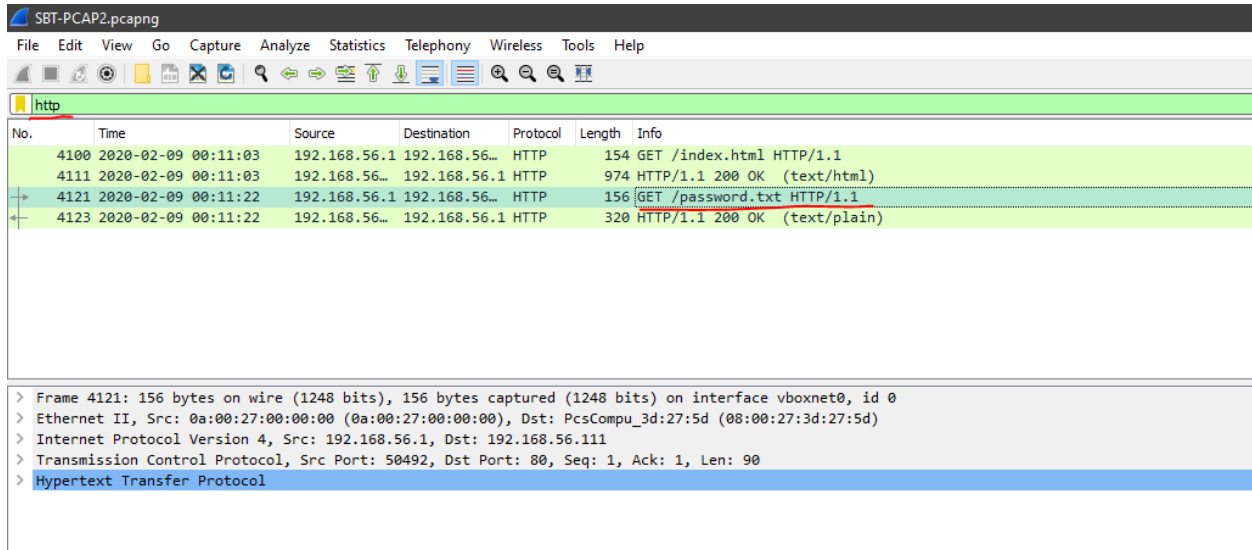


## Investigando con Wireshark - PCAP02

### PCAP 2

### ¿Qué es la contraseña de WebAdmin?



SBT-PCAP2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

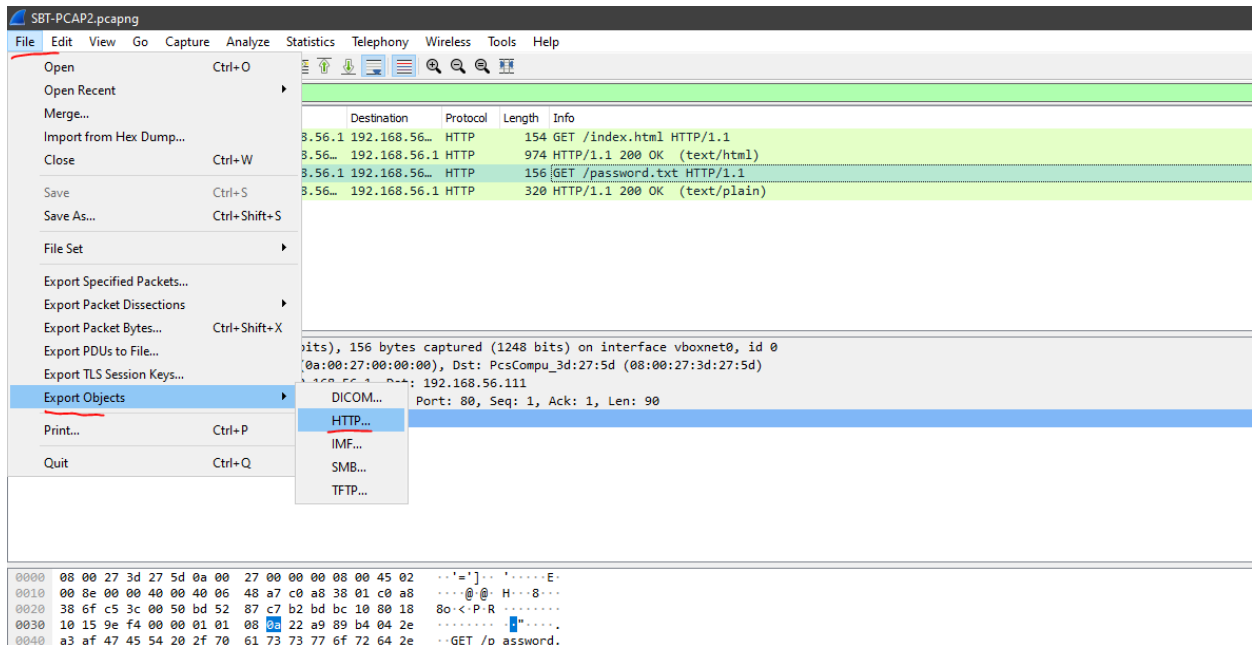
http

No.	Time	Source	Destination	Protocol	Length	Info
4100	2020-02-09 00:11:03	192.168.56.1	192.168.56...	HTTP	154	GET /index.html HTTP/1.1
4111	2020-02-09 00:11:03	192.168.56...	192.168.56.1	HTTP	974	HTTP/1.1 200 OK (text/html)
4121	2020-02-09 00:11:22	192.168.56.1	192.168.56...	HTTP	156	GET /password.txt HTTP/1.1
4123	2020-02-09 00:11:22	192.168.56...	192.168.56.1	HTTP	320	HTTP/1.1 200 OK (text/plain)

> Frame 4121: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits) on interface vboxnet0, id 0  
> Ethernet II, Src: 0a:00:27:00:00:00 (0a:00:27:00:00:00), Dst: PcsCompu\_3d:27:5d (08:00:27:3d:27:5d)  
> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.111  
> Transmission Control Protocol, Src Port: 50492, Dst Port: 80, Seq: 1, Ack: 1, Len: 90  
> Hypertext Transfer Protocol

Como sabemos que es la contraseña de una página web, filtraremos por **http** con el filtro "**http**".

