

Thực hành Tìm hiểu FTP Active và Passive mode

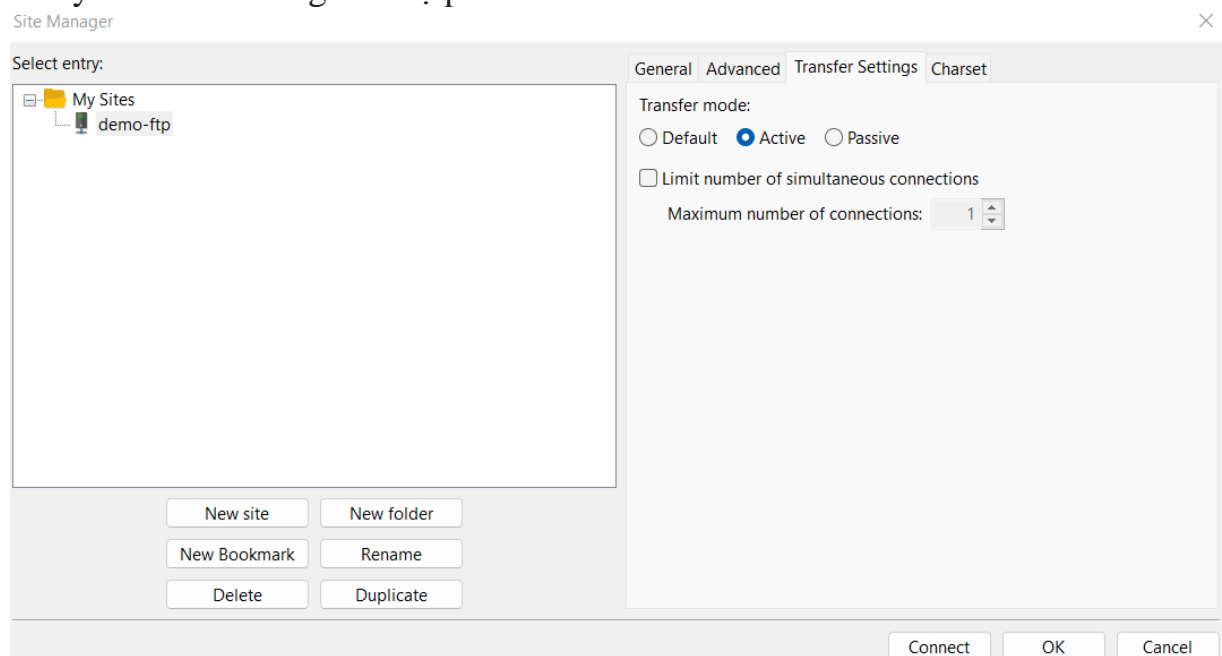
- Nhóm 9 -

Thành viên:

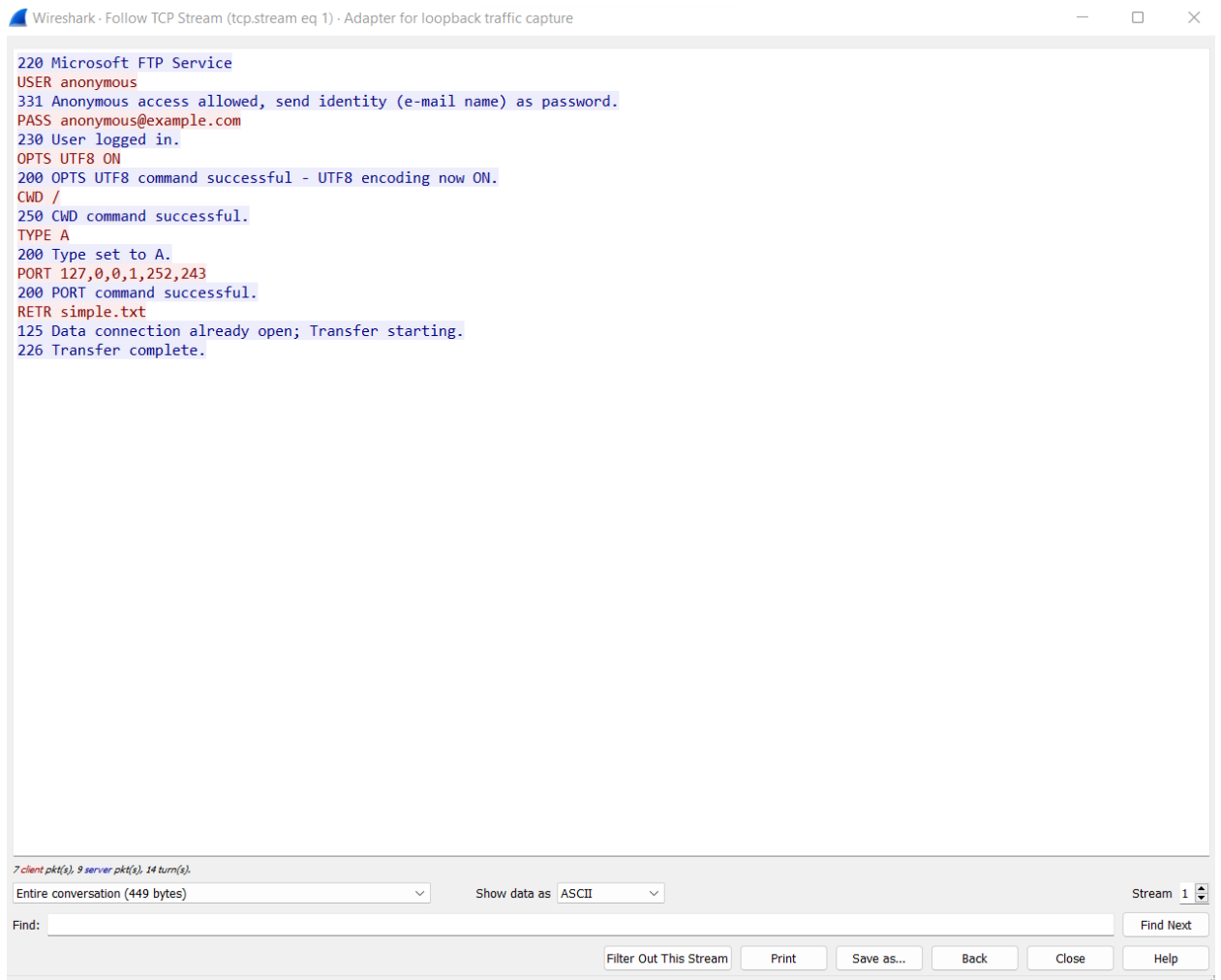
- 22520183 Trần Dương Minh Đại
- 22520810 Huỳnh Bảo Long
- 22520768 Nguyễn Gia Linh

1. FTP Server Active Mode

- Chuyển transfer sang chế độ passive:



- Download file simple.txt từ server về:



- Upload file hello.txt lên server:

Wireshark · Follow TCP Stream (tcp.stream eq 0) · Adapter for loopback traffic capture

220 Microsoft FTP Service
 USER anonymous
 331 Anonymous access allowed, send identity (e-mail name) as password.
 PASS anonymous@example.com
 230 User logged in.
 OPTS UTF8 ON
 200 OPTS UTF8 command successful - UTF8 encoding now ON.
 CWD /
 250 CWD command successful.
 TYPE A
 200 Type set to A.
 PORT 127,0,0,1,253,2
 200 PORT command successful.
 STOR hello.txt
 125 Data connection already open; Transfer starting.
 226 Transfer complete.
 TYPE I
 200 Type set to I.
 PORT 127,0,0,1,253,3
 200 PORT command successful.
 LIST
 125 Data connection already open; Transfer starting.
 226 Transfer complete.

10 client pkt(s), 13 server pkt(s), 20 turn(s).
 Entire conversation (610 bytes) Show data as ASCII Stream 0

