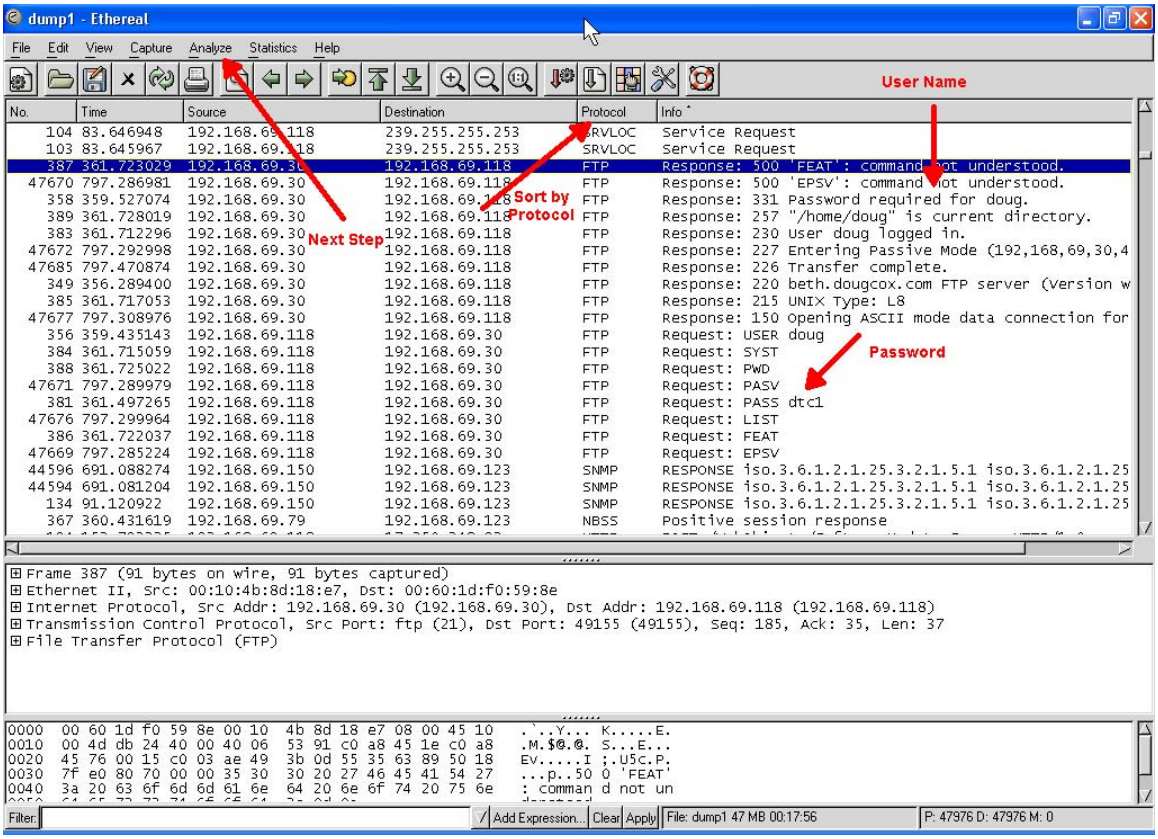
5.1.1

Network Sniffing (FTP / Telnet Sessions)

(Ethereal)



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.

