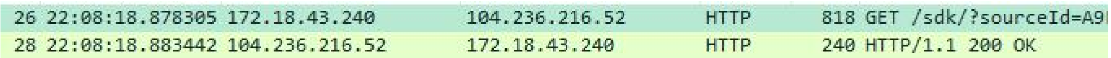
Xueyang (Sean) Wang
XW1154
02/05/2017
CS4793
Homework 01

1.
Some different protocols that appear in the protocol column in the unfiltered packet-listing window are: **ARP, UDP, SSL, and TCP**.

2.
In less than a second **(~0.005 secs)**



```
26 22:08:18.878305 172.18.43.240      104.236.216.52      HTTP      818 GET /sdk/?sourceId=A9
28 22:08:18.883442 104.236.216.52     172.18.43.240       HTTP      240 HTTP/1.1 200 OK
```

Fig. 2 Screen-shot

3.
Based on figure 2, my IP address is **172.18.43.240** and the website IP address is **104.236.216.52**.

4.
GET information:

```
No.     Time                    Source                  Destination             Protocol Length Info
     26 22:08:18.878305       172.18.43.240           104.236.216.52          HTTP     818    GET /sdk/?sourceId=A9LZecYD-vHUZ-Tufp-hrmp-bxorCHy6KmCR&sessionId=e033d0ad-a175-7690-a2ef-45a2707e543b&type=stats&userId=82622ff0-9278-fd01-c3bf-2e86ef41b60e&version=1.1.8&openerTabId=1638&tabId=1758&referrer=&fingerprint=97255916&events=JTVCJTVCJTIyaHR0cCUzQSUyRiUyRmdhaWEuY3MudW1hc3MuZWR1JTJGd2lyZXNoYXJrLWxhYnMlMkZJTlRSTy13aXJlc2hhcmstZmlsZTEuaHRtbCUyMiUyQzE0ODYzNTA0OTg3ODQuNjA3JTJDMTQ4NjM1MDQ5ODc4NS42NjYlMkMyMDAlNUQlNUQ%3D&requestType=main_frame&transitionType=link&transitionQualifiers= HTTP/1.1

Frame 26: 818 bytes on wire (6544 bits), 818 bytes captured (6544 bits) on interface 0
Ethernet II, Src: IntelCor_79:6a:e9 (ac:fd:ce:79:6a:e9), Dst: IETF-VRRP-VRID_53 (00:00:5e:00:01:53)
Internet Protocol Version 4, Src: 172.18.43.240, Dst: 104.236.216.52
Transmission Control Protocol, Src Port: 53894, Dst Port: 80, Seq: 1, Ack: 1, Len: 764
Hypertext Transfer Protocol
     [truncated]GET /sdk/?sourceId=A9LZecYD-vHUZ-Tufp-hrmp-bxorCHy6KmCR&sessionId=e033d0ad-a175-7690-a2ef-45a2707e543b&type=stats&userId=82622ff0-9278-fd01-c3bf-2e86ef41b60e&version=1.1.8&openerTabId=1638&tabId=1758&referrer=&fingerprint=97255
    Host: edatasales.com\r\n
    Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36\r\n
    Accept: */*\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8\r\n
    \r\n
    [Full request URI [truncated]: http://edatasales.com/sdk/?sourceId=A9LZecYD-vHUZ-Tufp-hrmp-bxorCHy6KmCR&sessionId=e033d0ad-a175-7690-a2ef-45a2707e543b&type=stats&userId=82622ff0-9278-fd01-c3bf-2e86ef41b60e&version=1.1.8&openerTabId=1638&tab]
    [HTTP request 1/1]
    [Response in frame: 28]
```

REPLY information:

```
No.     Time                    Source                  Destination             Protocol Length
Info
     28 22:08:18.883442     104.236.216.52          172.18.43.240           HTTP     240
HTTP/1.1 200 OK

Frame 28: 240 bytes on wire (1920 bits), 240 bytes captured (1920 bits) on interface 0
Ethernet II, Src: Cisco_bf:1e:40 (58:bf:ea:bf:1e:40), Dst: IntelCor_79:6a:e9 (ac:fd:ce:79:6a:e9)
Internet Protocol Version 4, Src: 104.236.216.52, Dst: 172.18.43.240
Transmission Control Protocol, Src Port: 80, Dst Port: 53894, Seq: 1, Ack: 765, Len: 186
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Server: nginx\r\n
    Date: Mon, 06 Feb 2017 03:08:15 GMT\r\n
    Content-Type: application/octet-stream\r\n
    Content-Length: 0\r\n
    Connection: keep-alive\r\n
    Content-Type: application/json\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.005137000 seconds]
    [Request in frame: 26]
```