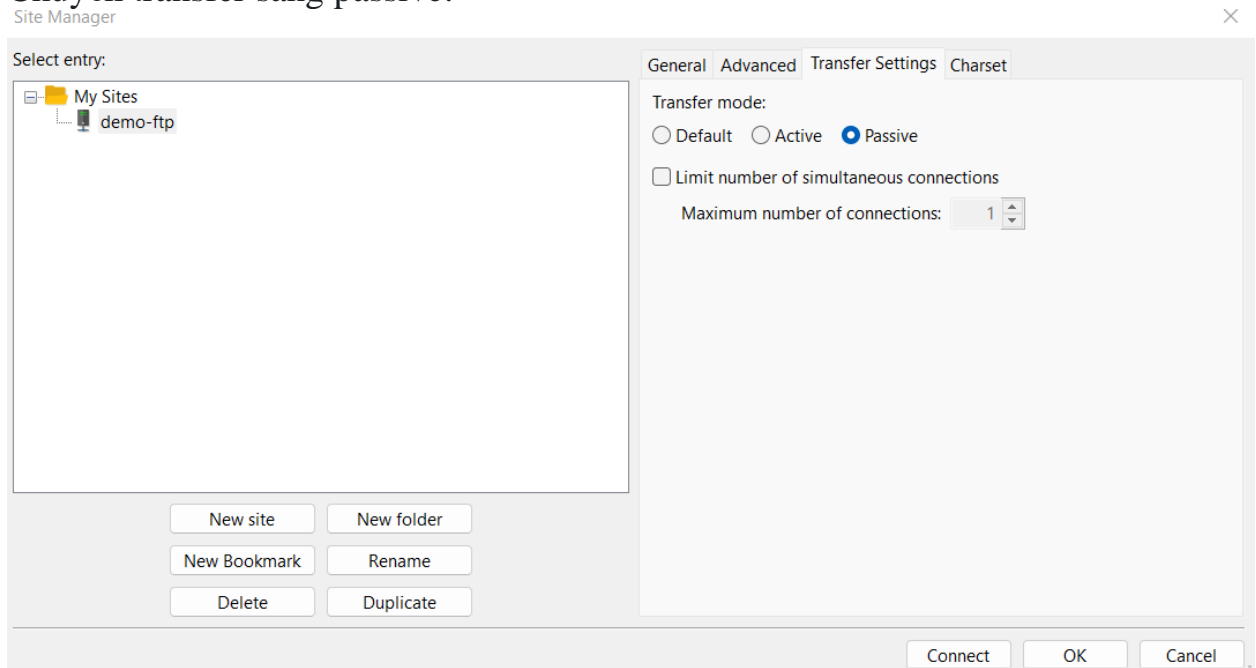
Find: Filter Out This Stream Print Save as... Back Close Help

Filename	Filesize	Filetype	Last modifi...	Permissi...	Owner/Gr...
..					
hello.txt	47	Text Doc...	13/04/2024...		
people-living-he...	15.298	AVIF File	23/03/2024...		
simple.txt	430	Text Doc...	27/03/2024...		
tkb.png	93.494	PNG File	06/02/2024...		

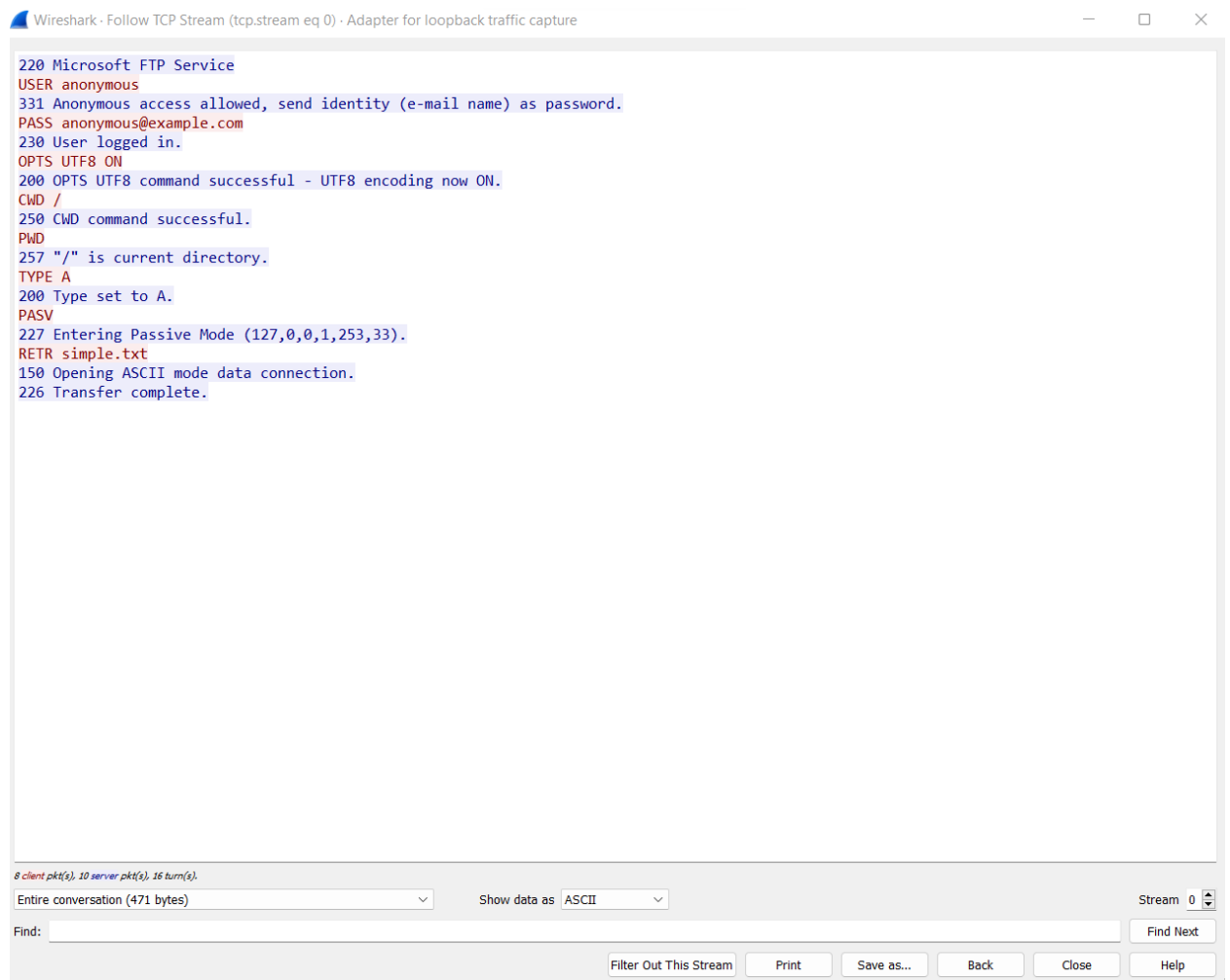
Selected 1 file. Total size: 430 bytes

2. FTP Server Passive Mode

- Chuyển transfer sang passive:



- Download file simple.txt về:



- Upload file blog.png lên server:

Wireshark · Follow TCP Stream (tcp.stream eq 1) · Adapter for loopback traffic capture

```

220 Microsoft FTP Service
USER anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
PASS anonymous@example.com
230 User logged in.
OPTS UTF8 ON
200 OPTS UTF8 command successful - UTF8 encoding now ON.
CWD /
250 CWD command successful.
TYPE I
200 Type set to I.
PASV
227 Entering Passive Mode (127,0,0,1,253,74).
STOR blog.png
125 Data connection already open; Transfer starting.
226 Transfer complete.
PASV
227 Entering Passive Mode (127,0,0,1,253,76).
LIST
150 Opening BINARY mode data connection.
226 Transfer complete.

```

9 client pkt(s), 12 server pkt(s), 18 turn(s).

Entire conversation (571 bytes) Show data as ASCII Stream 1

Find: Find Next

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

Filename	Filesize	Filetype	Last modifi...	Permissi...	Owner/Gr...
..					
blog.png	450.736	PNG File	13/04/2024...		
hello.txt	47	Text Doc...	13/04/2024...		
people-living-he...	15.298	AVIF File	23/03/2024...		
simple.txt	430	Text Doc...	27/03/2024...		
tkb.png	93.494	PNG File	06/02/2024...		

3. So sánh

- Trong Active mode, client sẽ gửi request đến server yêu cầu PORT chứa địa chỉ IP và cổng, sau đó server sẽ chủ động kết nối đến client theo như cổng đã chọn và truyền dữ liệu trên cổng này.

- Như trong file pcap của ftp-active-download, client sẽ dùng port 64754 để thiết lập kết nối đến port 21 của ftp server.