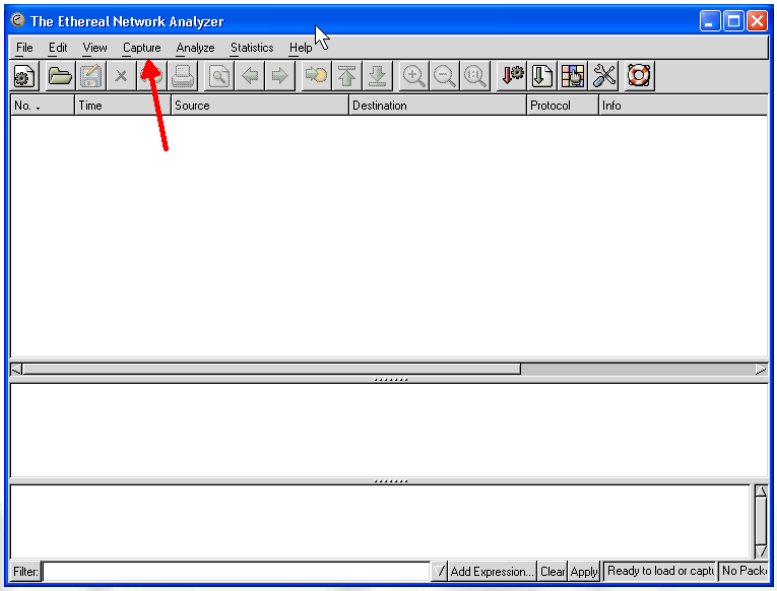
Network Analysis Software

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/

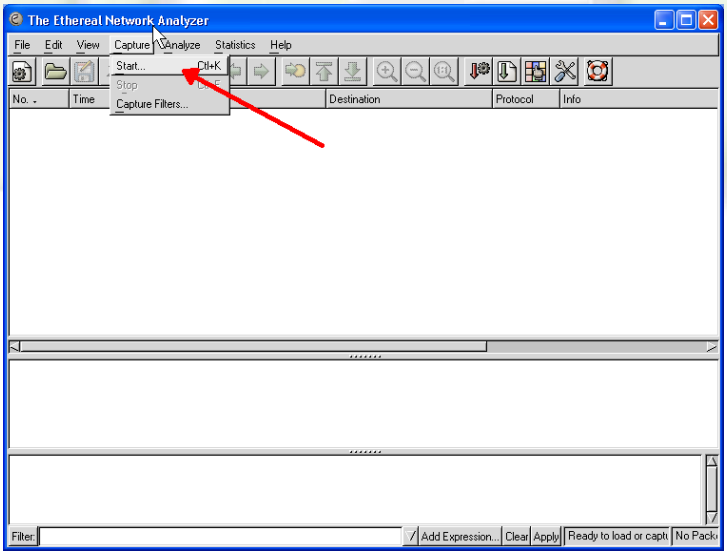
Step I: Open the Ethereal client.

