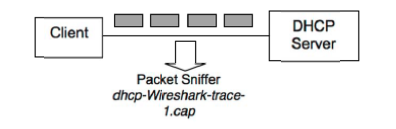
CSIT127

Lab 5 – Wireshark

One of the best ways to learn about computer networking protocols is to observe them working in the ‘wild’. In this lab, we will use a powerful packet sniffer call Wireshark. You will be given trace files containing packets captured on a test network. Then, using this trace file, you will observe how a number of applications behave. These are: dynamic host configuration protocol (DHCP), ARP, HTTP and DNS.

Use Windows: Start Wireshark. Spend some time reading eth-intro2.pdf. This will give you an overview of Wireshark.



DHCP

Included in the zip file you downloaded from Moodle is a file called dhcp-ethereal-trace-1.cap.

The file contains DHCP messages sent by clients to a DHCP server and also messages sent by a DHCP server. Load the trace file into Wireshark by going to “File->Open”

In the “Filter” field, type “bootp” and hit enter. You should now see only DHCP related packets. In the other words, the Protocol column only lists DHCP packets.

What are the 4 DHCP messages that you can see?

4 DHCP messages that I can see are DHCP Discover, DHCP Offer, DHCP Request and DHCP ACK.

Click on the first DHCP Discover message.

1. Notice that the source and destination address is 0.0.0.0 and 255.255.255.255 respectively. What is the reason for these addresses?

The device uses the addresses **0.0.0.0** and **255.255.255.255** in the source and destination address fields, respectively. The **0.0.0.0** and **255.255.255.255** are two special addresses. Any device, whether it has a valid IP configuration or not, can use these addresses to send local broadcast messages. From these addresses, the **0.0.0.0** is used as the source address. If a device does not have the source address, it can use this address to send broadcast messages. **255.255.255.255** is the local broadcast address. Any message sent to this address is received by all hosts of the local network.

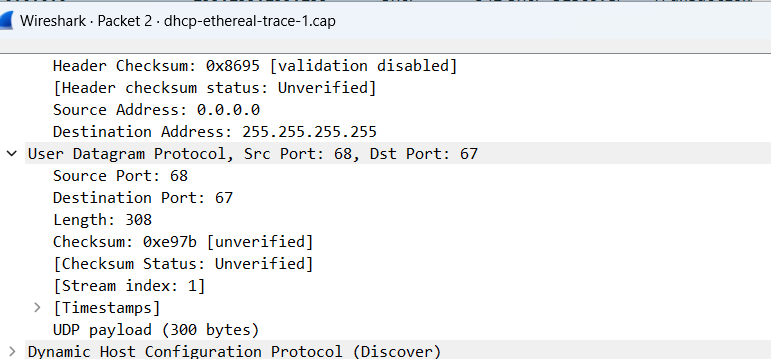
b. Is the DHCP Discovery message sent over UDP or TCP?

The DHCP Discovery message sent over UDP.

1. What is the source and destination port number?

The source port number is 68, destination port number is 67.

Prove:



d. In the middle window, click “Bootstrap Protocol”. What is the client’s MAC address? What is the name of the client? What IP address is the client requesting? In the “Parameter Request List”, identify other parameters that the client is requesting from the server.

The client’s MAC address is Dell\_4f:36:23 (00:08:74:4f:36:23)

The name of the client is

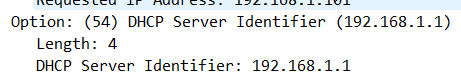
IP address the client is requesting is 0.0.0.0

The other parameters that the client request are Subnet Mask, Domian Name, Router, Domain Name Server, NetBIOS over TCP/IP Name Server, NetBIOS over TCP/IP Node Type, NetBIOS over TCP/IP Scope, Perform Router Discover, Static Route, Private/Classless Static Route (Microsoft), and Vendor-specific Information

4. What is the IP address of the DHCP server?

The IP address of the DHCP server is 192.168.1.1

Prove:



5. Click on the “DHCP Offer” message.

a. Identify the following network parameters: (i) subnet mask, (ii) router, (iii) domain name server addresses, (iv) IP address lease time, and (v) the IP address offered to the client.

1. Subnet mask:255.255.255.0
2. Router:192.168.1.1
3. Domain Name Server Address: 63.240.76.19 and 204.127.198.19
4. IP address lease time: (86400s) 1 day
5. IP address : 192.168.1.101

6. What is the purpose of the lease time in DHCP offer messages?

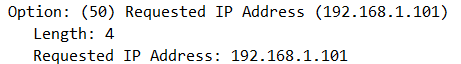
When DHCP sends configuration information to a client, the information is sent with a lease time. This is the length of time that the client can use the IP address it has been assigned.