Podemos observar que hay un archivo **txt** con el nombre contraseña.



SBT-PCAP2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Open Ctrl+O  
Open Recent  
Merge...  
Import from Hex Dump...  
Close Ctrl+W  
Save Ctrl+S  
Save As... Ctrl+Shift+S  
File Set  
Export Specified Packets...  
Export Packet Dissections  
Export Packet Bytes... Ctrl+Shift+X  
Export PDUs to File...  
Export TLS Session Keys...  
**Export Objects**  
Print... Ctrl+P  
Quit Ctrl+Q

Destination Protocol Length Info  
3.56.1 192.168.56... HTTP 154 GET /index.html HTTP/1.1  
3.56... 192.168.56.1 HTTP 974 HTTP/1.1 200 OK (text/html)  
3.56.1 192.168.56... HTTP 156 GET /password.txt HTTP/1.1  
3.56... 192.168.56.1 HTTP 320 HTTP/1.1 200 OK (text/plain)

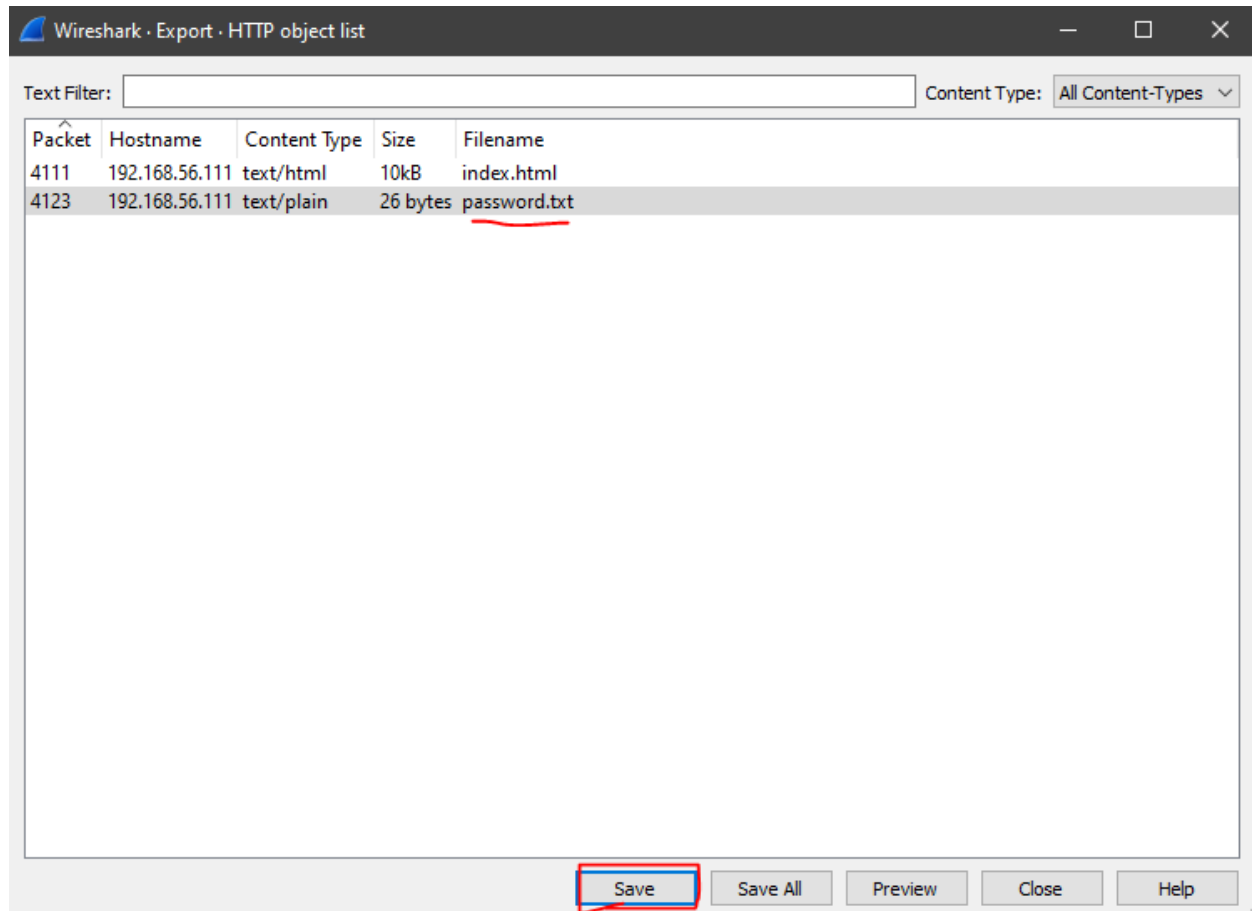
DICOM...  
**HTTP...**  
IMF...  
SMB...  
TFTP...

bits), 156 bytes captured (1248 bits) on interface vboxnet0, id 0  
(0a:00:27:00:00:00), Dst: PcsCompu\_3d:27:5d (08:00:27:3d:27:5d)  
192.168.56.1, Dst: 192.168.56.111  
Port: 80, Seq: 1, Ack: 1, Len: 90

0000 08 00 27 3d 27 5d 0a 00 27 00 00 00 00 45 02 ..'=]... ..E..  
0010 00 8e 00 00 40 00 00 06 48 a7 c0 a8 38 01 c0 a8 ...@...H...8..  
0020 38 6f c5 3c 00 50 bd 52 87 c7 b2 bd bc 10 80 18 8o<-P.R ....  
0030 10 15 9e f4 00 00 01 01 08 08 22 a9 89 b4 04 2e ... ..  
0040 a3 af 47 45 54 20 2f 70 61 73 73 77 6f 72 64 2e ...GET /p assword.

