Protocol Deep Dive: FTP and Its Variants

STARTING AT THE BEGINNING: FTP ACTIVE MODE

Nick Russo
NETWORK ENGINEER

@nickrusso42518 www.njrusmc.net

Agenda

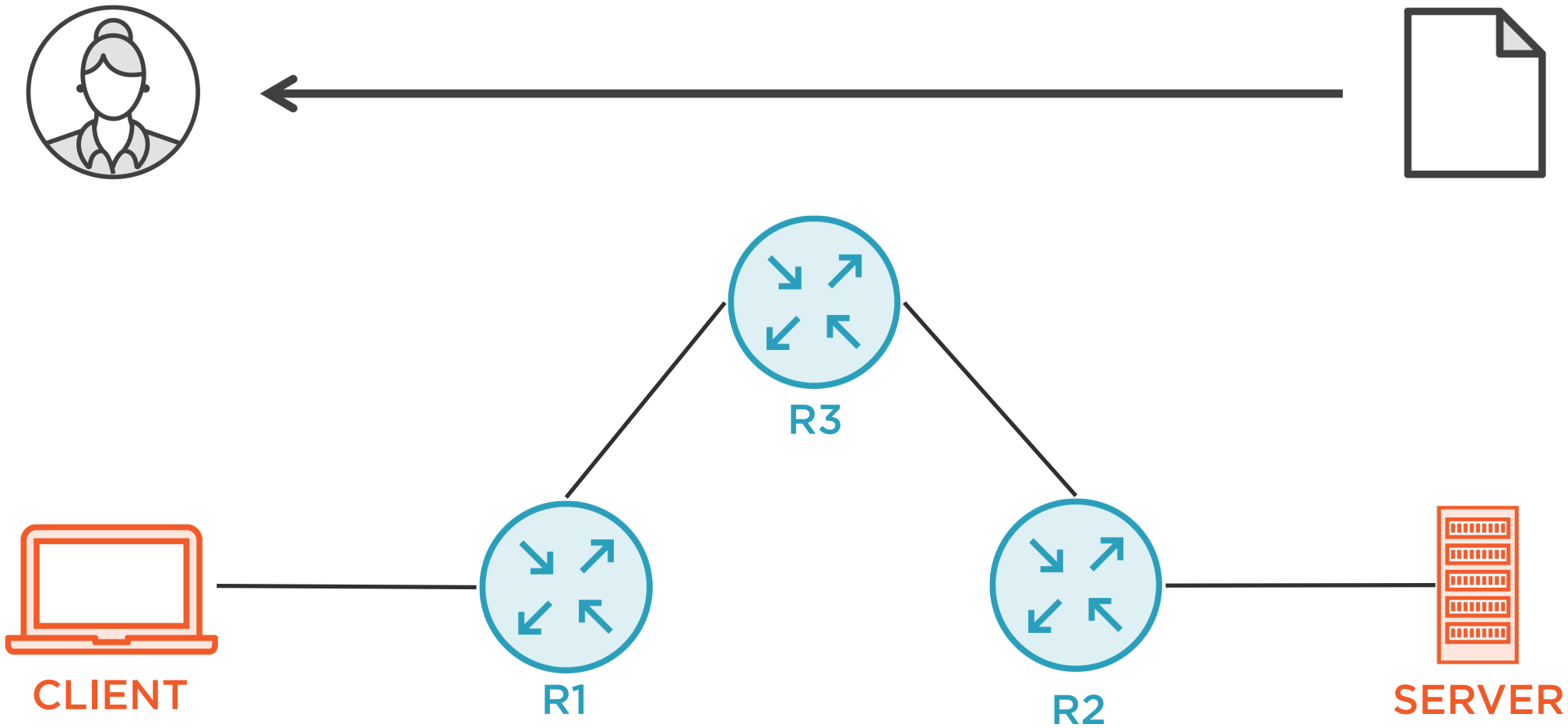
The Globomantics mission

FTP active mode operations

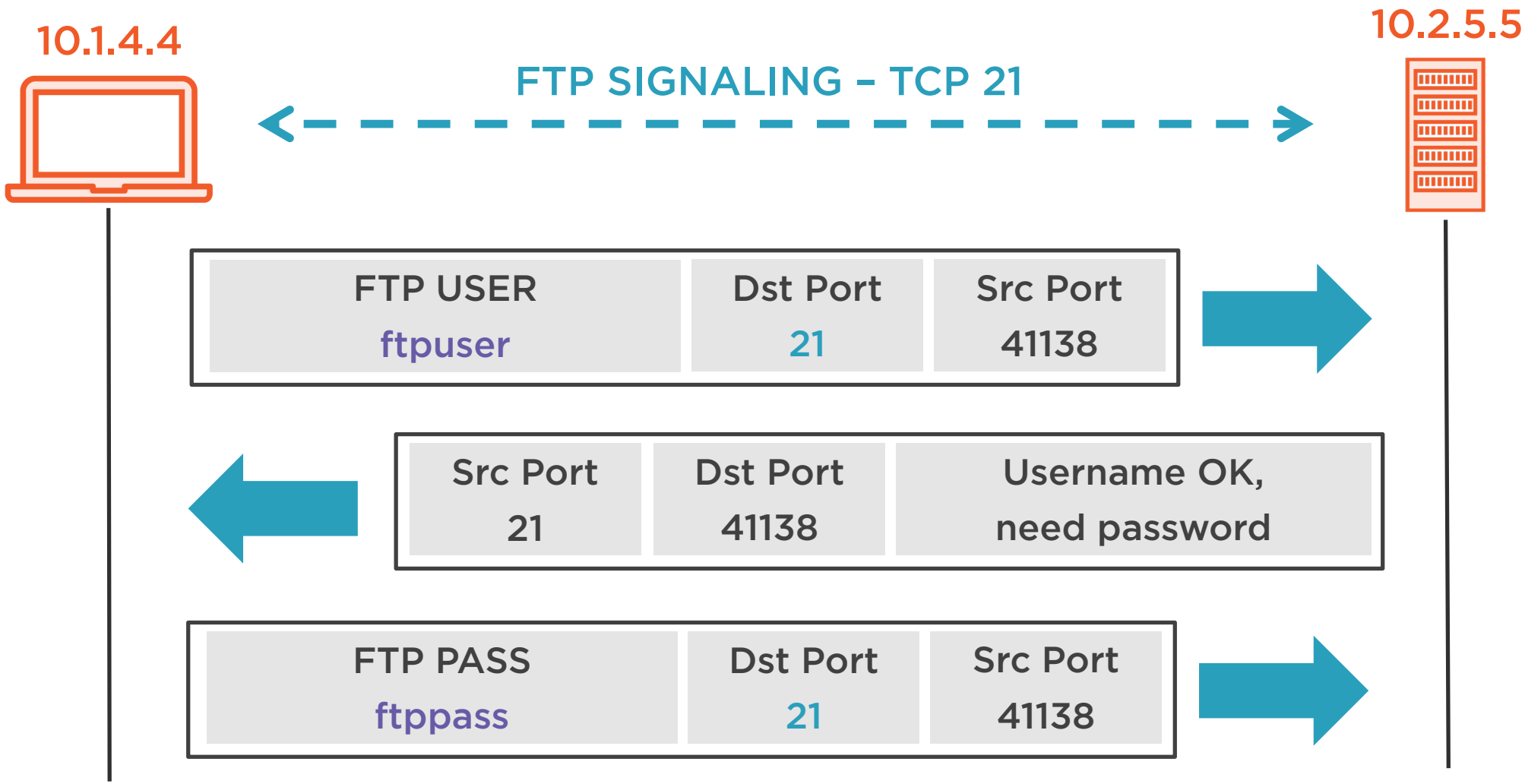
Demo and packet analysis

Active FTP through stateless firewalls

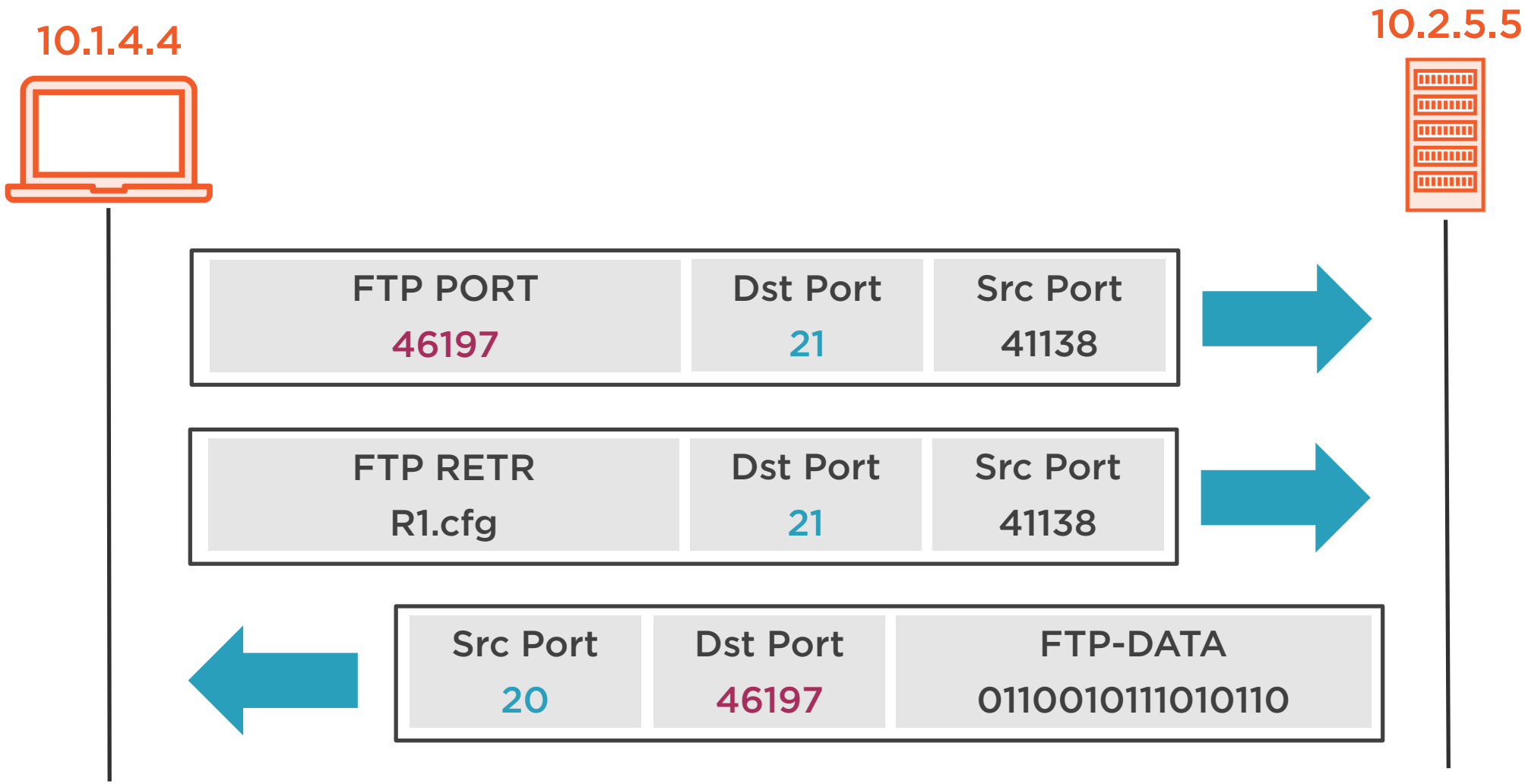
The Globomantics Network



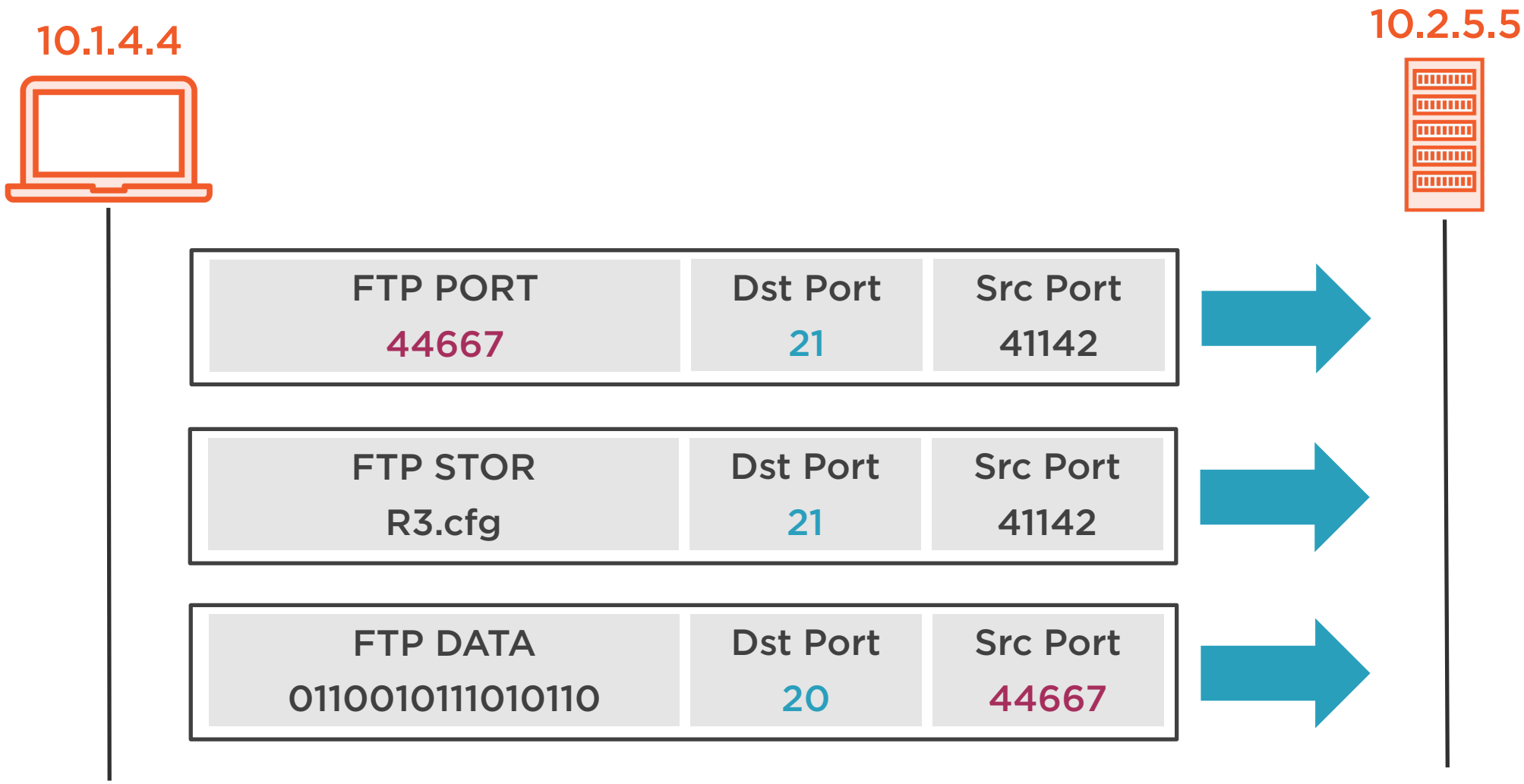