Select Capture

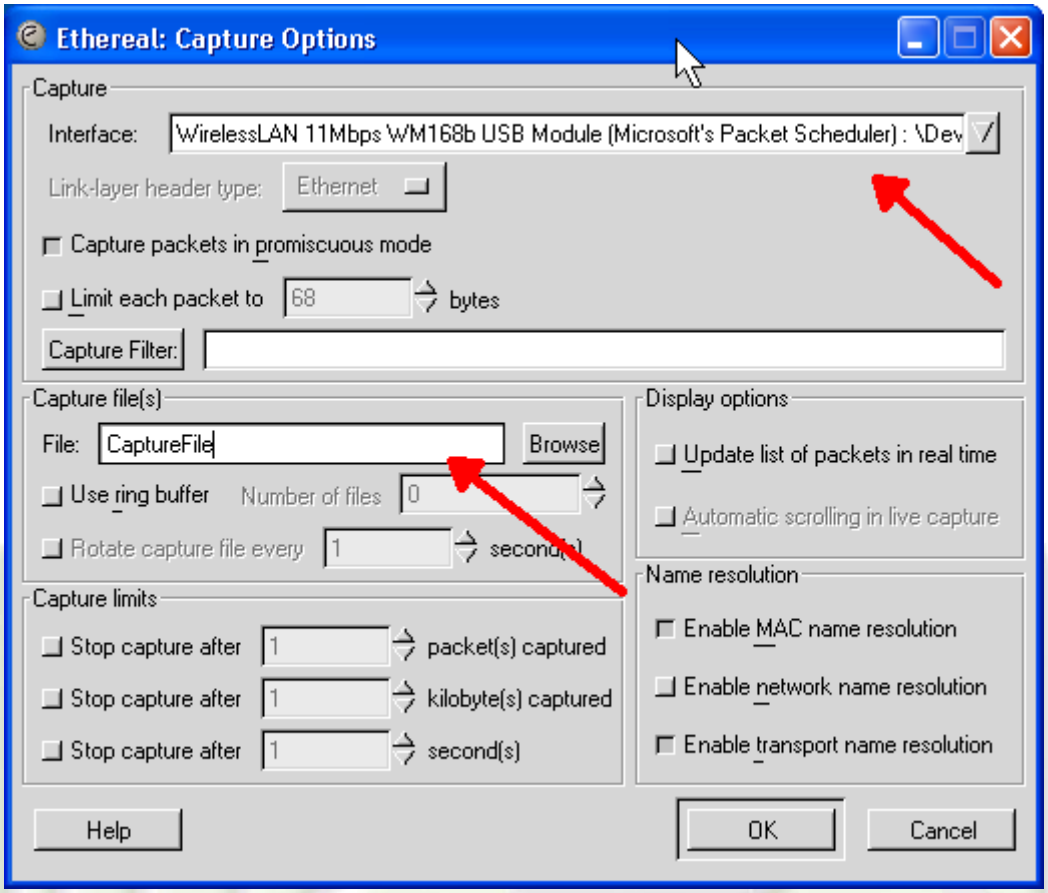


Step 2: Start Capture Process

Click Menu Item *Capture* then select *Start*

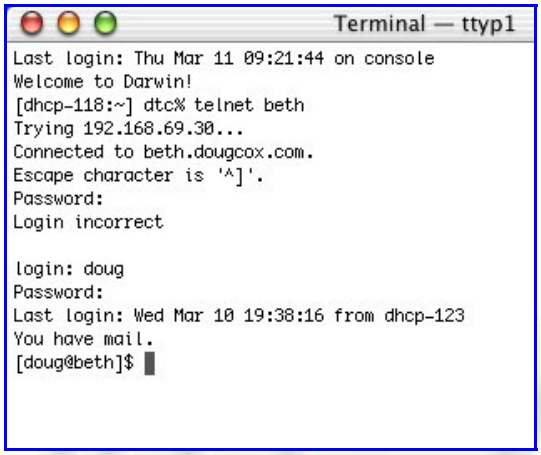


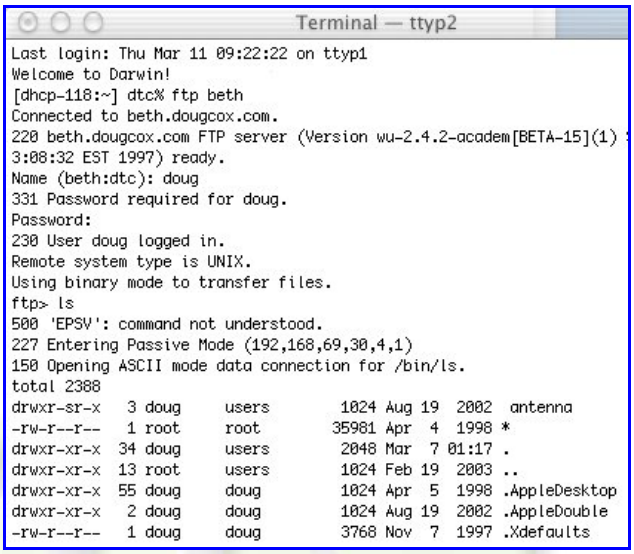
Step 3: Select the Interface and name capture file



