

5.1.1

Network Sniffing (FTP / Telnet Sessions) (Ethereal)

The screenshot displays the dump1 - Ethereal interface with a captured FTP session. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Info
104	83.646948	192.168.69.118	239.255.255.253	SRVLOC	Service Request
103	83.645967	192.168.69.118	239.255.255.253	SRVLOC	Service Request
387	361.723029	192.168.69.30	192.168.69.118	FTP	Response: 500 'FEAT': command not understood.
47670	797.286981	192.168.69.30	192.168.69.118	FTP	Response: 500 'EPSV': command not understood.
358	359.527074	192.168.69.30	192.168.69.118	FTP	Response: 331 Password required for doug.
389	361.728019	192.168.69.30	192.168.69.118	FTP	Response: 257 "/home/doug" is current directory.
383	361.712296	192.168.69.30	192.168.69.118	FTP	Response: 230 user doug logged in.
47672	797.292998	192.168.69.30	192.168.69.118	FTP	Response: 227 Entering Passive Mode (192,168,69,30,4
47685	797.470874	192.168.69.30	192.168.69.118	FTP	Response: 226 Transfer complete.
349	356.289400	192.168.69.30	192.168.69.118	FTP	Response: 220 beth.douglax.com FTP server (Version w
385	361.717053	192.168.69.30	192.168.69.118	FTP	Response: 215 UNIX Type: L8
47677	797.308976	192.168.69.30	192.168.69.118	FTP	Response: 150 opening ASCII mode data connection for
356	359.435143	192.168.69.118	192.168.69.30	FTP	Request: USER doug
384	361.715059	192.168.69.118	192.168.69.30	FTP	Request: SYST
388	361.725022	192.168.69.118	192.168.69.30	FTP	Request: PWD
47671	797.289979	192.168.69.118	192.168.69.30	FTP	Request: PASV
381	361.497265	192.168.69.118	192.168.69.30	FTP	Request: PASS dtc1
47676	797.299964	192.168.69.118	192.168.69.30	FTP	Request: LIST
386	361.722037	192.168.69.118	192.168.69.30	FTP	Request: FEAT
47669	797.285224	192.168.69.118	192.168.69.30	FTP	Request: EPSV
44596	691.088274	192.168.69.150	192.168.69.123	SNMP	RESPONSE iso.3.6.1.2.1.25.3.2.1.5.1 iso.3.6.1.2.1.25
44594	691.081204	192.168.69.150	192.168.69.123	SNMP	RESPONSE iso.3.6.1.2.1.25.3.2.1.5.1 iso.3.6.1.2.1.25
134	91.120922	192.168.69.150	192.168.69.123	SNMP	RESPONSE iso.3.6.1.2.1.25.3.2.1.5.1 iso.3.6.1.2.1.25
367	360.431619	192.168.69.79	192.168.69.123	NBSS	Positive session response

The bottom pane shows the details for Frame 387 (91 bytes on wire, 91 bytes captured):

- Ethernet II, Src: 00:10:4b:8d:18:e7, Dst: 00:60:1d:f0:59:8e
- Internet Protocol, Src Addr: 192.168.69.30 (192.168.69.30), Dst Addr: 192.168.69.118 (192.168.69.118)
- Transmission Control Protocol, Src Port: ftp (21), Dst Port: 49155 (49155), Seq: 185, Ack: 35, Len: 37
- File Transfer Protocol (FTP)

The hex dump at the bottom shows the raw data of the packet, including the ASCII text: "...Y... K....E..", ".M.\$0.0. S...E..", "Ev....I :U5C.P.", "...p..50 0 'FEAT'", and ": comman d not un".

Objective

At the end of this lab students will have demonstrated the clear text vulnerability of telnet and ftp and be able to retrieve user name and password.

Information for Laboratory

Students will require a platform with Ethereal functional and another with ftp and telnet clients on a non-switched or wireless network. Access and accounts to a telnet and ftp server.

Student Preparation

The student will have reviewed:

<http://www.ethereal.com> site

<http://www.ethereal.com/faq.html>

<http://www.ethereal.com/docs/user-guide/>

<http://www.ethereal.com/links.html>

The student will require paper for notes and should be prepared to discuss the exercises upon completion.

Note: This lab is to be done is either Linux or Windows.