During the lease time, the DHCP server cannot assign that IP address to any other clients. The purpose of a lease is to limit the length of time that a client can use an IP address. A lease prevents unused clients from taking up IP addresses when there are more clients than addresses. It also enables the administrator to make configuration changes to all of the clients on the network in a limited amount of time. When the lease expires, the client will request a new lease from DHCP. If the configuration data has changed, the new data will be sent to the client at that time.

7. Click on the first “DHCP Request” message. Which IP address did the client request?

IP address did the client request is 192.168.1.101

Prove:



**ARP**

Clear the “Filter” field then type arp

1. Why does a host need to use ARP?

ARP is necessary because the software address (IP address) of the host or computer connected to the network needs to be translated to a hardware address (MAC address). Without ARP, a host would not be able to figure out the hardware address of another host. The LAN keeps a table or directory that maps IP addresses to MAC addresses of the different devices, including both endpoints and routers on that network.

This table or directory is not maintained by users or even by IT administrators. Instead, the ARP protocol creates entries on the fly. If a user's device does not know the hardware address of the destination host, the device will send a message to every host on the network asking for this address. When the proper destination host learns of the request, it will reply back with its hardware address, which will then be stored in the ARP directory or table.

If ARP is not supported, manual entries can be made to this directory.

2. Identify the MAC address corresponding to the IP address 192.168.1.101.

The Internet owes much of its success to the World Wide Web. In this lab, you will observe two protocols that are crucial to the Web; Hypertext Transfer Protocol (HTTP) and Domain Name System (DNS). Using Google or your textbook, describe briefly how the aforementioned protocols work.

**HTTP**

Step 1: Load the file “http-Wireshark-trace-1.cap” (included in the zip file) into Wireshark.

Step 2: At this step, you should have the trace file loaded. If you’re unsure, ask the lab demonstrator. You are now ready to answer the following questions.

Type http into the filter field

1. Identify the client and server’s IP address.

2. Did the client connect using TCP or UDP?

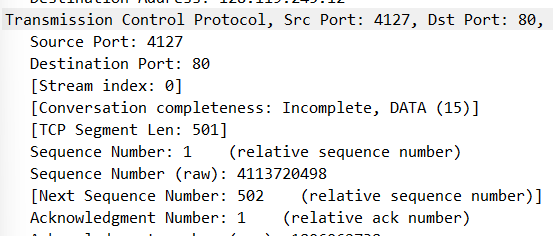
The client connected using TCP.

1. What is the source and destination port?

The source port is 4127.

The destination port is 80.

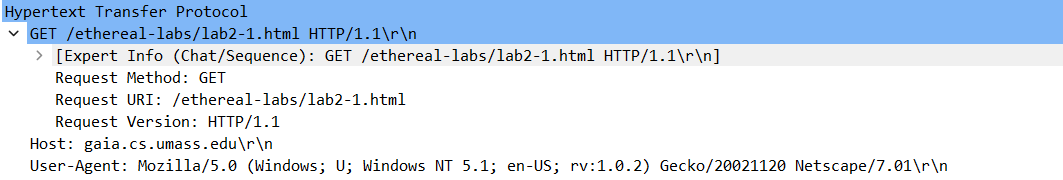
Prove:



4. Click on the first GET message. Then in the middle window, expand the label “Hypertext Transfer Protocol”.

a. Name the HTML file which the client is trying to get?

The client is trying to get /ethereal-labs/lab2-1.html



1. What version of HTTP is the client running?

The version of HTTP is the client running is HTTP/1.1

1. Which web browser is the client using?

The client is using Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape /7.01\r\n

1. Determine the purpose of the following fields: (i) Host, (ii) Accept, (iii) Keep-Alive, and (iv) Connection.

(i) Host:

Purpose: The "Host" field specifies the domain name or IP address of the target server to which the HTTP request is being sent. It's used when a single web server hosts multiple websites on the same IP address. The "Host" field helps the server route the request to the correct website.

(ii) Accept:

Purpose: The "Accept" field specifies the types of media or data formats that the client (usually a web browser) can handle or prefers. It informs the server about the types of responses (e.g., HTML, JSON, XML) that the client can accept.

(iii) Keep-Alive:

Purpose: The "Keep-Alive" field, often referred to as the "Connection: keep-alive" header, is used to maintain a persistent connection between the client and the server. This allows multiple HTTP requests and responses to be sent over the same connection, reducing the overhead of establishing a new connection for each request, thus improving performance.

(iv) Connection:

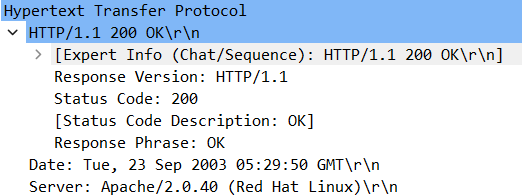
Purpose: The "Connection" field is used to control the behaviour of the connection between the client and server. It can specify whether the connection should be kept alive for future requests or closed after a single request-response cycle. Common values include "keep-alive" (to maintain the connection) and "close" (to close the connection after a single request).

