CS 716: Introduction to communication networks

- 16th class; 28th Sept 2011

Instructor: Sridhar Iyer

Demo by: Swati Patil

IIT Bombay

What is IP address

An identifier for a computer or device on a TCP/IP network.

Networks using the TCP/IP protocol route messages based on the IP address of the destination.

The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255.

For example: 10.129.50.94 could be an IP address.

You can assign IP addresses at random as long as each one is unique.

The four numbers in an IP address are used in different ways to identify a particular network and a host on that network.

Classes of IP

There are five classes of available IP ranges:

Class A, Class B, Class C, Class D and Class E, while only A, B and C are commonly used.

Class A : Supports 16 million hosts on each of 127 networks.
1.0.0.1 to 126.255.255.254

Class B : Supports 65,000 hosts on each of 16,00 networks.
128.1.0.1 to 191.255.255.254

Class C : Supports 254 hosts on each of 2 million networks.
192.0.1.1 to 223.255.254.254

Class D : Reserved for multicast groups.
224.0.0.0 to 239.255.255.255

Class E : Reserved for future use, or Research and Development Purposes. 240.0.0.0 to 254.255.255.254

Network Configuration

GUI : Graphical User Interface

System----Preferences----Network Settings

i) DHCP : Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers configured for a given network.

ii) Manual

Netmask : The Netmask, together with the IP address, defines the network the computer belongs to, that is which other IP addresses the computer can touch directly in the same LAN.

Gateway: A node on a network that serves as an entrance to another network. In enterprises, the gateway is the computer that routes the traffic from a workstation to the outside network that is serving the Web pages.

