Computer Networks
Project 1

CSI4106-01

Fall, 2020

(Difficulty ★☆☆☆☆)

Prelim.

Before you do this project, you must be fully aware of **“Project Policy Notice”**

To do

Assignment 1-1: wireshark

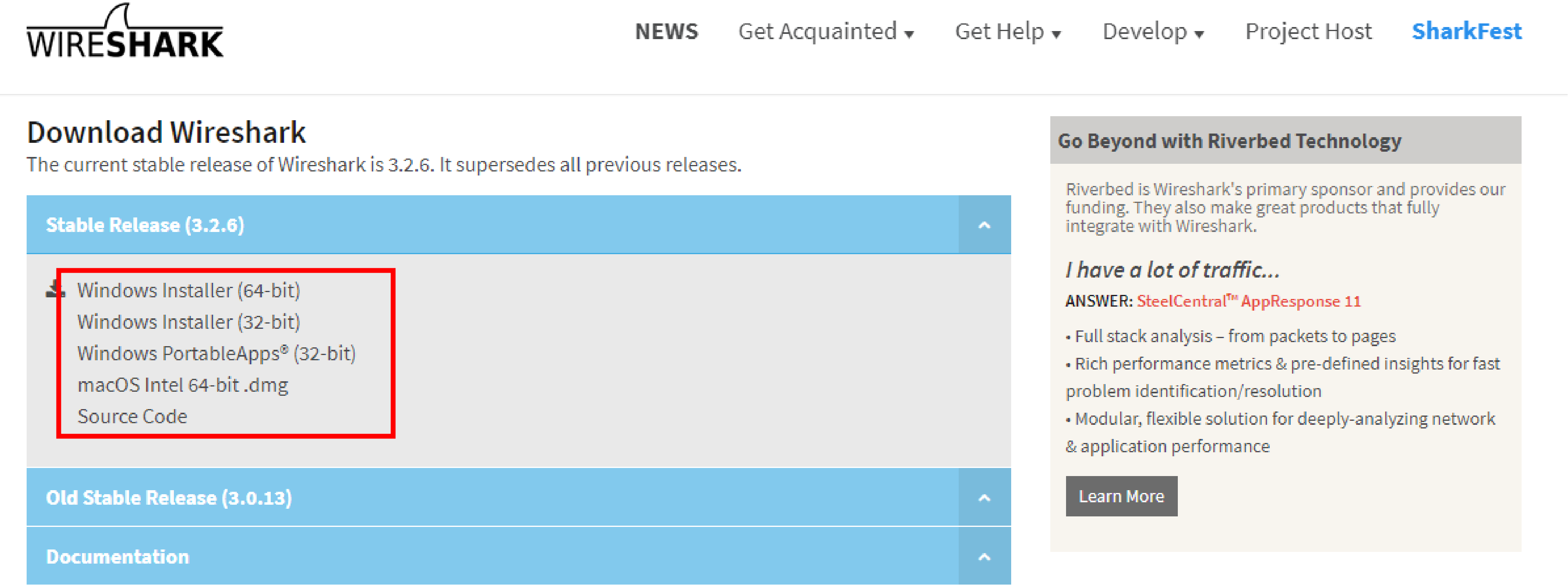
Assignment 1-2: iPerf3

Assignment 1-3: packet capture coding

1. Wireshark

The world's foremost and widely-used network protocol analyzer

Download : https://www.wireshark.org/download.html



WIRESHARK

NEWS Get Acquainted ▾ Get Help ▾ Develop ▾ Project Host SharkFest

Download Wireshark

The current stable release of Wireshark is 3.2.6. It supersedes all previous releases.

Stable Release (3.2.6)

- Windows Installer (64-bit)
- Windows Installer (32-bit)
- Windows PortableApps® (32-bit)
- macOS Intel 64-bit .dmg
- Source Code

Old Stable Release (3.0.13)

Documentation

Go Beyond with Riverbed Technology

Riverbed is Wireshark's primary sponsor and provides our funding. They also make great products that fully integrate with Wireshark.