## Investigando con Wireshark - PCAP02

Para guardarlo, hacemos clic en Archivo, luego en Exportar Objetos, y luego en HTTP.



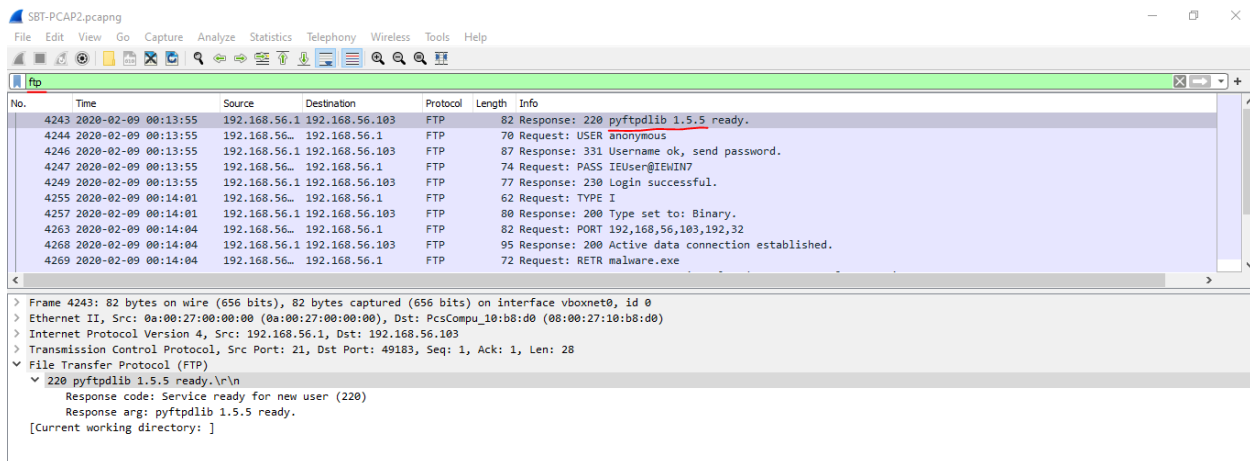
Seleccionamos el archivo "password.txt" y hacemos clic en el botón Guardar.



## Investigando con Wireshark - PCAP02

Si abrimos el archivo podemos ver la contraseña, la contraseña de WebAdmin es **sbt123**

¿Cuál es el número de versión del servidor FTP del atacante?



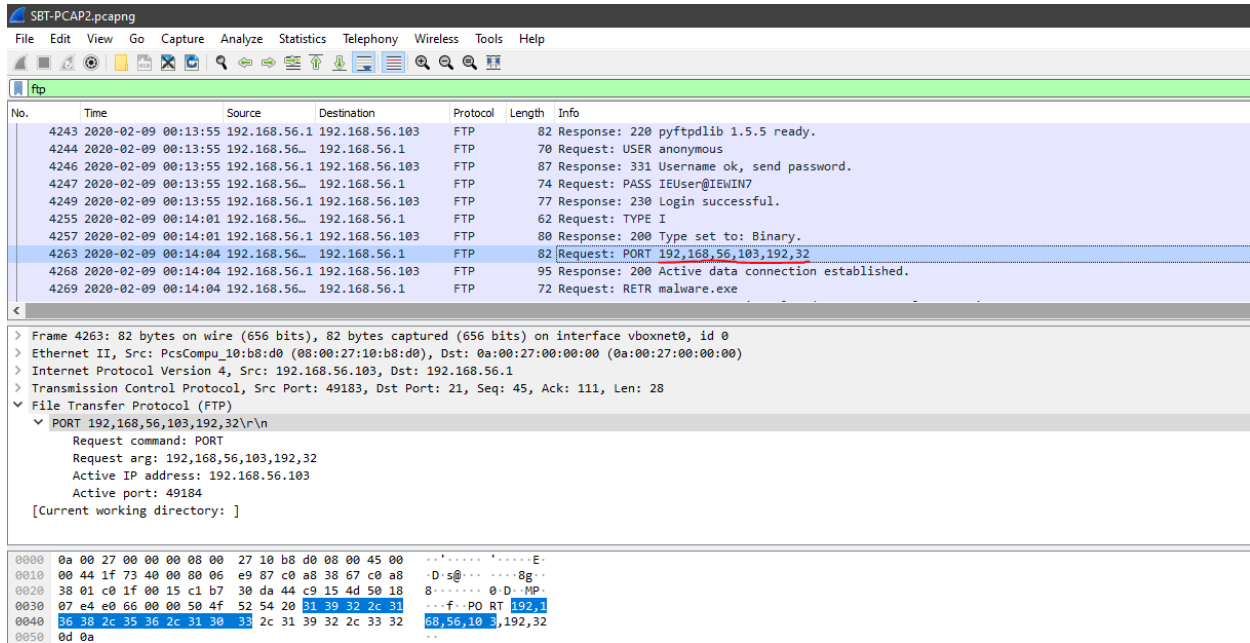
Esta vez tenemos que filtrar por **ftp**, en Wireshark utilizamos el filtro "**ftp**". El primer paquete que fue capturado por tráfico FTP tiene información sobre **pyftplib 1.5.5**.

PyFTP Lib es una librería de servidor FTP en Python que proporciona una interfaz portable de alto nivel para escribir fácilmente servidores FTP muy eficientes, escalables y asíncronos con Python.

La versión utilizada es la 1.5.5.

## Investigando con Wireshark - PCAP02

¿Qué puerto se utilizó para acceder al host Windows de la víctima?



