

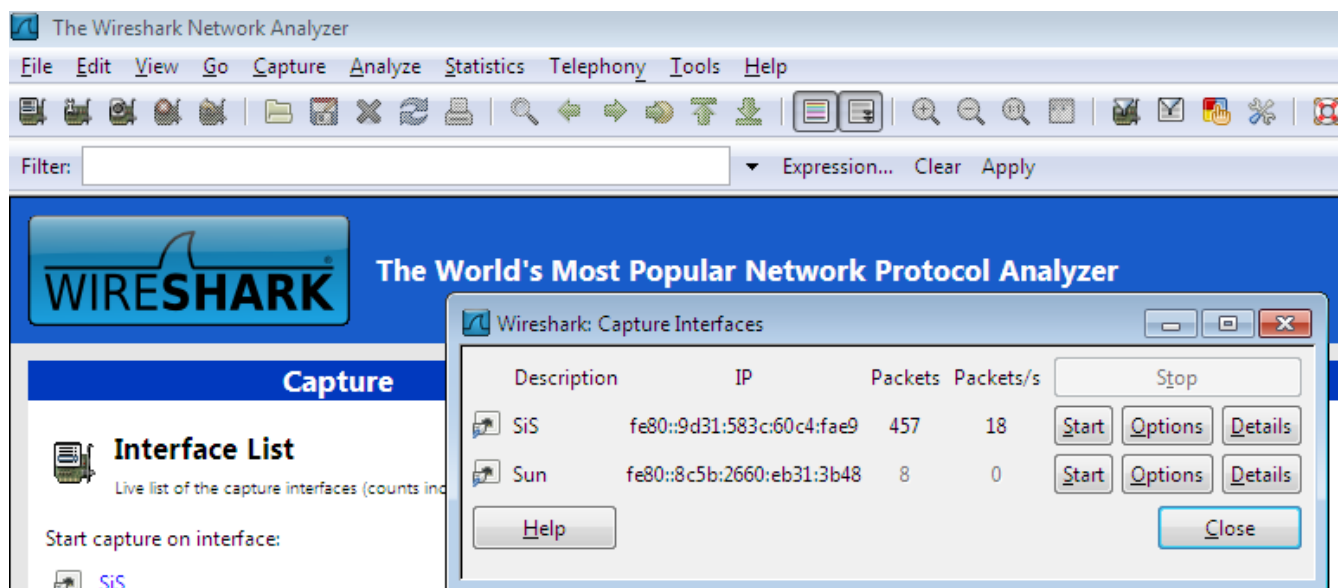


Hack Your Own Password Using Wireshark Lab

AP Computer Science Principles

In this lab you will use a web browser and with a protocol analyzer program called wireshark to learn how hackers can gain access to passwords and other sensitive information if it is not encrypted. This is sometimes called "replay."

1. Start wireshark by going to the start menu and choose *All programs / wireshark*.
2. Click on the interface list. You may see two interfaces. One may be labeled "sun" for the virtual machine. You'll be using other interface that has more traffic.



3. Open the Chrome web browser (other browsers may not work). We need to find a website that uses an unsecured login like <ftp://ftp.frognet.net/> <ftp://ftp.fuller.net/> <ftp://tigertech.net/> <ftp://ftp.got.net/> <ftp://ftp.iconnect.net/>
4. Don't log in yet though, first you need to start capturing the packets in wireshark.
5. Click *Start* for the interface in wireshark.
6. Since we are logging into an unsecured site, don't use the same password you use at secure sites. For this activity you don't actually have to login. Just try to login using a bogus email address and password.
7. After attempting to login, you can go back to wireshark and stop capturing packets. Choose *Capture / Stop*.
8. In the filter box, type **ftp** and hit enter.



The image shows a Wireshark packet capture window titled "*Local Area Connection [Wireshark 1.10.1 (SVN Rev 50926 from /trunk-1.10)]". The filter is set to "ftp". The packet list shows several FTP packets. The selected packet is number 632, which is a response from 198.57.170.33 to 10.66.14.159.

No.	Time	Source	Destination	Protocol	Length	Info
632	14.30369600	198.57.170.33	10.66.14.159	FTP	375	Response: 220----- welcome to Pure-FTPd [priv
633	14.30409700	10.66.14.159	198.57.170.33	FTP	75	Request: USER bozo@clown.com
635	14.32953000	198.57.170.33	10.66.14.159	FTP	101	Response: 331 User bozo@clown.com OK. Password rec
636	14.32977100	10.66.14.159	198.57.170.33	FTP	65	Request: PASS bozo
998	19.98661900	198.57.170.33	10.66.14.159	FTP	87	Response: 530 Login authentication failed
999	19.98688600	10.66.14.159	198.57.170.33	FTP	60	Request: QUIT
1005	20.01554200	198.57.170.33	10.66.14.159	FTP	121	Response: 221-Goodbye. You uploaded 0 and downloa

9. You should be able to find two packets whose *source* starts with **10.66** (the ip address of your computer) and whose *destination* is **198.57.170.33** (the ip address of frognet.net) that contain your **USER** name and **PASS** word. Show your instructor the username and password on before moving to part two.