol:

21

FTPLogin.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp + DAB TCP

	Destination	Protocol	Length	Info
50	172.16.40.104	FTP	86	Response: 220 (vsFTPd 3.0.3)
4	159.203.238.50	FTP	76	Request: AUTH TLS
50	172.16.40.104	FTP	104	Response: 530 Please login with USER and PASS.
4	159.203.238.50	FTP	76	Request: AUTH SSL
50	172.16.40.104	FTP	104	Response: 530 Please login with USER and PASS.
4	159.203.238.50	FTP	77	Request: USER john
50	172.16.40.104	FTP	100	Response: 331 Please specify the password.
4	159.203.238.50	FTP	80	Request: PASS Flapper
50	172.16.40.104	FTP	89	Response: 230 Login successful.
50	172.16.40.104	FTP	86	Response: 220 (vsFTPd 3.0.3)
4	159.203.238.50	FTP	76	Request: AUTH TLS
50	172.16.40.104	FTP	104	Response: 530 Please login with USER and PASS.
4	159.203.238.50	FTP	76	Request: AUTH SSL
50	172.16.40.104	FTP	104	Response: 530 Please login with USER and PASS.
4	159.203.238.50	FTP	77	Request: USER john
50	172.16.40.104	FTP	100	Response: 331 Please specify the password.
4	159.203.238.50	FTP	80	Request: PASS Flapper
50	172.16.40.104	FTP	89	Response: 230 Login successful.

> Internet Protocol Version 4, Src: 172.16.40.104, Dst: 159.203.238.50  
 > Transmission Control Protocol, Src Port: 50699, Dst Port: 21, Seq: 32, Ack: 131, Len: 14  
 v File Transfer Protocol (FTP)  
 v PASS Flapper\r\n

0000 58 69 6c 35 38 33 ac bc 32 c3 9e b3 08 00 45 00 Xil583.. 2....E.  
 0010 00 42 8d 52 40 00 40 06 4a ed ac 10 28 68 9f cb .B.R@.@. J...(h..  
 0020 ee 32 c6 0b 00 15 f3 ed af 54 d8 fb eb f6 80 18 -2.....-T.....  
 0030 10 11 12 8f 00 00 01 01 08 0a 41 85 72 d9 16 42 .....-A.r.-B  
 0040 e5 70 50 41 53 53 20 46 6c 61 70 70 65 72 0d 0a -pPASS Flapper..

FTPLogin.pcapng | Packets: 296 · Displayed: 39 (13.2%) | Profile: Ibrana Choudhry

FTPlogin.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp X → + DAB TCP

No.	Time	Source	Destination	Protocol	Length	Info
161	2018-05-11 03:45:...	159.203.238.50	172.16.40.104	FTP	86	Response: 220
163	2018-05-11 03:45:...	172.16.40.104	159.203.238.50	FTP	76	Request: AUTH
175	2018-05-11 03:45:...	159.203.238.50	172.16.40.104	FTP	104	Response: 530
177	2018-05-11 03:45:...	172.16.40.104	159.203.238.50	FTP	76	Request: AUTH
188	2018-05-11 03:45:...	159.203.238.50	172.16.40.104	FTP	104	Response: 530
190	2018-05-11 03:45:...	172.16.40.104	159.203.238.50	FTP	77	Request: USER
202	2018-05-11 03:45:...	159.203.238.50	172.16.40.104	FTP	100	Response: 331
204	2018-05-11 03:45:...	172.16.40.104	159.203.238.50	FTP	80	Request: PASS
212	2018-05-11 03:45:...	159.203.238.50	172.16.40.104	FTP	89	Response: 230
218	2018-05-11 03:45:...	159.203.238.50	172.16.40.104	FTP	86	Response: 220
220	2018-05-11 03:45:...	172.16.40.104	159.203.238.50	FTP	76	Request: AUTH
222	2018-05-11 03:45:...	159.203.238.50	172.16.40.104	FTP	104	Response: 530
224	2018-05-11 03:45:...	172.16.40.104	159.203.238.50	FTP	76	Request: AUTH
225	2018-05-11 03:45:...	159.203.238.50	172.16.40.104	FTP	104	Response: 530
227	2018-05-11 03:45:...	172.16.40.104	159.203.238.50	FTP	77	Request: USER
228	2018-05-11 03:45:...	159.203.238.50	172.16.40.104	FTP	100	Response: 331
230	2018-05-11 03:45:...	172.16.40.104	159.203.238.50	FTP	80	Request: PASS
232	2018-05-11 03:45:...	159.203.238.50	172.16.40.104	FTP	89	Response: 230

< >

> Internet Protocol Version 4, Src: 159.203.238.50, Dst: 172.16.40.104

✓ Transmission Control Protocol, Src Port: 21, Dst Port: 50699, Seq: 21, Ack: 11, Len: 38

Source Port: 21

Destination Port: 50699

[Stream index: 14]

> [Conversation completeness: Complete, WITH DATA (63)]

< >

0000	ac bc 32 c3 9e b3 58 69 6c 35 38 33 08 00 45 00	--2...Xi 1583..E.
0010	00 5a 08 75 40 00 32 06 dd b2 9f cb ee 32 ac 10	-Z·u@-2- .....2..
0020	28 68 00 15 c6 0b d8 fb eb 88 f3 ed af 3f 80 18	(h·... ..?..

FTPlogin.pcapng | Packets: 296 · Displayed: 39 (13.2%) | Profile: Ibrana Choudhry