Linux requires (is included with most current distributions):

libpcap

tcpdump

ethereal-0.10.2.tar.gz

Windows requires:

WinPcap_3_0.exe

ethereal-setup-0.10.2.exe



Estimated Completion Time

60 - 90 Minutes

Username and Password Sniffing Telnet & FTP

Having the ability to look at and analyze packets on a network can be very informative. There are many reasons an administrator may want to see what is traversing the network. On a wireless or non-switched network packets can be seen by both those that have legitimate needs and those that are up to nefarious activities.

Network Analysis Software

There are several different programs, both commercial and shareware/freeware that incorporate the many different Packet Sniffing techniques on the market today (some are).

Ethereal

dsniff

Windump

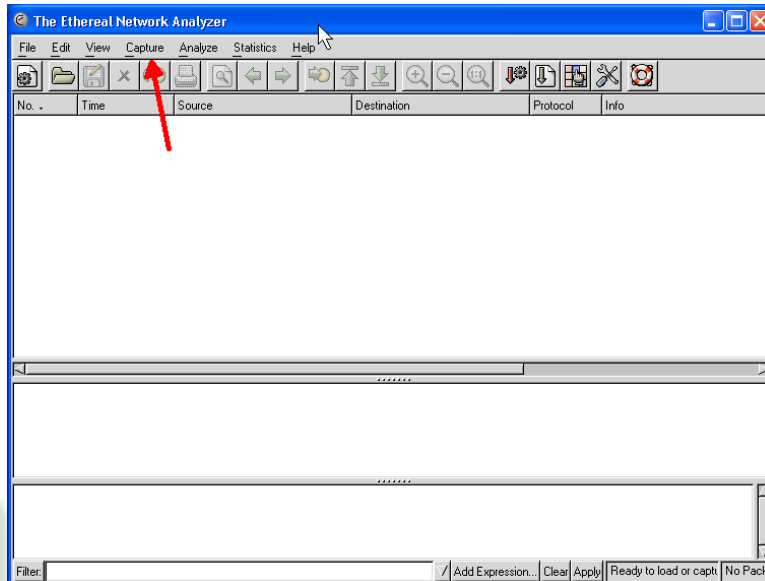
Analyzer

more <http://www.mirrors.wiretapped.net/security/packet-capture/>



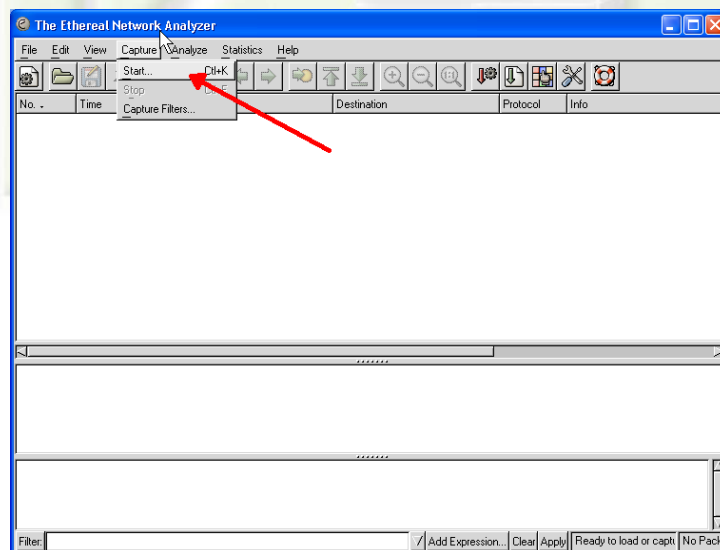
Step 1: Open the Ethereal client.

Select Capture

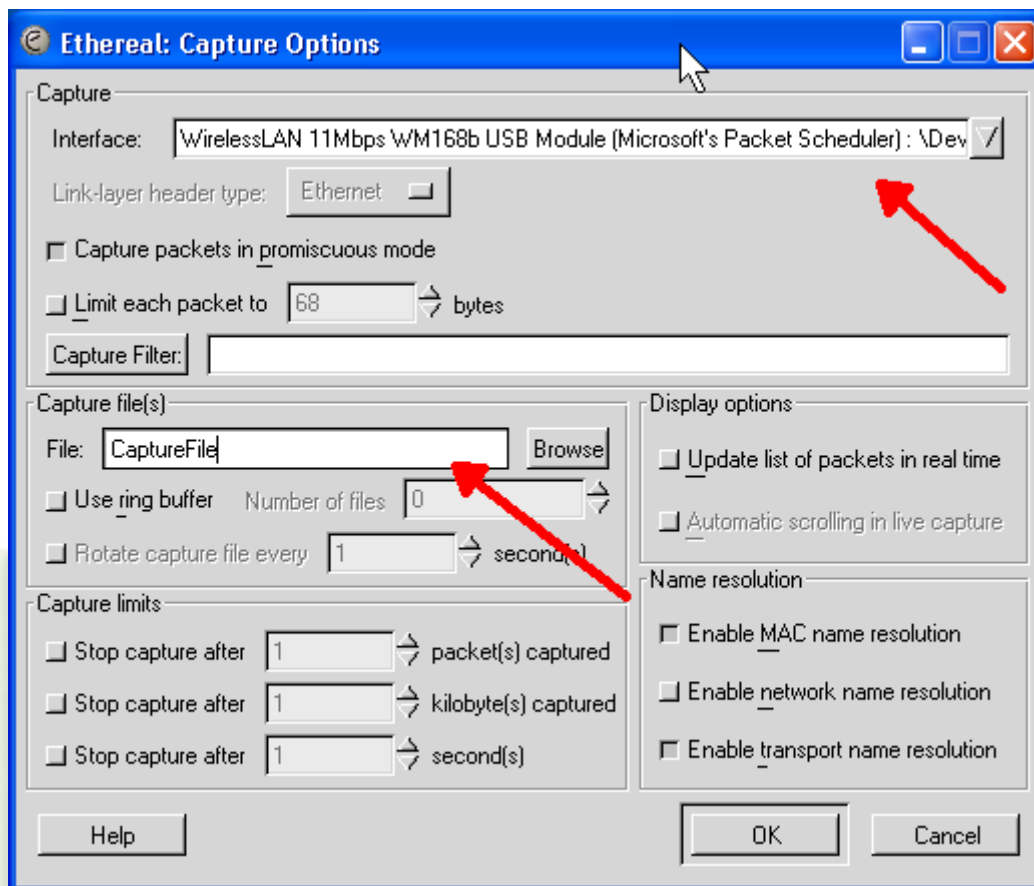


Step 2: Start Capture Process

Click Menu Item *Capture* then select *Start*



Step 3: Select the Interface and name capture file



Step 4: Initiate Telnet and FTP sessions

On another machine establish a telnet and ftp sessions.
(If on a switched network use the same machine as other techniques are required to sniff a switched network.)

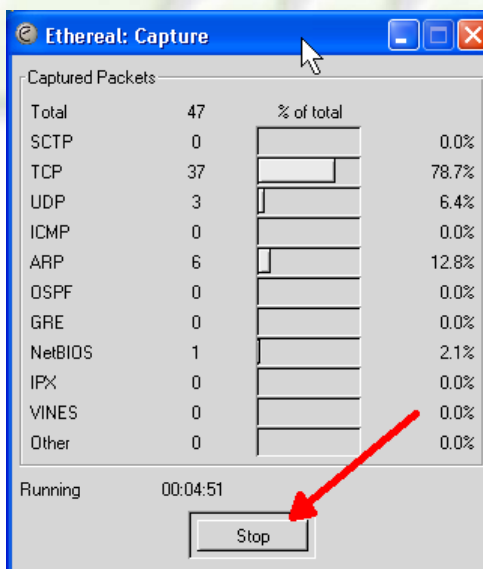
```
Terminal — ttyt1
Last login: Thu Mar 11 09:21:44 on console
Welcome to Darwin!
[dhcp-118:~] dtc% telnet beth
Trying 192.168.69.30...
Connected to beth.dougcox.com.
Escape character is '^]'.
Password:
Login incorrect

login: doug
Password:
Last login: Wed Mar 10 19:38:16 from dhcp-123
You have mail.
[doug@beth]$
```

```
Terminal — ttyt2
Last login: Thu Mar 11 09:22:22 on ttyt1
Welcome to Darwin!
[dhcp-118:~] dtc% ftp beth
Connected to beth.dougcox.com.
220 beth.dougcox.com FTP server (Version wu-2.4.2-academ[BETA-15](1)
3:08:32 EST 1997) ready.
Name (beth:dtc): doug
331 Password required for doug.
Password:
230 User doug logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
500 'EPSV': command not understood.
227 Entering Passive Mode (192,168,69,30,4,1)
150 Opening ASCII mode data connection for /bin/ls.
total 2388
drwxr-sr-x  3 doug  users      1024 Aug 19  2002 antenna
-rw-r--r--  1 root   root       35981 Apr  4  1998 *
drwxr-xr-x 34 doug  users      2048 Mar  7  01:17 .
drwxr-xr-x 13 root   users      1024 Feb 19  2003 ..
drwxr-xr-x 55 doug  doug       1024 Apr  5  1998 .AppleDesktop
drwxr-xr-x  2 doug  doug       1024 Aug 19  2002 .AppleDouble
-rw-r--r--  1 doug  doug       3768 Nov  7  1997 .Xdefaults
```