Step 4: Initiate Telnet and FTP sessions

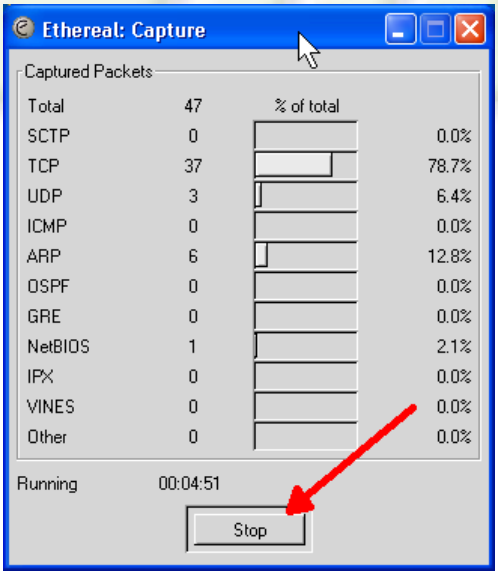
On another machine establish a telnet and ftp sessions. (If on a switched network use the same machine as other techniques are required to sniff a switched network.)





Step 5: Stop Capture

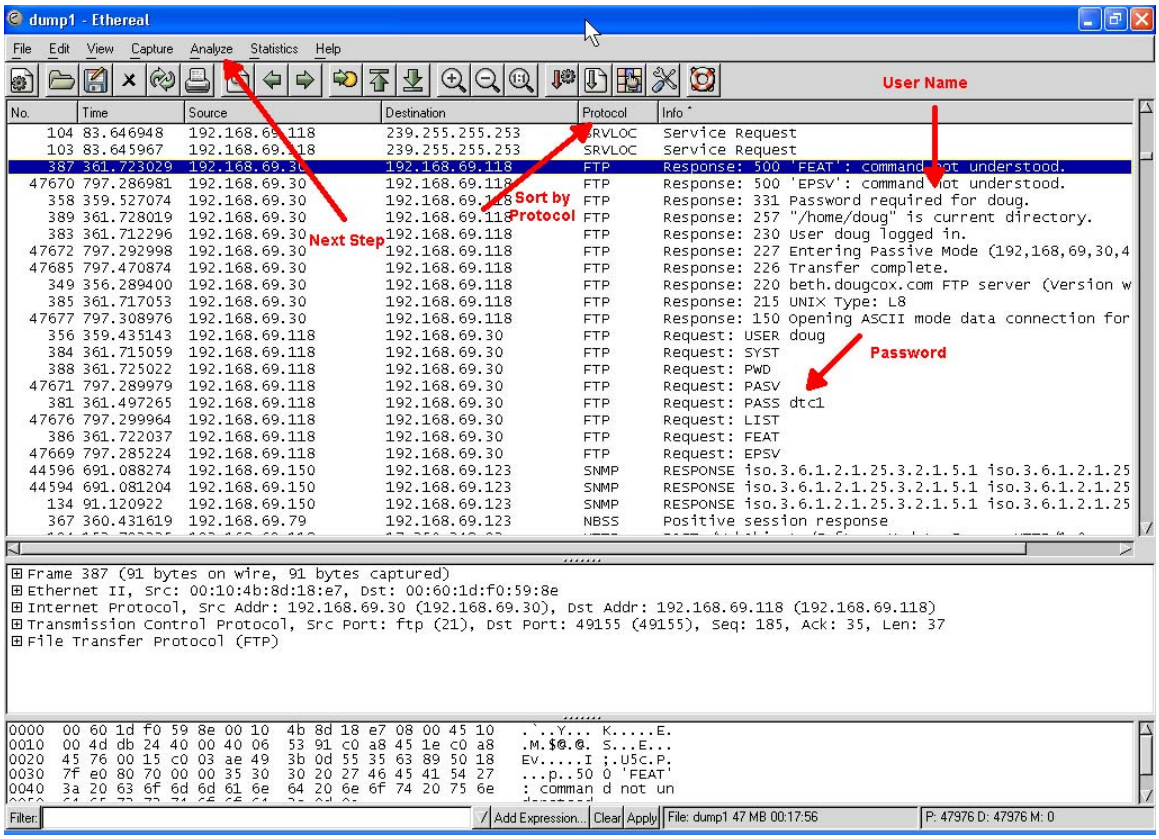
After establishing connections via telnet and ftp stop the capture. On a busy network these files can grow very large.