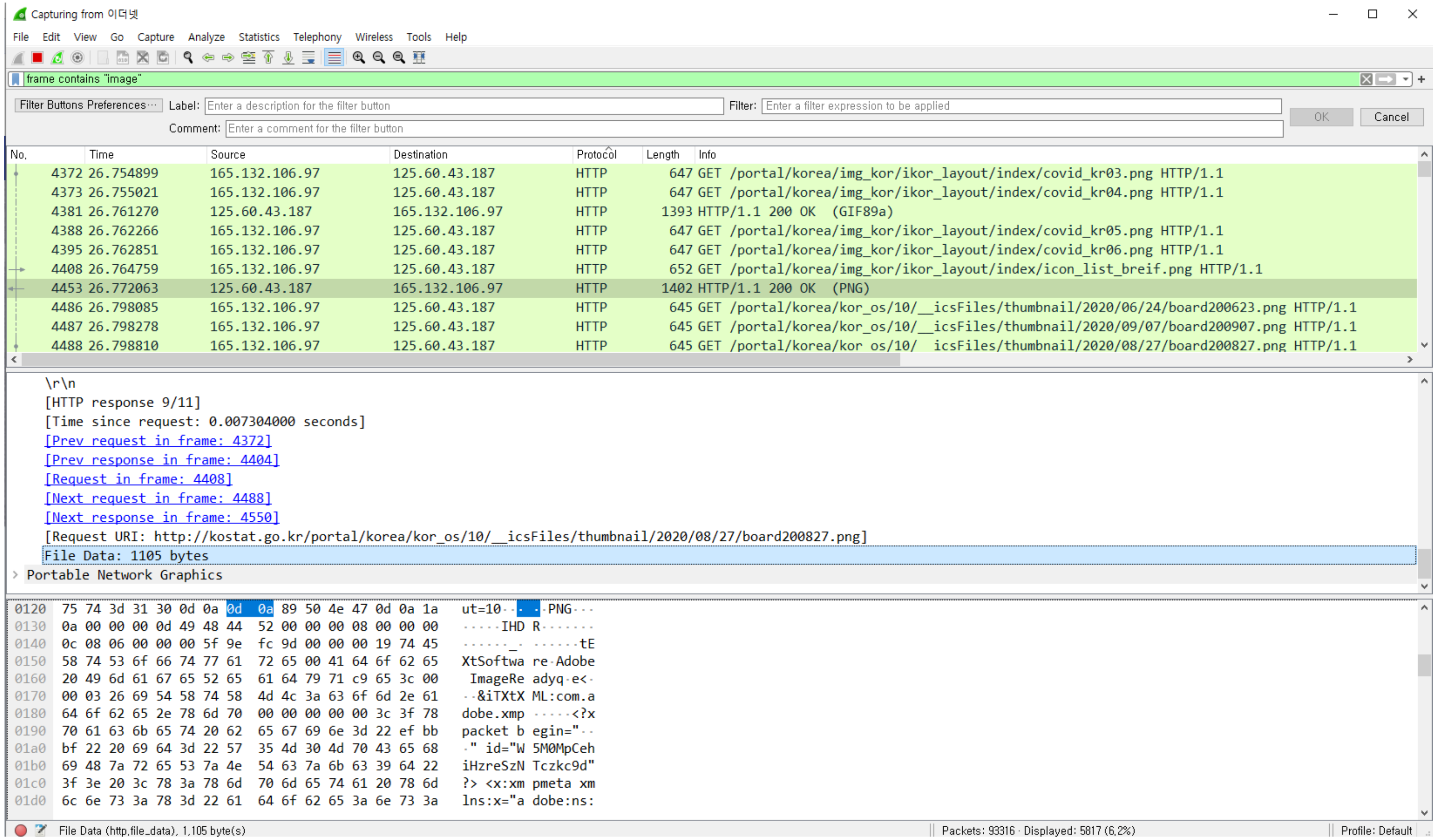
I have a lot of traffic...

ANSWER: SteelCentral™ AppResponse 11

- Full stack analysis – from packets to pages
- Rich performance metrics & pre-defined insights for fast problem identification/resolution
- Modular, flexible solution for deeply-analyzing network & application performance

Learn More

Packet Capturing



frame contains "image"

