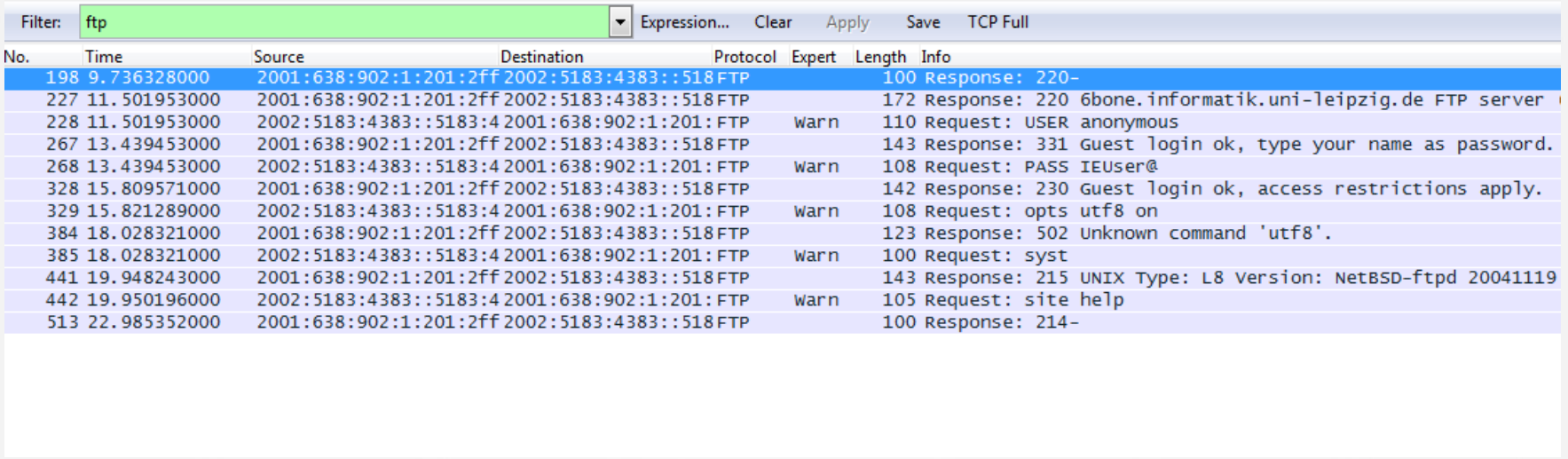
Capturing FTP

Capturing FTP

- What is FTP?
- Wireshark and FTP
  - Used to capture communication issues
  - Can capture cleartext transmissions
  - Used to find issues such as traversal problems

Capturing FTP

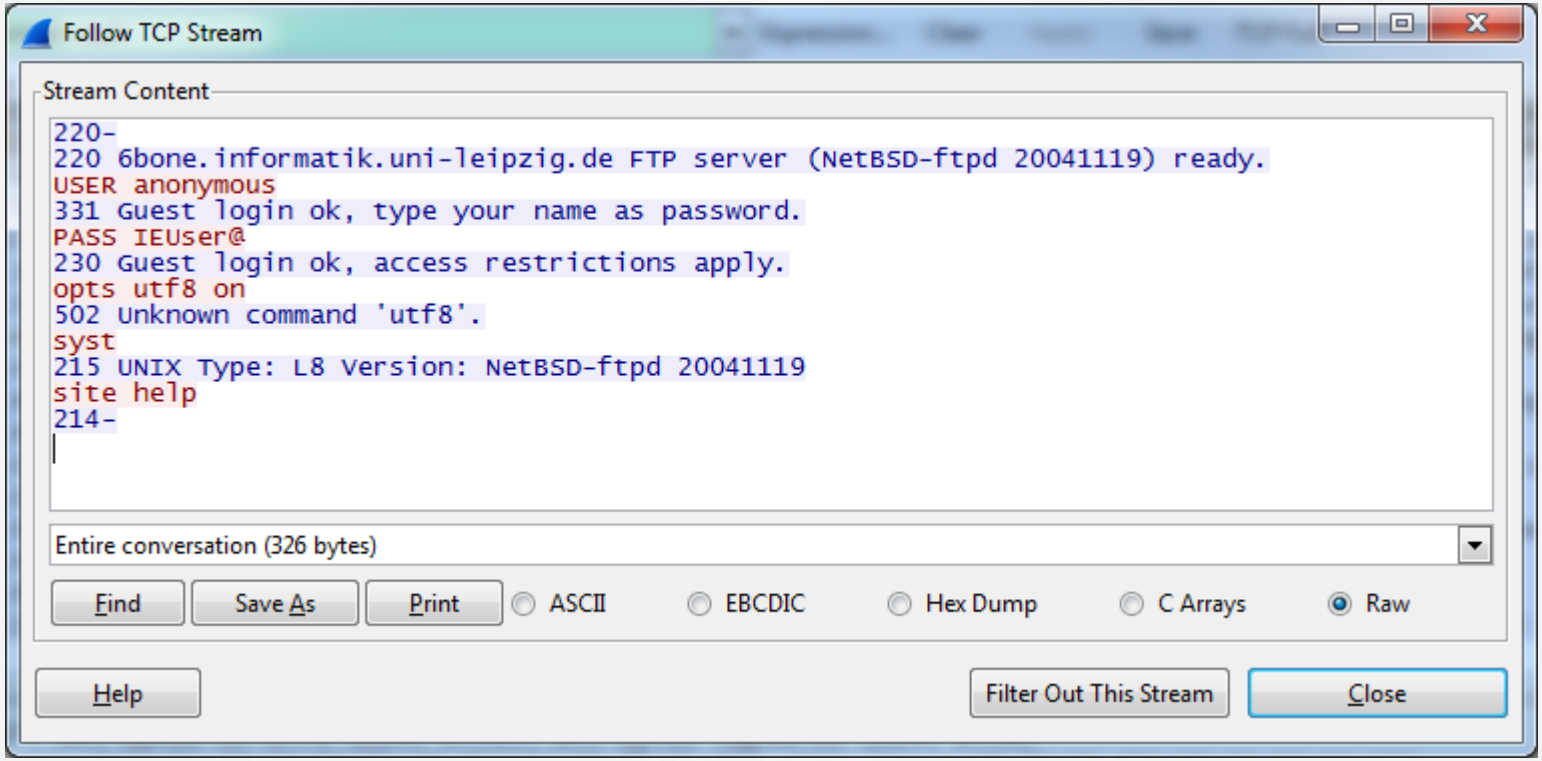


No.	Time	Source	Destination	Protocol	Expert	Length	Info
198	9.736328000	2001:638:902:1:201:2ff	2002:5183:4383::518	FTP		100	Response: 220-
227	11.501953000	2001:638:902:1:201:2ff	2002:5183:4383::518	FTP		172	Response: 220 6bone.informatik.uni-leipzig.de FTP server
228	11.501953000	2002:5183:4383::5183:4	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-

Capturing FTP

- **Problems with FTP**
  - Unsecured passwords, susceptible to a myriad of security attacks… use SSH-based FTP, or SFTP
  - Problems with NAT and firewalls (PASV)
- **TCP stream**
  - You can analyze the TCP stream to determine whether data has been encrypted or sent in plaintext
  - You can validate whether the session (communication) is being blocked or broken via NAT

Capturing FTP



Questions?