Step 5: Stop Capture

After establishing connections via telnet and ftp stop the capture. On a busy network these files can grow very large.



Step 6: Return to Ethereal Main Screen

If the capture screen does not appear, Use *File -> Open* and load capture file.

- 1) Sort by Protocol
- 2) The server will respond with a password required for username
- 3) Password in clear text is after "PASS"
- 4) Next Step is to Analyze the Stream

The screenshot shows the Ethereal (Wireshark) interface with a capture of an FTP session. The main packet list is sorted by Protocol. The selected packet (No. 387) is an FTP Response (500) indicating a command not understood. The packet details pane shows the FTP session structure, including the 'PASS' command and the response. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Info
104	83.646948	192.168.69.118	239.255.255.253	SRVLOC	Service Request
103	83.645967	192.168.69.118	239.255.255.253	SRVLOC	Service Request
387	361.723029	192.168.69.30	192.168.69.118	FTP	Response: 500 'FEAT': command not understood.
47670	797.286981	192.168.69.30	192.168.69.118	FTP	Response: 500 'EPSV': command not understood.
358	359.527074	192.168.69.30	192.168.69.118	FTP	Response: 331 Password required for doug.
389	361.728019	192.168.69.30	192.168.69.118	FTP	Response: 257 "/home/doug" is current directory.
383	361.712296	192.168.69.30	192.168.69.118	FTP	Response: 230 User doug logged in.
47672	797.292998	192.168.69.30	192.168.69.118	FTP	Response: 227 Entering Passive Mode (192,168,69,30,4
47685	797.470874	192.168.69.30	192.168.69.118	FTP	Response: 226 Transfer complete.
349	356.289400	192.168.69.30	192.168.69.118	FTP	Response: 220 beth.dougcox.com FTP server (Version w
385	361.717053	192.168.69.30	192.168.69.118	FTP	Response: 215 UNIX Type: L8
47677	797.308976	192.168.69.30	192.168.69.118	FTP	Response: 150 opening ASCII mode data connection for
356	359.435143	192.168.69.30	192.168.69.118	FTP	Request: USER doug
384	361.715059	192.168.69.30	192.168.69.118	FTP	Request: SYST
388	361.725022	192.168.69.30	192.168.69.118	FTP	Request: PWD
47671	797.289979	192.168.69.118	192.168.69.30	FTP	Request: PASV
381	361.497265	192.168.69.118	192.168.69.30	FTP	Request: PASS dtcl
47676	797.299964	192.168.69.118	192.168.69.30	FTP	Request: LIST
386	361.722037	192.168.69.118	192.168.69.30	FTP	Request: FEAT
47669	797.285224	192.168.69.118	192.168.69.30	FTP	Request: EPSV
44596	691.088274	192.168.69.150	192.168.69.123	SNMP	RESPONSE iso.3.6.1.2.1.25.3.2.1.5.1 iso.3.6.1.2.1.25
44594	691.081204	192.168.69.150	192.168.69.123	SNMP	RESPONSE iso.3.6.1.2.1.25.3.2.1.5.1 iso.3.6.1.2.1.25
134	91.120922	192.168.69.150	192.168.69.123	SNMP	RESPONSE iso.3.6.1.2.1.25.3.2.1.5.1 iso.3.6.1.2.1.25
367	360.431619	192.168.69.79	192.168.69.123	NBSS	Positive session response