El atacante utilizó el comando FTP PORT. Este comando indica al servidor FTP el puerto en el que se espera la conexión.

Primero, hay que mapear un puerto en el router

Así mapeando un puerto hacemos que, cuando el servidor FTP se conecte con nuestro router para establecer el canal secundario en el puerto que le indiquemos, esta conexión sea redirigida a nuestro PC y así no se quede "parada" en nuestro router.

Supongamos que asignamos el puerto 6970. A efectos prácticos, cualquier conexión que llegue a la IP del router (192.168.56.1) al puerto 49183 será redirigida a nuestra IP privada (192.168.56.103) por el puerto 49183.

Así que debemos decirle al servidor FTP que queremos que establezca el canal secundario con otra IP en el puerto 49183 (192.168.56.103:49183). Esto lo hacemos de la siguiente manera

**PORT 192,168,56,103,192,32**

Veamos en detalle de dónde han salido estos números:

## Investigando con Wireshark - PCAP02

Los 4 primeros 192 168 56 y 103 se refieren a nuestra IP

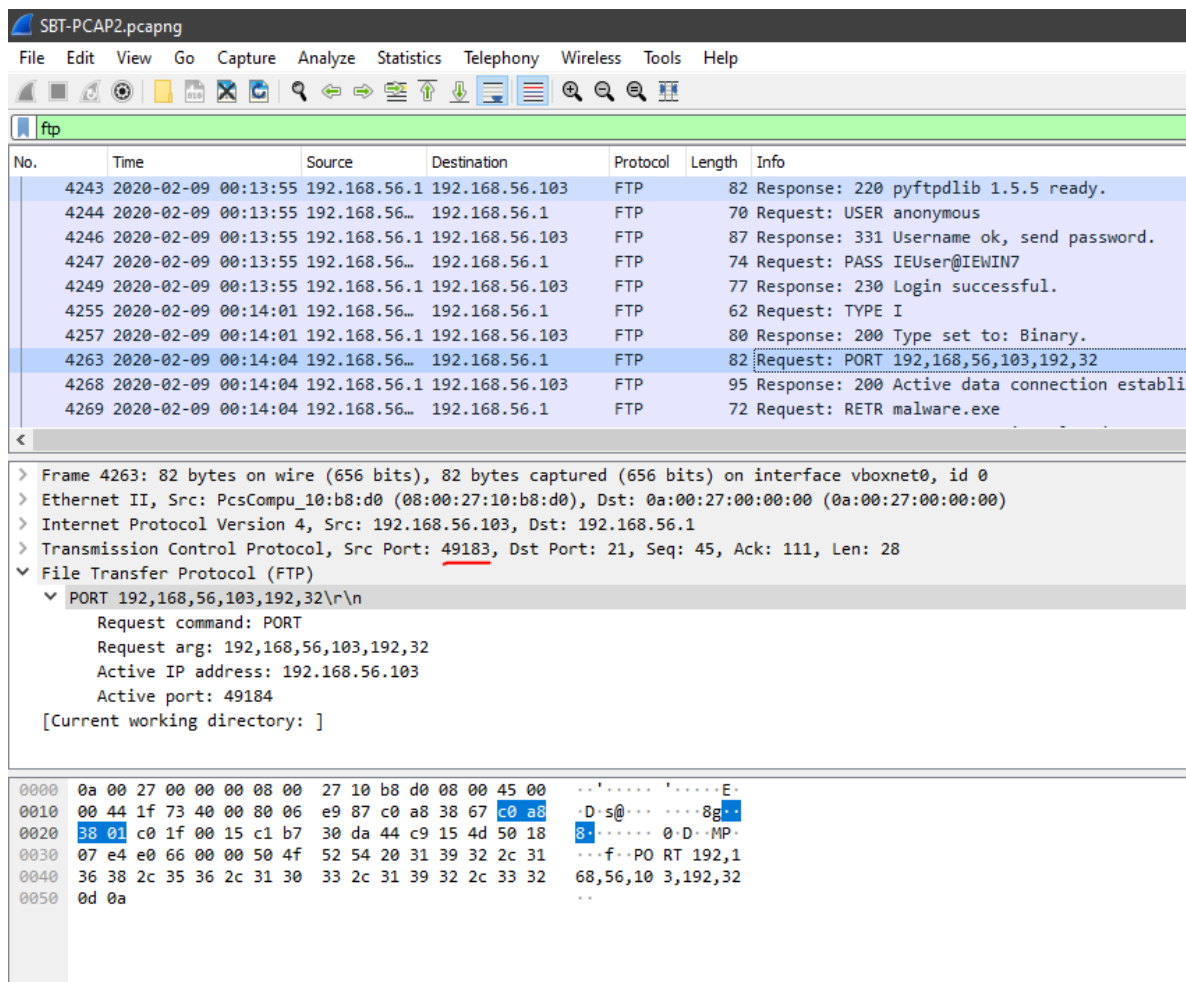
Los 2 siguientes 192 y 32 al puerto.

¿Cómo se han calculado?

Queríamos indicar al servidor el puerto 49183; entonces hemos hecho lo siguiente:  
 $192 \times 256 = 49152$ ;  $49152 + 32 = 49183$

Si quiere calcular estos 2 componentes para cualquier puerto, primero divida el puerto por 256, conserve la parte entera, luego multiplique la parte entera por 256, el segundo número es la diferencia entre el resultado obtenido y el puerto en cuestión.

El puerto que se utilizó para acceder fue el **49183**.



