Analyzing Web Traffic with Wireshark

# Addressing Table

|  |  |  |  |
| --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask |
| Web server |  | 10.10.10.2 | 255.255.255.0 |
| PC1 | Wlan interface | DHCP/ 192.168.0.127 | DHCP/ 255.255.255.0 |

# Objectives

Part 1: Install Wireshark on a PC/MAC

Part 2: Analyze web traffic

# Background / Scenario

Install Wireshark to a PC/Mac and use it to analyze TCP and HTTP traffic.

# Instructions

Install Wireshark from Wireshark.org/download and use it analyze traffic to a web server. Before staring the capture look at your PC’s IP-address from command prompt by issuing from the command ipconfig /all and fill it in the table above (For non-windows PC’s google for the correct command).

## Install Wireshark on PC/MAC

Go to the <https://www.wireshark.org/download.html> and download the newest stable version of Wireshark to your computer. If you are using a Linux computer, you can download Wireshark directly using Linux distributions packet management system. In widows machine You can install it by using default settings.

## Open a web browser and capture traffic to <http://kmd658ope.asuscomm.com/>

we are going to use normal http traffic not secure https traffic in this lab. Capture traffic with Wireshark when you are making a connection to <http://kmd658ope.asuscomm.com/>. Look at the DNS query for md658ope.asuscomm.com. Enter a display filter in Wireshark to show only DNS traffic. Google to find the correct syntax for Display filter.

* + - * 1. What is the display filter to display only DNS traffic?
* dns
  + - * 1. Look at the DNS-query and what is the destination port and protocol (TCP/UDP)
* Destination port: 53; Protocol: UDP
  + - * 1. What is the source port for this DNS query?
* Source port: 53009
  + - * 1. What is the IPv4 -address for kmd658ope.asuscomm.com?
* 194.110.231.215
  + - * 1. Do You get an answer for IPv6 address (AAAA record in DNS) for kmd658ope.asuscomm.com
* No

Enter a different display filter to only show traffic that has either source or destination address of the kmd658ope.asuscomm.com. (hint ip.addrr=xxx.xxx.xxx.xxx)

* + - * 1. What is source and destination port for the first TCP connection to kmd658ope.asuscomm.com?

SRC Port: 50065 DST Port: 80

* + - * 1. How many milliseconds did the 3-way handshake take (SYN, SYN+ACK and ACK) \_\_\_\_\_\_\_\_\_ms

(You can see the timestamps in the second column in Wireshark)

* 5.506ms
  + - * 1. Look at HTTP GET / packet in Wireshark; What all kind of information does the Browser provide for the Web server? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
        2. What is the hostname submitted to the server in the HTTP Get message? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
        3. Look at HTTP/1.1 200 OK message in Wireshark and answer following questions:

What does the result code 200 mean?

* + It means that the request has succeeded

What information does the resulting webpage have? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the TCP source port of this HTTP/1.1 200 OK message?

* + Source port: 80

What is the TCP destination port of this HTTP/1.1 200 OK message?

* + Destination port: 50093
    - * 1. Save captured traffic with the name YourFirstaname.LAstname\_Wireshark capture and submit it with this filled word document as an answer for this assignment.