

# 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	<input checked="" type="checkbox"/>
TASK 2	<input checked="" type="checkbox"/>
TASK 3	<input checked="" type="checkbox"/>
TASK 4	<input checked="" type="checkbox"/>
TASK 5	<input checked="" type="checkbox"/>

## 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:**

No.	Time	Source	Destination	Protocol	Length	Info
4805	02:39:25.750642	20.73.130.64	152.66.159.134	TLSv1.2	1508	Application Data
4806	02:39:25.750773	152.66.159.134	20.73.130.64	TCP	54	63070 → 443 [ACK] Seq=2526 Ack=8650 Win=132352 Len=0
4807	02:39:25.751018	152.66.159.134	20.73.130.64	TLSv1.2	85	Encrypted Alert
4808	02:39:25.751129	152.66.159.134	20.73.130.64	TCP	54	63070 → 443 [FIN, ACK] Seq=2557 Ack=8650 Win=132352 Len=0
4809	02:39:25.775715	20.73.130.64	152.66.159.134	TCP	60	443 → 63070 [ACK] Seq=8650 Ack=2558 Win=525568 Len=0
4810	02:39:25.803474	128.119.245.12	152.66.159.134	TCP	60	80 → 63068 [ACK] Seq=1 Ack=511 Win=30336 Len=0
4811	02:39:25.803885	128.119.245.12	152.66.159.134	HTTP	492	HTTP/1.1 200 OK (text/html)
4812	02:39:25.813043	Cisco_6a:ae:9f	Broadcast	ARP	60	Who has 152.66.156.82? Tell 152.66.159.254
4813	02:39:25.813043	Cisco_6a:ae:9f	Broadcast	ARP	60	Who has 152.66.156.58? Tell 152.66.159.254
4814	02:39:25.813639	Cisco_6a:ae:9f	Broadcast	ARP	60	Who has 152.66.159.132? Tell 152.66.159.254

```

> Frame 4811: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{1CB2C3C3-6F37-4C43-B74F-18335A6EBF37}, id 0
> Ethernet II, Src: Cisco_6a:ae:9f (dc:8c:37:6a:ae:9f), Dst: Apple_0a:8a:00 (a4:83:e7:0a:8a:00)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 152.66.159.134
> Transmission Control Protocol, Src Port: 80, Dst Port: 63068, Seq: 1, Ack: 511, Len: 438
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Wed, 04 May 2022 09:39:25 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.28 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 04 May 2022 05:59:02 GMT\r\n
    ETag: "51-5de2952766e0b"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 81\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.119449000 seconds]
    [Request in frame: 4796]
    [Request URI: http://naia.ce.umass.edu/winechank-lake/TMTR0-winechank-f11a1.html]
0000  a4 83 e7 0a 8a 00 dc 8c 37 6a ae 9f 08 00 45 00  ....7j...E
0010  01 de 86 be 40 00 2c 06 19 0f 80 77 f5 0c 98 42  ....@...w...B
0020  9f 86 00 50 76 5d 8b e9 f0 4e 53 eb 29 64 50 18  ...P...NS)dP

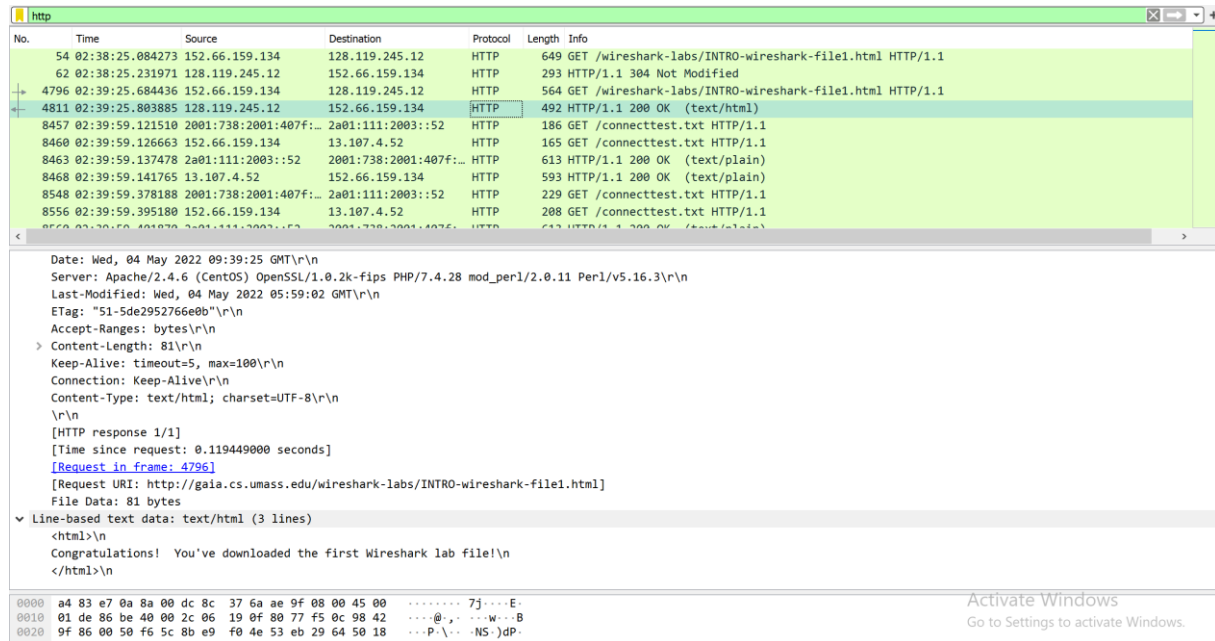
```