6. Now click on the second message. In the middle window, identify the following:

a. What is the version of the web server?

The version of the web server is Apache/2.0.40 (Ret Hat Linux)\r\n

Prove:



b. Is the server running on a Linux or Windows machine?

The server is running on a Linux machine.

**DNS**

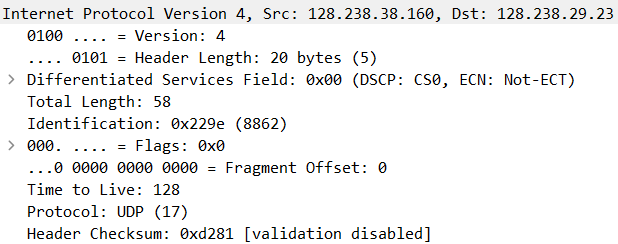
Load dns-Wireshark-trace-1.cap into Wireshark

Type dns in the Filter field

1. Identify the source and destination IP address.

Source IP address is 128.238.38.160

Destination IP address is 128.238.29.23



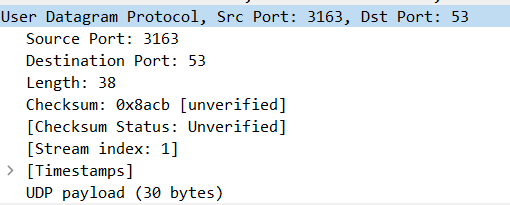
1. Are DNS messages sent over UDP or TCP?

DNS messages are sent over UDP.

1. What is the source and destination port number?

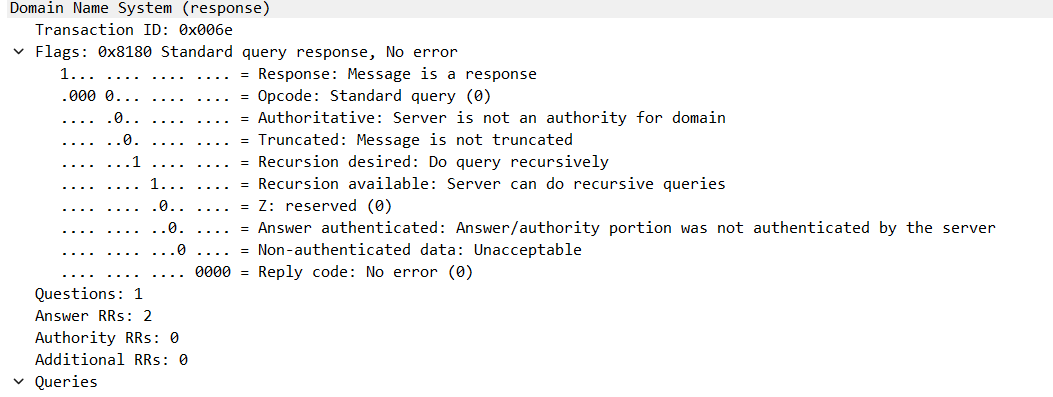
Source port number is 3163.

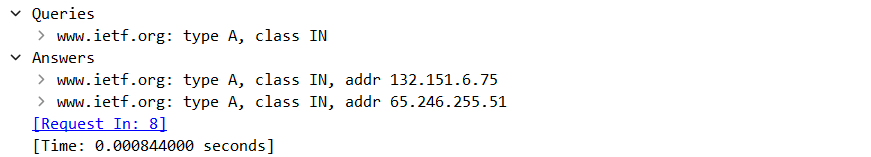
Destination port number is 53.



4. In the middle window, click on “Domain Name System”.

a. What is the client trying to resolve?

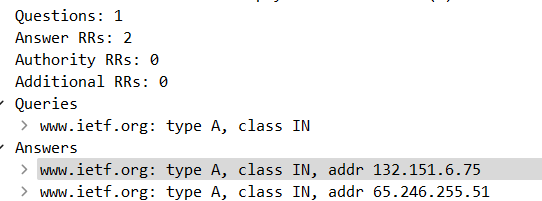




5. Now, click on the second packet.

a. How many answers did the server give the client? What are they?

The server give the client 2 answers. They are [www.ietf.org](http://www.ietf.org): type A, class IN, addr 132.151.6.75 and [www.ietf.org](http://www.ietf.org): type A, class IN, addr 65.246.255.51.



1. How long is the client allowed to keep the answer?

The client is allowed to keep the answer for 1678 (27 minutes, 58 seconds)

Prove:

