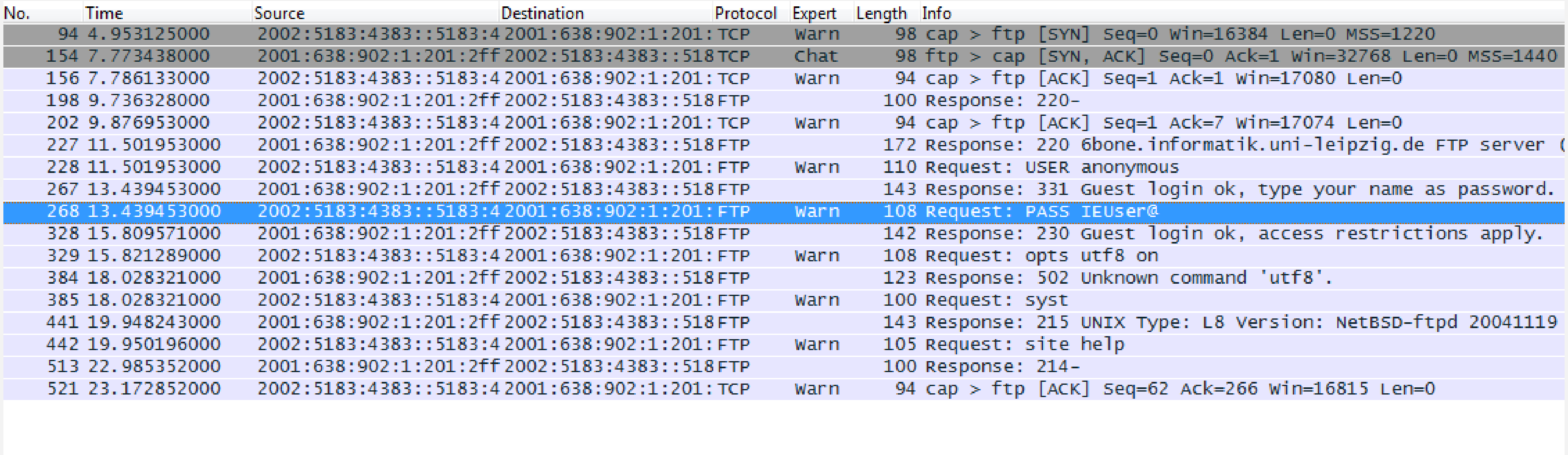
Analyzing Data Transfer

Analyzing Data Transfer

- What are the concerns with data transfer?
  - Latency
  - Bandwidth
  - I/O
  - Other
- How can Wireshark solve this problem?
  - Capture data from source to destination and find facts about time, throughput, and other key output to prove transfer issues

Analyzing Data Transfer



No.	Time	Source	Destination	Protocol	Expert	Length	Info
94	4.953125000	2002:5183:4383::5183:4	2001:638:902:1:201:	TCP	Warn	98	cap > ftp [SYN] Seq=0 Win=16384 Len=0 MSS=1220
154	7.773438000	2001:638:902:1:201:2ff	2002:5183:4383::518	TCP	Chat	98	ftp > cap [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1440
156	7.786133000	2002:5183:4383::5183:4	2001:638:902:1:201:	TCP	Warn	94	cap > ftp [ACK] Seq=1 Ack=1 Win=17080 Len=0
198	9.736328000	2001:638:902:1:201:2ff	2002:5183:4383::518	FTP		100	Response: 220-
202	9.876953000	2002:5183:4383::5183:4	2001:638:902:1:201:	TCP	Warn	94	cap > ftp [ACK] Seq=1 Ack=7 Win=17074 Len=0
227	11.501953000	2001:638:902:1:201:2ff	2002:5183:4383::518	FTP		172	Response: 220 6bone.informatik.uni-leipzig.de FTP server (
228	11.501953000	2002:5183:4383::5183:4	2001:638:902:1:201:	FTP	Warn	110	Request: USER anonymous
267	13.439453000	2001:638:902:1:201:2ff	2002:5183:4383::518	FTP		143	Response: 331 Guest login ok, type your name as password.
268	13.439453000	2002:5183:4383::5183:4	2001:638:902:1:201:	FTP	Warn	108	Request: PASS IEUser@
328	15.809571000	2001:638:902:1:201:2ff	2002:5183:4383::518	FTP		142	Response: 230 Guest login ok, access restrictions apply.
329	15.821289000	2002:5183:4383::5183:4	2001:638:902:1:201:	FTP	Warn	108	Request: opts utf8 on
384	18.028321000	2001:638:902:1:201:2ff	2002:5183:4383::518	FTP		123	Response: 502 Unknown command 'utf8'.
385	18.028321000	2002:5183:4383::5183:4	2001:638:902:1:201:	FTP	Warn	100	Request: syst
441	19.948243000	2001:638:902:1:201:2ff	2002:5183:4383::518	FTP		143	Response: 215 UNIX Type: L8 Version: NetBSD-ftpd 20041119
442	19.950196000	2002:5183:4383::5183:4	2001:638:902:1:201:	FTP	Warn	105	Request: site help
513	22.985352000	2001:638:902:1:201:2ff	2002:5183:4383::518	FTP		100	Response: 214-
521	23.172852000	2002:5183:4383::5183:4	2001:638:902:1:201:	TCP	Warn	94	cap > ftp [ACK] Seq=62 Ack=266 Win=16815 Len=0

