FTP ACTIVE MODE

Tạo Connection Control

(1) FTP Client: Mở một port cao bất kỳ gửi gói tin **SYN**, ví dụ từ Port 50258 -> Port 21 trên FTP Server với mục đích thông báo.

(2) FTP Server: Đồng ý và gửi lại gói tin **SYN/ACK** từ Port 21 -> Port 50258 trên FTP Client.

(3) FTP Client: Sẽ gửi lại gói tín **ACK** từ Port 50258 -> Port 21 trên FTP Server đồng ý tạo kết nối. *Tại thời điểm này Connection Control đã được khởi tạo xong*.

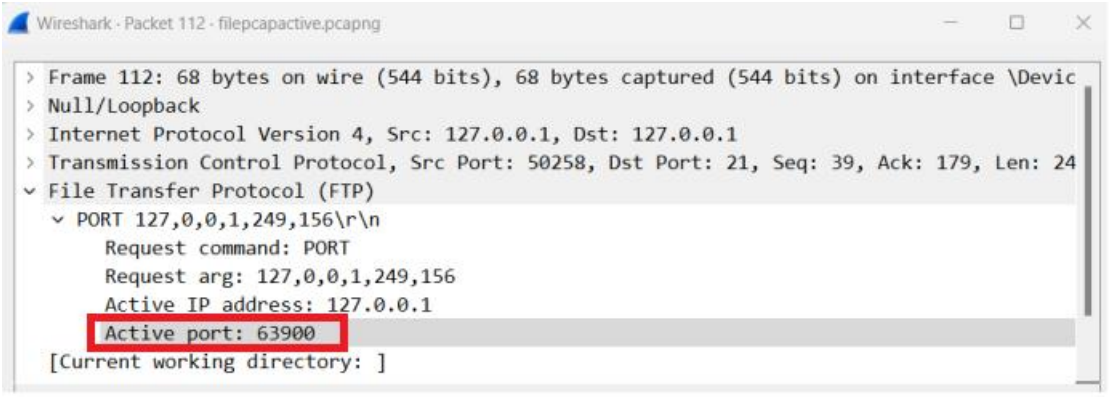
	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	TCP	56	50258 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=65495 WS=1 SACK_PERM
2	0.000137	127.0.0.1	127.0.0.1	TCP	56	21 → 50258 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
3	0.000214	127.0.0.1	127.0.0.1	TCP	44	50258 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0

Tạo Connection Data

(4) FTP Client: Sử dụng Connection Control được tạo trước đó để gửi command **PORT** yêu cầu FTP Server dùng Active Mode để truyền file,từ Port 50258 -> Port 21 trên FTP Server. Đồng thời thông báo cho FTP Server biết nó sẽ mở **Port 63900** mới để chờ tạo Connection Data.

(5) FTP Server: Nhận được yêu cầu và tiến hành đàm phán bắt tay 3 bước với FTP Client. Nó sẽ gửi gói SYN từ Port 20 -> Port 63900, rồi nhận lại SYN/ACK rồi tiếp tục gửi ACK đến khi quá trình bắt tay 3 bước hoàn tất.