FTP General Login Process



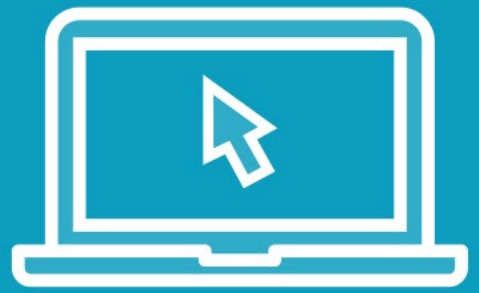
FTP Active Mode Download



FTP Active Mode Upload



Demo



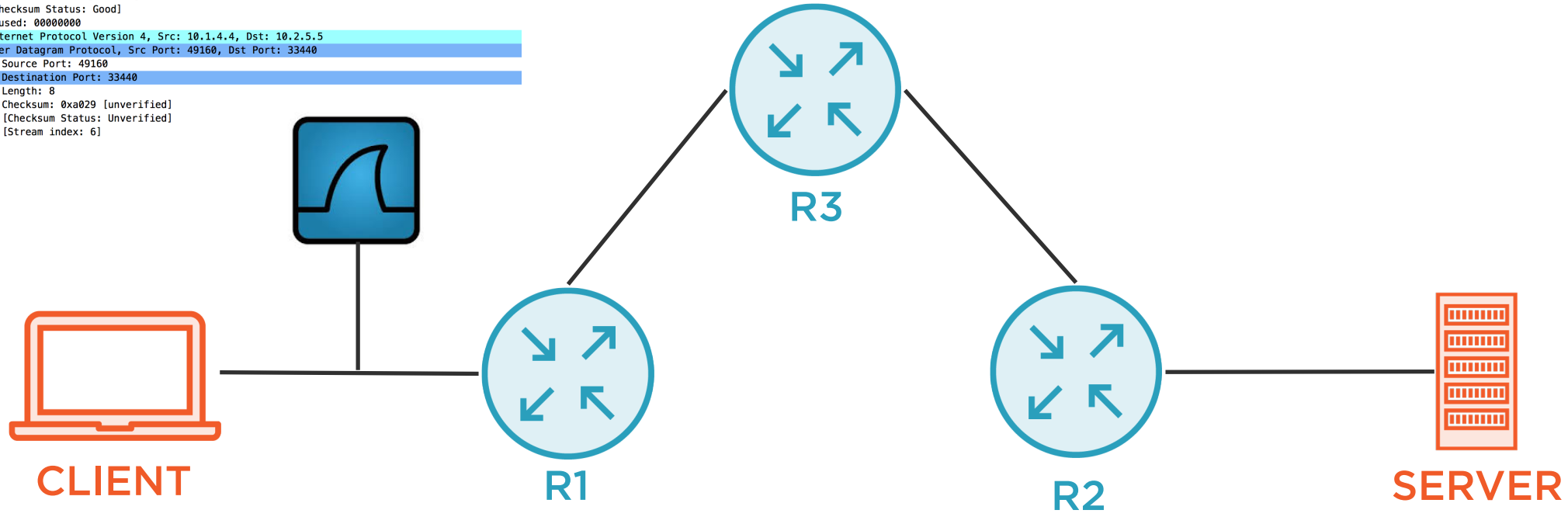
FTP active mode download

Detour: Wireshark

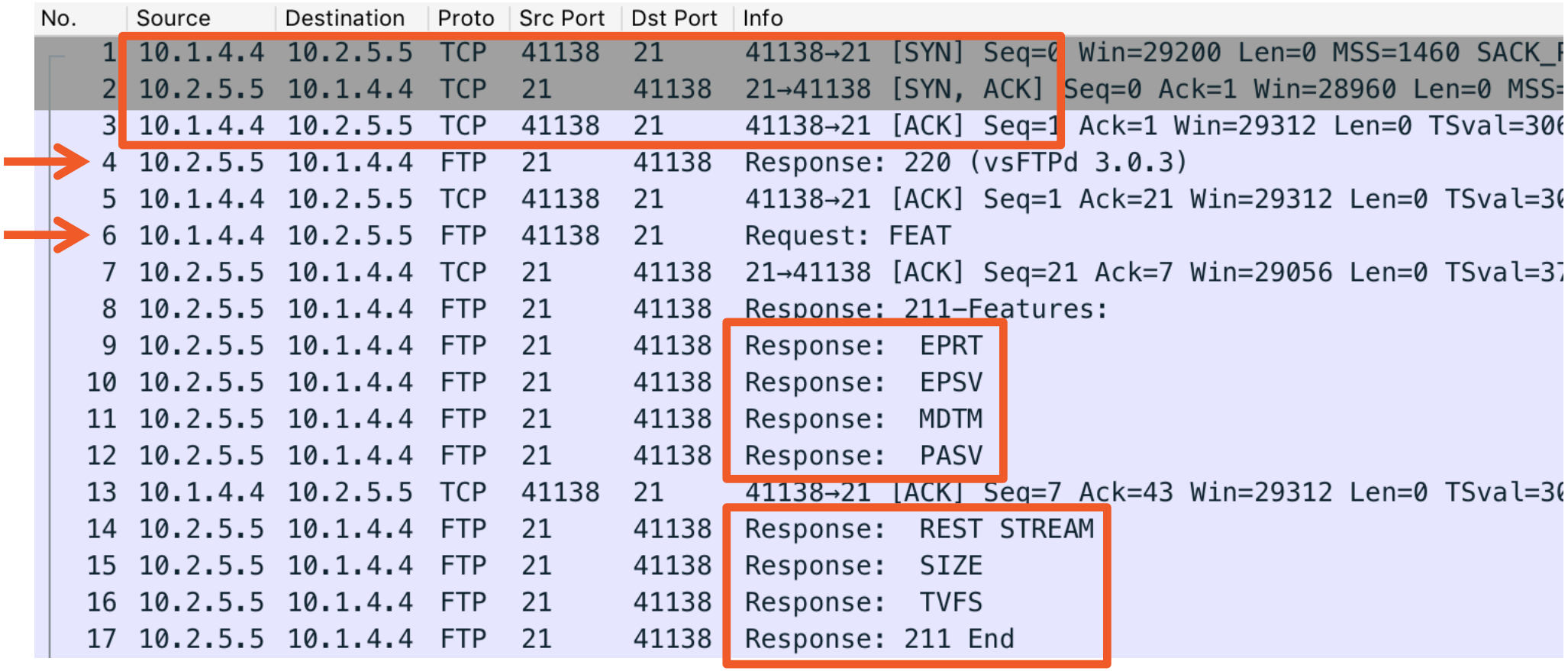
No.	Time	Source	Destination	Protocol	Time to live	Info
	0.012680	10.1.4.4	10.2.5.5	UDP	3	49160→33440 Len=0
	0.013327	10.2.5.5	10.1.4.4	ICMP	253,1	Destination unreachable (Port unreachable)
	0.013513	10.1.4.4	10.2.5.5	UDP	3	49161→33441 Len=0
	0.013760	10.2.5.5	10.1.4.4	ICMP	253,1	Destination unreachable (Port unreachable)
	0.018151	10.1.4.4	10.2.5.5	UDP	3	49162→33442 Len=0
	0.018852	10.2.5.5	10.1.4.4	ICMP	253,1	Destination unreachable (Port unreachable)

```
▶ Frame 14: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
▶ Ethernet II, Src: 00:00:a6:16:00:01, Dst: 00:00:a6:16:00:04
▶ Internet Protocol Version 4, Src: 10.2.5.5, Dst: 10.1.4.4
▼ Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 3 (Port unreachable)
    Checksum: 0x1a22 [correct]
    [Checksum Status: Good]
    Unused: 00000000
  ▶ Internet Protocol Version 4, Src: 10.1.4.4, Dst: 10.2.5.5
  ▼ User Datagram Protocol, Src Port: 49160, Dst Port: 33440
      Source Port: 49160
    ▶ Destination Port: 33440
      Length: 8
      Checksum: 0xa029 [unverified]
      [Checksum Status: Unverified]
      [Stream index: 6]
```