Length Info

```
56 64754 → ftp(21) [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
56 ftp(21) → 64754 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK
44 64754 → ftp(21) [ACK] Seq=1 Ack=1 Win=327424 Len=0
71 Response: 220 Microsoft FTP Service
44 64754 → ftp(21) [ACK] Seq=1 Ack=28 Win=327424 Len=0
60 Request: USER anonymous
44 ftp(21) → 64754 [ACK] Seq=28 Ack=17 Win=2161152 Len=0
116 Response: 331 Anonymous access allowed, send identity (e-mail name) as passw
44 64754 → ftp(21) [ACK] Seq=17 Ack=100 Win=327168 Len=0
72 Request: PASS anonymous@example.com
```

- Sau đó là dùng port 64755 như yêu cầu PORT 127,0,0,1,252,243 -> $252 \times 256 + 243 = 64755$ để kết nối port 20 của ftp để truyền data

```
48 13.563657 removeallblocksite... removeallblocksite... TCP 44 ftp-data(20) → 64755 [FIN, ACK] Seq=431 Ack=1 Win=327424 Len=0
49 13.563688 removeallblocksite... removeallblocksite... TCP 44 64755 → ftp-data(20) [ACK] Seq=1 Ack=432 Win=4193792 Len=0
50 13.563811 removeallblocksite... removeallblocksite... FTP 68 Response: 226 Transfer complete.
> Frame 48: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface \Device\NPF_{...}
> Null/Loopback
Internet Protocol Version 4, Src: removeallblocksite.SW (127.0.0.1), Dst: removeallblocksite.SW (127.0.0.1)
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 40
  Identification: 0xd60d (54797)
  > 010. .... = Flags: 0x2, Don't fragment
  ... 0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: TCP (6)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: removeallblocksite.SW (127.0.0.1)
  Destination Address: removeallblocksite.SW (127.0.0.1)
  Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: 64755 (64755), Seq: 431, Ack: 1, Len
  Source Port: ftp-data (20)
  Destination Port: 64755 (64755)
```

- Còn đối với Passive mode, khi một client muốn truyền hay nhận dữ liệu thì client sẽ gửi yêu cầu PASV (Passive) đến server và server sẽ phản hồi về cổng mà nó đang lắng nghe, sau đó client sẽ thực hiện kết nối đến cổng này.
- Trong file ftp-passive-download, server response cổng 64801 để kết nối:

```
50 Request: PASV
44 ftp(21) → 64800 [ACK] Seq=259 Ack=85 Win=2161152 Len=0
91 Response: 227 Entering Passive Mode (127,0,0,1,253,33).
44 64800 → ftp(21) [ACK] Seq=85 Ack=306 Win=327168 Len=0
```

- Client dùng port 64802 để kết nối 64801 để nhận dữ liệu:

41 6.677227	removeallblocksite...	removeallblocksite...	TCP	56 64802 → 64801 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=128 SACK_PERM
42 6.677291	removeallblocksite...	removeallblocksite...	TCP	56 64801 → 64802 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
43 6.677319	removeallblocksite...	removeallblocksite...	TCP	44 64802 → 64801 [ACK] Seq=1 Ack=1 Win=4194304 Len=0
44 6.677473	removeallblocksite...	removeallblocksite...	FTP	85 Response: 150 Opening ASCII mode data connection.
45 6.677499	removeallblocksite...	removeallblocksite...	TCP	44 64800 → ftp(21) [ACK] Seq=102 Ack=347 Win=326912 Len=0
46 6.677638	removeallblocksite...	removeallblocksite...	FTP-DA...	474 FTP Data: 430 bytes (PASV) (RETR simple.txt)
47 6.677654	removeallblocksite...	removeallblocksite...	TCP	44 64802 → 64801 [ACK] Seq=1 Ack=431 Win=4193792 Len=0
48 6.677711	removeallblocksite...	removeallblocksite...	TCP	44 64801 → 64802 [FIN, ACK] Seq=431 Ack=1 Win=2161152 Len=0
49 6.677732	removeallblocksite...	removeallblocksite...	TCP	44 64802 → 64801 [ACK] Seq=1 Ack=432 Win=4193792 Len=0
50 6.677826	removeallblocksite...	removeallblocksite...	FTP	68 Response: 226 Transfer complete.
51 6.677853	removeallblocksite...	removeallblocksite...	TCP	44 64800 → ftp(21) [ACK] Seq=102 Ack=371 Win=326912 Len=0
52 6.677959	removeallblocksite...	removeallblocksite...	TCP	44 64802 → 64801 [FIN, ACK] Seq=1 Ack=432 Win=4193792 Len=0
53 6.678001	removeallblocksite...	removeallblocksite...	TCP	44 64801 → 64802 [ACK] Seq=432 Ack=2 Win=2161152 Len=0