Label: Enter a description for the filter button

Filter: Enter a filter expression to be applied

Comment: Enter a comment for the filter button

```
No.   Time       Source          Destination     Protocol Length Info
 4372 26.754899  165.132.106.97  125.60.43.187   HTTP      647 GET /portal/korea/img_kor/ikor_layout/index/covid_kr03.png HTTP/1.1
 4373 26.755021  165.132.106.97  125.60.43.187   HTTP      647 GET /portal/korea/img_kor/ikor_layout/index/covid_kr04.png HTTP/1.1
 4381 26.761270  125.60.43.187   165.132.106.97  HTTP     1393 HTTP/1.1 200 OK  (GIF89a)
 4388 26.762266  165.132.106.97  125.60.43.187   HTTP      647 GET /portal/korea/img_kor/ikor_layout/index/covid_kr05.png HTTP/1.1
 4395 26.762851  165.132.106.97  125.60.43.187   HTTP      647 GET /portal/korea/img_kor/ikor_layout/index/covid_kr06.png HTTP/1.1
 4408 26.764759  165.132.106.97  125.60.43.187   HTTP      652 GET /portal/korea/img_kor/ikor_layout/index/icon_list_breif.png HTTP/1.1
 4453 26.772063  125.60.43.187   165.132.106.97  HTTP     1402 HTTP/1.1 200 OK  (PNG)
 4486 26.798085  165.132.106.97  125.60.43.187   HTTP      645 GET /portal/korea/kor_os/10/__icsFiles/thumbnail/2020/06/24/board200623.png HTTP/1.1
 4487 26.798278  165.132.106.97  125.60.43.187   HTTP      645 GET /portal/korea/kor_os/10/__icsFiles/thumbnail/2020/09/07/board200907.png HTTP/1.1
 4488 26.798810  165.132.106.97  125.60.43.187   HTTP      645 GET /portal/korea/kor_os/10/__icsFiles/thumbnail/2020/08/27/board200827.png HTTP/1.1
```

```
    \r\n
    [HTTP response 9/11]
    [Time since request: 0.007304000 seconds]
    [Prev request in frame: 4372]
    [Prev response in frame: 4404]
    [Request in frame: 4408]
    [Next request in frame: 4488]
    [Next response in frame: 4550]
    [Request URI: http://kostat.go.kr/portal/korea/kor_os/10/__icsFiles/thumbnail/2020/08/27/board200827.png]
    File Data: 1105 bytes
> Portable Network Graphics
```

```
0120  75 74 3d 31 30 0d 0a 0d  0a 89 50 4e 47 0d 0a 1a   ut=10·· ··PNG···
0130  0a 00 00 00 0d 49 48 44  52 00 00 00 08 00 00 00   ·····IHD R·······
0140  0c 08 06 00 00 00 5f 9e  fc 9d 00 00 00 19 74 45   ······_· ······tE
0150  58 74 53 6f 66 74 77 61  72 65 00 41 64 6f 62 65   XtSoftwa re·Adobe
0160  20 49 6d 61 67 65 52 65  61 64 79 71 c9 65 3c 00    ImageRe adyq·e<·
0170  00 03 26 69 54 58 74 58  4d 4c 3a 63 6f 6d 2e 61   ··&iTXtX ML:com.a
0180  64 6f 62 65 2e 78 6d 70  00 00 00 00 00 3c 3f 78   dobe.xmp ·····<?x
0190  70 61 63 6b 65 74 20 62  65 67 69 6e 3d 22 ef bb   packet b egin="··
01a0  bf 22 20 69 64 3d 22 57  35 4d 30 4d 70 43 65 68   ·" id="W 5M0MpCeh
01b0  69 48 7a 72 65 53 7a 4e  54 63 7a 6b 63 39 64 22   iHzreSzN Tczkc9d"
01c0  3f 3e 20 3c 78 3a 78 6d  70 6d 65 74 61 20 78 6d   ?> <x:xm pmeta xm
01d0  6c 6e 73 3a 78 3d 22 61  64 6f 62 65 3a 6e 73 3a   lns:x="a dobe:ns:
```

File Data (http.file_data), 1,105 byte(s) | Packets: 93316 · Displayed: 5817 (6.2%) | Profile: Default

Assignment1-1(20pts)

