Computer Network Project 1

HTTP Header Sniffer

CSI4106-01

Fall, 2016

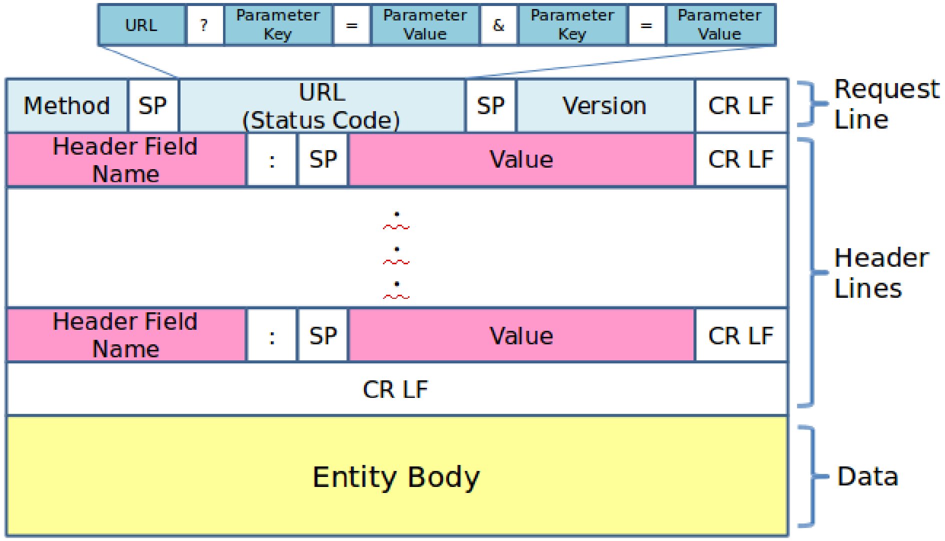
Prelim.

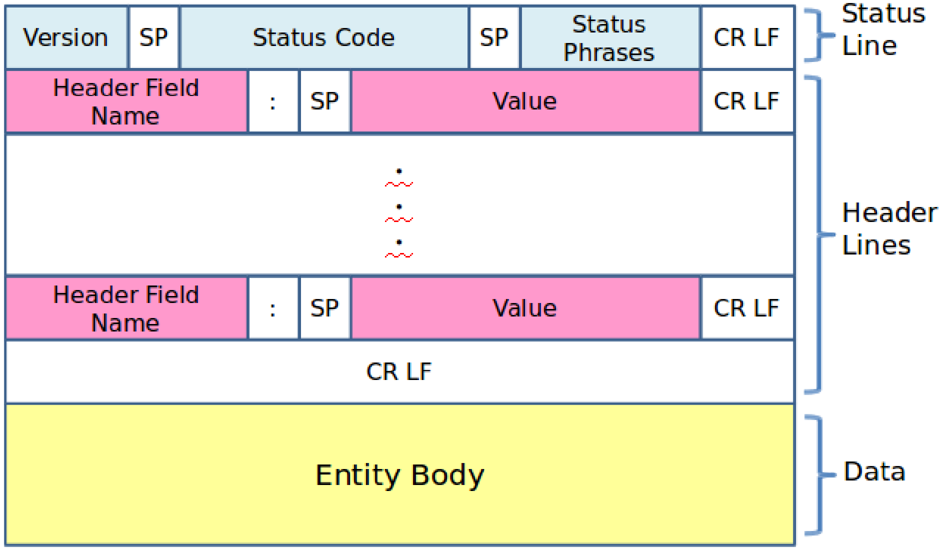
- You have total 4 projects in this class.
- Each project has “**Mandatory**” assignment and “**Additional**” assignment (optional).
  - Mandatory(100 pts) + Additional(α pts)
- You should follow the **print format of screen** and the **file format of your deliverables**.
- We provide the example version of deliverables so we can grade your projects automatically.