SBT-PCAP2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp

No.	Time	Source	Destination	Protocol	Length	Info
4243	2020-02-09 00:13:55	192.168.56.1	192.168.56.103	FTP	82	Response: 220 pyftplib 1.5.5 ready.
4244	2020-02-09 00:13:55	192.168.56...	192.168.56.1	FTP	70	Request: USER anonymous
4246	2020-02-09 00:13:55	192.168.56.1	192.168.56.103	FTP	87	Response: 331 Username ok, send password.
4247	2020-02-09 00:13:55	192.168.56...	192.168.56.1	FTP	74	Request: PASS IEUser@IEWIN7
4249	2020-02-09 00:13:55	192.168.56.1	192.168.56.103	FTP	77	Response: 230 Login successful.
4255	2020-02-09 00:14:01	192.168.56...	192.168.56.1	FTP	62	Request: TYPE I
4257	2020-02-09 00:14:01	192.168.56.1	192.168.56.103	FTP	80	Response: 200 Type set to: Binary.
4263	2020-02-09 00:14:04	192.168.56...	192.168.56.1	FTP	82	Request: PORT 192,168,56,103,192,32
4268	2020-02-09 00:14:04	192.168.56.1	192.168.56.103	FTP	95	Response: 200 Active data connection establi
4269	2020-02-09 00:14:04	192.168.56...	192.168.56.1	FTP	72	Request: RETR malware.exe

> Frame 4263: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface vboxnet0, id 0

> Ethernet II, Src: PcsCompu\_10:b8:d0 (08:00:27:10:b8:d0), Dst: 0a:00:27:00:00:00 (0a:00:27:00:00:00)

> Internet Protocol Version 4, Src: 192.168.56.103, Dst: 192.168.56.1

> Transmission Control Protocol, Src Port: 49183, Dst Port: 21, Seq: 45, Ack: 111, Len: 28

> File Transfer Protocol (FTP)

PORT 192,168,56,103,192,32\r\n

Request command: PORT

Request arg: 192,168,56,103,192,32

Active IP address: 192.168.56.103

Active port: 49184

[Current working directory: ]

0000 0a 00 27 00 00 00 08 00 27 10 b8 d0 08 00 45 00 ..E..

0010 00 44 1f 73 40 00 80 06 e9 87 c0 a8 38 67 c0 a8 .D.s@...8g..

0020 38 01 c0 1f 00 15 c1 b7 30 da 44 c9 15 4d 50 18 8...0.D..MP..

0030 07 e4 e0 66 00 00 50 4f 52 54 20 31 39 32 2c 31 ...f..PO RT 192,1

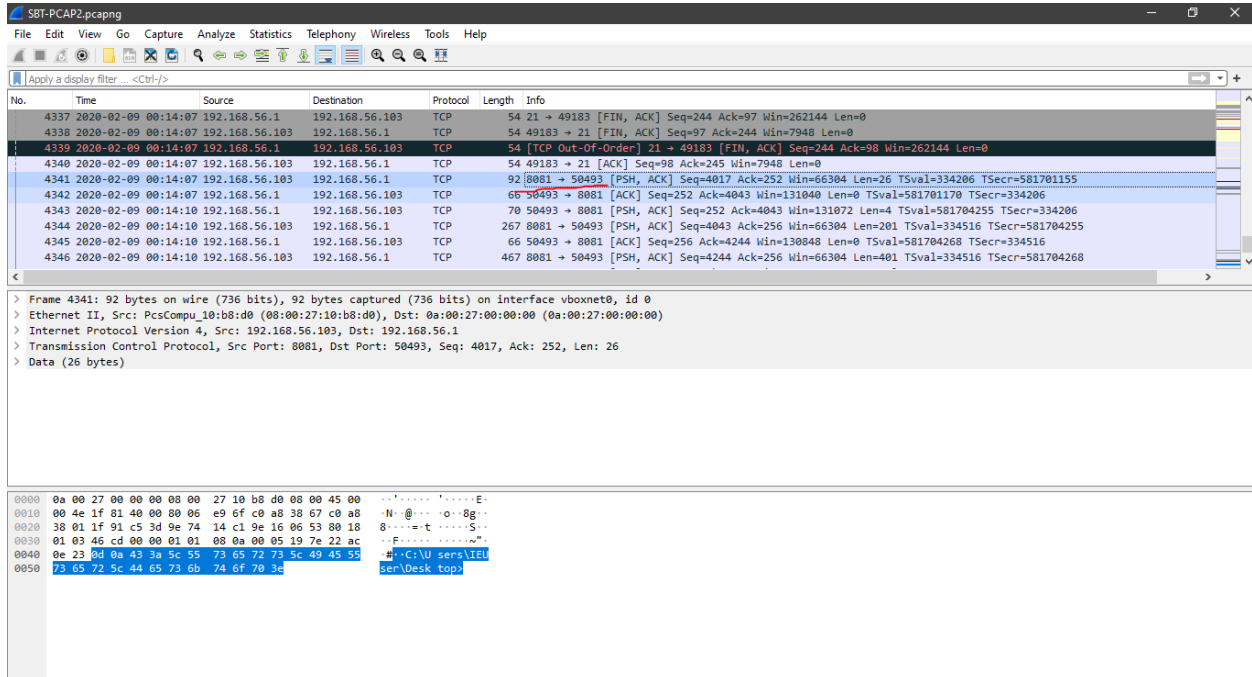
0040 36 38 2c 35 36 2c 31 30 33 2c 31 39 32 2c 33 32 68,56,10 3,192,32

0050 0d 0a ..

También podemos verlo aquí, en el puerto TCP Src.

## Investigando con Wireshark - PCAP02

¿Cuál es el nombre de un archivo confidencial que se encuentra en el host de Windows?



Wireshark interface showing a packet capture of an FTP session. The packet list shows a sequence of packets, including a FIN packet (4337) and a TCP Reset (4339). The packet details for packet 4341 show the data payload of the FTP session, which includes the command 'USER' and the response '331 Password required for user'.