- **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:**



The screenshot shows a Wireshark packet capture of an HTTP transaction. The packet list pane at the top shows several packets, with the 481st packet (HTTP GET) and the 492nd packet (HTTP 200 OK) highlighted. The packet details pane for the 492nd packet is expanded, showing the response status and headers. The response status is 200 OK (text/html). The headers include Date, Server, Last-Modified, ETag, Accept-Ranges, Content-Length, Keep-Alive, Connection, and Content-Type. The packet data pane shows the raw data of the response, which is a 200 OK status and a 200 OK (text/html) response.

No.	Time	Source	Destination	Protocol	Length	Info
54	02:38:25.084273	152.66.159.134	128.119.245.12	HTTP	649	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
62	02:38:25.231971	128.119.245.12	152.66.159.134	HTTP	293	HTTP/1.1 304 Not Modified
4796	02:39:25.684436	152.66.159.134	128.119.245.12	HTTP	564	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
4811	02:39:25.803885	128.119.245.12	152.66.159.134	HTTP	492	HTTP/1.1 200 OK (text/html)

Details of the 492nd packet (HTTP 200 OK):

- Date: Wed, 04 May 2022 09:39:25 GMT\r\n
- Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.28 mod\_perl/2.0.11 Perl/v5.16.3\r\n
- Last-Modified: Wed, 04 May 2022 05:59:02 GMT\r\n
- ETag: "51-5de295276e0b"\r\n
- Accept-Ranges: bytes\r\n
- Content-Length: 81\r\n
- Keep-Alive: timeout=5, max=100\r\n
- Connection: Keep-Alive\r\n
- Content-Type: text/html; charset=UTF-8\r\n
- \r\n
- [HTTP response 1/1]
- [Time since request: 0.119449000 seconds]
- [Request in frame: 4796]
- [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
- File Data: 81 bytes

Line-based text data: text/html (3 lines)

```
<html>\n<body>\n<h1>Congratulations! You've downloaded the first Wireshark lab file!\n</h1>\n</body>\n</html>\n
```