Free download:
wireshark.org



FTP Initial Actions



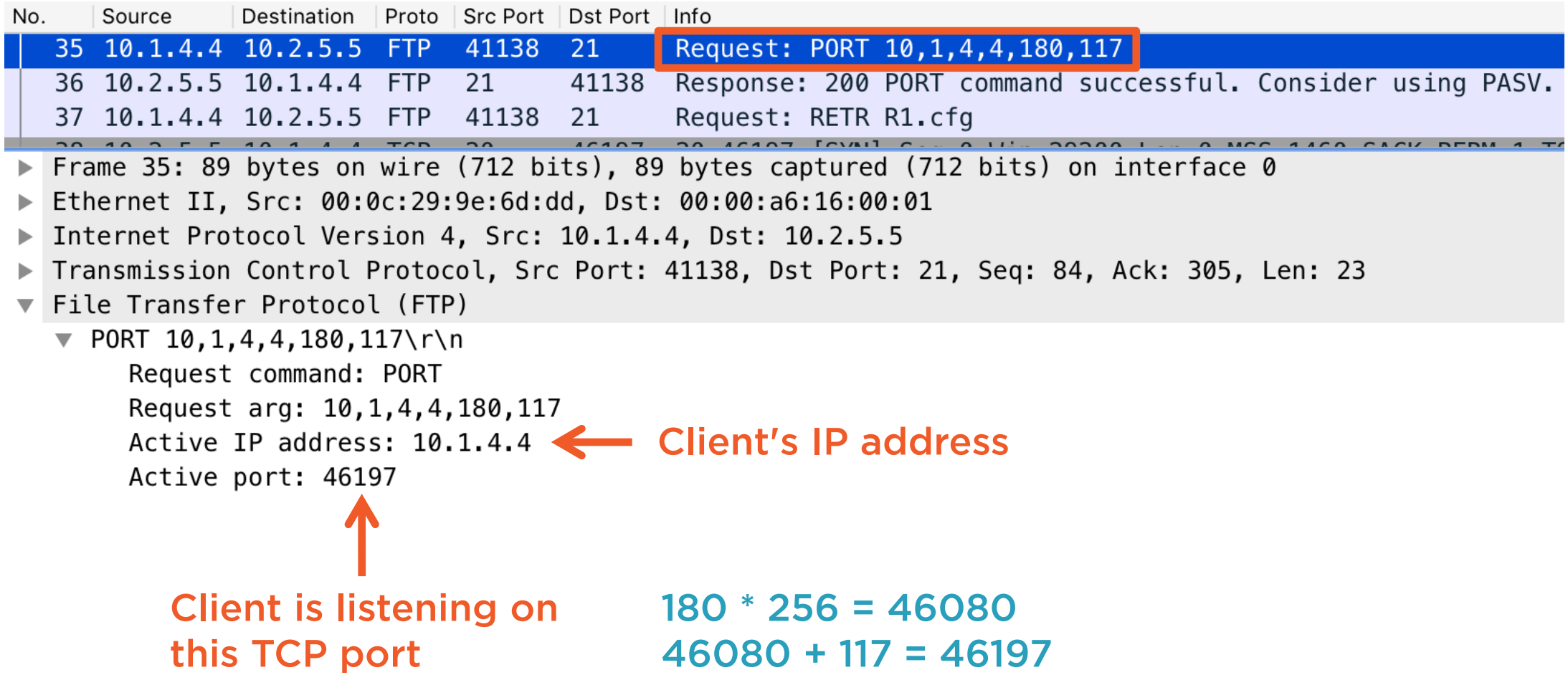
No.	Source	Destination	Proto	Src Port	Dst Port	Info
1	10.1.4.4	10.2.5.5	TCP	41138	21	41138→21 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_P
2	10.2.5.5	10.1.4.4	TCP	21	41138	21→41138 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=
3	10.1.4.4	10.2.5.5	TCP	41138	21	41138→21 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=306
4	10.2.5.5	10.1.4.4	FTP	21	41138	Response: 220 (vsFTPd 3.0.3)
5	10.1.4.4	10.2.5.5	TCP	41138	21	41138→21 [ACK] Seq=1 Ack=21 Win=29312 Len=0 TSval=30
6	10.1.4.4	10.2.5.5	FTP	41138	21	Request: FEAT
7	10.2.5.5	10.1.4.4	TCP	21	41138	21→41138 [ACK] Seq=21 Ack=7 Win=29056 Len=0 TSval=37
8	10.2.5.5	10.1.4.4	FTP	21	41138	Response: 211-Features:
9	10.2.5.5	10.1.4.4	FTP	21	41138	Response: EPRT
10	10.2.5.5	10.1.4.4	FTP	21	41138	Response: EPSV
11	10.2.5.5	10.1.4.4	FTP	21	41138	Response: MDTM
12	10.2.5.5	10.1.4.4	FTP	21	41138	Response: PASV
13	10.1.4.4	10.2.5.5	TCP	41138	21	41138→21 [ACK] Seq=7 Ack=43 Win=29312 Len=0 TSval=30
14	10.2.5.5	10.1.4.4	FTP	21	41138	Response: REST STREAM
15	10.2.5.5	10.1.4.4	FTP	21	41138	Response: SIZE
16	10.2.5.5	10.1.4.4	FTP	21	41138	Response: TVFS
17	10.2.5.5	10.1.4.4	FTP	21	41138	Response: 211 End