Using Terminal

a) ifconfig

b) sudo vi /etc/network/interfaces

c) sudo /etc/init.d/networking restart

d) sudo /etc/hostname

e) sudo /etc/host

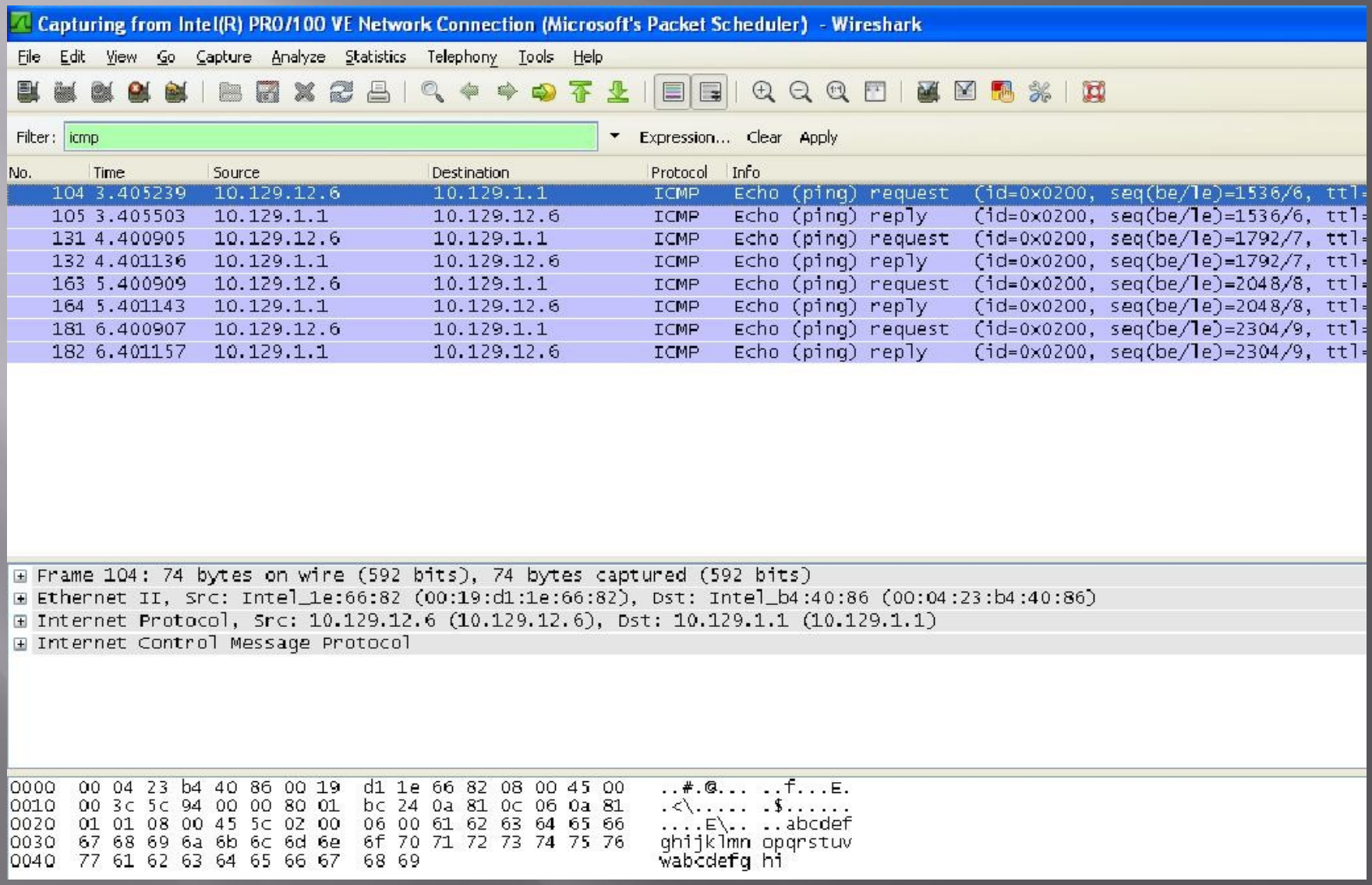
f) vi /etc/resolv.conf

PING : COMMAND

Ping is a basic Internet program that allows a user to verify that a particular IP address exists and can accept requests.

Ping works by sending an Internet Control Message Protocol (ICMP) Echo Request to a specified interface on the network and waiting for a reply.