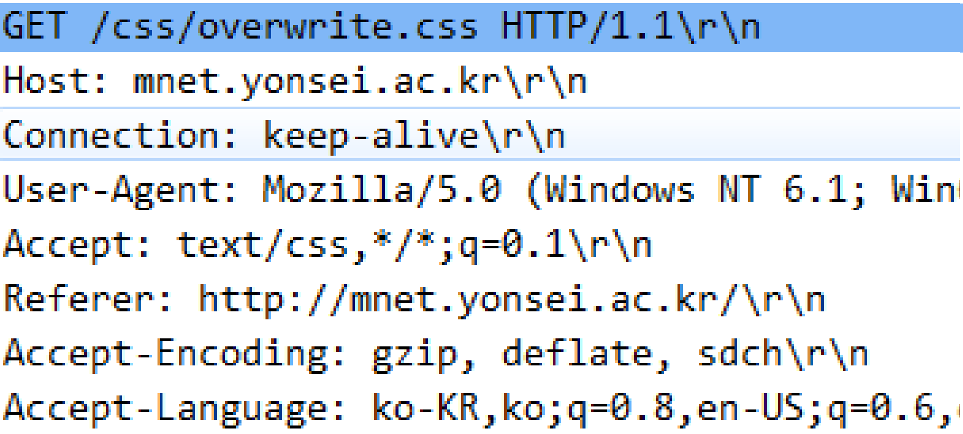
HTTP Header

Request

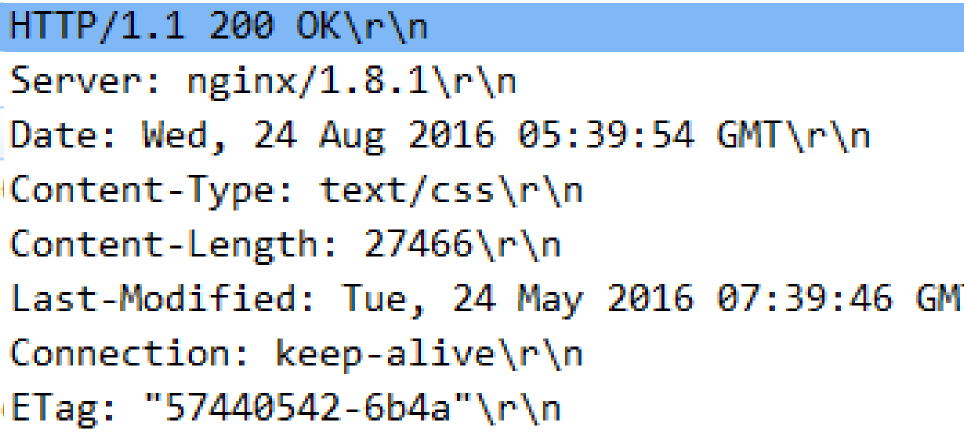
Response





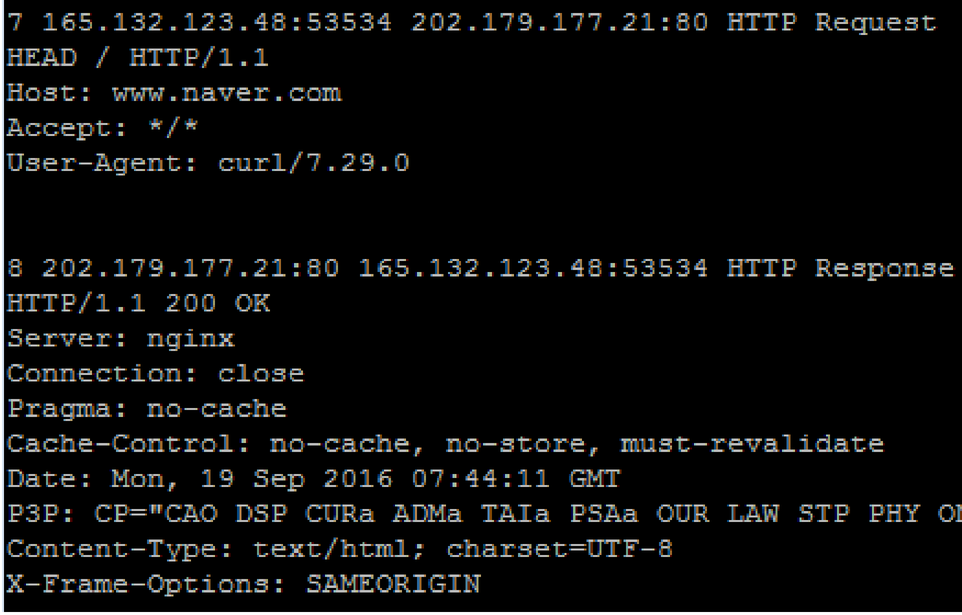


```
GET /css/overwrite.css HTTP/1.1\r\n
Host: mnet.yonsei.ac.kr\r\n
Connection: keep-alive\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win
Accept: text/css,*/*;q=0.1\r\n
Referer: http://mnet.yonsei.ac.kr/\r\n
Accept-Encoding: gzip, deflate, sdch\r\n
Accept-Language: ko-KR,ko;q=0.8,en-US;q=0.6,
```



```
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 GM
Connection: keep-alive\r\n
ETag: "57440542-6b4a"\r\n
```

Mandatory Assignment



```
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 ON
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
```

- Write the code of Simple HTTP header sniffer
- Print headers of Requests and Responses
  - **Without entity body**
- Display Format
  - You should follow this format or you get -10pts