Packet 4341 details:

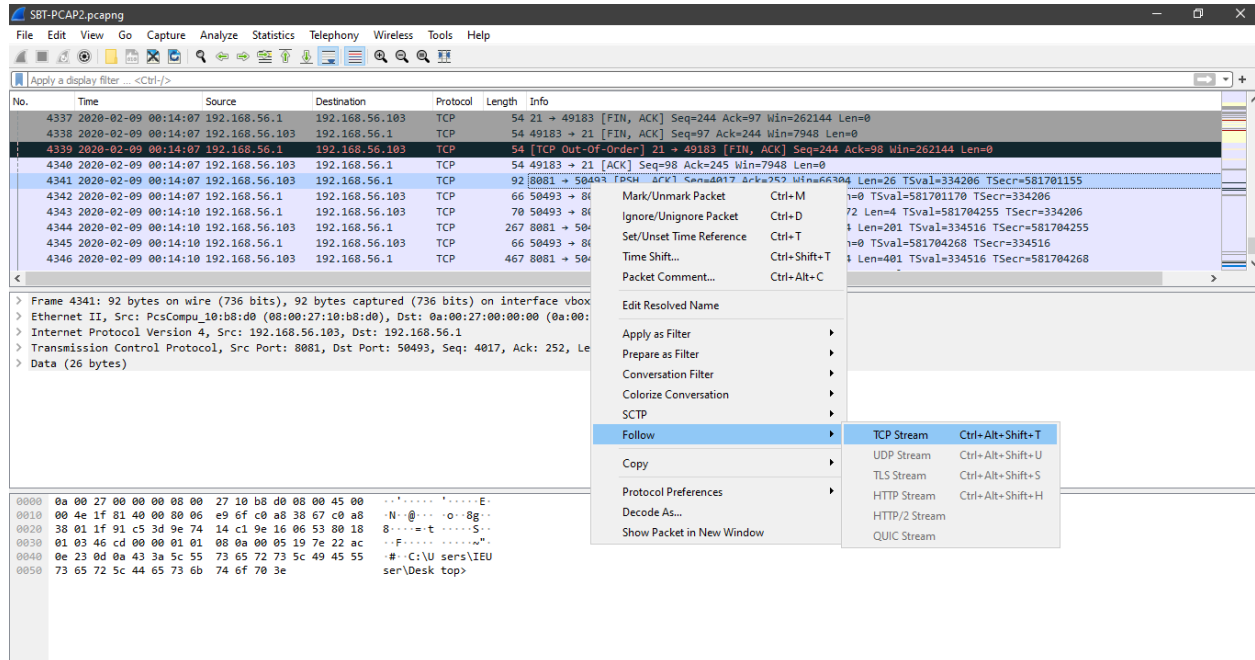
- Frame 4341: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface vboxnet0, id 0
- Ethernet II, Src: PcsCompu\_10:b8:d0 (08:00:27:10:b8:d0), Dst: 0a:00:27:00:00:00 (0a:00:27:00:00:00)
- Internet Protocol Version 4, Src: 192.168.56.103, Dst: 192.168.56.1
- Transmission Control Protocol, Src Port: 8081, Dst Port: 50493, Seq: 4017, Ack: 252, Len: 26
- Data (26 bytes)

Data payload (hex):

```
0000 0a 00 27 00 00 00 00 27 10 b8 d0 08 00 45 00  ...E
0010 00 4e 1f 81 40 00 00 06 e9 6f c0 a8 38 67 c0 a8  ...N...o...8g...
0020 38 01 1f 91 c5 3d 9e 74 14 c1 9e 16 06 53 80 18  8...=t...S...
0030 01 03 46 cd 00 00 01 01 08 0a 00 05 19 7e 22 ac  ...F...~...
0040 0e 23 0d 0a 43 3a 5c 55 73 65 72 73 5c 49 45 55  ...#...C:\U sers\IEU
0050 73 65 72 5c 44 65 73 6b 74 6f 70 3e             ser\Desk top>
```

Después de terminar la conexión FTP, podemos ver otro paquete en el puerto 8081.