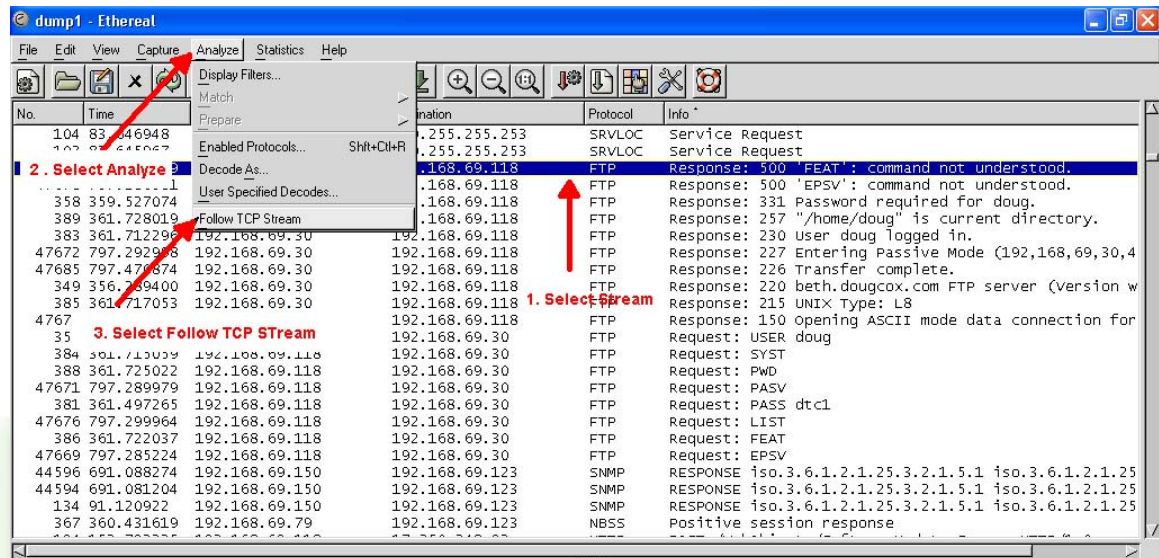
Frame 387 (91 bytes on wire, 91 bytes captured)
Ethernet II, Src: 00:10:4b:8d:18:e7, Dst: 00:60:1d:f0:59:8e
Internet Protocol, Src Addr: 192.168.69.30 (192.168.69.30), Dst Addr: 192.168.69.118 (192.168.69.118)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 49155 (49155), Seq: 185, Ack: 35, Len: 37
File Transfer Protocol (FTP)

0000 00 60 1d f0 59 8e 00 10 4b 8d 18 e7 08 00 45 10 . . . Y . . . K E .
0010 00 4d db 24 40 00 40 06 53 91 c0 a8 45 1e c0 a8 . M . \$. . . S . . . E . .
0020 45 76 00 15 c0 03 ae 49 3b 0d 55 35 63 89 50 18 EV I . . . U5C.P.
0030 7f e0 80 70 00 00 35 30 20 27 46 45 41 54 27 . . . p . 50 0 'FEAT'
0040 3a 20 63 6f 6d 61 6e 64 20 6e 6f 74 20 75 6e : command not un