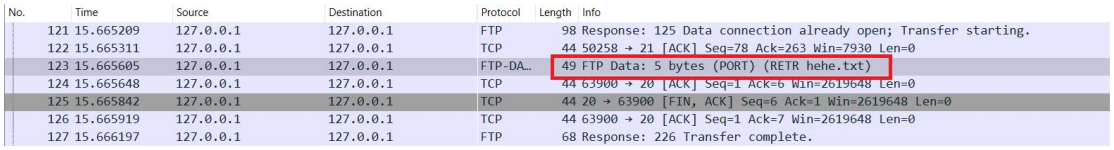
	Time	Source	Destination	Protocol	Length	Info
112	15.647503	127.0.0.1	127.0.0.1	FTP	68	Request: PORT 127,0,0,1,249,156
113	15.647570	127.0.0.1	127.0.0.1	TCP	44	21 → 50258 [ACK] Seq=179 Ack=63 Win=2619648 Len=0
114	15.648542	127.0.0.1	127.0.0.1	TCP	56	20 → 63900 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
115	15.648635	127.0.0.1	127.0.0.1	TCP	56	63900 → 20 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
116	15.648763	127.0.0.1	127.0.0.1	FTP	74	Response: 200 PORT command successful.
117	15.648771	127.0.0.1	127.0.0.1	TCP	44	20 → 63900 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
118	15.648829	127.0.0.1	127.0.0.1	TCP	44	50258 → 21 [ACK] Seq=63 Ack=209 Win=7984 Len=0
119	15.664314	127.0.0.1	127.0.0.1	FTP	59	Request: RETR hehe.txt
120	15.664427	127.0.0.1	127.0.0.1	TCP	44	21 → 50258 [ACK] Seq=209 Ack=78 Win=2619648 Len=0
121	15.665209	127.0.0.1	127.0.0.1	FTP	98	Response: 125 Data connection already open; Transfer starting.
122	15.665311	127.0.0.1	127.0.0.1	TCP	44	50258 → 21 [ACK] Seq=78 Ack=263 Win=7930 Len=0
123	15.665605	127.0.0.1	127.0.0.1	FTP-DA…	49	FTP Data: 5 bytes (PORT) (RETR hehe.txt)
124	15.665648	127.0.0.1	127.0.0.1	TCP	44	63900 → 20 [ACK] Seq=1 Ack=6 Win=2619648 Len=0



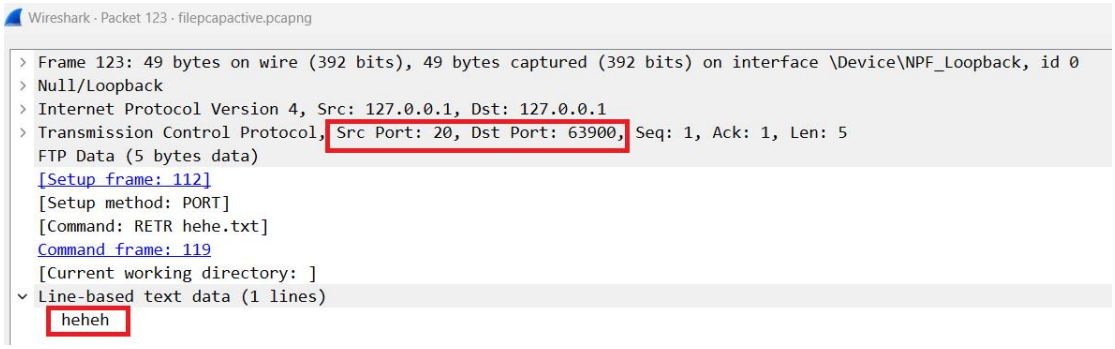
Lưu ý, hình bên trên, khi quá trình đàm phán 3 bước đang diễn ra, thì FTP Client cũng gửi một **Request: RETR hehe.txt** trên Connection Control đến FTP Server để yêu cầu download file **hehe*.txt***, đây là file mình dùng demo.

Quá trình tạo Connection Data diễn ra rất nhanh. Sau đấy, FTP Server chỉ việc gửi data về cho FTP Client thôi.

(6) **FTP Server**: Gửi file cho FTP Client



No.	Time	Source	Destination	Protocol	Length	Info
121	15.665209	127.0.0.1	127.0.0.1	FTP	98	Response: 125 Data connection already open; Transfer starting.
122	15.665311	127.0.0.1	127.0.0.1	TCP	44	50258 → 21 [ACK] Seq=78 Ack=263 Win=7930 Len=0
123	15.665605	127.0.0.1	127.0.0.1	FTP-DA…	49	FTP Data: 5 bytes (PORT) (RETR hehe.txt)
124	15.665648	127.0.0.1	127.0.0.1	TCP	44	63900 → 20 [ACK] Seq=1 Ack=6 Win=2619648 Len=0
125	15.665842	127.0.0.1	127.0.0.1	TCP	44	20 → 63900 [FIN, ACK] Seq=6 Ack=1 Win=2619648 Len=0
126	15.665919	127.0.0.1	127.0.0.1	TCP	44	63900 → 20 [ACK] Seq=1 Ack=7 Win=2619648 Len=0
127	15.666197	127.0.0.1	127.0.0.1	FTP	68	Response: 226 Transfer complete.