## Investigando con Wireshark - PCAP02

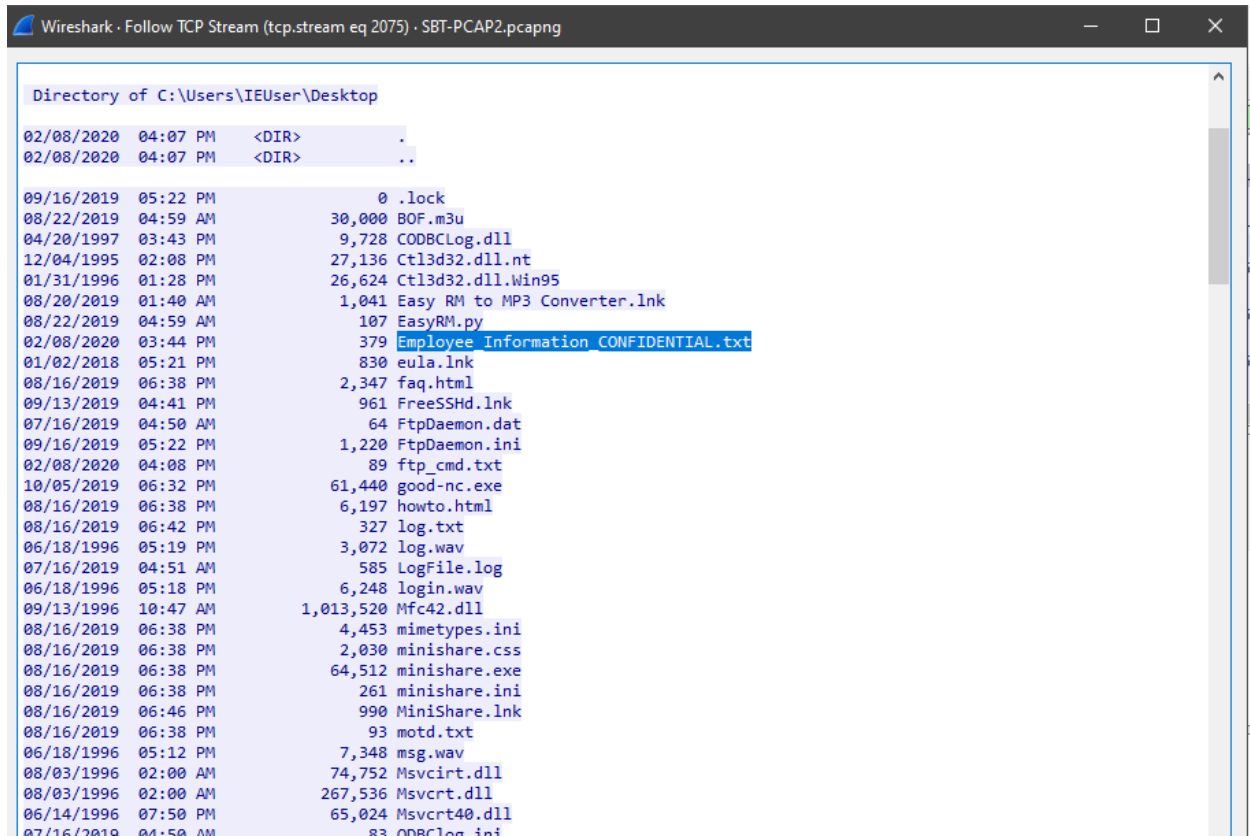


The screenshot shows the Wireshark interface with a packet capture of a TCP connection. The packet list shows a sequence of packets from 192.168.56.1 to 192.168.56.103. The packet details pane shows the structure of a TCP segment. The packet bytes pane shows the raw data. A context menu is open over the selected packet, with options like 'Follow', 'Copy', 'Protocol Preferences', etc. The 'Follow' option is highlighted, and a submenu is visible showing 'TCP Stream', 'UDP Stream', 'TLS Stream', 'HTTP/2 Stream', and 'QUIC Stream'.

Haga clic con el botón derecho en este paquete, luego haga clic en seguir y luego haga clic en TCP stream.



## Investigando con Wireshark - PCAP02



Wireshark · Follow TCP Stream (tcp.stream eq 2075) · SBT-PCAP2.pcapng

```
Directory of C:\Users\IEUser\Desktop

02/08/2020  04:07 PM    <DIR>      .
02/08/2020  04:07 PM    <DIR>      ..

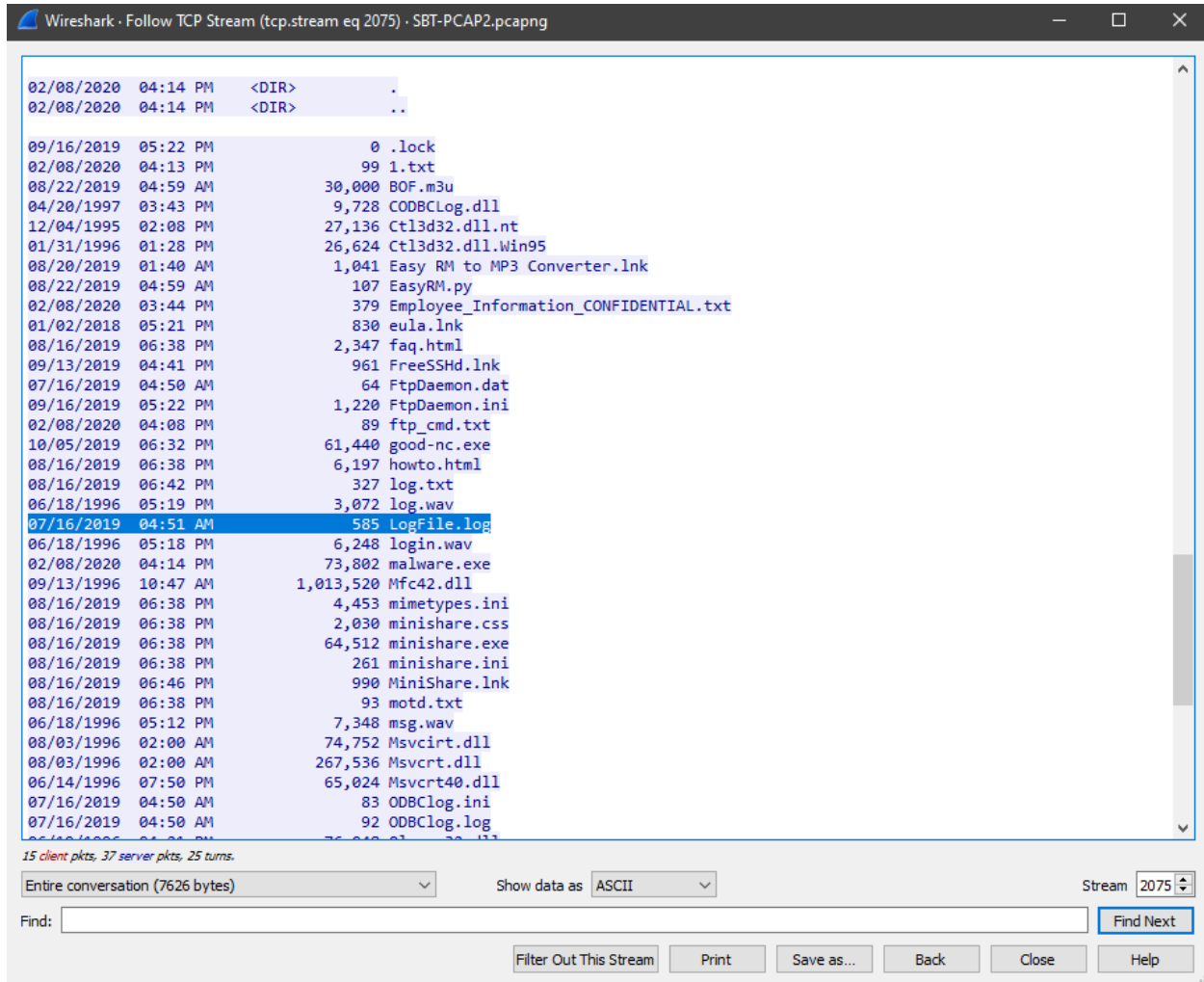
09/16/2019  05:22 PM             0 .lock
08/22/2019  04:59 AM          30,000 BOF.m3u
04/20/1997  03:43 PM           9,728 CODBCLog.dll
12/04/1995  02:08 PM          27,136 Ct13d32.dll.nt
01/31/1996  01:28 PM          26,624 Ct13d32.dll.Win95
08/20/2019  01:40 AM           1,041 Easy RM to MP3 Converter.lnk
08/22/2019  04:59 AM           107 EasyRM.py
02/08/2020  03:44 PM           379 Employee_Information_CONFIDENTIAL.txt
01/02/2018  05:21 PM           830 eula.lnk
08/16/2019  06:38 PM          2,347 faq.html
09/13/2019  04:41 PM           961 FreeSSHd.lnk
07/16/2019  04:50 AM            64 FtpDaemon.dat
09/16/2019  05:22 PM          1,220 FtpDaemon.ini
02/08/2020  04:08 PM            89 ftp_cmd.txt
10/05/2019  06:32 PM         61,440 good-nc.exe
08/16/2019  06:38 PM          6,197 howto.html
08/16/2019  06:42 PM           327 log.txt
06/18/1996  05:19 PM          3,072 log.wav
07/16/2019  04:51 AM           585 LogFile.log
06/18/1996  05:18 PM          6,248 login.wav
09/13/1996  10:47 AM        1,013,520 Mfc42.dll
08/16/2019  06:38 PM          4,453 mimetypes.ini
08/16/2019  06:38 PM          2,030 minishare.css
08/16/2019  06:38 PM          64,512 minishare.exe
08/16/2019  06:38 PM           261 minishare.ini
08/16/2019  06:46 PM           990 MiniShare.lnk
08/16/2019  06:38 PM            93 motd.txt
06/18/1996  05:12 PM          7,348 msg.wav
08/03/1996  02:00 AM          74,752 Msvcrt.dll
08/03/1996  02:00 AM         267,536 Msvcrt.dll
06/14/1996  07:50 PM          65,024 Msvcrt40.dll
07/16/2019  04:50 AM            83 ONBCLog.txt
```

Siguiendo el flujo TCP podemos ver un archivo con el nombre **"Employee\_Information\_CONFIDENTIAL.txt"**.



## Investigando con Wireshark - PCAP02

¿Cuál es el nombre del archivo de registro que se creó a las 4:51 AM en el host de Windows?



Wireshark · Follow TCP Stream (tcp.stream eq 2075) · SBT-PCAP2.pcapng

Time	Source	Destination	Length	File Name
02/08/2020 04:14 PM	<DIR>	.		
02/08/2020 04:14 PM	<DIR>	..		
09/16/2019 05:22 PM		0		.lock
02/08/2020 04:13 PM		99		1.txt
08/22/2019 04:59 AM		30,000		BOF.m3u
04/20/1997 03:43 PM		9,728		CODBCLog.dll
12/04/1995 02:08 PM		27,136		Ctl3d32.dll.nt
01/31/1996 01:28 PM		26,624		Ctl3d32.dll.win95
08/20/2019 01:40 AM		1,041		Easy RM to MP3 Converter.lnk
08/22/2019 04:59 AM		107		EasyRM.py
02/08/2020 03:44 PM		379		Employee_Information_CONFIDENTIAL.txt
01/02/2018 05:21 PM		830		eula.lnk
08/16/2019 06:38 PM		2,347		faq.html
09/13/2019 04:41 PM		961		FreeSSHd.lnk
07/16/2019 04:50 AM		64		FtpDaemon.dat
09/16/2019 05:22 PM		1,220		FtpDaemon.ini
02/08/2020 04:08 PM		89		ftp_cmd.txt
10/05/2019 06:32 PM		61,440		good-nc.exe
08/16/2019 06:38 PM		6,197		howto.html
08/16/2019 06:42 PM		327		log.txt
06/18/1996 05:19 PM		3,072		log.wav
07/16/2019 04:51 AM		585		LogFile.log
06/18/1996 05:18 PM		6,248		login.wav
02/08/2020 04:14 PM		73,802		malware.exe
09/13/1996 10:47 AM		1,013,520		Mfc42.dll
08/16/2019 06:38 PM		4,453		mimetypes.ini
08/16/2019 06:38 PM		2,030		minishare.css
08/16/2019 06:38 PM		64,512		minishare.exe
08/16/2019 06:38 PM		261		minishare.ini
08/16/2019 06:46 PM		990		MiniShare.lnk
08/16/2019 06:38 PM		93		motd.txt
06/18/1996 05:12 PM		7,348		msg.wav
08/03/1996 02:00 AM		74,752		Msvcrt.dll
08/03/1996 02:00 AM		267,536		Msvcrt.dll
06/14/1996 07:50 PM		65,024		Msvcrt40.dll
07/16/2019 04:50 AM		83		ODBClog.ini
07/16/2019 04:50 AM		92		ODBClog.log

15 client pkts, 37 server pkts, 25 turns.

Entire conversation (7626 bytes) Show data as ASCII Stream 2075

Find: Find Next

Filter Out This Stream Print Save as... Back Close Help

Siguiendo el mismo TCP Stream, abajo, podemos ver que el archivo "LogFile.log" fue creado a las 4:51 AM.