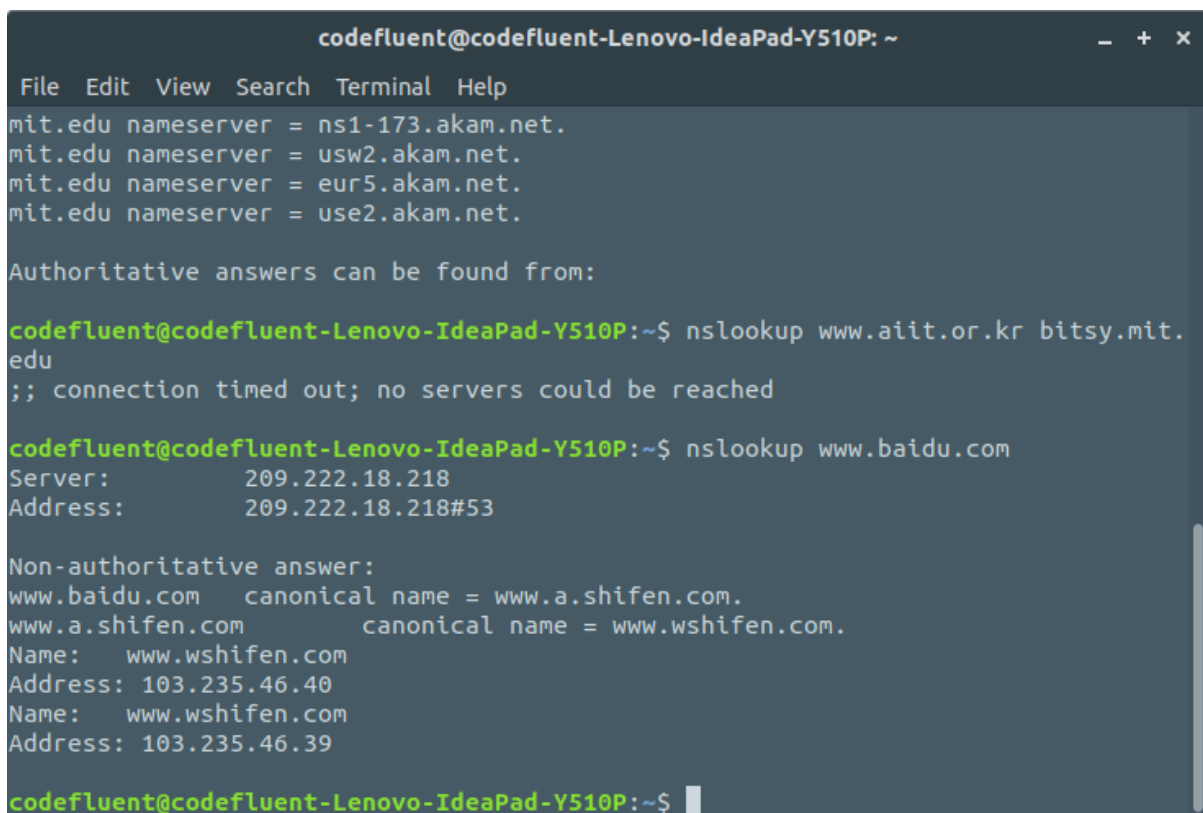


Section 1

1.
 - a. A vm is an important tool for a cyber security engineer in order to test, develop, and deploy code that protect systems that the engineer wishes to target.
 - b. A vm is important for a hacker in order to have a copy of his/her target that was found out in initial recon. A hacker will be able to use a vm to explore the best techniques for infiltration.

Section 2

2. The IP address of the baidu server is 103.235.46.39



```
codefluent@codefluent-Lenovo-IdeaPad-Y510P: ~  
File Edit View Search Terminal Help  
mit.edu nameserver = ns1-173.akam.net.  
mit.edu nameserver = usw2.akam.net.  
mit.edu nameserver = eur5.akam.net.  
mit.edu nameserver = use2.akam.net.  
  
Authoritative answers can be found from:  
  
codefluent@codefluent-Lenovo-IdeaPad-Y510P:~$ nslookup www.aait.or.kr bitsy.mit.  
edu  
;; connection timed out; no servers could be reached  
  
codefluent@codefluent-Lenovo-IdeaPad-Y510P:~$ nslookup www.baidu.com  
Server:      209.222.18.218  
Address:     209.222.18.218#53  
  
Non-authoritative answer:  
www.baidu.com canonical name = www.a.shifen.com.  
www.a.shifen.com canonical name = www.wshifen.com.  
Name:   www.wshifen.com  
Address: 103.235.46.40  
Name:   www.wshifen.com  
Address: 103.235.46.39  
  
codefluent@codefluent-Lenovo-IdeaPad-Y510P:~$
```

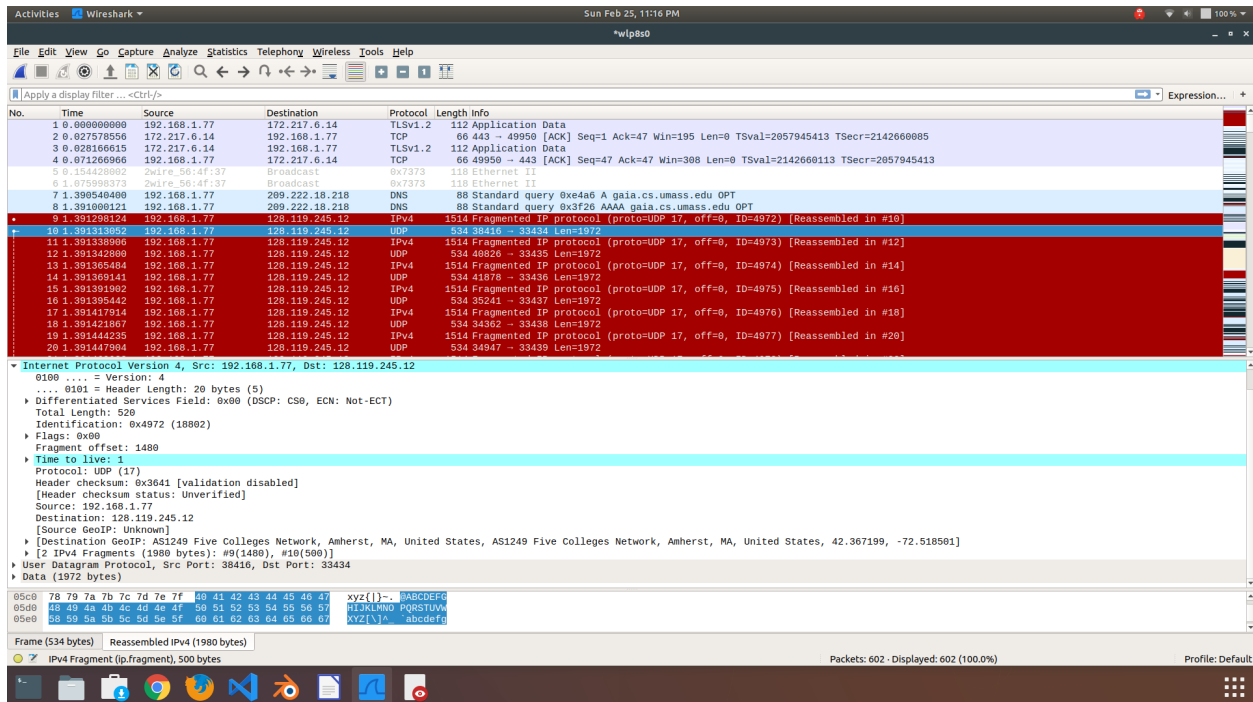
3. My DNS queries were sent to 209.222.18.222, which is indeed my local DNS server. I used “cat /etc/resolv.conf” find my local DNS server with “systemd-resolve -status”.

```
codefluent@codefluent-Lenovo-IdeaPad-Y510P:~$ cat /etc/resolv.conf
# This file is managed by man:systemd-resolved(8). Do not edit.
#
# 127.0.0.53 is the systemd-resolved stub resolver.
# run "systemd-resolve --status" to see details about the actual nameservers.
nameserver 127.0.0.53

search attlocal.net
codefluent@codefluent-Lenovo-IdeaPad-Y510P:~$ systemd-resolve --status
Global
DNS Servers: 209.222.18.222
              209.222.18.218
DNSSEC NTA: 10.in-addr.arpa
            16.172.in-addr.arpa
            168.192.in-addr.arpa
            17.172.in-addr.arpa
            18.172.in-addr.arpa
            19.172.in-addr.arpa
            20.172.in-addr.arpa
            21.172.in-addr.arpa
            22.172.in-addr.arpa
            23.172.in-addr.arpa
            24.172.in-addr.arpa
            25.172.in-addr.arpa
            26.172.in-addr.arpa
            27.172.in-addr.arpa
            28.172.in-addr.arpa
            29.172.in-addr.arpa
            30.172.in-addr.arpa
            31.172.in-addr.arpa
            corp
            d.f.in6.arpa
```