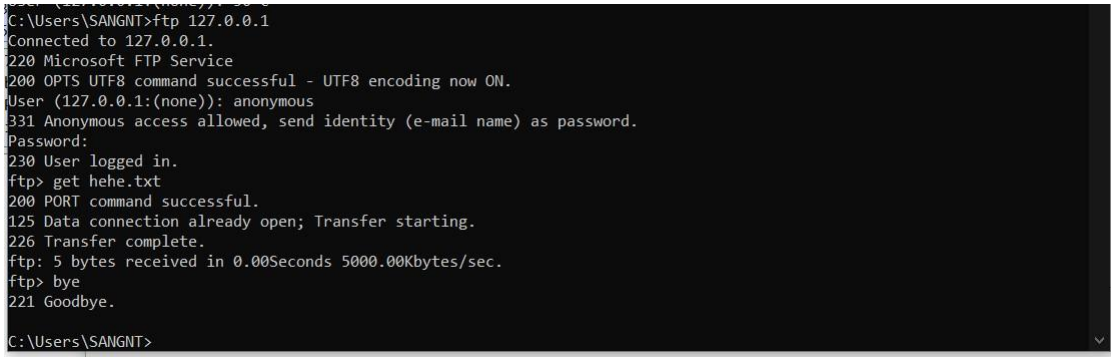


```
Wireshark · Packet 123 · filepcapactive.pcapng
> Frame 123: 49 bytes on wire (392 bits), 49 bytes captured (392 bits) on interface \Device\NPF_Loopback, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 20, Dst Port: 63900, Seq: 1, Ack: 1, Len: 5
  FTP Data (5 bytes data)
  [Setup frame: 112]
  [Setup method: PORT]
  [Command: RETR hehe.txt]
  Command frame: 119
  [Current working directory: ]
v Line-based text data (1 lines)
    heheh
```

Trên hình ta có thể thấy data được truyền đi trên Connection Data từ Port 20 FTP Server -> Port 63900 FTP Client, file có dung lượng 5 Bytes có nội dung là: **heheh**

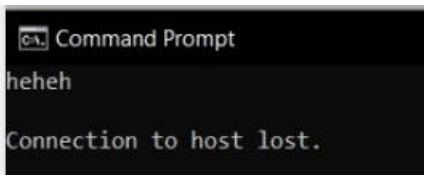
Cách hoạt động của FTP Active Mode được tóm tắt lại như sau:

FTP Client khởi tạo Connection Control, còn FTP Server khởi tạo Connection Data. FTP Server là bên chủ động gửi Data cho FTP Client.



```
C:\Users\SANGNT>ftp 127.0.0.1
Connected to 127.0.0.1.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (127.0.0.1:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
ftp> get hehe.txt
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp: 5 bytes received in 0.00Seconds 5000.00Kbytes/sec.
ftp> bye
221 Goodbye.

C:\Users\SANGNT>
```



```
Command Prompt
heheh

Connection to host lost.
```

FTP PASSIVE MODE

Tạo Connection Control

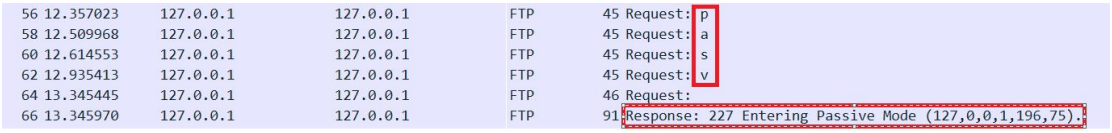
Quá trình đàm phán để tạo Connection Control cũng tuần tự theo các bước (1) -> (3) trong Active Mode.

