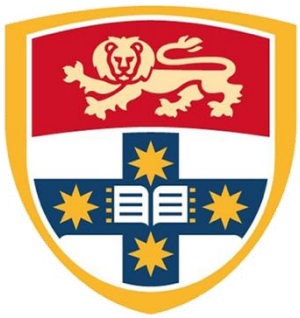
University of Sydney

ELEC3506 Data Communications and Internet – Lab Report 1

Student: Mengzhen Chen
SID:480462613



THE UNIVERSITY OF SYDNEY

Table of Contents

1 Introduction

This report is aimed to demonstrating the basic operations of Wireshark. It then took a closer look upon ethernet frames and hopefully reveal how HTTP and ARP protocol works.

2 Phase I: Wireshark

Step1: 1.TCP
2. HTTP
3. ARP

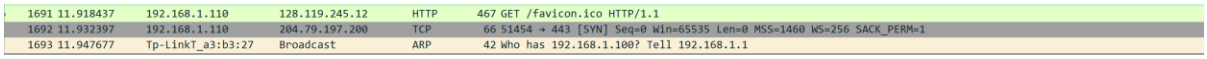


Figure 1. protocols examples

Step2:

$$09:35:37.624921 - 09:35:37.343532 \approx 0.2814 \text{ seconds}$$

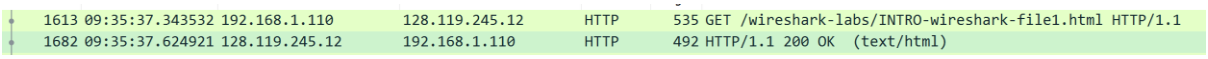


Figure 2. GET-OK pair

Step3:

IP address for gaia.cs.umass.edu is 128.119.245.12
IP address for my laptop is192.168.1.110

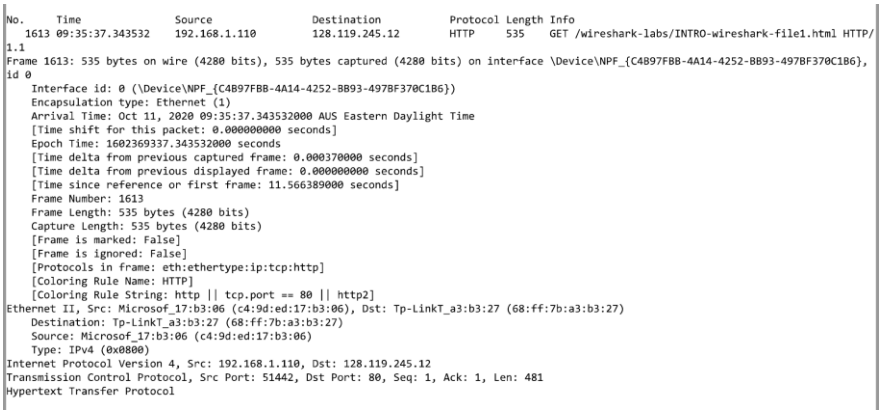


Figure 3. Message for GET

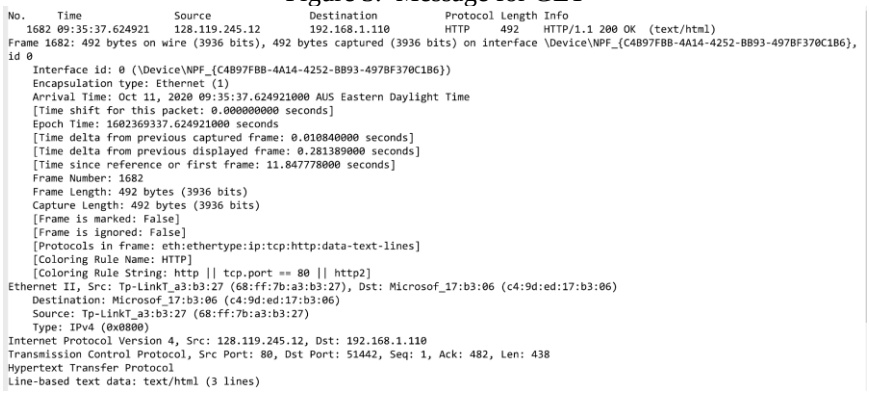


Figure 4. Message for OK

3 Phase II: Ethernet and Address Resolution Protocol

3.1 Capture and analyzing Ethernet frames

Step 4:

HTTP GET message:

I. The MAC address of my laptop is c4:9d:ed:17:b3:06

II. The MAC address of destination is 68:ff:7b:a3:b3:27. It is the MAC address of my router which is connected to my laptop.

III. That "0x0800" is corresponding to the Internet Protocol.

IV. The "G" from GET starts from the 54th (in decimal) byte.

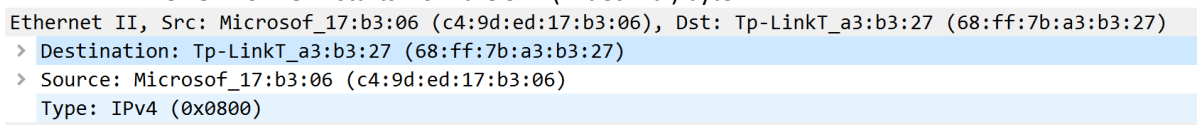


Figure 5. Ethernet II information

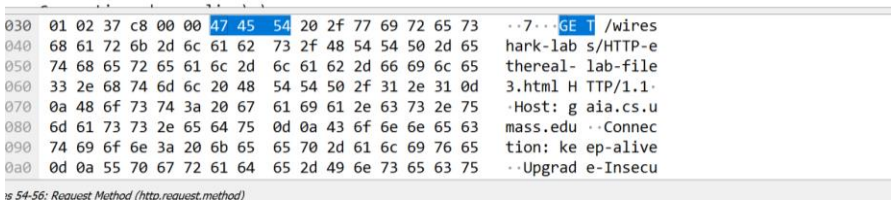


Figure 6.