PING PACKET SNIFFING USING WIRESHARK



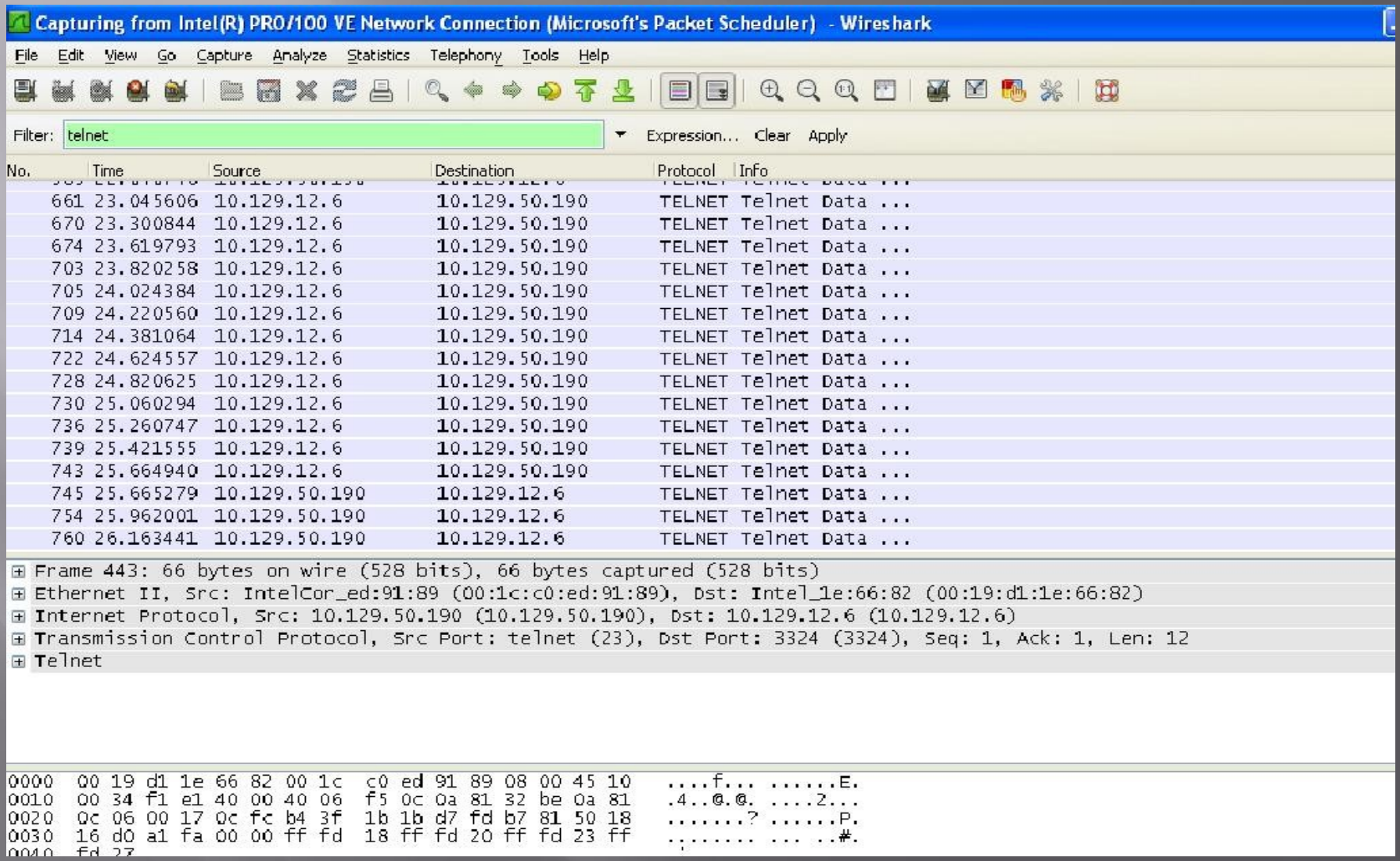
Telnet

Telnet is a protocol that allows you to connect to remote computers over a TCP/IP network.

Command for telnet telnet <host>

To create a connection with the remote host. The Telnet client will send a request to the Telnet server (remote host). The server will reply asking for a user name and password. If accepted, the Telnet client will establish a connection to the host and allows you to access the host's computer.

Telnet Packet Sniffing using Wireshark



How to send email using Telnet and sense SMPT with Wireshark

Start a Telnet session from a command line by entering:

Telnet your.mailserver.com 25

220 a.mail.server.com Microsoft ESMTP MAIL Service, Version: 6.0.3790.2499 ready at Thu, 29 Jun 2006 15:59:02 -0600

helo

250 a.mail.server.com Hello [192.168.125.237]

mail from: test@test.org

250 2.1.0 email@test.org... Sender OK

rcpt to: test@test.com

250 2.1.5 test@test.com

data

354 Start mail input; end with .

This is a test.

. (enter a dot/period to end the data)