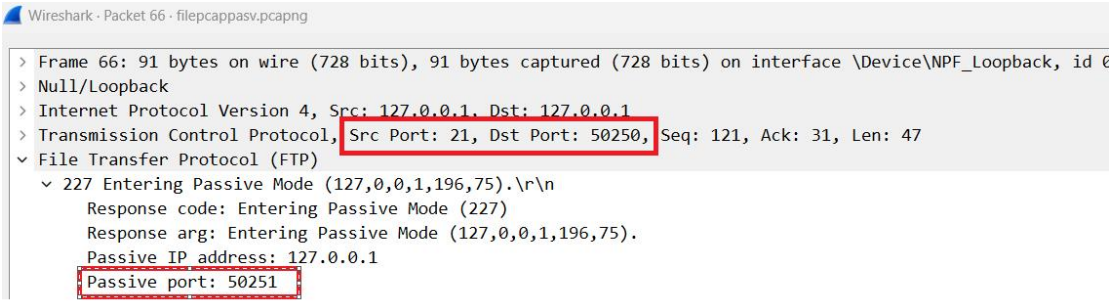
Tạo Connection Data

Đến đây Connection Control đã tạo xong giữa FTP Client Port 47962 <-> FTP Server Port 21.

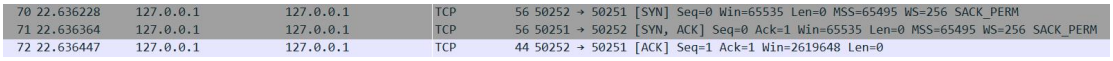
(4) FTP Client: Để truyền dữ liệu theo Passive Mode, FTP Client chủ động gửi command **PASV** trên Connection Control.

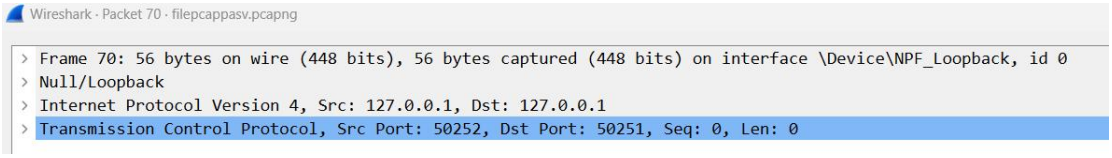
(5) Server: Nhận được yêu cầu phải dùng Passive Mode để truyền dữ liệu, nó mở Port 50251 và response lại cho FTP Client biết sẽ dùng **Port 50251** để tạo Connection Data.





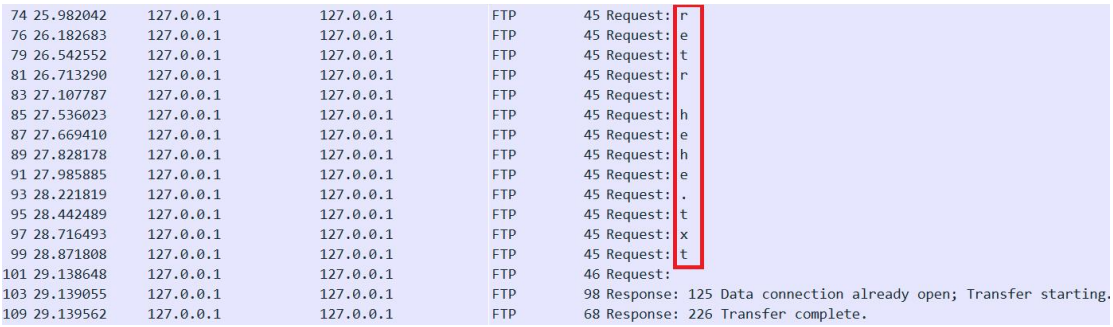
(6) FTP Client: Nhận được phản hồi, nó sẽ mở Port 50252 để tiến hành đàm phán 3 bước với FTP Server. Các bước diễn ra tuần tự như hình bên dưới.