- **Export images** from the packet using Wireshark

  - Write a report with how you captured an image from the packet

  - Any image file (**png, jpg, gif**) from any website is acceptable

  - Don’t submit the image file but screenshot is necessary

  - Try loading website with HTTP instead of HTTPS

- **Requirements**

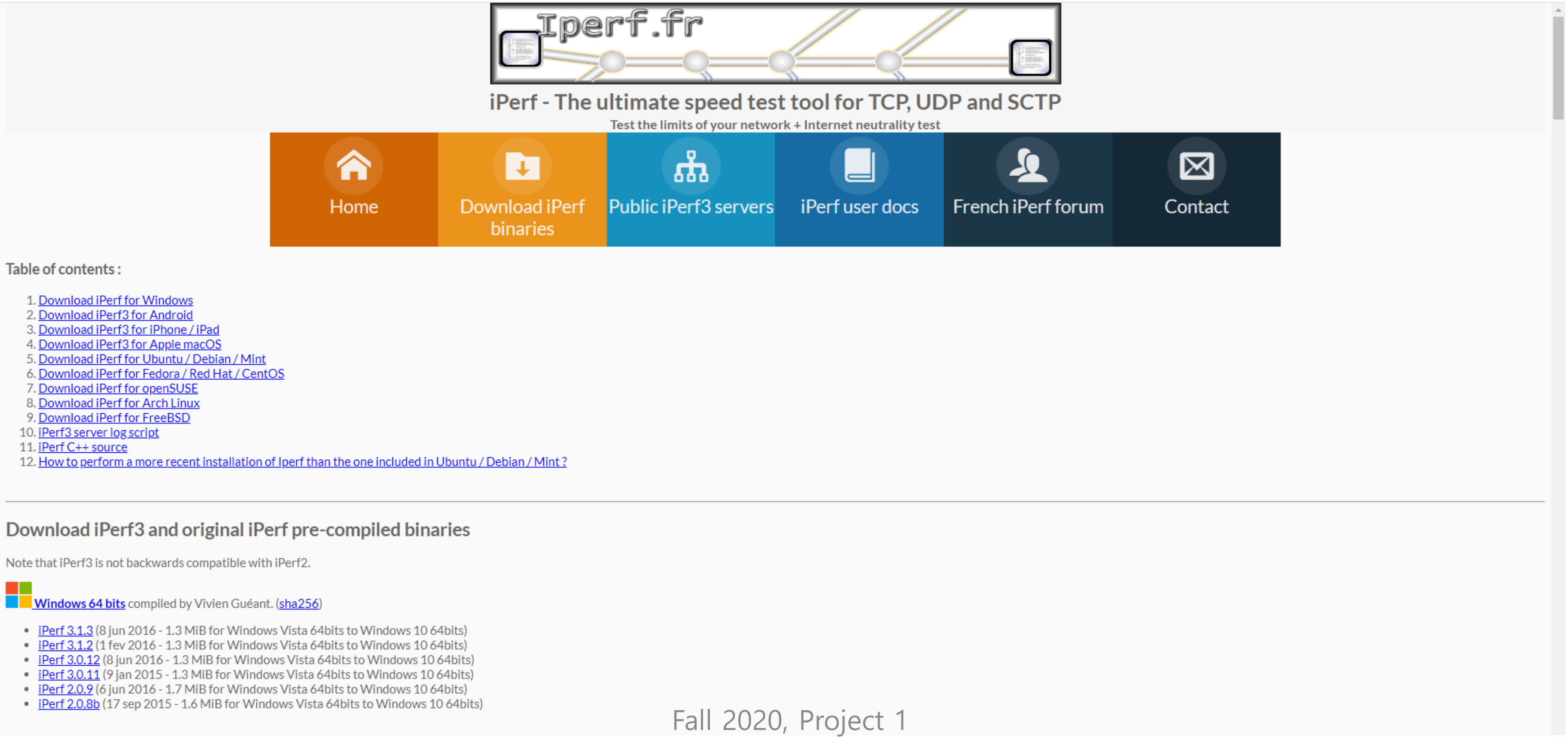
  - Specify the webpage, exported image and packet information with screenshots [10pts]

  - Comments for each step on capturing packets and exporting images [10pts]

2. iPerf3

iPerf3 is a real-time network throughput measurement tool.

You can generate traffic & test quality traffic.



iPerf - The ultimate speed test tool for TCP, UDP and SCTP

Test the limits of your network + Internet neutrality test

Table of contents :

1. Download iPerf for Windows
2. Download iPerf3 for Android
3. Download iPerf3 for iPhone / iPad
4. Download iPerf3 for Apple macOS
5. Download iPerf for Ubuntu / Debian / Mint
6. Download iPerf for Fedora / Red Hat / CentOS
7. Download iPerf for openSUSE
8. Download iPerf for Arch Linux
9. Download iPerf for FreeBSD
10. iPerf3 server log script
11. iPerf C++ source
12. How to perform a more recent installation of Iperf than the one included in Ubuntu / Debian / Mint ?

Download iPerf3 and original iPerf pre-compiled binaries

Note that iPerf3 is not backwards compatible with iPerf2.