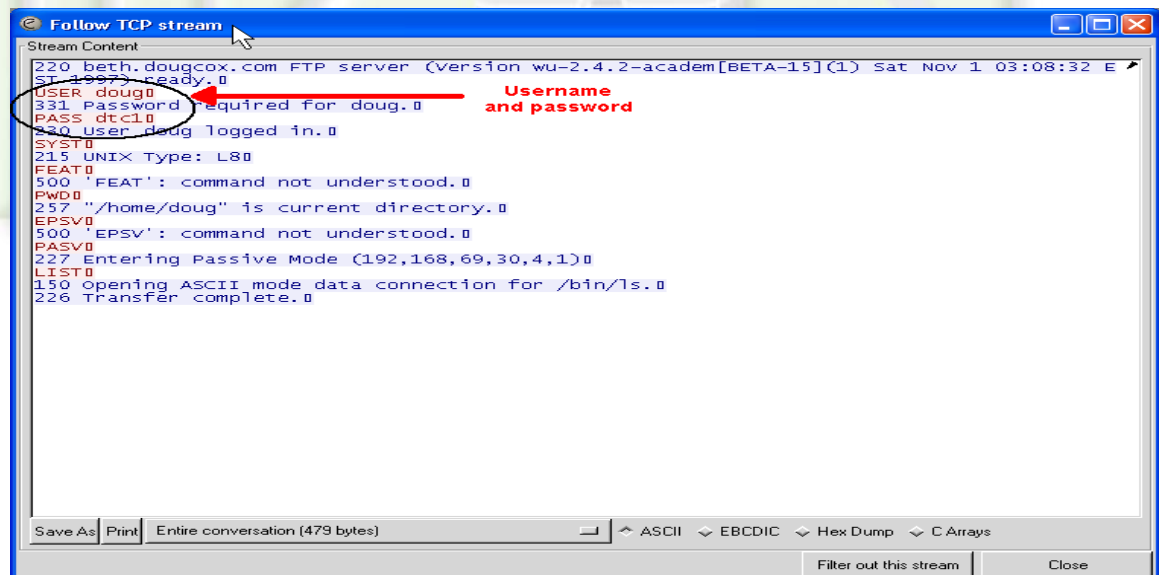


Step 7: Analyze Stream

- 1) Select Stream (close to the beginning)
- 2) Select Analyze
- 3) Select Follow Stream



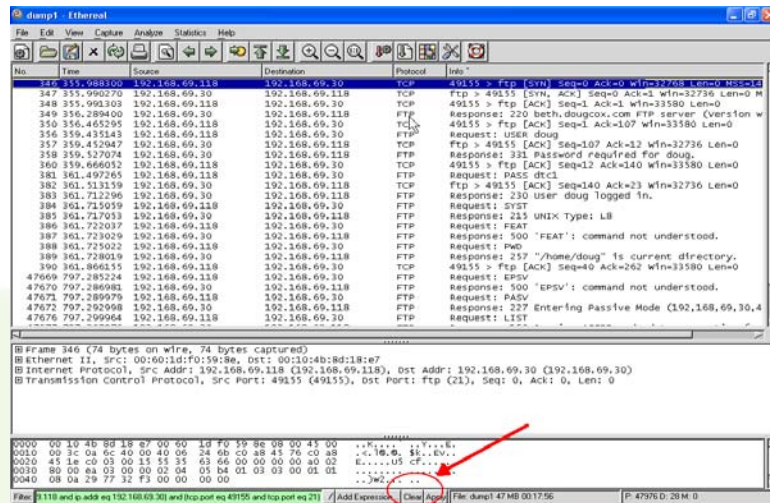
The program will process the stream and display the contents:



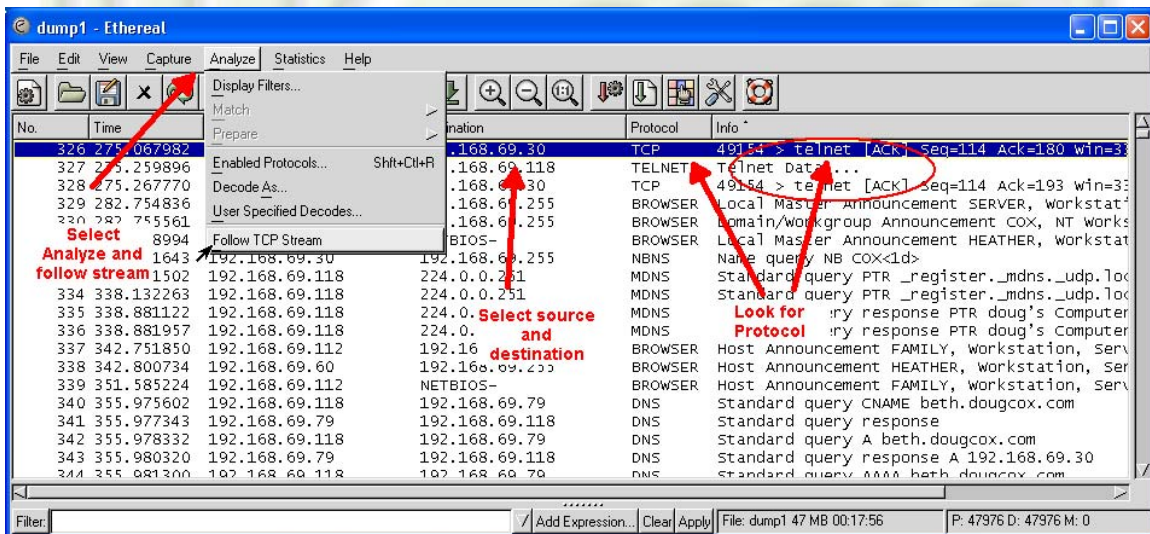
Step 8: Following a telnet steam

Telnet does not put the username and passwords in the headers as obviously as ftp. However, they are still passed in clear text and easily sniffed.