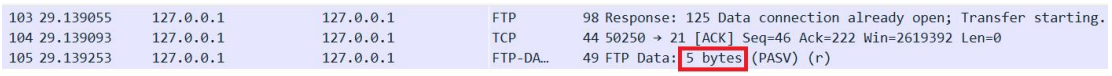


Sau bước này Connection Data đã khởi tạo xong giữa FTP Client Port 50252 <=> FTP Server Port 50251.

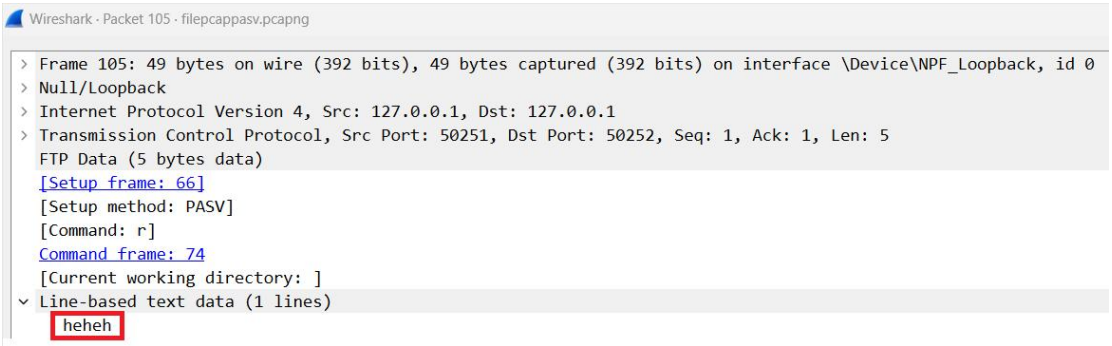
(7) FTP Client: Muốn download file về máy FTP Client chỉ việc gửi **Request: RETR hehe.txt** đến FTP Server qua Connection Control. FTP Server sẽ truyền dữ liệu lại cho FTP Client qua Connection Data.



74	25.982042	127.0.0.1	127.0.0.1	FTP	45 Request: r
76	26.182683	127.0.0.1	127.0.0.1	FTP	45 Request: e
79	26.542552	127.0.0.1	127.0.0.1	FTP	45 Request: t
81	26.713290	127.0.0.1	127.0.0.1	FTP	45 Request: r
83	27.107787	127.0.0.1	127.0.0.1	FTP	45 Request:
85	27.536023	127.0.0.1	127.0.0.1	FTP	45 Request: h
87	27.669410	127.0.0.1	127.0.0.1	FTP	45 Request: e
89	27.828178	127.0.0.1	127.0.0.1	FTP	45 Request: h
91	27.985885	127.0.0.1	127.0.0.1	FTP	45 Request: e
93	28.221819	127.0.0.1	127.0.0.1	FTP	45 Request: .
95	28.442489	127.0.0.1	127.0.0.1	FTP	45 Request: t
97	28.716493	127.0.0.1	127.0.0.1	FTP	45 Request: x
99	28.871808	127.0.0.1	127.0.0.1	FTP	45 Request: t
101	29.138648	127.0.0.1	127.0.0.1	FTP	46 Request:
103	29.139055	127.0.0.1	127.0.0.1	FTP	98 Response: 125 Data connection already open; Transfer starting.
109	29.139562	127.0.0.1	127.0.0.1	FTP	68 Response: 226 Transfer complete.



103	29.139055	127.0.0.1	127.0.0.1	FTP	98 Response: 125 Data connection already open; Transfer starting.
104	29.139093	127.0.0.1	127.0.0.1	TCP	44 50250 → 21 [ACK] Seq=46 Ack=222 Win=2619392 Len=0
105	29.139253	127.0.0.1	127.0.0.1	FTP-DA…	49 FTP Data: 5 bytes (PASV) (r)



Cách hoạt động của FTP Passive Mode được tóm tắt lại như sau:

FTP Client khởi tạo cả hai connection, FTP Client là phía đòi nhận Data. Trong trường hợp này FTP Server sẽ không dùng Port 20 để truyền Data.