Step 6: Return to Ethereal Main Screen

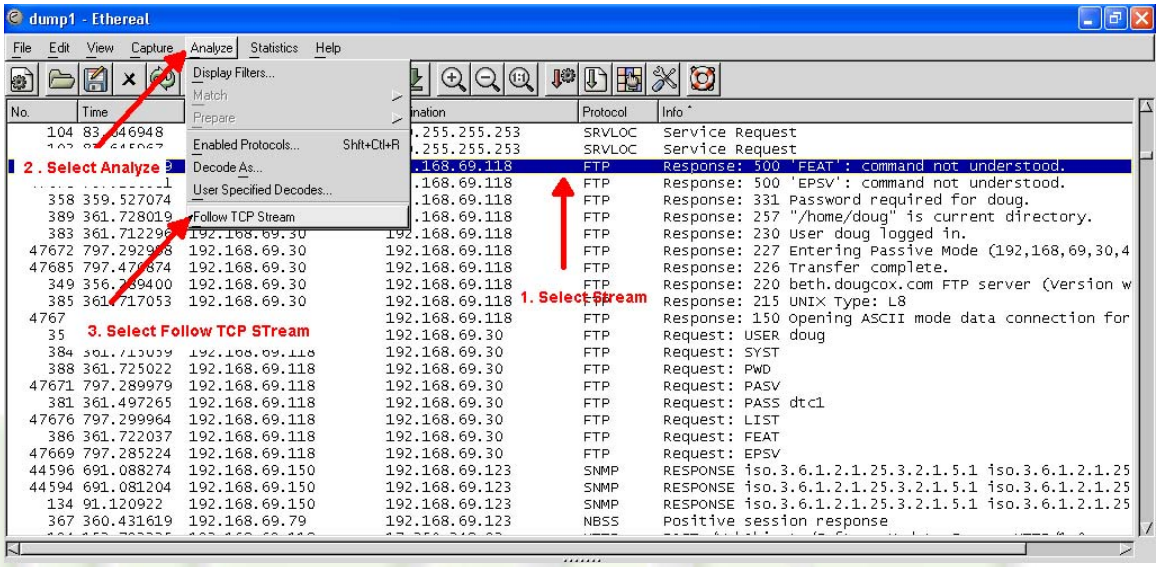
If the capture screen does not appear, Use *File -> Open* and load capture file.