HTTP GET at: 02:39:25.684436

HTTP OK at: 02:39:25.803885

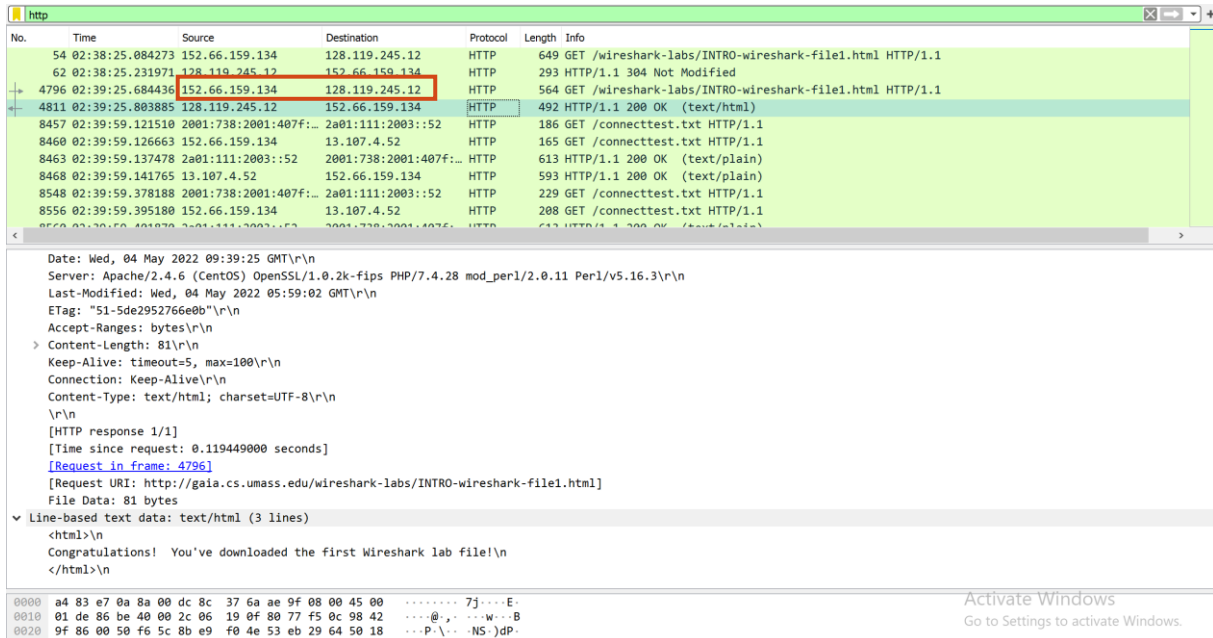
Time taken: 0.119449 s

## Laboratory Report – Informatics 2

### 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:**



No.	Time	Source	Destination	Protocol	Length	Info
54	02:38:25.084273	152.66.159.134	128.119.245.12	HTTP	649	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
62	02:38:25.231971	128.119.245.12	152.66.159.134	HTTP	293	HTTP/1.1 304 Not Modified
4796	02:39:25.684436	152.66.159.134	128.119.245.12	HTTP	564	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
4811	02:39:25.803885	128.119.245.12	152.66.159.134	HTTP	492	HTTP/1.1 200 OK (text/html)
8457	02:39:59.121510	2001:738:2001:407f::...	2a01:111:2003::52	HTTP	186	GET /connecttest.txt HTTP/1.1
8460	02:39:59.126663	152.66.159.134	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
8463	02:39:59.137478	2a01:111:2003::52	2001:738:2001:407f::...	HTTP	613	HTTP/1.1 200 OK (text/plain)
8468	02:39:59.141765	13.107.4.52	152.66.159.134	HTTP	593	HTTP/1.1 200 OK (text/plain)
8548	02:39:59.378188	2001:738:2001:407f::...	2a01:111:2003::52	HTTP	229	GET /connecttest.txt HTTP/1.1
8556	02:39:59.395180	152.66.159.134	13.107.4.52	HTTP	208	GET /connecttest.txt HTTP/1.1