Windows 64 bits compiled by Vivien Guéant. (sha256)

- iPerf 3.1.3 (8 jun 2016 - 1.3 MiB for Windows Vista 64bits to Windows 10 64bits)
- iPerf 3.1.2 (1 fev 2016 - 1.3 MiB for Windows Vista 64bits to Windows 10 64bits)
- iPerf 3.0.12 (8 jun 2016 - 1.3 MiB for Windows Vista 64bits to Windows 10 64bits)
- iPerf 3.0.11 (9 jan 2015 - 1.3 MiB for Windows Vista 64bits to Windows 10 64bits)
- iPerf 2.0.9 (6 jun 2016 - 1.7 MiB for Windows Vista 64bits to Windows 10 64bits)
- iPerf 2.0.8b (17 sep 2015 - 1.6 MiB for Windows Vista 64bits to Windows 10 64bits)

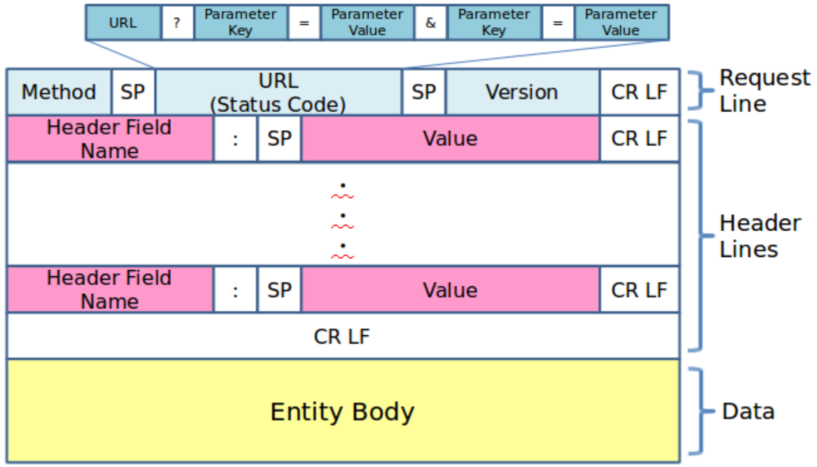
Assignment1-2(20pts)

- Write a report with **requirements** below
- **Requirements**
  - Screenshot of iPerf3 execution on localhost (server, client) [6pts]
  - Explanation of transfer, bitrate, and cwnd of result screen [7pts]
  - Description of several commands: -b, -n, -w, -l [7pts]