250 2.6.0 Queued mail for delivery

quit

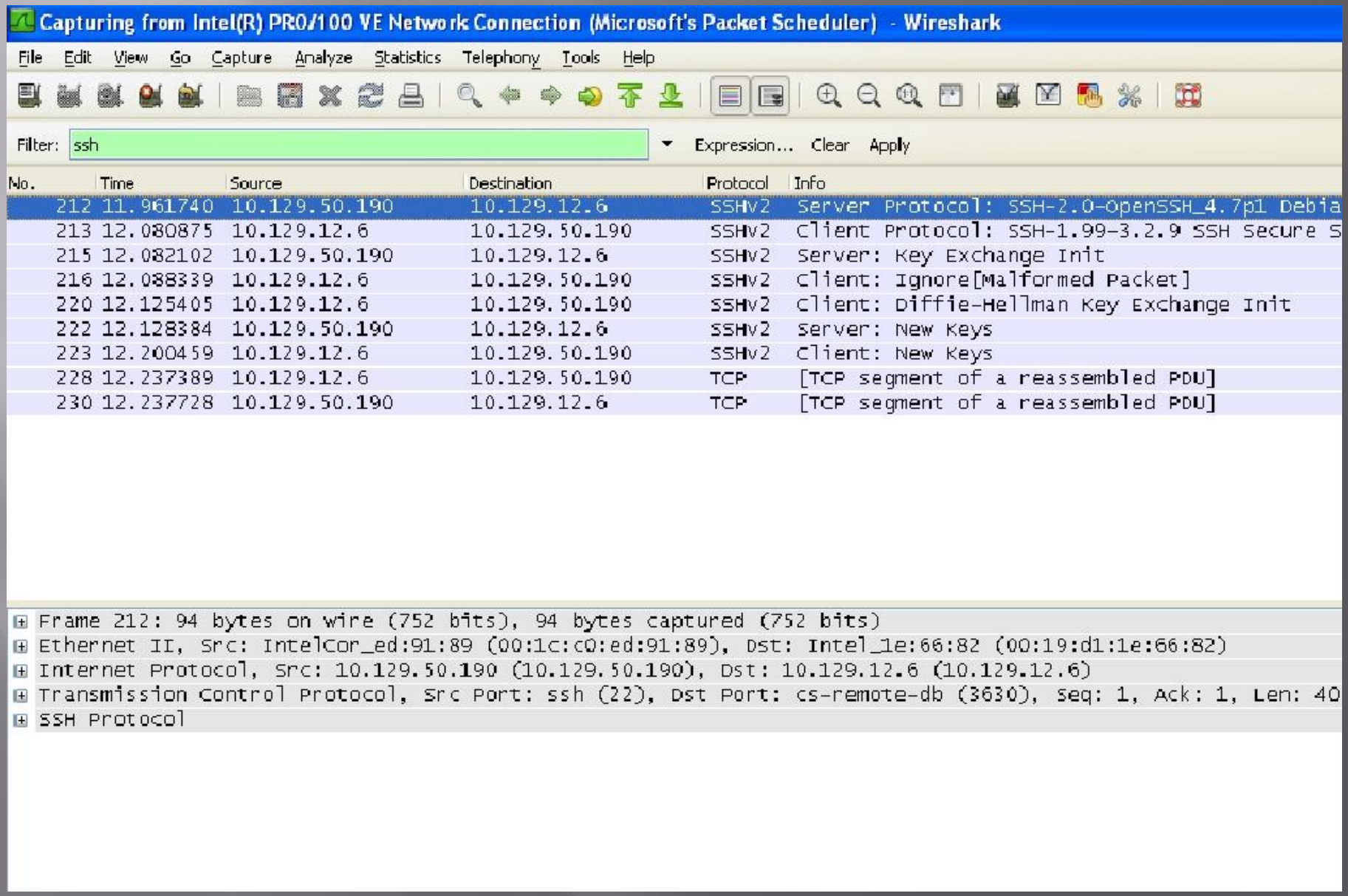
Connection to host lost.

Secure Shell

Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels.

When using ssh, the entire login session, including transmission of password , is encrypted, therefore it is almost impossible for an outsider to collect passwords.

SSH Packet Sniffing using Wireshark



Telnet Vs SSH

TELNET, by default, does not encrypt any data sent over the connection including password, and so it is often practical to eavesdrop on the communications and use the password later for malicious purposes.

SSH by default encrypts password and traffic. SSH is recommended for all use.