Details of selected packet (No. 4796):

Date: Wed, 04 May 2022 09:39:25 GMT\r\n  
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.28 mod\_perl/2.0.11 Perl/v5.16.3\r\n  
Last-Modified: Wed, 04 May 2022 05:59:02 GMT\r\n  
ETag: "51-5de2952766e0b"\r\n  
Accept-Ranges: bytes\r\n  
Content-Length: 81\r\n  
Keep-Alive: timeout=5, max=100\r\n  
Connection: Keep-Alive\r\n  
Content-Type: text/html; charset=UTF-8\r\n  
[HTTP response 1/1]  
[Time since request: 0.119449000 seconds]  
[Request in frame: 4796]  
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]  
File Data: 81 bytes

Line-based text data: text/html (3 lines)

```
<html>\nCongratulations! You've downloaded the first Wireshark lab file!\n</html>\n
```

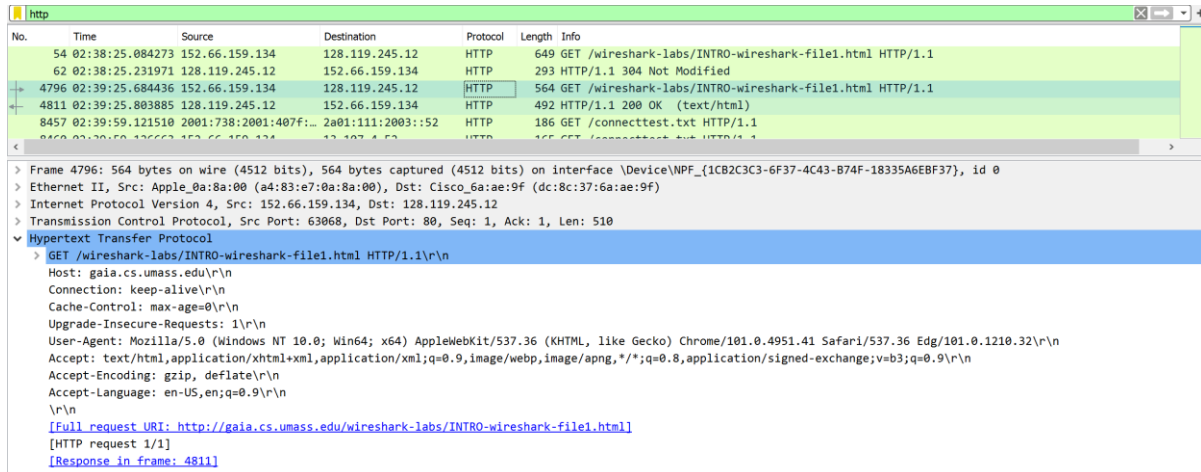
Internet address of my computer: 152.66.159.13