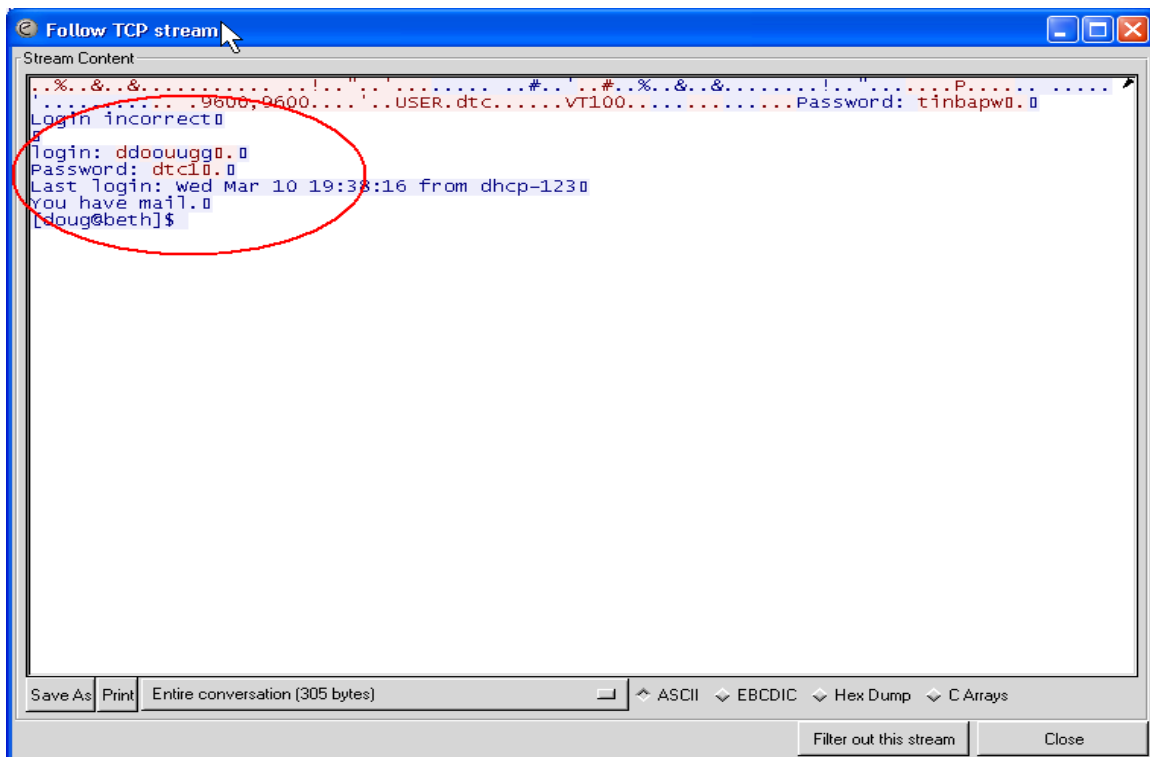
First clear the Filter by clicking the Clear Button at the bottom of the Ethereal window.



Select target machine and telnet session. Analyze and follow stream.



Step 9: Examine the stream



- 1) Why does the login have double characters (one red and one blue)?
- 2) Look at the TCP streams for FTP and Telnet and discuss how they are similar and different.
- 3) Discuss how you would use the FTP-DATA stream to grab a file.
- 4) Discuss the Protocol Column focusing on TCP, FTP-DATA, FTP and TELNET.

Summary Discussion

Analyzing traffic on a network can provide a clearer picture of what is happening. It can be used to follow break-in attempts as well as spying on users. If you are running the packet sniffer on against your machine you can see what the applications are doing. Who does your machine talk to when it boots? Does it call home? This has been a quick look at one of the many features of network analyzers.



Appendix:

This lab was developed using Ethereal 0.10.8, which can be obtained from:

www.ethereal.com

-or-

<http://www.download.com>

and WinPcap (Windows Packet Capturing software), which can be obtained from:

<http://winpcap.polito.it/>

-or-

www.ethereal.com

-or-

<http://www.download.com>

Note that Ethereal, in particular WinPcap, may have difficulty starting a capture from a wireless network adaptor.

The OS environment for this lab was Windows XP Professional, Version 2002, Service Pack 2 (8/04).