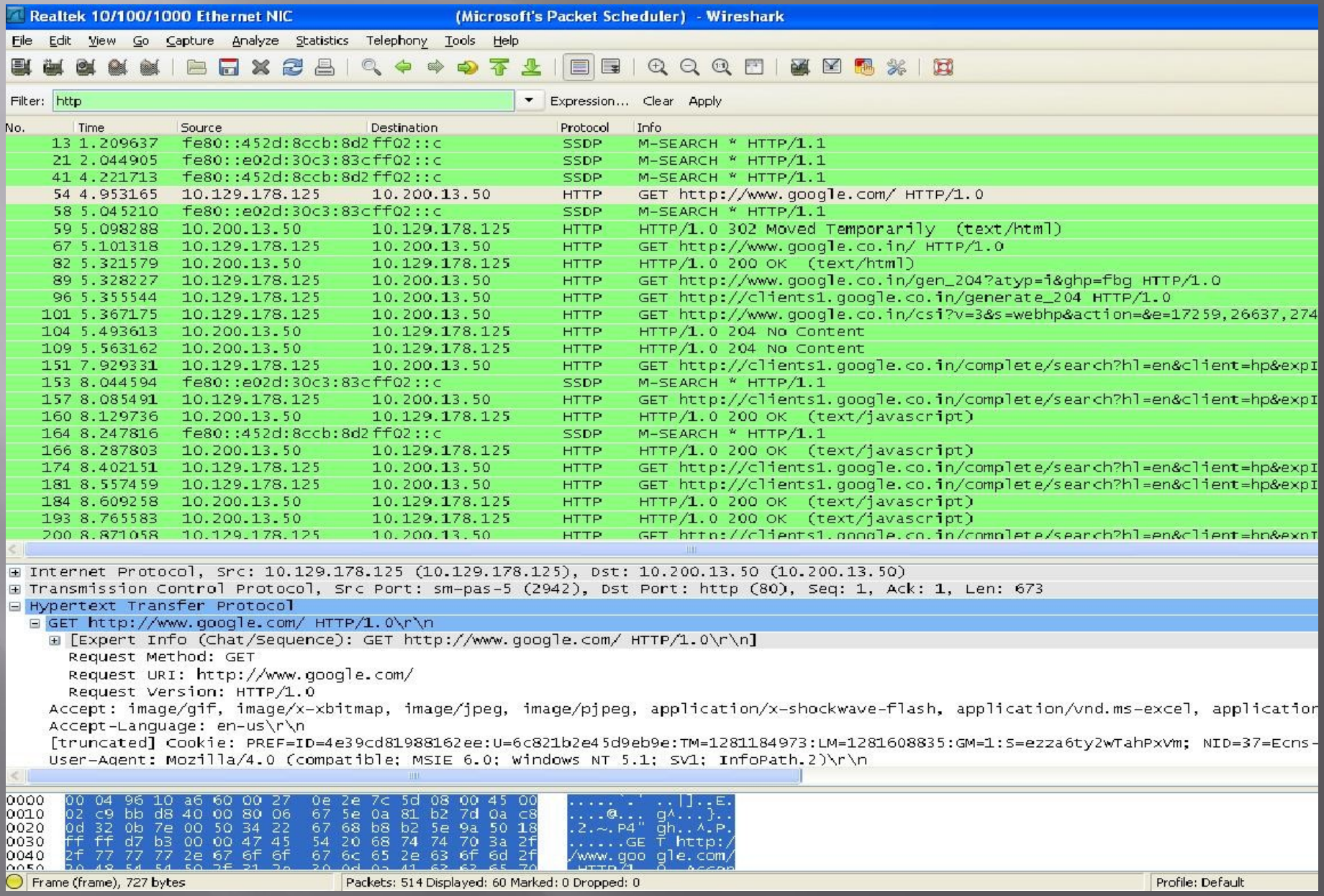
HTTP

HTTP - the Hypertext Transfer Protocol - provides a standard for Web browsers and servers to communicate.

HTTP is an application layer network protocol built on top of TCP. HTTP clients (such as Web browsers) and servers communicate via HTTP request and response messages.

HTTP utilizes TCP port 80 by default

HTTP Packet Sniffing using Wireshark



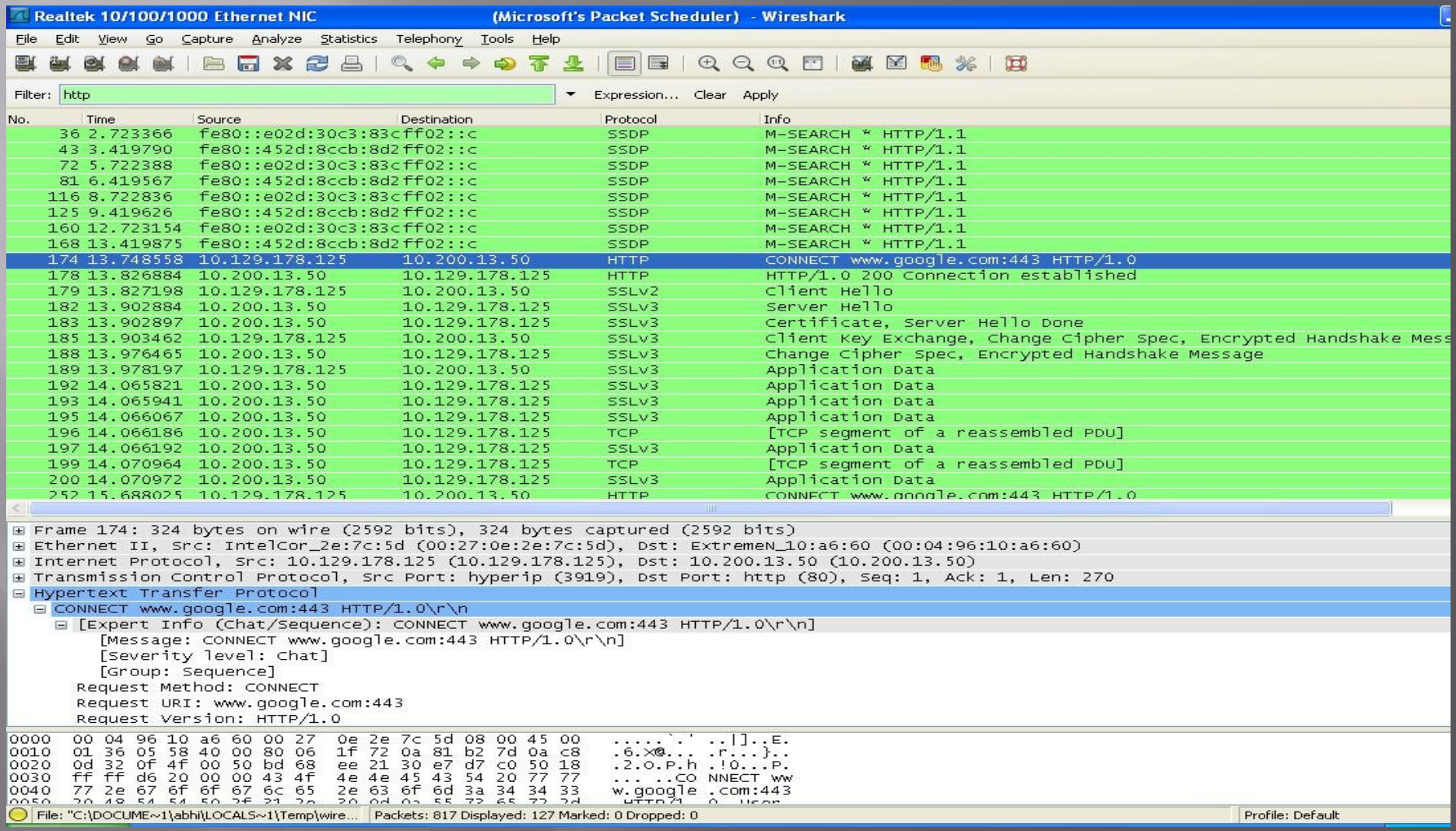
HTTPS

HTTPS stands for Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL.

HTTPS encrypts and decrypts the page requests and page information between the client browser and the web server using a Secure Socket Layer (SSL).

HTTPS by default uses port 443

HTTPS Packet Sniffing using Wireshark



HTTP Vs HTTPS

HTTP doesn't encrypt data at all with all its communication pretty much readable, with no decoding, translation or decryption required, Completely insecure

HTTPS is a secure connection, which means the data between the client and Web server is encrypted.

HTTPS uses public key encryption to secure data