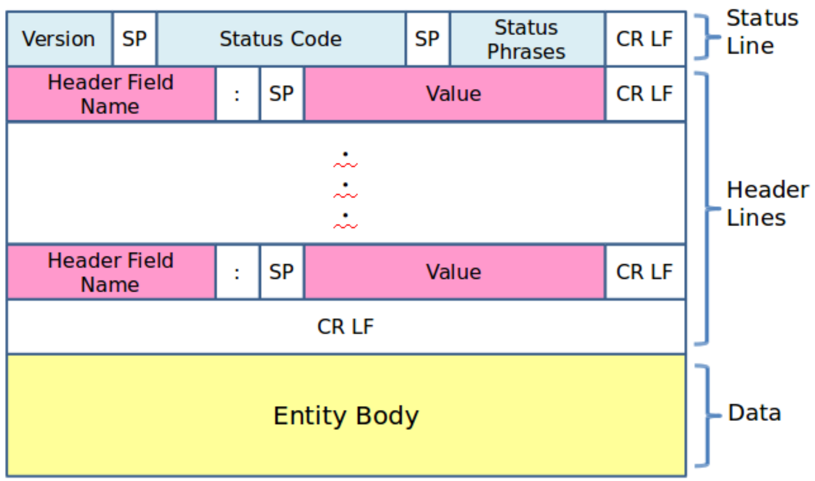
3. Packet capture coding

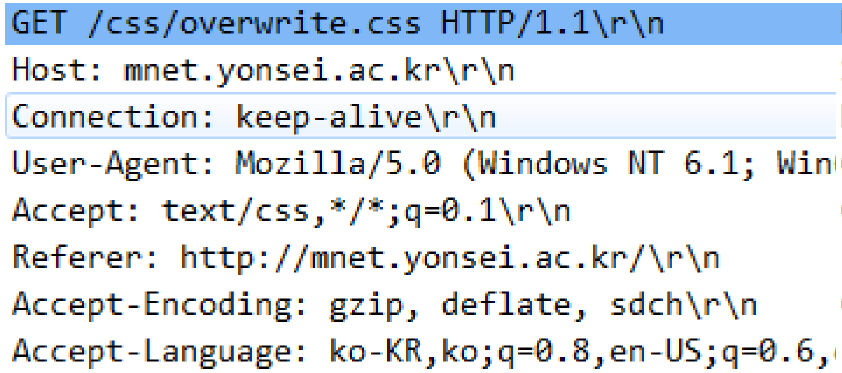
HTTP Header

Request

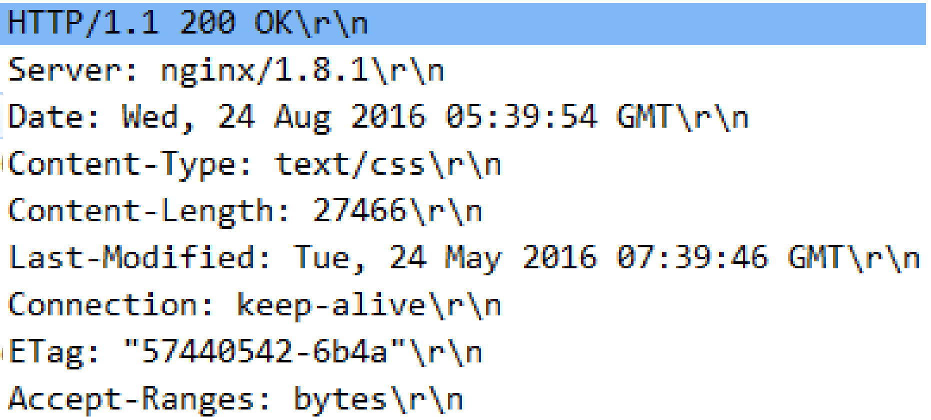


Response





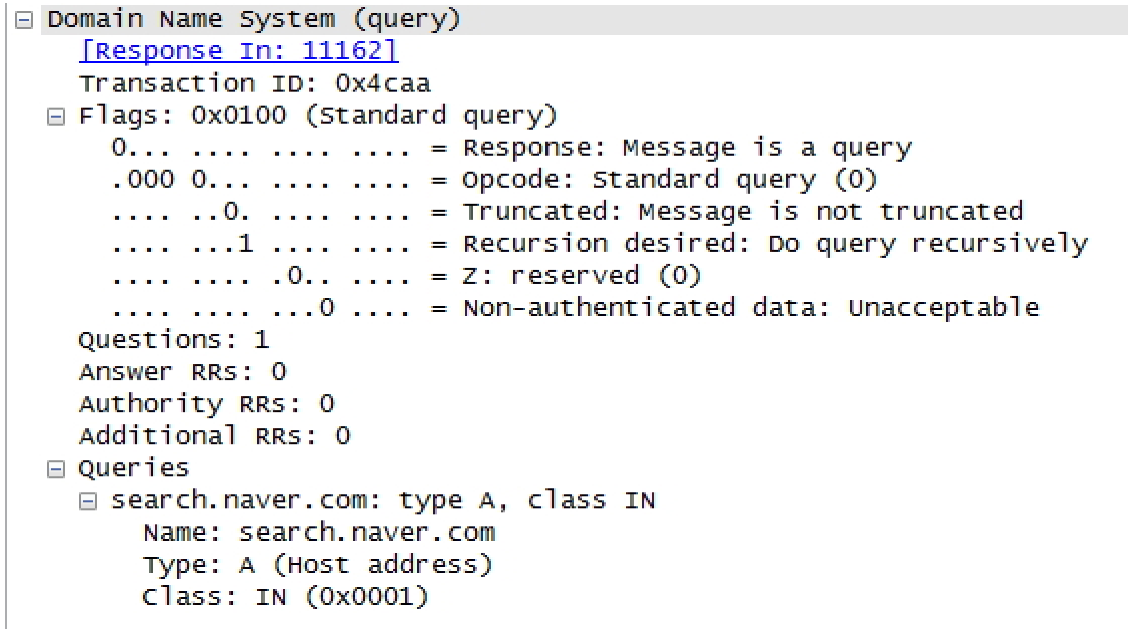
```
GET /css/overwrite.css HTTP/1.1\r\n
Host: mnet.yonsei.ac.kr\r\n
Connection: keep-alive\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win
Accept: text/css,*/*;q=0.1\r\n
Referer: http://mnet.yonsei.ac.kr/\r\n
Accept-Encoding: gzip, deflate, sdch\r\n
Accept-Language: ko-KR,ko;q=0.8,en-US;q=0.6,
```



```
HTTP/1.1 200 OK\r\n
Server: nginx/1.8.1\r\n
Date: Wed, 24 Aug 2016 05:39:54 GMT\r\n
Content-Type: text/css\r\n
Content-Length: 27466\r\n
Last-Modified: Tue, 24 May 2016 07:39:46 GMT\r\n
Connection: keep-alive\r\n
ETag: "57440542-6b4a"\r\n
Accept-Ranges: bytes\r\n
```

