Analyzing Web Traffic with Wireshark

# Addressing Table

|  |  |  |  |
| --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask |
| Web server |  | 194.110.231.215 | 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: 50093 DST Port: 80

* + - * 1. How many milliseconds did the 3-way handshake take (SYN, SYN+ACK and ACK)
* 5ms
  + - * 1. Look at HTTP GET / packet in Wireshark; What all kind of information does the Browser provide for the Web server?

Hypertext Transfer Protocol

GET / HTTP/1.1\r\n

[Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]

Request Method: GET

Request URI: /

Request Version: HTTP/1.1

Host: kmd658ope.asuscomm.com\r\n

Connection: keep-alive\r\n

Cache-Control: max-age=0\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n

Accept-Encoding: gzip, deflate\r\n

Accept-Language: en-US,en;q=0.9,vi;q=0.8,fi;q=0.7\r\n

If-None-Match: "6e-5f2114ca3461e-gzip"\r\n

If-Modified-Since: Thu, 12 Jan 2023 13:43:17 GMT\r\n

\r\n

[Full request URI: http://kmd658ope.asuscomm.com/]

[HTTP request 1/1]

[Response in frame: 17]

* + - * 1. What is the hostname submitted to the server in the HTTP Get message?

→ kmd658ope.asuscomm.com

* + - * 1. 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?

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

Date: Wed, 08 Feb 2023 11:40:07 GMT\r\n

Server: Apache/2.4.54 (Raspbian)\r\n

Last-Modified: Thu, 12 Jan 2023 13:43:17 GMT\r\n

ETag: "6e-5f2114ca3461e-gzip"\r\n

Accept-Ranges: bytes\r\n

Vary: Accept-Encoding\r\n

Content-Encoding: gzip\r\n

Content-Length: 98\r\n

Keep-Alive: timeout=5, max=100\r\n

Connection: Keep-Alive\r\n

Content-Type: text/html\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.012948000 seconds]

[Request in frame: 15]

[Request URI: http://kmd658ope.asuscomm.com/]

Content-encoded entity body (gzip): 98 bytes -> 110 bytes

File Data: 110 bytes

Line-based text data: text/html (10 lines)

<!DOCTYPE html>\r\n

<html>\r\n

<body>\r\n

\r\n

<h1>My First Heading</h1>\r\n

\r\n

<p>My 1st paragraph.</p>\r\n

\r\n

</body>\r\n

</html>\r\n

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.