

www.ine.com

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



ftp		<ul> <li>Expression</li> </ul>	n Clear	Apply	/ Save TCP Full	
Time	Source	Destination	Protocol E	xpert Le	ength Info	
9.736328000	2001:638:902:1:201:21	ff2002:5183:4383::51	8 FTP		100 Response: 2	220-
11.501953000	2001:638:902:1:201:21	ff2002:5183:4383::51	8 FTP		172 Response: 2	220 6bone.informatik.uni-leipzig.de FTP server
3 11.501953000	2002:5183:4383::5183:	:42001:638:902:1:201	:FTP V	varn	110 Request: US	SER anonymous
13.439453000	2001:638:902:1:201:21	ff 2002:5183:4383::51	8 FTP		143 Response: 3	331 Guest login ok, type your name as password.
3 13.439453000	2002:5183:4383::5183:	:42001:638:902:1:201	:FTP V	varn	108 Request: P/	ASS IEUser@
3 15.809571000	2001:638:902:1:201:21	ff 2002:5183:4383::51	8 FTP		142 Response: 2	230 Guest login ok, access restrictions apply.
15.821289000	2002:5183:4383::5183:	:42001:638:902:1:201	:FTP V	varn	108 Request: op	pts utf8 on
18.028321000	2001:638:902:1:201:21	ff 2002:5183:4383::51	8 FTP		123 Response:	502 Unknown command 'utf8'.
18.028321000	2002:5183:4383::5183:	:42001:638:902:1:201	:FTP V	varn	100 Request: sy	yst
19.948243000	2001:638:902:1:201:21	ff 2002:5183:4383::51	8 FTP		143 Response: 2	215 UNIX Type: L8 Version: NetBSD-ftpd 20041119
19.950196000	2002:5183:4383::5183:	:42001:638:902:1:201	:FTP V	varn	105 Request: st	ite help
22.985352000	2001:638:902:1:201:21	ff 2002:5183:4383::51	8 FTP		100 Response: 2	214-
	Time 9.736328000 11.501953000 13.439453000 13.439453000 13.439453000 15.809571000 15.821289000 18.028321000 18.028321000 19.948243000 19.950196000	Time         Source           9.736328000         2001:638:902:1:201:21           11.501953000         2001:638:902:1:201:21           11.501953000         2002:5183:4383:5183           13.439453000         2001:638:902:1:201:21           13.439453000         2002:5183:4383:5183           15.809571000         2001:638:902:1:201:21           15.821289000         2002:5183:4383:5183           18.028321000         2001:638:902:1:201:21           18.028321000         2002:5183:4383:5183           19.948243000         2001:638:902:1:201:21           219.950196000         2002:5183:4383:5183	Time         Source         Destination           9.736328000         2001:638:902:1:201:2ff 2002:5183:4383::51           11.501953000         2001:638:902:1:201:2ff 2002:5183:4383::51           11.501953000         2002:5183:4383::5183:4 2001:638:902:1:201           13.439453000         2001:638:902:1:201:2ff 2002:5183:4383::51           13.439453000         2001:638:902:1:201:2ff 2002:5183:4383::51           13.439453000         2001:638:902:1:201:2ff 2002:5183:4383::51           15.809571000         2001:638:902:1:201:2ff 2002:5183:4383::51           15.821289000         2002:5183:4383::5183:4 2001:638:902:1:201           18.028321000         2001:638:902:1:201:2ff 2002:5183:4383::51           18.028321000         2001:638:902:1:201:2ff 2002:5183:4383::51           19.948243000         2001:638:902:1:201:2ff 2002:5183:4383::51           19.950196000         2002:5183:4383::5183:4 2001:638:902:1:201	Time         Source         Destination         Protocol         E           9.736328000         2001:638:902:1:201:2ff 2002:5183:4383:518 FTP         11.501953000         2001:638:902:1:201:2ff 2002:5183:4383:518 FTP         11.501953000         2002:5183:4383:5183:42001:638:902:1:201:FTP         11.50195300         2002:5183:4383:5183:42001:638:902:1:201:FTP         11.50195300         2002:5183:4383:5183:42001:638:902:1:201:FTP         11.50195300         2002:5183:4383:5183:42001:638:902:1:201:FTP         11.50195300         2002:5183:4383:5183:42001:638:902:1:201:FTP         11.50195300         2002:5183:4383:5183:42001:638:902:1:201:FTP         11.50195300         2002:5183:4383:5183:42001:638:902:1:201:FTP         11.50195000         2002:5183:4383:5183:42001:638:902:1:20	Time         Source         Destination         Protocol         Expert         L           9.736328000         2001:638:902:1:201:2ff 2002:5183:4383:518 FTP         11.501953000         2001:638:902:1:201:2ff 2002:5183:4383:518 FTP         11.501953000         2002:5183:4383:5183:4 2001:638:902:1:201:FTP         Warn           13.439453000         2001:638:902:1:201:2ff 2002:5183:4383:518 FTP         13.439453000         2001:638:902:1:201:2ff 2002:5183:4383:518 FTP           13.439453000         2002:5183:4383:5183:4 2001:638:902:1:201:FTP         Warn           13.639571000         2001:638:902:1:201:2ff 2002:5183:4383:518 FTP         15.821289000         2002:5183:4383:5183:4 2001:638:902:1:201:FTP         Warn           18.028321000         2001:638:902:1:201:2ff 2002:5183:4383:518 FTP         18.028321000         2001:638:902:1:201:2ff 2002:5183:4383:518 FTP           19.948243000         2001:638:902:1:201:2ff 2002:5183:4383:518 FTP         Warn         19.948243000         2001:638:902:1:201:2ff 2002:5183:4383:518 FTP	Time         Source         Destination         Protocol         Expert         Length         Info           9.736328000         2001:638:902:1:201:2ff 2002:5183:4383:518 FTP         100         Response:         11.501953000         2001:638:902:1:201:2ff 2002:5183:4383:518 FTP         172         Response:         11.501953000         2002:5183:4383:5183:42001:638:902:1:201:FTP         Warn         110         Request:         00           11.501953000         2002:5183:4383:5183:42001:638:902:1:201:FTP         Warn         110         Request:         00           13.439453000         2002:5183:4383:5183:42001:638:902:1:201:FTP         Warn         108         Request:         01           15.809571000         2002:5183:4383:5183:42001:638:902:1:201:FTP         Warn         108         Request:         01           15.821289000         2002:5183:4383:5183:42001:638:902:1:201:FTP         Warn         108         Request:         01           18.028321000         2001:638:902:1:201:2ff 2002:5183:4383:518         FTP         123         Response:         13           19.948243000         2001:638:902:1:201:2ff 2002:5183:4383:518         FTP         143         Response:         143           19.950196000         2002:5183:4383:5183:42001:638:902:1:201:FTP         Warn         100         Request:         10



#### » 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



Follow TCP Stream
Stream Content
<pre>220- 220 6bone.informatik.uni-leipzig.de FTP server (NetBSD-ftpd 20041119) ready. USER anonymous 331 Guest login ok, type your name as password. PASS IEUser@ 230 Guest login ok, access restrictions apply. opts utf8 on 502 Unknown command 'utf8'. syst 215 UNIX Type: L8 Version: NetBSD-ftpd 20041119 site help 214-</pre>
Entire conversation (326 bytes)
<u>Find</u> Save <u>As</u> <u>Print</u> ASCII © EBCDIC © Hex Dump © C Arrays @ Raw
Help Filter Out This Stream Close



# Questions?

Copyright © www.ine.com All rights reserved.