DNS header

<table>
<tr><td colspan="8">ID</td></tr>
<tr><td>OR</td><td>Opcode</td><td>AA</td><td>TC</td><td>RD</td><td>RA</td><td>Z</td><td>RCODE</td></tr>
<tr><td colspan="8">QDCOUNT</td></tr>
<tr><td colspan="8">ANCOUNT</td></tr>
<tr><td colspan="8">NSCOUNT</td></tr>
<tr><td colspan="8">ARCOUNT</td></tr>
</table>



```
⊟ Domain Name System (query)
    [Response In: 11162]
    Transaction ID: 0x4caa
  ⊟ Flags: 0x0100 (Standard query)
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ search.naver.com: type A, class IN
        Name: search.naver.com
        Type: A (Host address)
        Class: IN (0x0001)
```

Assignment1-3 (60pts)
Write a code of Simple HTTP & DNS sniffer

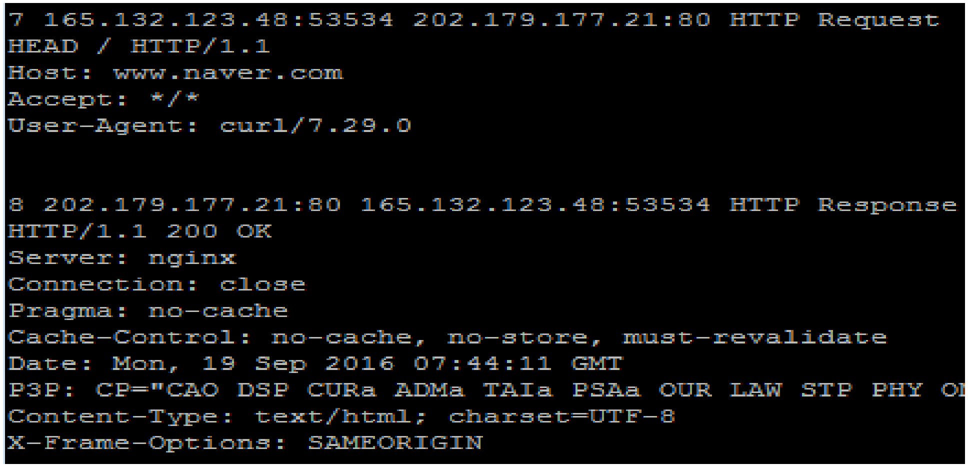
- In case of HTTP : print the headers of Requests and Responses [30pts]
  - **<u>“Without entity body”</u>**
- **Display Format (S=source, D=destination)**

- Output screen -

#No S_IP:S_Port D_IP:D_Port HTTP [Request|Response]

[Request Line](or [Status Line])

[Header Lines]



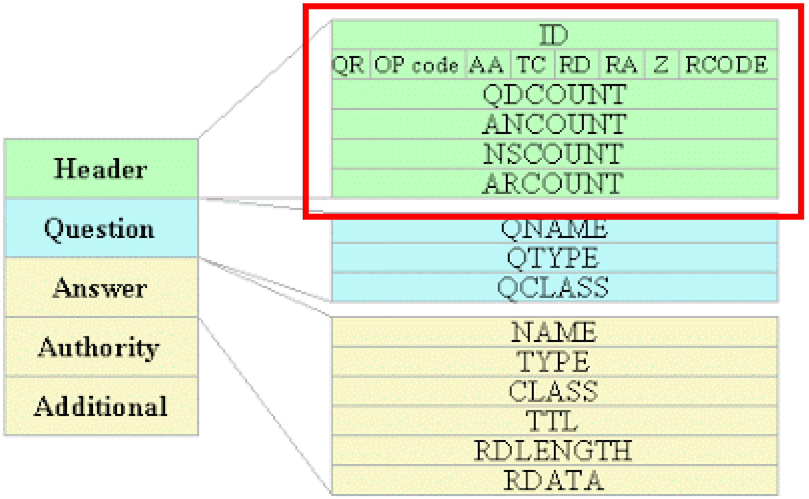
```
7 165.132.123.48:53534 202.179.177.21:80 HTTP Request
HEAD / HTTP/1.1
Host: www.naver.com
Accept: */*
User-Agent: curl/7.29.0


8 202.179.177.21:80 165.132.123.48:53534 HTTP Response
HTTP/1.1 200 OK
Server: nginx
Connection: close
Pragma: no-cache
Cache-Control: no-cache, no-store, must-revalidate
Date: Mon, 19 Sep 2016 07:44:11 GMT
P3P: CP="CAO DSP CURa ADMa TAIa PSAa OUR LAW STP PHY OI
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
```

Assignment1-3 (60pts) -continuous

- In case of DNS : print only headers [30pts]

- **Display Format (S=source, D=destination)**



- Output screen -

#No S_IP:S_Port D_IP:D_Port DNS ID : [0x format]