Analyzing Data Transfer

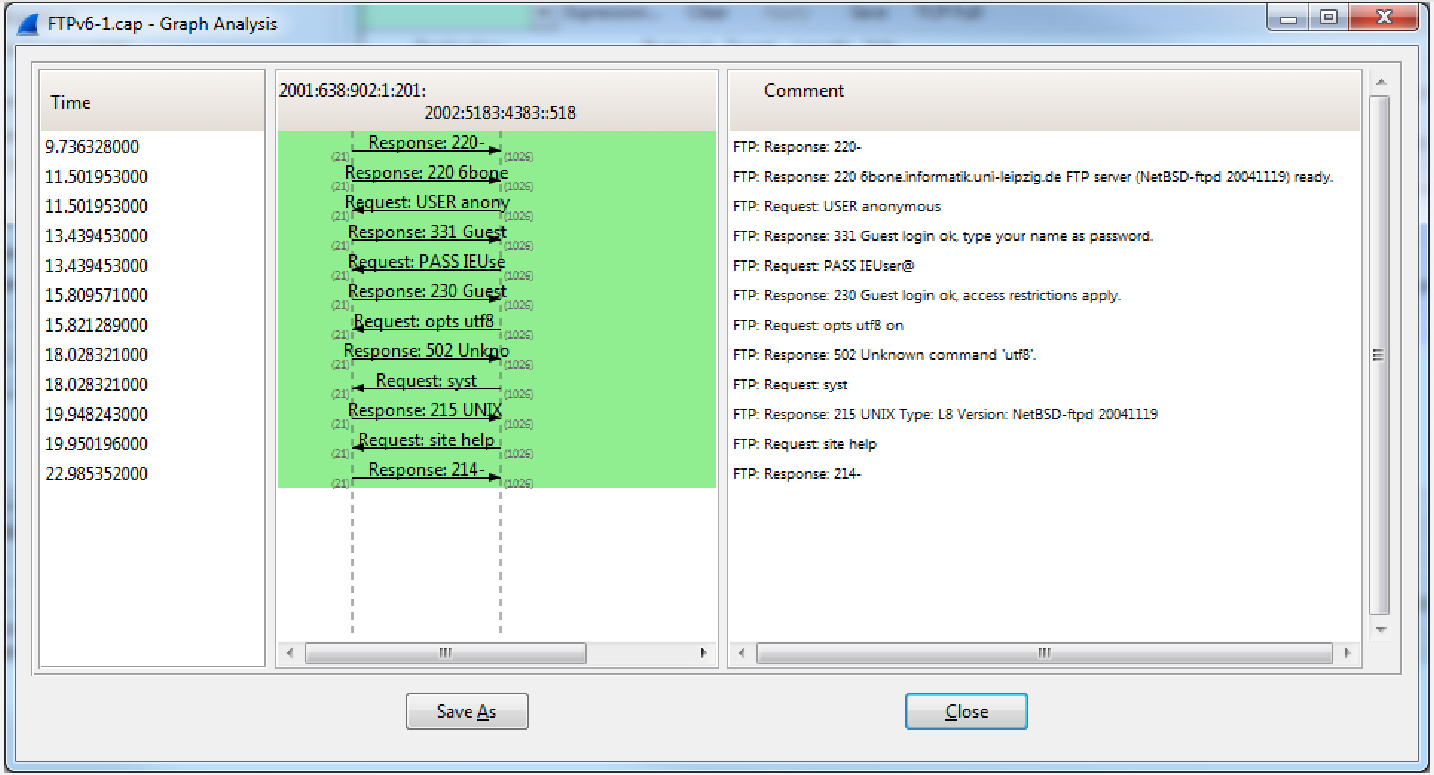
What do we look for in Wireshark?

- Timing problems
- Retransmissions (problems with TCP, etc.)
- Buffering issues
- Broadcasts
- Duplicate ACKs

Flow analysis

- Review Wireshark tools for a clear view of what the issue is stemming from (flow graphs, stream graphs, etc.)

Analyzing Data Transfer



Time	2001:638:902:1:201: 2002:5183:4383::518	Comment
9.736328000	Response: 220-	FTP: Response: 220-
11.501953000	Response: 220 6bone	FTP: Response: 220 6bone.informatik.uni-leipzig.de FTP server (NetBSD-ftpd 20041119) ready.
11.501953000	Request: USER anony	FTP: Request: USER anonymous
13.439453000	Response: 331 Guest	FTP: Response: 331 Guest login ok, type your name as password.
13.439453000	Request: PASS IEUse	FTP: Request: PASS IEUser@
15.809571000	Response: 230 Guest	FTP: Response: 230 Guest login ok, access restrictions apply.
15.821289000	Request: opts utf8	FTP: Request: opts utf8 on
18.028321000	Response: 502 Unkno	FTP: Response: 502 Unknown command 'utf8'.
18.028321000	Request: syst	FTP: Request: syst
19.948243000	Response: 215 UNIX	FTP: Response: 215 UNIX Type: L8 Version: NetBSD-ftpd 20041119
19.950196000	Request: site help	FTP: Request: site help
22.985352000	Response: 214-	FTP: Response: 214-

Questions?