FTP Login and Transfer Setup

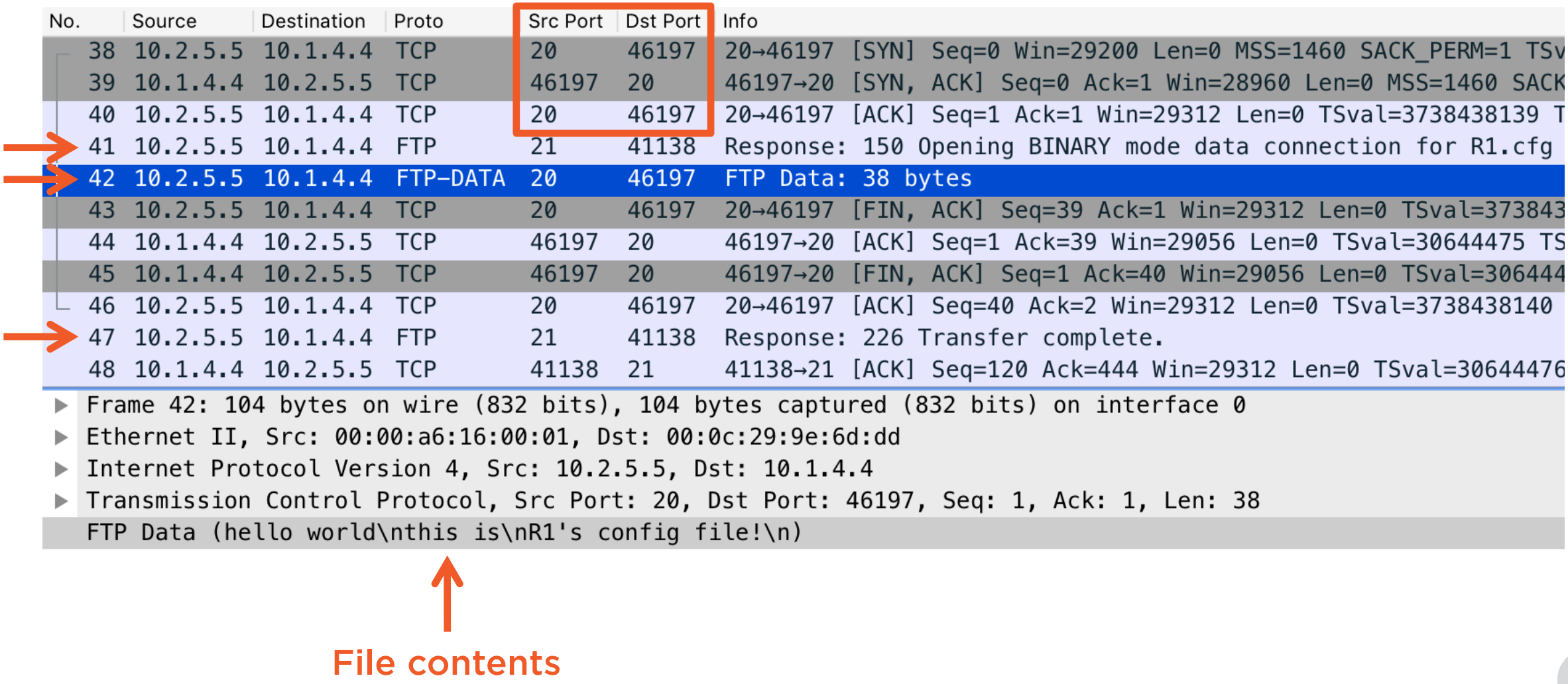
No.	Source	Destination	Proto	Src Port	Dst Port	Info
21	10.1.4.4	10.2.5.5	FTP	41138	21	Request: AUTH TLS
22	10.2.5.5	10.1.4.4	FTP	21	41138	Response: 530 Please login with USER and PASS.
23	10.1.4.4	10.2.5.5	FTP	41138	21	Request: USER ftpuser
24	10.2.5.5	10.1.4.4	FTP	21	41138	Response: 331 Please specify the password.
25	10.1.4.4	10.2.5.5	FTP	41138	21	Request: PASS ftppass
26	10.2.5.5	10.1.4.4	FTP	21	41138	Response: 230 Login successful.
27	10.1.4.4	10.2.5.5	FTP	41138	21	Request: PWD
28	10.2.5.5	10.1.4.4	FTP	21	41138	Response: 257 "/home/ftpuser/ftp" is the current directory
29	10.1.4.4	10.2.5.5	FTP	41138	21	Request: TYPE I
30	10.2.5.5	10.1.4.4	FTP	21	41138	Response: 200 Switching to Binary mode.
31	10.1.4.4	10.2.5.5	FTP	41138	21	Request: SIZE R1.cfg
32	10.2.5.5	10.1.4.4	FTP	21	41138	Response: 213 38
33	10.1.4.4	10.2.5.5	FTP	41138	21	Request: MDTM R1.cfg
34	10.2.5.5	10.1.4.4	FTP	21	41138	Response: 213 20190325101318
35	10.1.4.4	10.2.5.5	FTP	41138	21	Request: PORT 10,1,4,4,180,117
36	10.2.5.5	10.1.4.4	FTP	21	41138	Response: 200 PORT command successful. Consider using PASV.
37	10.1.4.4	10.2.5.5	FTP	41138	21	Request: RETR R1.cfg

Client: Open a session to me!