Section 4

4. The IP address of my computer is 192.168.1.77
5. The upper layer protocol field value is ICMP protocol.
6. 20 bytes in the IP header. There are 520 bytes for the total UDP length, so $520 - 20 = 500$ bytes for the payload.
7. Yes the IP datagram has been fragmented since there is a flag set to 0x01, meaning the IP was fragmented.



```
codefluent@codefluent-Lenovo-IdeaPad-Y510P: ~  
File Edit View Search Terminal Tabs Help  
codefluent@codefluent-Lenovo-IdeaPad-Y510P: ~  
codefluent@codefluent-Lenovo-IdeaPad-Y510P:~$ traceroute gaia.cs.umass.edu 56  
traceroute to gaia.cs.umass.edu (128.119.245.12), 30 hops max, 56 byte packets  
1 dslddevice (192.168.1.254) 13.988 ms 15.247 ms 15.238 ms  
2 172-125-252-1.lightspeed.tukrga.sbcglobal.net (172.125.252.1) 10.285 ms 16.547 ms 25.704 ms  
3 107.212.169.56 (107.212.169.56) 13.698 ms 14.914 ms 15.790 ms  
4 * * *  
5 12.83.82.161 (12.83.82.161) 24.676 ms 24.345 ms 12.83.82.165 (12.83.82.165) 24.308 ms  
6 12.122.141.233 (12.122.141.233) 24.649 ms 23.026 ms 20.237 ms  
7 ae15.edges5.atlanta2.level3.net (4.68.62.225) 18.759 ms 19.075 ms 18.307 ms  
8 * * *  
9 UNIVERSITY.ear3.NewYork1.Level3.net (4.71.230.234) 33.728 ms 42.918 ms 43.105 ms  
10 core2-rt-et-8-3-0.gw.umass.edu (192.80.83.113) 43.090 ms 35.092 ms 47.311 ms  
11 n5-rt-1-1-et-7-0-0.gw.umass.edu (128.119.0.10) 34.173 ms 34.928 ms 35.315 ms  
12 cics-rt-xe-0-0-0.gw.umass.edu (128.119.3.32) 44.898 ms 47.261 ms 47.251 ms  
13 nscs1bb51.cs.umass.edu (128.119.240.253) 47.241 ms 47.232 ms 40.790 ms  
14 gaia.cs.umass.edu (128.119.245.12) 39.393 ms !X 39.995 ms !X 42.032 ms !X  
codefluent@codefluent-Lenovo-IdeaPad-Y510P:~$ traceroute gaia.cs.umass.edu 2000  
traceroute to gaia.cs.umass.edu (128.119.245.12), 30 hops max, 2000 byte packets  
1 dslddevice (192.168.1.254) 14.562 ms 14.924 ms 14.913 ms  
2 172-125-252-1.lightspeed.tukrga.sbcglobal.net (172.125.252.1) 113.433 ms 117.383 ms 117.385 ms  
3 107.212.169.56 (107.212.169.56) 58.242 ms 60.195 ms 60.246 ms  
4 * * *  
5 12.83.82.161 (12.83.82.161) 61.693 ms 65.681 ms 65.681 ms  
6 12.122.141.233 (12.122.141.233) 67.171 ms 51.838 ms 51.741 ms  
7 ae15.edges5.atlanta2.level3.net (4.68.62.225) 51.677 ms 13.581 ms 12.687 ms  
8 ae-1-3501.ear3.NewYork1.Level3.net (4.69.150.202) 30.896 ms 32.487 ms 31.278 ms  
9 UNIVERSITY.ear3.NewYork1.Level3.net (4.71.230.234) 36.971 ms 35.973 ms 35.955 ms  
10 core2-rt-et-8-3-0.gw.umass.edu (192.80.83.113) 41.476 ms 41.472 ms 36.986 ms  
11 n5-rt-1-1-et-7-0-0.gw.umass.edu (128.119.0.10) 35.310 ms 38.802 ms 36.043 ms  
12 cics-rt-xe-0-0-0.gw.umass.edu (128.119.3.32) 70.291 ms 67.889 ms 67.453 ms  
13 * * *  
14 gaia.cs.umass.edu (128.119.245.12) 64.559 ms !X 64.560 ms !X 59.624 ms !X  
codefluent@codefluent-Lenovo-IdeaPad-Y510P:~$
```