[QR | Opcode | AA | TC | RD | RA | Z | RCODE]

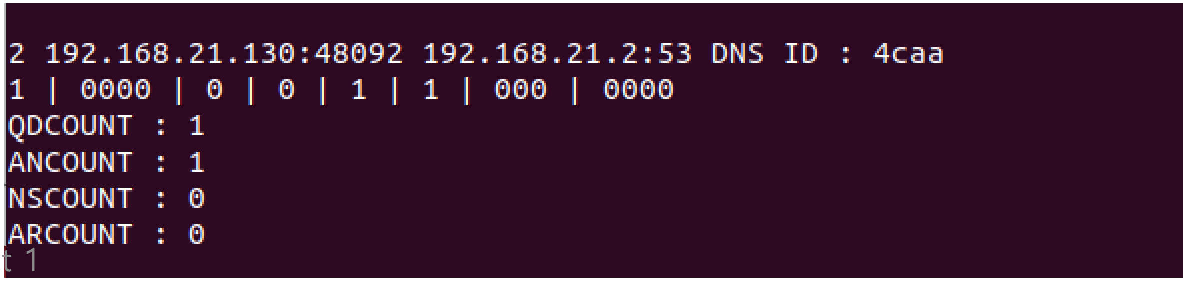
Binary number format

QDCOUNT : [0x format]

ANCOUNT : [0x format]

NSCOUNT : [0x format]

ARCOUNT : [0x format]



```
2 192.168.21.130:48092 192.168.21.2:53 DNS ID : 4caa
1 | 0000 | 0 | 0 | 1 | 1 | 000 | 0000
QDCOUNT : 1
ANCOUNT : 1
NSCOUNT : 0
ARCOUNT : 0
```

Assignment1-3 (60pts) -continuous

- At start, you must add selection of networks (hint: pcap_findalldevs)
- Need interface code to choose whether to sniff DNS or HTTP

Directions

- **This is an individual project**
- Language: **C or Python**
  - **C: gcc 7.5.0**
  - **Python: Python 3 (>=3.5.2)**
- OS:
  - **Ubuntu 16.04** or higher for assignment1-3
  - You may use **windows** for assignment1-1,2
- You must use only ***pcap*** library.
  - C (pcap): #include <pcap.h>
    - gcc –o <output> project_1.c -lpcap
  - Python (pcapy): import pcapy
  - ***scapy or 3rd party framework: NOT ALLOWED***

Deliverables: **YourID_ProjectNo.zip (e.g., `2020147000_1.zip`)**

>>>>>> Do not include any folders in the zip file

TA tests with `./setup.sh && ./run.sh`

- **project.[py|c]**
  - Your code with detail comments
- **run.sh**
  - This should work with the command ***"run.sh > results.txt"***
- **setup.sh**
  - This should install dependencies or compile your code
- **report.pdf**
  - Asssignment1-1~3
  - Your comprehensive comments of this project

Helpful Keywords

- **Wireshark**: an open-source protocol analyzer
  - This helps you understand the protocol structure
  - Use “http” or “tcp port 80” for this project.

- **TCP/IP 5-Layer Model**
- **Pcap Library (http://www.tcpdump.org)**
  - A portable C/C++ library for network traffic capture.
- **HTTP Header Format of Request/Response**
- **HTTP is 80 port, and DNS is 53 port**

Tip

- Your program is running in background and you can test yours with any **Web Browser**.
- Also you can test your code with...
  - **Postman** ➔ A chrome extension of HTTP request
  - **libcurl** ➔ curl –Is http://hello.com
  - **wget** ➔ wget –p http://world.com –O /dev/null

- DUE DATE

  27/Sep/2020 23:55:00 KST

  No exception for exceeding deadline

- Delay Policy

  -33%pts for ~28/Sep 23:55:00

  -66%pts for ~29/Sep 23:55:00

  -100%pts for 30/Sep 23:55:00~

You agree with the following statement by submitting your assignment on YSCEC

Plagiarizing = 0pts = Fail

No exception for any kinds of cheating and copying

Score Policy: *Max. 100 pts*

1	Not submitted / not working / missing files	**0 pts**
2	Overdue → Delay	-33% pts/day
3	**The rules or directions are not followed**	-10 pts/rule
4	**Scapy or 3rd party framework is used**	**0 pts**
5	**Plagiarizing / Over-implementation** **(Any kinds of Suspicion of Code-copy)**	**0 pts**
6	**Impolite Report / Lack of Comments**	**0 pts / -50% pts**

Questions are welcome on YSCEC

but,

“Try Google first”

“Look up others’ questions”