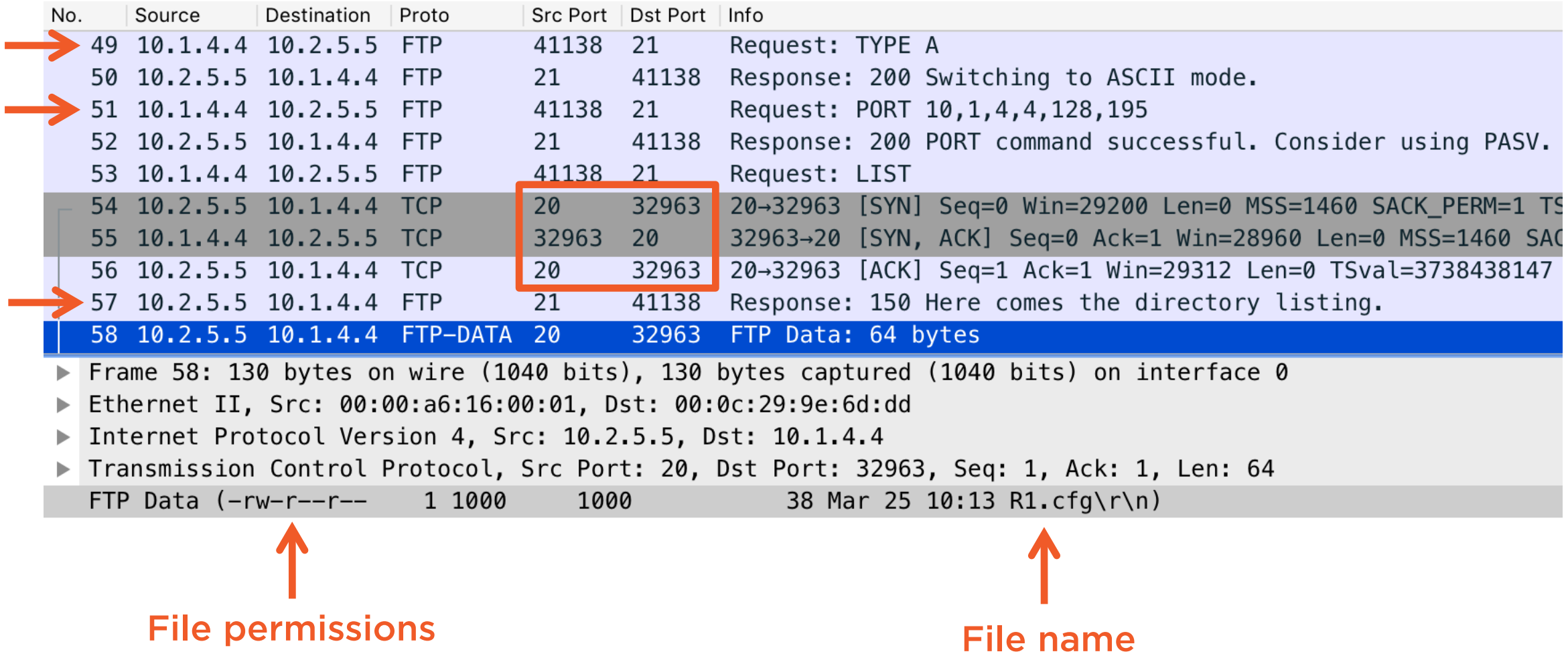
FTP PORT Command Deep Dive



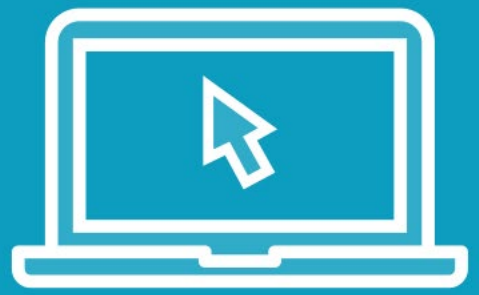
FTP Active Mode Download



FTP Interactive Commands



Demo

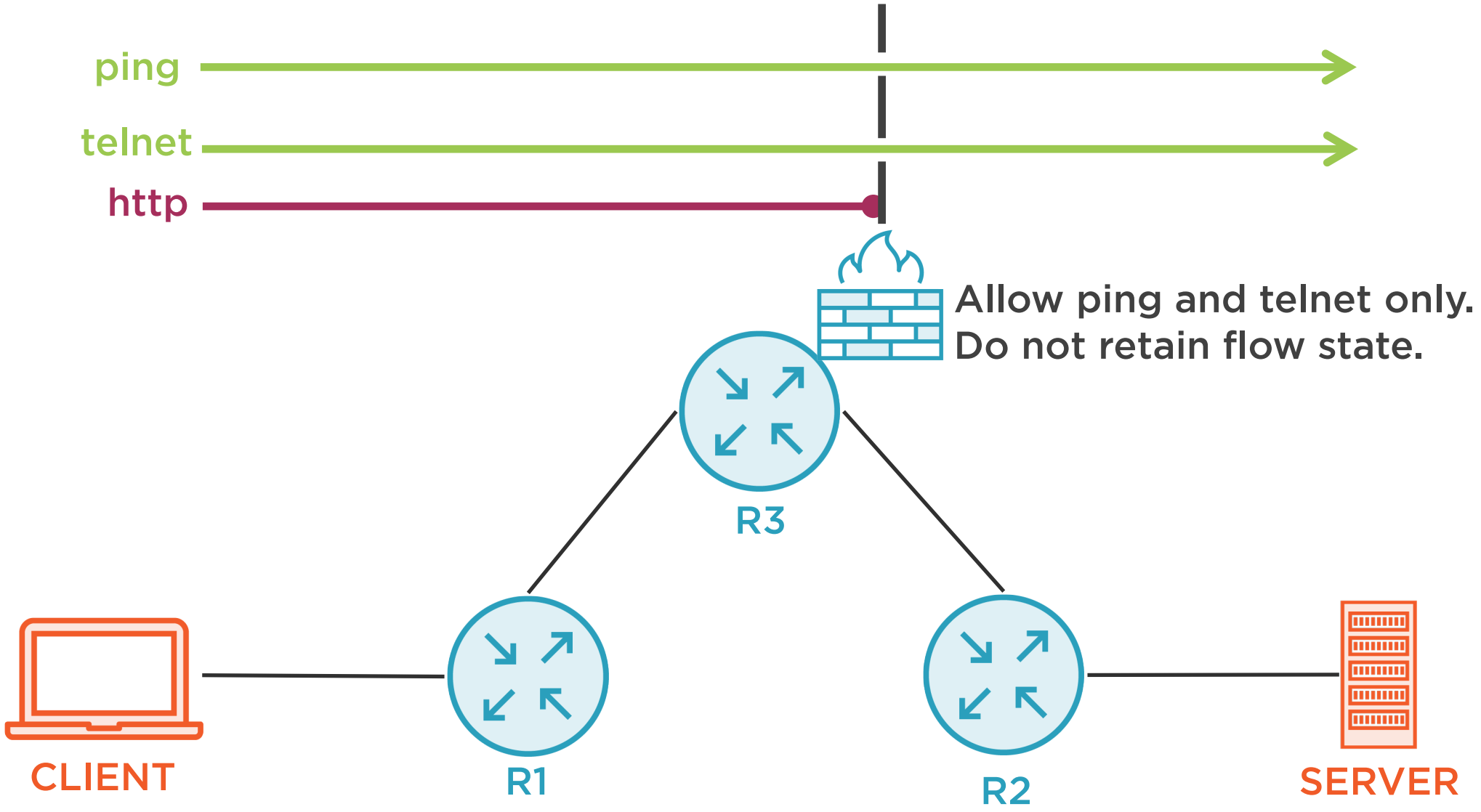


Can we upload files too?

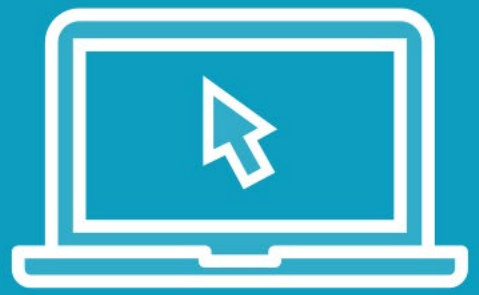
FTP Active Mode Upload

No.	Source	Destination	Proto	Src Port	Dst Port	Info
54	10.1.4.4	10.2.5.5	FTP	41142	21	Request: PORT 10,1,4,4,174,123
55	10.2.5.5	10.1.4.4	FTP	21	41142	Response: 200 PORT command successful. Consider using PASV.
56	10.1.4.4	10.2.5.5	FTP	41142	21	Request: ALLO 48
57	10.2.5.5	10.1.4.4	FTP	21	41142	Response: 202 ALLO command ignored.
58	10.1.4.4	10.2.5.5	FTP	41142	21	Request: STOR R3.cfg
59	10.2.5.5	10.1.4.4	TCP	20	44667	20→44667 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TS
60	10.1.4.4	10.2.5.5	TCP	44667	20	44667→20 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SA
61	10.2.5.5	10.1.4.4	TCP	20	44667	20→44667 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3738631017
62	10.2.5.5	10.1.4.4	FTP	21	41142	Response: 150 Ok to send data.
63	10.1.4.4	10.2.5.5	FTP-DATA	44667	20	FTP Data: 48 bytes
64	10.1.4.4	10.2.5.5	TCP	44667	20	44667→20 [FIN, ACK] Seq=49 Ack=1 Win=29056 Len=0 TSval=3083
65	10.2.5.5	10.1.4.4	TCP	20	44667	20→44667 [ACK] Seq=1 Ack=49 Win=29312 Len=0 TSval=373863101
66	10.2.5.5	10.1.4.4	TCP	20	44667	20→44667 [FIN, ACK] Seq=1 Ack=50 Win=29312 Len=0 TSval=3738
67	10.1.4.4	10.2.5.5	TCP	44667	20	44667→20 [ACK] Seq=50 Ack=2 Win=29056 Len=0 TSval=30837356
68	10.2.5.5	10.1.4.4	FTP	21	41142	Response: 226 Transfer complete.

FTP Active Mode Security Challenge



Demo



Securing active mode FTP

FTP Active Mode in Review

Old school

Outside in

Difficult to secure