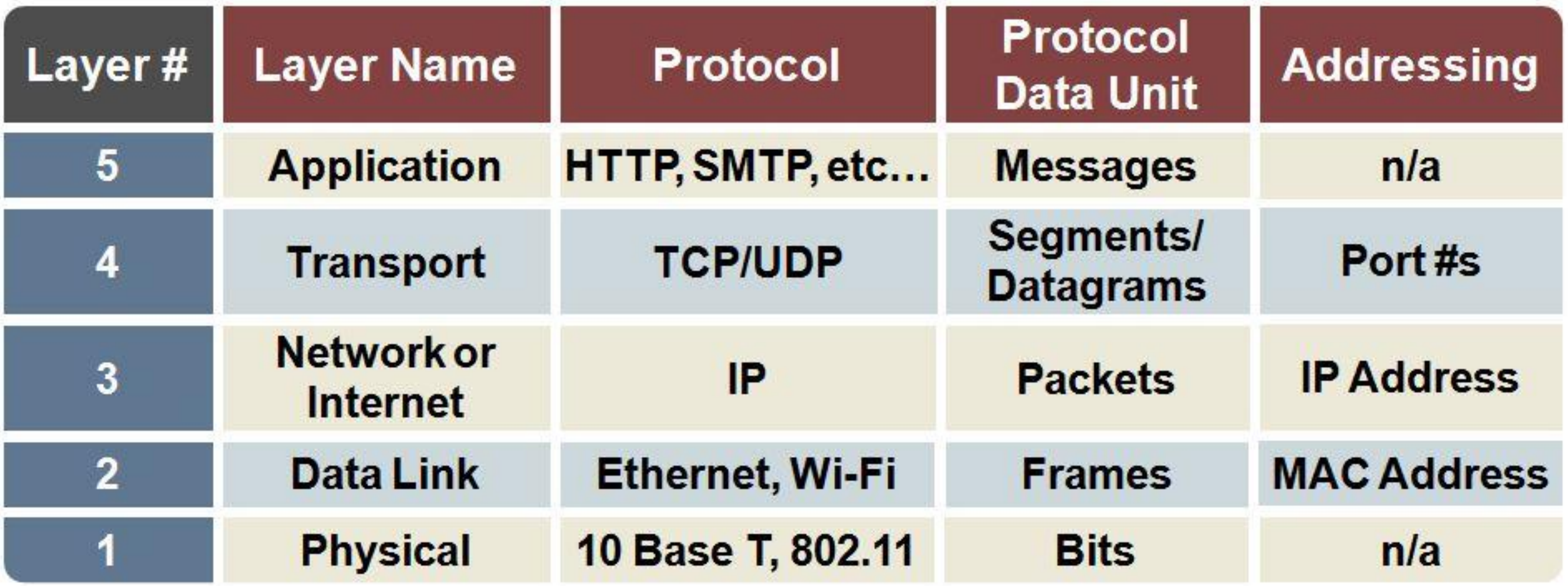
```
#No S_IP:S_Port D_IP:D_Port HTTP [Request|Response]\r\n
[Request Line](or [Status Line])\r\n
[Header Lines] \r\n\r\n
```

Additional Assignment (Optional)

- **+10pts**
- The goal is to make text files of the entity body of POST request.
- The entity body has parameters and values.
- **post/**`#no`**.txt**
  - `par1=value1&par2=value2`
- **(example) post/**`5`**.txt**
  - `id=hello&password=hello`

Background

- **TCP/IP 5-Layer Model**



Layer #	Layer Name	Protocol	Protocol Data Unit	Addressing
5	Application	HTTP, SMTP, etc…	Messages	n/a
4	Transport	TCP/UDP	Segments/ Datagrams	Port #s
3	Network or Internet	IP	Packets	IP Address
2	Data Link	Ethernet, Wi-Fi	Frames	MAC Address
1	Physical	10 Base T, 802.11	Bits	n/a

Background

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

- **Pcap Library (**http://www.tcpdump.org**)**
  - A portable C/C++ library for network traffic capture.

- **HTTP Header Format of Request/Response**

Deliverables: **2016147xxx_1.zip** ***must include***

- **readme.txt** ***(follow the example format)***
  - The language, version and dependencies of your code
- **project_1.[py|c]**
  - Your code with detail comments
- **run.sh**
  - This should be able to ***"run.sh > 2016147xxx.txt"***
- **setup.sh**
  - This should install dependencies or compile your code
- **report.pdf** ***(free-form)***
  - Your comprehensive manual of this project
  - How to use, code commentaries and so on.

Language / Library

- Language: **C or Python**
  - C and Python run on both Windows and Linux, but we grade your score in Linux (CentOS 7).
  - **C: gcc 4.8.5**
  - **Python: Python 2 (>=2.7.5) or Python 3 (>=3.5.2)**
- 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**

Directions

- **This is an <u>individual</u> project**
- **You should follow the file/output format**
- You can test your code with...
  - Postman ➔ A chrome extension of GET/POST request
  - libcurl ➔ curl –Is http://hello.com
  - wget ➔ wget –p http://world.com –O /dev/null
- The example of ***Deliverables*** is available on YSCEC Project page.

Due Date / Delay Policy

- **DUE DATE**

  3/Oct/2016 23:55:00 KST

- **Delay Policy**

  -10pts per day

Remember...

- **DO NOT COPY CODE**
  - We run Code-plagiarism Program.
  - The fastest way to get 0 points.
- **YOU WILL GET 0 POINTS if you CHEAT**

Score Policy ***(*tentative)***

Maximum Score = 100+10 pts

1	Not submitted or not working or missing files	**0 pts**
2	Overdue → Delay	**-10pts/day**
3	Only one of Request/Response is working	-40 pts
4	Additional assignment is implemented	+10 pts
5	Bad display formatting	-10 pts
6	IP address or Port number is not correct	-20 pts
7	**Scapy or 3rd party framework is used**	**0 pts**

Please use YSCEC Q&A board to leave your question.