LABORATORY REPORT

LABORATORY REPORT

COMMON DATA	
STUDENT NAME	KORMOUA KHONGMENG
NEPTUN CODE	I3MLPQ
DEPARTMENT	DEPT. OF AUTOMATION AND APPLIED INFORMATICS
INSTRUCTOR NAME	AL-Magsoosi Husam Kareem Farhan
LABORATORY PLACE	BME IL206
LABORATORY TIME	10:15 – 12:00
TITLE OR SEQUENCE NUMBER	5

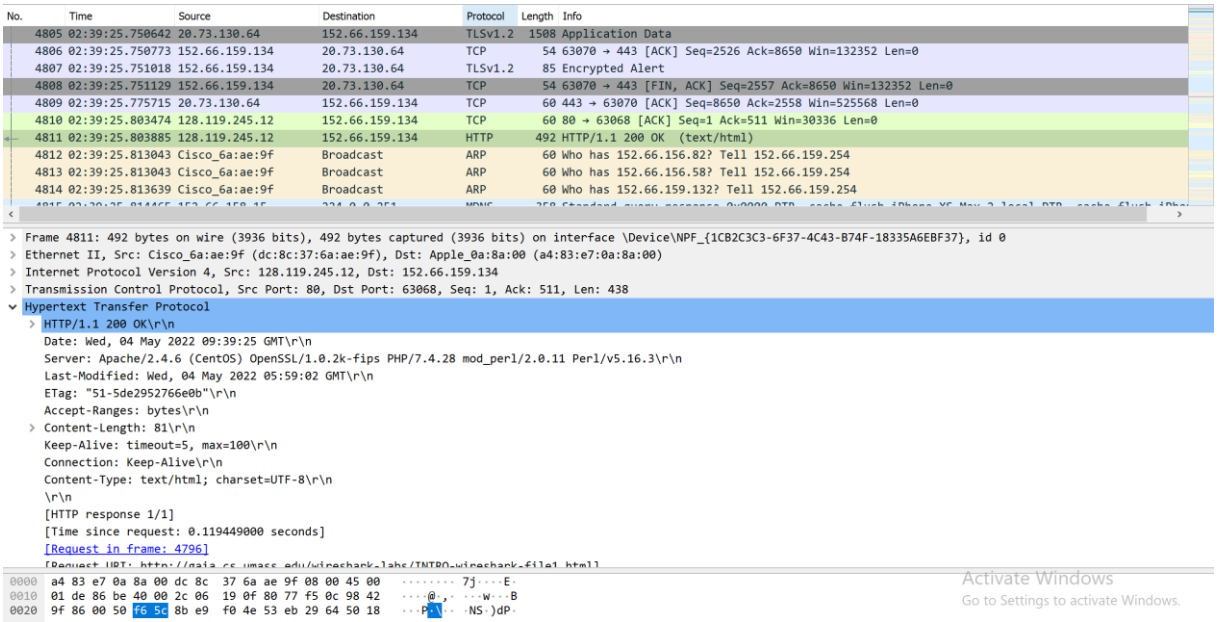
EXERCISES	
TASK 1	☒
TASK 2	☒
TASK 3	☒
TASK 4	☒
TASK 5	☒

EXERCISES

TASK #1

Problem statement: List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above. Explain them.

Solution:

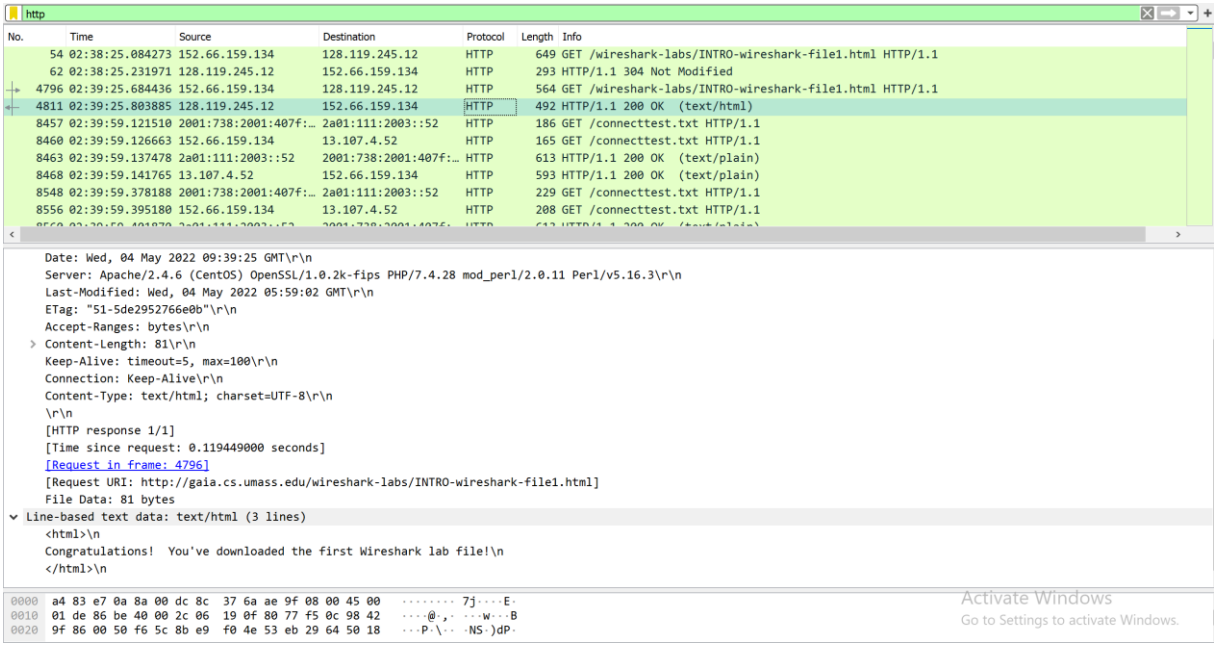


- **HTTP (Hypertext Transfer Protocol):** is an application-layer protocol for transmitting hypermedia documents, such as HTML. It was designed for communication between web browsers and web servers, but it can also be used for other purposes.
- **TCP (Transfer Control Protocol):** is a communications standard that enables application programs and computing devices to exchange messages over a network. It is designed to send packets across the internet and ensure the successful delivery of data and messages over networks.
- **ARP (Address Resolution Protocol):** broadcasts a request packet to all the machines on the LAN and asks if any of the machines are using that particular IP address. When a machine recognizes the IP address as its own, it sends a reply so ARP can update the cache for future reference and proceed with the communication. It is also referred as a procedure that connects an ever-changing Internet Protocol (IP) address to a fixed physical machine address, also known as a media access control (MAC) address, in a local-area network (LAN).

TASK #2

Problem statement: How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packetlisting window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)

Solution:



HTTP GET at: 02:39:25.684436

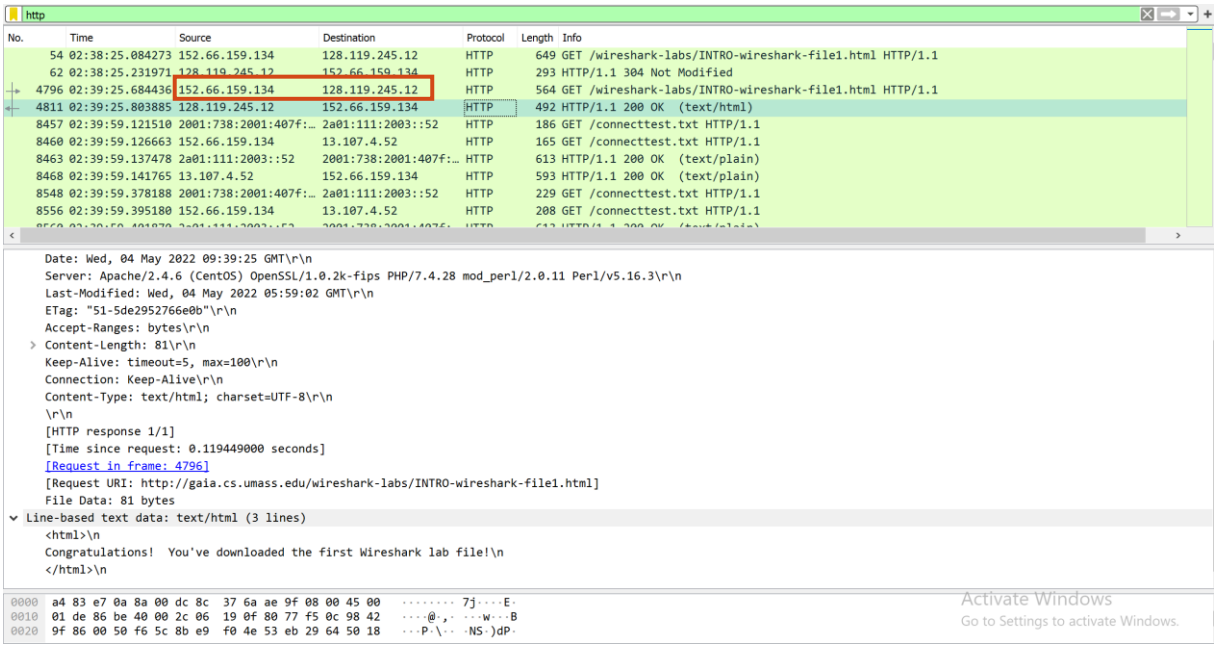
HTTP OK at: 02:39:25.803885

Time taken: 0.119449 s

TASK #3

Problem statement: what is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer?

Solution:



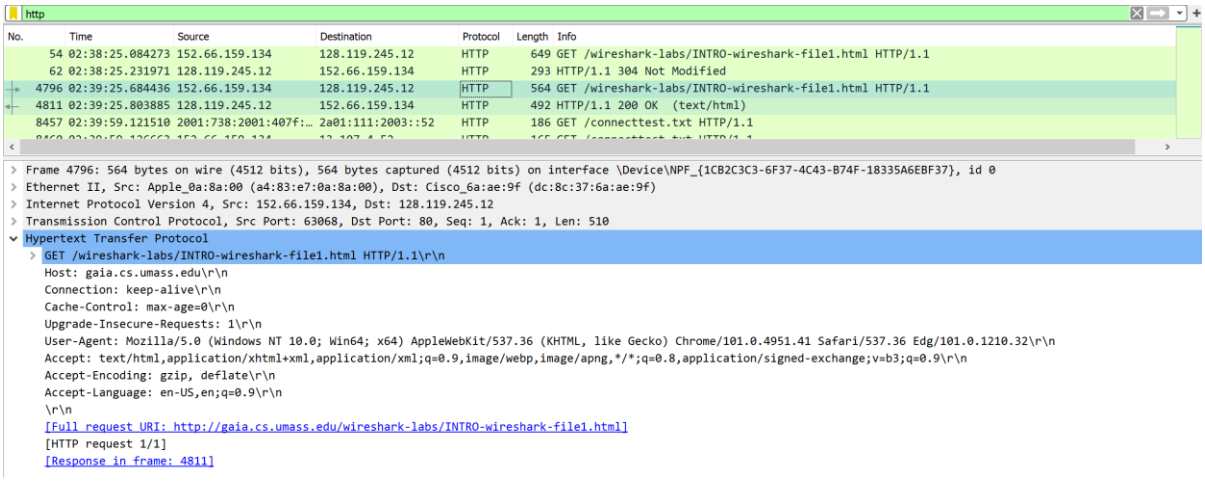
Internet address of my computer: 152.66.159.13

Internet address of gaia.cs.umass.edu (as www-net.cs.umass.edu): 128.119.245.12

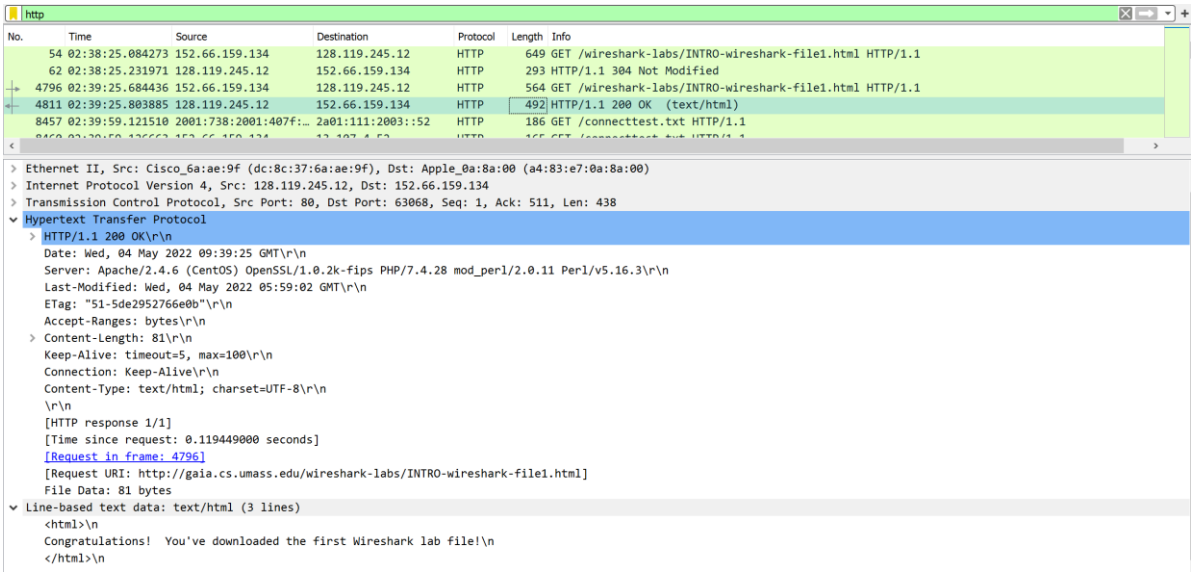
TASK #4

Problem statement: In Wireshark you can print selected messages. To do so, select Print from the Wireshark File command menu. However, sending packets to a printer is not available in the Laboratory room, therefore just make a screenshot of the two HTTP messages (GET and OK) referred to the Question 2 above, and copy them to your Report. Check the value and explain the role of at least 6 header fields in these messages.

Solution:



HTTP GET message



HTTP OK message

Reasoning:

- GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n:
  Is the a request message that ask for a given webpage.
- Host: gaia.cs.umass.edu\r\n:
  Is the destination server
- Connection: keep-alive\r\n:
  Indicates that this http connection will keep the TCP connection connected until the client tells the server to terminate the connection.
- Accept-Language: en-US, en;q=0.9\r\n
  Specify the language that is supported or understand by the client.
- Accept-Encoding: gzip, deflate\r\n
  Indicates the content encoding (usually a compression algorithm) that the client can understand
- Cache-Control: max-age=0\r\n
  This contain the instructions (in both requests and response) that control caching in browsers and shared caches. The header Cache-Control: max-age=0 implies that the content is considered stale (and must be re-fetched) immediately.

TASK #5

Problem statement: Choose a webserver in your home country (or any other country outside Hungary). Determine the website's IP address, and display the route from you PC to that website. Determine the geographical location (country) of the routers in the route (you can use Whois Internet services, e.g. http://whois.domaintools.com/) and record the route history.

Solution:

We will try to access www.kooora.com

We get can get the IP address by ping www.kooora.com and we know that the IP address is: `104.18.8.101`

Now we can use this IP address in http://whois.domaintools.com/ then we can determine the geographical location of each router inside the route. Below here, is the result of http://whois.domaintools.com/

IP Location	United States San Jose Cloudflare Inc.
ASN	AS13335 CLOUDFLARENET, US (registered Jul 14, 2010)
Whois Server	whois.arin.net
IP Address	104.18.8.101
Reverse IP	12 websites use this address.

```
NetRange:       104.16.0.0 - 104.31.255.255
CIDR:           104.16.0.0/12
NetName:        CLOUDFLARENET
NetHandle:      NET-104-16-0-0-1
Parent:         NET104 (NET-104-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS13335
Organization:   Cloudflare, Inc. (CLOUD14)
RegDate:        2014-03-28
Updated:        2021-05-26
Comment:        All Cloudflare abuse reporting can be done via
https://www.cloudflare.com/abuse
Ref:            https://rdap.arin.net/registry/ip/104.16.0.0

OrgName:        Cloudflare, Inc.
OrgId:          CLOUD14
Address:        101 Townsend Street
City:           San Francisco
StateProv:      CA
PostalCode:     94107
Country:        US
RegDate:        2010-07-09
Updated:        2021-07-01
Ref:            https://rdap.arin.net/registry/entity/CLOUD14

OrgTechHandle: ADMIN2521-ARIN
OrgTechName:   Admin
```

```
OrgTechPhone:  +1-650-319-8930
OrgTechEmail:   rir@cloudflare.com
OrgTechRef:    https://rdap.arin.net/registry/entity/ADMIN2521-ARIN

OrgAbuseHandle: ABUSE2916-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-650-319-8930
OrgAbuseEmail:   abuse@cloudflare.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE2916-ARIN

OrgRoutingHandle: CLOUD146-ARIN
OrgRoutingName:   Cloudflare-NOC
OrgRoutingPhone:  +1-650-319-8930
OrgRoutingEmail:   noc@cloudflare.com
OrgRoutingRef:    https://rdap.arin.net/registry/entity/CLOUD146-ARIN

OrgNOCHandle: CLOUD146-ARIN
OrgNOCName:   Cloudflare-NOC
OrgNOCPhone:  +1-650-319-8930
OrgNOCEmail:   noc@cloudflare.com
OrgNOCRef:    https://rdap.arin.net/registry/entity/CLOUD146-ARIN

RAbuseHandle: ABUSE2916-ARIN
RAbuseName:   Abuse
RAbusePhone:  +1-650-319-8930
RAbuseEmail:   abuse@cloudflare.com
RAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE2916-ARIN

RTechHandle: ADMIN2521-ARIN
RTechName:   Admin
RTechPhone:  +1-650-319-8930
RTechEmail:   rir@cloudflare.com
RTechRef:    https://rdap.arin.net/registry/entity/ADMIN2521-ARIN

RNOCHandle: NOC11962-ARIN
RNOCName:   NOC
RNOCPhone:  +1-650-319-8930
```

Here is another trace route where I use **tracert command** to check each geographical location that my package go through. I want to trace www.hal-logistics.la which is from Laos (south-east Asia).

```
$ tracert www.hal-logistics.la

Tracing route to www.hal-logistics.la [157.245.52.170]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  vl81.kiwi.net.bme.hu [152.66.147.254]
  2     2 ms     2 ms     2 ms  xge0-0-0-3.rax.net.bme.hu [152.66.0.90]
  3     2 ms     2 ms     2 ms  tg0-2-0-2.rtr.bme.hbone.hu [152.66.0.125]
  4     3 ms     2 ms     2 ms  hge0-1-0-2.core1.vh.hbone.hu [195.111.96.226]
  5    42 ms     2 ms     2 ms  hge0-4-0-3.rtr2.vh.hbone.hu [195.111.98.71]
  6    48 ms     2 ms     2 ms  te0-3-1-3.rcr51.b020664-1.bud01.atlas.cogentco.c
om [149.11.10.9]
  7     4 ms     3 ms     3 ms  be2246.ccr31.bud01.atlas.cogentco.com [130.117.1
.13]
  8     7 ms     5 ms     5 ms  be3261.ccr21.bts01.atlas.cogentco.com [130.117.3
.137]
  9     6 ms     6 ms     6 ms  be2988.ccr51.vie01.atlas.cogentco.com [154.54.59
.86]
 10    11 ms    11 ms    13 ms  be2974.ccr21.muc03.atlas.cogentco.com [154.54.58.5]
 11    17 ms    17 ms    17 ms  be2959.ccr41.fra03.atlas.cogentco.com [154.54.36.53]
 12    17 ms     *        *     tata.fra03.atlas.cogentco.com [130.117.15.114]
 13     *        *        *     Request timed out.
 14     *      261 ms     *     if-ae-55-2.tcore2.pvu-paris.as6453.net [80.231.245.6]
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *      258 ms     *     if-be-7-2.ecore1.emrs2-marseille.as6453.net [195.219.174.8]
 18     *        *        *     Request timed out.
 19     *      259 ms     *     if-ae-31-5.tcore1.svw-singapore.as6453.net [80.231.217.197]
 20     *        *      256 ms  if-be-45-2.ecore2.esin4-singapore.as6453.net [180.87.108.4]
 21     *        *      262 ms  if-be-10-2.ecore2.svq-singapore.as6453.net [180.87.107.0]
 22   259 ms   258 ms   262 ms  if-ae-46-2.thar1.svq-singapore.as6453.net [120.29.214.10]
 23   256 ms   259 ms   257 ms  120.29.214.142
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28   257 ms   256 ms   256 ms  157.245.52.170

Trace complete.
```

We can say roughly that the packages went from Budapest to Paris to Singapore and should arrive at Laos.

INSTRUCTIONS

1. **Problem statement is mandatory.**
2. **A solution without explanation is NOT accepted.**
3. **If you need to copy the source code, you can do it with copy/paste commands. Please do not use screenshots for code listings.**
4. **Other screenshots (figures, graphs, etc.) should be scaled appropriately. Please cut off unnecessary elements on the images.**