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

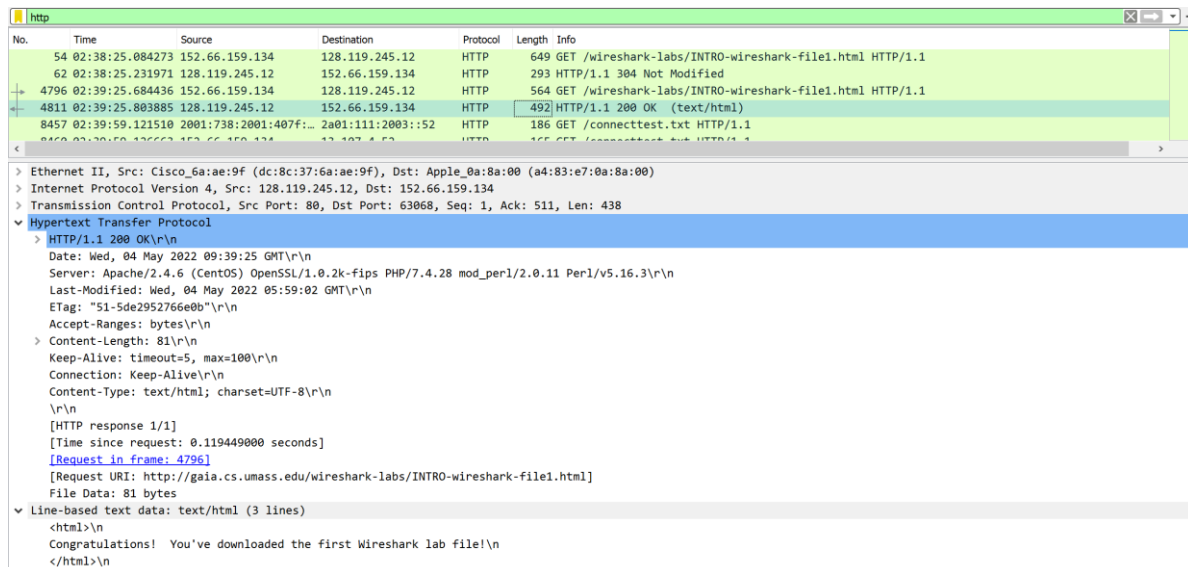
### TASK #4

**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

## Laboratory Report – Informatics 2

### 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](http://www.kooora.com)

We get can get the IP address by ping [www.kooora.com](http://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-104-16-0-1
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
```

## Laboratory Report – Informatics 2

```
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](http://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:
  0  1 ms  1 ms  1 ms  v181.kiwi.net.bme.hu [152.66.147.254]
  1  2 ms  2 ms  2 ms  xge0-0-0-3.rax.net.bme.hu [152.66.0.90]
  2  2 ms  2 ms  2 ms  tg0-2-0-2.rtr.bme.hbone.hu [152.66.0.125]
  3  3 ms  2 ms  2 ms  hge0-1-0-2.core1.vh.hbone.hu [195.111.96.226]
  4  42 ms  2 ms  2 ms  hge0-4-0-3.rtr2.vh.hbone.hu [195.111.98.71]
  5  48 ms  2 ms  2 ms  te0-3-1-3.rcr51.b020664-1.bud01.atlas.cogentco.c
om [149.111.10.9]
  6  4 ms  3 ms  3 ms  be2246.ccr31.bud01.atlas.cogentco.com [130.117.1
.13]
  7  7 ms  5 ms  5 ms  be3261.ccr21.bts01.atlas.cogentco.com [130.117.3
.137]
  8  6 ms  6 ms  6 ms  be2988.ccr51.vie01.atlas.cogentco.com [154.54.59
.86]
  9  11 ms  11 ms  13 ms  be2974.ccr21.muc03.atlas.cogentco.com [154.54.58.5]
 10  17 ms  17 ms  17 ms  be2959.ccr41.fra03.atlas.cogentco.com [154.54.36.53]
 11  17 ms  *  *  tata.fra03.atlas.cogentco.com [130.117.15.114]
 12  *  *  *  Request timed out.
 13  *  *  *  if-ae-55-2.tcore2.pvu-paris.as6453.net [80.231.245.6]
 14  *  *  *  Request timed out.
 15  *  *  *  Request timed out.
 16  *  *  *  if-be-7-2.ecore1.emrs2-marseille.as6453.net [195.219.174.8]
 17  *  *  *  Request timed out.
 18  *  *  *  if-ae-31-5.tcore1.svw-singapore.as6453.net [80.231.217.197]
 19  *  *  *  if-be-45-2.ecore2.esin4-singapore.as6453.net [180.87.108.4]
 20  *  *  *  if-be-10-2.ecore2.svq-singapore.as6453.net [180.87.107.0]
 21  259 ms  258 ms  262 ms  if-ae-46-2.thar1.svq-singapore.as6453.net [120.29.214.10]
 22  259 ms  258 ms  262 ms  120.29.214.142
 23  256 ms  259 ms  257 ms  Request timed out.
 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.**