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

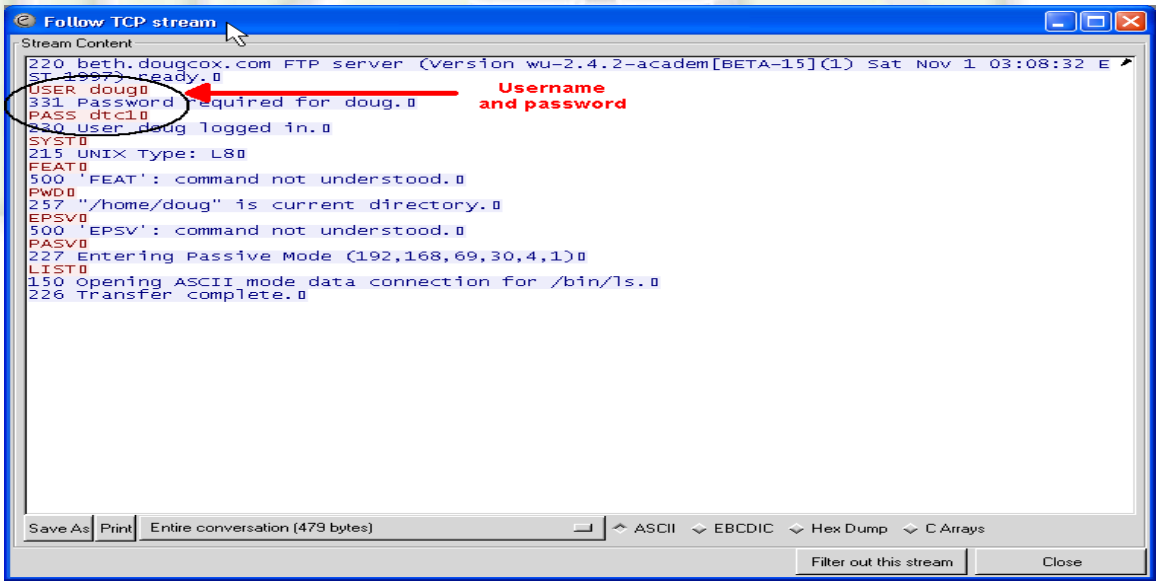


Step 7: Analyze Stream

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



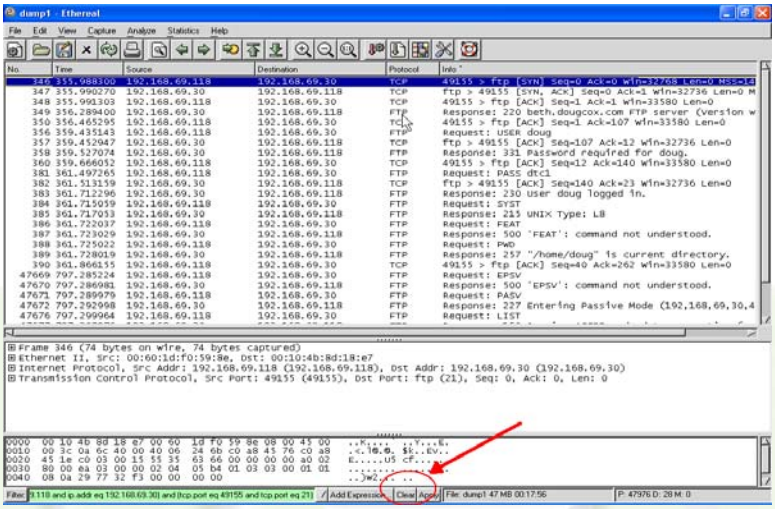
The program will process the stream and display the contents:



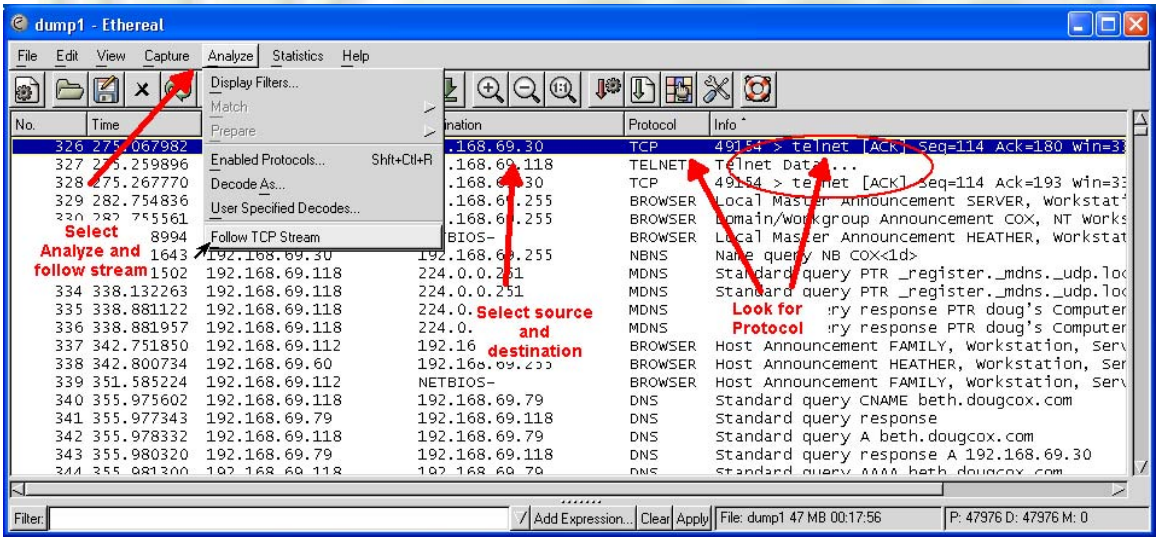
Step 8: Following a telnet steam

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.

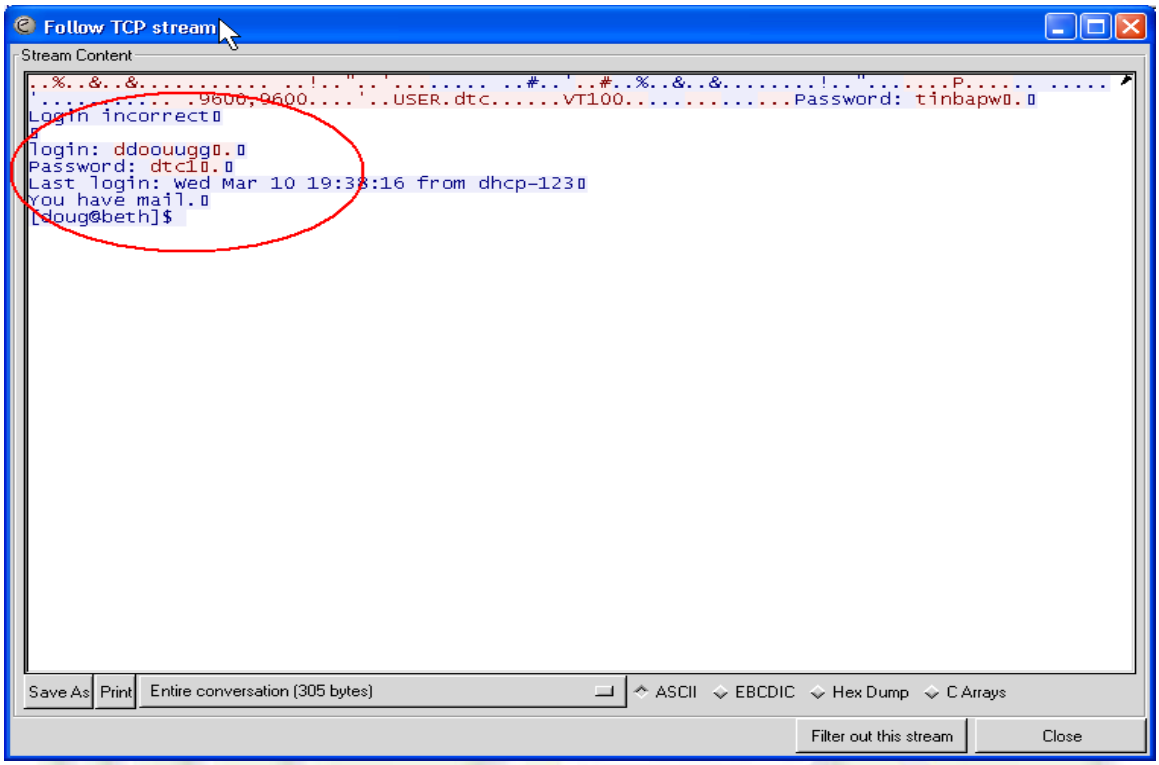
First clear the Filter by clicking the Clear Button at the bottom of the Ethereal window.



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).