HTTP response message:

I. The MAC address of source is 68:ff:7b:a3:b3:27. It is the MAC address of my router which is connected to my laptop.

II. The destination address is c4:9d:ed:17:b3:06. It is the MAC address of my laptop.

III. That "0x0800" is corresponding to the Internet Protocol.

IV. The "O" from the 13th (in decimal) byte.

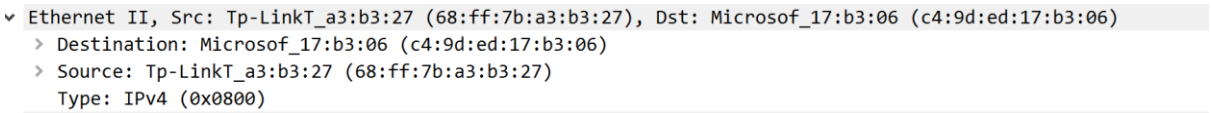


Figure 7. Packet information

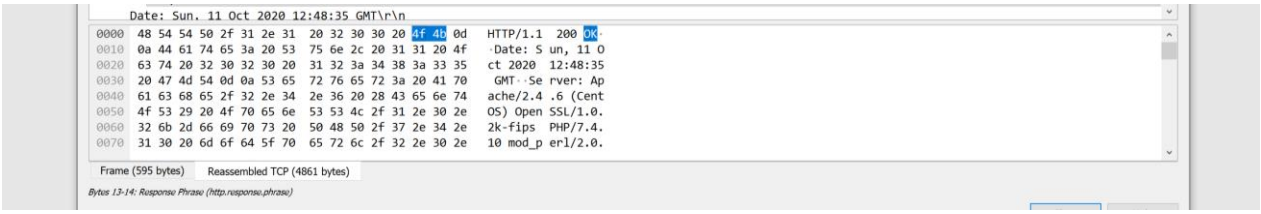


Figure 8.

3.2 Address Resolution Protocol

Step 9: We have IP address, Physical address and type columns in ARP Caching table. Physical address is the MAC address. The Type stands for the protocol type which is indicated about the mapping methods.

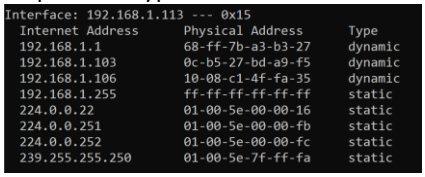


Figure 9. Result for arp -a

Step 10: Source address is c4:9d:ed:17:b3:06. it is the MAC address of my laptop
Destination address is ff:ff:ff:ff:ff:ff, namely, the broadcasting address

Step 11: 0x0806. It is corresponding to Address Resolution Protocol.

Step 12:

a) The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.

b) 0x00 01 for request.

c) Yes, it does contain the ip address of sender.

d) The target MAC address, namely, the 00:00:00:00:00:00 part. It is set to broadcasting MAC

address to question the machine whose corresponding IP address (in this case, 192.168.1.106) is being queried.

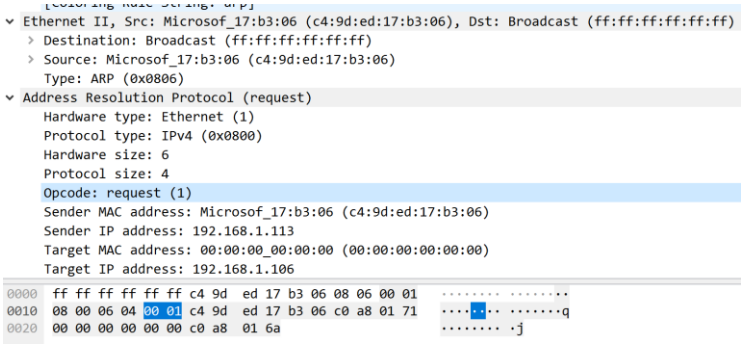


Figure 10. ARP request

Step 13:

a) The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.

b) 0x 00 02 for reply.

c) The sender Mac address (10:08:c1:4f:fa:35). It indicates the MAC address for IP: 192.168.1.10

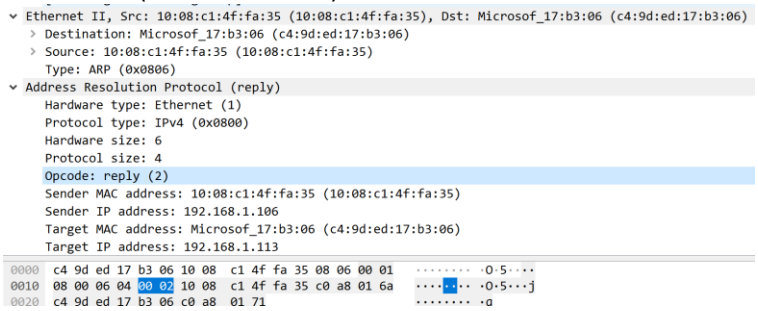


Figure 11. ARP reply

Step 14: Destination MAC address: c4:9d:ed:17:b3:06, namely, the MAC address of my laptop.
Source MAC address: 10:08:c1:4f:fa:35.

Step 15:

Although ARP request is broadcast massage, but the ARP reply is not. The ARP reply only send from the sender node to the destination node, s.t. there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace.