Trace one:

```
austin@kali:~$ traceroute www.cmu.edu
traceroute to www.cmu.edu (128.2.42.52), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  1.018 ms  0.978 ms  0.954 ms
 2  10.0.0.1 (10.0.0.1)  7.341 ms  8.137 ms  9.719 ms
 3  100.76.169.1 (100.76.169.1)  26.871 ms  27.714 ms  27.906 ms
 4  po-302-1210-rur02.spokane.wa.seattle.comcast.net (68.85.145.197)  27.332 ms  32.413 ms
32.554 ms
 5  be-37-ar01.seattle.wa.seattle.comcast.net (68.86.96.5)  47.649 ms  47.495 ms  48.446 ms
 6  be-33650-cr01.seattle.wa.ibone.comcast.net (68.86.93.165)  46.325 ms  23.754 ms  30.503 ms
 7  be-10820-cr01.champa.co.ibone.comcast.net (68.86.84.206)  65.626 ms  62.166 ms  61.656 ms
 8  be-12021-cr02.1601milehigh.co.ibone.comcast.net (68.86.84.226)  65.547 ms  65.635 ms
65.271 ms
 9  be-10521-cr02.350ecermak.il.ibone.comcast.net (68.86.85.169)  94.484 ms  94.622 ms  94.770
ms
10  be-1402-cs04.350ecermak.il.ibone.comcast.net (96.110.36.109)  94.196 ms  99.659 ms  98.755
ms
11  be-1414-cr14.350ecermak.il.ibone.comcast.net (96.110.35.62)  99.781 ms  99.961 ms  80.038
ms
12  be-301-cr12.pittsburgh.pa.ibone.comcast.net (96.110.39.158)  98.022 ms  98.201 ms  95.272
ms
13  be-1412-cs04.pittsburgh.pa.ibone.comcast.net (96.110.38.157)  95.154 ms  95.947 ms
102.428 ms
14  be-1311-cr11.pittsburgh.pa.ibone.comcast.net (96.110.38.138)  91.915 ms
be-1111-cr11.pittsburgh.pa.ibone.comcast.net (96.110.38.130)  95.198 ms
be-1411-cr11.pittsburgh.pa.ibone.comcast.net (96.110.38.142)  94.988 ms
15  be-302-cr12.ashburn.va.ibone.comcast.net (96.110.32.101)  100.078 ms  107.078 ms  94.882
ms
16  be-1212-cs02.ashburn.va.ibone.comcast.net (96.110.32.205)  100.067 ms
be-1112-cs01.ashburn.va.ibone.comcast.net (96.110.32.201)  99.350 ms
be-1312-cs03.ashburn.va.ibone.comcast.net (96.110.32.209)  99.616 ms
17  be-1202-cr02.ashburn.va.ibone.comcast.net (96.110.32.174)  103.455 ms
be-1302-cr02.ashburn.va.ibone.comcast.net (96.110.32.178)  102.995 ms
be-1402-cr02.ashburn.va.ibone.comcast.net (96.110.32.182)  108.309 ms
18  be-7922-ar01.mckeesport.pa.pitt.comcast.net (68.86.91.26)  112.255 ms  112.020 ms  116.068
ms
19  96.108.91.122 (96.108.91.122)  100.839 ms  104.619 ms  104.874 ms
20  96.108.91.77 (96.108.91.77)  104.164 ms  108.776 ms 69.139.195.158 (69.139.195.158)
109.856 ms
21  te-8-1-ur01.stclairsvill.oh.pitt.comcast.net (68.86.100.25)  110.073 ms 162.151.152.154
(162.151.152.154)  109.465 ms  108.383 ms
22  50-202-216-186-static.hfc.comcastbusiness.net (50.202.216.186)  107.102 ms  107.325 ms
111.366 ms
23  CORE0-POD-I-CYH.GW.CMU.NET (128.2.0.249)  112.116 ms  112.297 ms  117.784 ms
24  POD-D-CYH-CORE0.GW.CMU.NET (128.2.0.202)  118.256 ms  102.265 ms  106.364 ms
25  WWW-CMU-PROD-VIP.ANDREW.CMU.EDU (128.2.42.52)  106.109 ms  105.829 ms  110.971 ms
austin@kali:~$ date
Mon 06 Apr 2020 12:57:38 PM PDT
austin@kali:~$ ping www.cmu.edu
PING WWW.R53.cmu.edu (128.2.42.52) 56(84) bytes of data.
64 bytes from WWW-CMU-PROD-VIP.ANDREW.CMU.EDU (128.2.42.52): icmp_seq=1 ttl=63 time=102 ms
64 bytes from WWW-CMU-PROD-VIP.ANDREW.CMU.EDU (128.2.42.52): icmp_seq=2 ttl=63 time=107 ms
64 bytes from WWW-CMU-PROD-VIP.ANDREW.CMU.EDU (128.2.42.52): icmp_seq=3 ttl=63 time=113 ms
64 bytes from WWW-CMU-PROD-VIP.ANDREW.CMU.EDU (128.2.42.52): icmp_seq=4 ttl=63 time=108 ms
64 bytes from WWW-CMU-PROD-VIP.ANDREW.CMU.EDU (128.2.42.52): icmp_seq=5 ttl=63 time=104 ms
64 bytes from WWW-CMU-PROD-VIP.ANDREW.CMU.EDU (128.2.42.52): icmp_seq=6 ttl=63 time=104 ms
64 bytes from WWW-CMU-PROD-VIP.ANDREW.CMU.EDU (128.2.42.52): icmp_seq=7 ttl=63 time=103 ms
```

```
64 bytes from WWW-CMU-PROD-VIP.ANDREW.CMU.EDU (128.2.42.52): icmp_seq=8 ttl=63 time=103 ms
^C
--- WWW.R53.cmu.edu ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7074ms
rtt min/avg/max/mdev = 102.206/105.513/113.348/3.510 ms
austin@kali:~$
```

Trace two:

```
austin@kali:~$ traceroute cmu.edu
traceroute to cmu.edu (128.2.42.10), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  0.294 ms  0.246 ms  0.221 ms
 2  10.0.0.1 (10.0.0.1)  11.031 ms  11.160 ms  11.227 ms
 3  100.76.169.1 (100.76.169.1)  25.681 ms  27.495 ms  27.933 ms
 4  po-302-1210-rur02.spokane.wa.seattle.comcast.net (68.85.145.197)  27.593 ms  28.173 ms
28.381 ms
 5  be-37-ar01.seattle.wa.seattle.comcast.net (68.86.96.5)  35.802 ms  35.960 ms  36.402 ms
 6  be-33650-cr01.seattle.wa.ibone.comcast.net (68.86.93.165)  40.317 ms  22.058 ms  25.852 ms
 7  be-10820-cr01.champa.co.ibone.comcast.net (68.86.84.206)  63.940 ms  61.720 ms  65.225 ms
 8  be-12021-cr02.1601milehigh.co.ibone.comcast.net (68.86.84.226)  66.501 ms  66.041 ms
65.381 ms
 9  be-10521-cr02.350ecermak.il.ibone.comcast.net (68.86.85.169)  96.411 ms  96.102 ms  96.058
ms
10  be-1202-cs02.350ecermak.il.ibone.comcast.net (96.110.36.101)  91.279 ms  99.160 ms  99.450
ms
11  be-1214-cr14.350ecermak.il.ibone.comcast.net (96.110.35.54)  99.491 ms  99.729 ms  80.423
ms
12  be-302-cr12.pittsburgh.pa.ibone.comcast.net (96.110.39.162)  92.413 ms
be-301-cr12.pittsburgh.pa.ibone.comcast.net (96.110.39.158)  98.590 ms  93.853 ms
13  be-1312-cs03.pittsburgh.pa.ibone.comcast.net (96.110.38.153)  97.928 ms  97.395 ms
be-1212-cs02.pittsburgh.pa.ibone.comcast.net (96.110.38.149)  97.237 ms
14  be-1411-cr11.pittsburgh.pa.ibone.comcast.net (96.110.38.142)  92.796 ms
be-1311-cr11.pittsburgh.pa.ibone.comcast.net (96.110.38.138)  91.555 ms
be-1211-cr11.pittsburgh.pa.ibone.comcast.net (96.110.38.134)  98.337 ms
15  be-301-cr12.ashburn.va.ibone.comcast.net (96.110.39.165)  102.881 ms  102.583 ms  108.294
ms
16  be-1212-cs02.ashburn.va.ibone.comcast.net (96.110.32.205)  107.315 ms
be-1112-cs01.ashburn.va.ibone.comcast.net (96.110.32.201)  107.950 ms
be-1312-cs03.ashburn.va.ibone.comcast.net (96.110.32.209)  107.563 ms
17  be-1202-cr02.ashburn.va.ibone.comcast.net (96.110.32.174)  96.537 ms  101.895 ms
be-1102-cr02.ashburn.va.ibone.comcast.net (96.110.32.170)  101.388 ms
18  be-7922-ar01.mckeesport.pa.pitt.comcast.net (68.86.91.26)  106.308 ms  109.771 ms  108.905
ms
19  96.108.91.122 (96.108.91.122)  109.242 ms  111.904 ms  101.028 ms
20  69.139.195.158 (69.139.195.158)  106.112 ms 96.108.91.77 (96.108.91.77)  105.017 ms
105.228 ms
21  162.151.152.154 (162.151.152.154)  110.153 ms te-8-1-ur01.stclairsvill.oh.pitt.comcast.net
(68.86.100.25)  110.548 ms  110.644 ms
22  50-202-216-186-static.hfc.comcastbusiness.net (50.202.216.186)  117.199 ms  102.641 ms
105.656 ms
23  CORE0-POD-I-CYH.GW.CMU.NET (128.2.0.249)  106.422 ms  106.178 ms  110.469 ms
24  POD-D-CYH-CORE0.GW.CMU.NET (128.2.0.202)  111.106 ms  110.758 ms  112.939 ms
25  CMU-VIP.ANDREW.CMU.EDU (128.2.42.10)  102.598 ms  107.358 ms  107.469 ms
austin@kali:~$ ping cmu.edu
PING cmu.edu (128.2.42.10) 56(84) bytes of data.
64 bytes from CMU-VIP.ANDREW.CMU.EDU (128.2.42.10): icmp_seq=2 ttl=63 time=103 ms
64 bytes from CMU-VIP.ANDREW.CMU.EDU (128.2.42.10): icmp_seq=3 ttl=63 time=103 ms
64 bytes from CMU-VIP.ANDREW.CMU.EDU (128.2.42.10): icmp_seq=4 ttl=63 time=99.1 ms
```

```
64 bytes from CMU-VIP.ANDREW.CMU.EDU (128.2.42.10): icmp_seq=5 ttl=63 time=98.3 ms
64 bytes from CMU-VIP.ANDREW.CMU.EDU (128.2.42.10): icmp_seq=6 ttl=63 time=99.0 ms
64 bytes from CMU-VIP.ANDREW.CMU.EDU (128.2.42.10): icmp_seq=7 ttl=63 time=99.2 ms
64 bytes from CMU-VIP.ANDREW.CMU.EDU (128.2.42.10): icmp_seq=8 ttl=63 time=97.3 ms
64 bytes from CMU-VIP.ANDREW.CMU.EDU (128.2.42.10): icmp_seq=10 ttl=63 time=98.9 ms
^C
--- cmu.edu ping statistics ---
10 packets transmitted, 8 received, 20% packet loss, time 9090ms
rtt min/avg/max/mdev = 97.284/99.830/103.485/2.150 ms
austin@kali:~$ date
Tue 07 Apr 2020 09:06:33 AM PDT
austin@kali:~$
```

Trace Three:

```
austin@kali:~$ traceroute cmu.edu
traceroute to cmu.edu (128.2.42.10), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  0.144 ms  0.060 ms  0.157 ms
 2  10.0.0.1 (10.0.0.1)  9.531 ms  10.251 ms  10.781 ms
 3  100.76.169.1 (100.76.169.1)  27.835 ms  36.535 ms  28.377 ms
 4  po-302-1210-rur02.spokane.wa.seattle.comcast.net (68.85.145.197)  36.963 ms  36.856 ms
36.830 ms
 5  be-37-ar01.seattle.wa.seattle.comcast.net (68.86.96.5)  36.620 ms  38.563 ms  39.503 ms
 6  be-33650-cr01.seattle.wa.ibone.comcast.net (68.86.93.165)  42.913 ms  27.719 ms  33.221 ms
 7  be-10820-cr01.champa.co.ibone.comcast.net (68.86.84.206)  71.929 ms  64.914 ms  64.953 ms
 8  be-12021-cr02.1601milehigh.co.ibone.comcast.net (68.86.84.226)  64.184 ms  98.896 ms
108.904 ms
 9  be-10521-cr02.350ecermak.il.ibone.comcast.net (68.86.85.169)  126.745 ms  127.630 ms
131.624 ms
10  be-1202-cs02.350ecermak.il.ibone.comcast.net (96.110.36.101)  131.431 ms  131.380 ms
131.356 ms
11  be-1214-cr14.350ecermak.il.ibone.comcast.net (96.110.35.54)  135.847 ms  135.408 ms
82.944 ms
12  be-302-cr12.pittsburgh.pa.ibone.comcast.net (96.110.39.162)  96.861 ms  96.756 ms
be-301-cr12.pittsburgh.pa.ibone.comcast.net (96.110.39.158)  96.119 ms
13  be-1112-cs01.pittsburgh.pa.ibone.comcast.net (96.110.38.145)  99.285 ms  98.807 ms
be-1312-cs03.pittsburgh.pa.ibone.comcast.net (96.110.38.153)  97.537 ms
14  be-1111-cr11.pittsburgh.pa.ibone.comcast.net (96.110.38.130)  98.602 ms  100.101 ms
be-1411-cr11.pittsburgh.pa.ibone.comcast.net (96.110.38.142)  92.775 ms
15  be-302-cr12.ashburn.va.ibone.comcast.net (96.110.32.101)  102.588 ms
be-301-cr12.ashburn.va.ibone.comcast.net (96.110.39.165)  102.764 ms  102.809 ms
16  be-1312-cs03.ashburn.va.ibone.comcast.net (96.110.32.209)  105.891 ms
be-1212-cs02.ashburn.va.ibone.comcast.net (96.110.32.205)  106.604 ms
be-1112-cs01.ashburn.va.ibone.comcast.net (96.110.32.201)  105.183 ms
17  be-1402-cr02.ashburn.va.ibone.comcast.net (96.110.32.182)  93.324 ms
be-1202-cr02.ashburn.va.ibone.comcast.net (96.110.32.174)  105.387 ms
be-1402-cr02.ashburn.va.ibone.comcast.net (96.110.32.182)  105.374 ms
18  be-7922-ar01.mckeesport.pa.pitt.comcast.net (68.86.91.26)  117.678 ms  120.720 ms  120.528
ms
19  96.108.91.122 (96.108.91.122)  121.020 ms  120.859 ms  106.534 ms
20  69.139.195.158 (69.139.195.158)  111.870 ms  111.918 ms 96.108.91.77 (96.108.91.77)
111.681 ms
21  162.151.152.154 (162.151.152.154)  118.742 ms  118.817 ms  118.724 ms
22  50-202-216-186-static.hfc.comcastbusiness.net (50.202.216.186)  123.215 ms * *
23  CORE0-POD-I-CYH.GW.CMU.NET (128.2.0.249)  120.907 ms  120.686 ms  125.798 ms
24  POD-D-CYH-CORE0.GW.CMU.NET (128.2.0.202)  125.867 ms  127.227 ms  126.830 ms
25  CMU-VIP.ANDREW.CMU.EDU (128.2.42.10)  102.362 ms  120.543 ms  119.221 ms
austin@kali:~$ ping cmu.edu
```

```
PING cmu.edu (128.2.42.10) 56(84) bytes of data.
64 bytes from CMU-VIP.ANDREW.CMU.EDU (128.2.42.10): icmp_seq=1 ttl=63 time=107 ms
64 bytes from CMU-VIP.ANDREW.CMU.EDU (128.2.42.10): icmp_seq=2 ttl=63 time=105 ms
64 bytes from CMU-VIP.ANDREW.CMU.EDU (128.2.42.10): icmp_seq=3 ttl=63 time=102 ms
64 bytes from CMU-VIP.ANDREW.CMU.EDU (128.2.42.10): icmp_seq=4 ttl=63 time=98.8 ms
64 bytes from CMU-VIP.ANDREW.CMU.EDU (128.2.42.10): icmp_seq=5 ttl=63 time=103 ms
64 bytes from CMU-VIP.ANDREW.CMU.EDU (128.2.42.10): icmp_seq=6 ttl=63 time=104 ms
64 bytes from CMU-VIP.ANDREW.CMU.EDU (128.2.42.10): icmp_seq=7 ttl=63 time=112 ms
^C
--- cmu.edu ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6011ms
rtt min/avg/max/mdev = 98.766/104.578/111.942/3.838 ms
austin@kali:~$ date
Mon 06 Apr 2020 08:45:20 PM PDT
austin@kali:~$
```

1.)
There are 25 routers in the path in all three runs. The path changed at the 13th hop for all three runs.

2.)
It appears that the packets only pass through two ISPs through the whole route (Comcast.net and CMU.net)

3.)
It took about 3-5 seconds to complete the traceroute. The reason it was so much longer than indicated by ping is because ping just takes the time to get to the final destination and back, but traceroute essentially pings each router along the way and there are 25 stops. Also traceroute can have timeouts along the way.

4.)
The relationship between ping and traceroute is that both send packets to a server to check the round trip times, but traceroute checks the rtt of every stop along the way.

5.)
Yes, I get the same three intermediate machines

```
austin@kali:~$ for i in {1..3}; do ping -t $i -c 1 google.com; done | grep "Time to
live exceeded"
From 10.0.2.2 (10.0.2.2) icmp_seq=1 Time to live exceeded
From 10.0.0.1 (10.0.0.1) icmp_seq=1 Time to live exceeded
From 100.76.169.1 (100.76.169.1) icmp_seq=1 Time to live exceeded
```

6.)
The question (or query) section displays the queried input from the user, the default record for input is A. The answer section displays the returned value from the query, in most cases the A record. The authority section displays the DNS name server that has the authority to responed

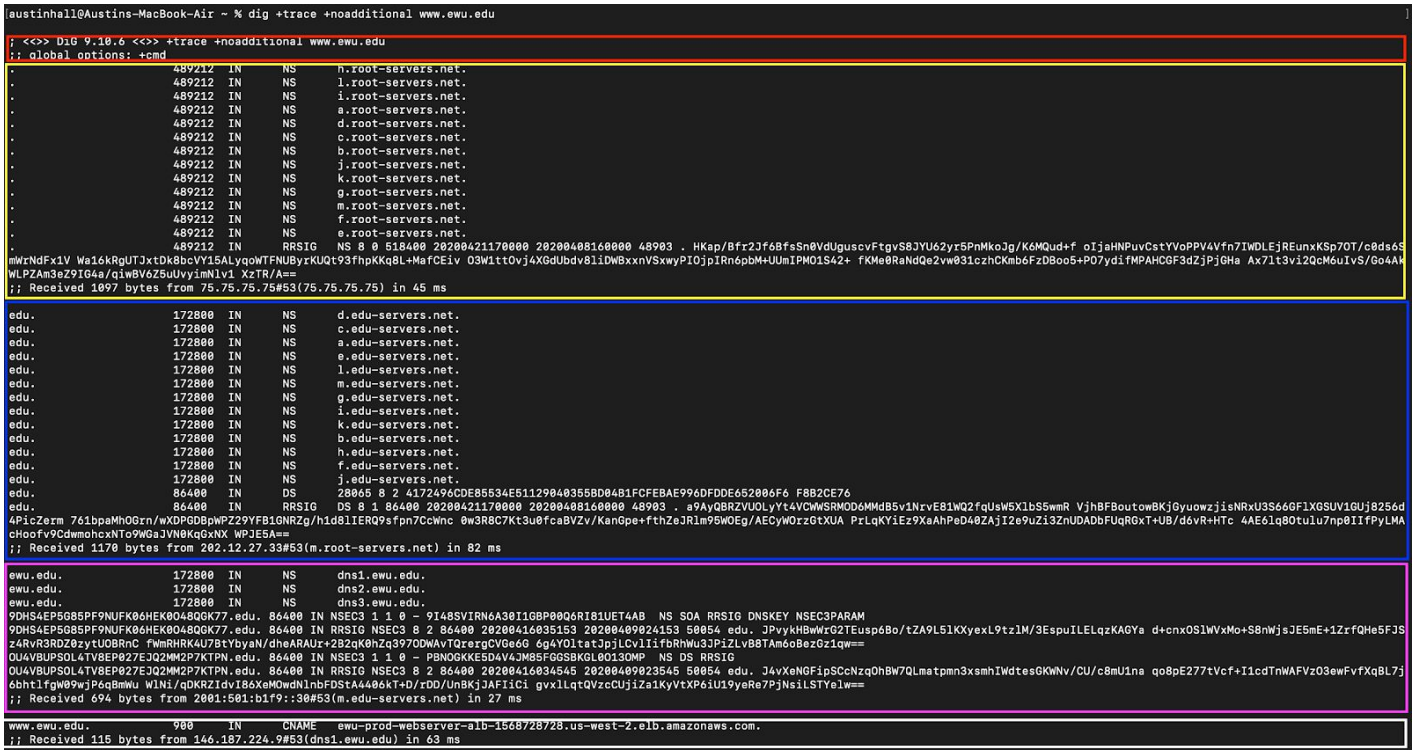
to this query, the available name servers of the requested address. The Additional section displays the IP addresses of the name servers listed in the authority section.

7.)
-q

8.)
-x is a simplified reverse lookup. The same query can be achieved with nslookup (example below). This works because both search a DNS library to resolve the hostname. It does not work for every IP address because some IP addresses don't have a PTR record associated with it (not all IP addresses have a reverse entry).

```
austin@kali:~$ dig -x 172.217.3.206

; <<>> DiG 9.11.16-2-Debian <<>> -x 172.217.3.206
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59041
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;206.3.217.172.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
206.3.217.172.in-addr.arpa. 11480 IN    PTR     sea15s12-in-f206.1e100.net.
206.3.217.172.in-addr.arpa. 11480 IN    PTR     sea15s12-in-f14.1e100.net.

;; Query time: 32 msec
;; SERVER: 75.75.75.75#53(75.75.75.75)
;; WHEN: Mon Apr 06 19:58:30 PDT 2020
;; MSG SIZE  rcvd: 125

austin@kali:~$ nslookup 172.217.3.206
206.3.217.172.in-addr.arpa      name = sea15s12-in-f206.1e100.net.
206.3.217.172.in-addr.arpa      name = sea15s12-in-f14.1e100.net.

Authoritative answers can be found from:

austin@kali:~$
```

9.)



In the red section the version of dig that's installed is displayed along with the keywords and the domain to be queried. The next line shows the global options set, which in this case is cmd.
In the yellow section there is the first step of the trace that starts at the root servers. There is a . at the beginning of each line to show what part of the domain name is being searched. Then the ttl, the class (IN is internet) the record (NS is name server), then the server name is shown. Then the RRSIG (DNSSEC signature) is shown which is the signature for a DNSSEC-secured record set. It specifies the name, ttl, resource record type, NS is the type covered field, 8 identifies the algorithm used, 0 is the number of labels in originial owners name, 518400 is the original ttl, the next two long numbers are the expiration and inception date, 48903 is the key tag, the remaining text is base64 encoding of the signature. The next comment shows the amount of information recieved from a DNS search, the rtt, and the ip address of this server.
In the Blue section there is the second step of the traceroute that carries on from the previous step, the root server returns the top level domain edu. The next several lines display the same kind of information as the yellow section until we the DS (delegation signer) is shown which is the record used to identify the DNSSEC signing key of a delegated zone. This has the same kind of info as the RRSIG except no type covered field and the final hex numbers are the digest. The following comment shows the amount of info recieved from a random root server chosen, its IP, and the rtt.
The Pink section is similar to the previous two, except now we have the domain name of ewu and its servers. It has hex info of the server name, and more information relating to the previous sections. The comment shows the data size revieved and the ip address of the edu server.

Finally in the white section we are shown the domain www.ewu.edu, the ttl, class, record (which is the cname), and the canonical name. Then, the final line is a comment showing the amount recieved and the name server used to resolve the cname.

Cname is the canonical name or alias record. It specifies that one domain name is an alias for another name. The benefit of this is that we can have multiple domain names that point to the same cname that then points to the correct server IP. The major advantage of using Cname is that if we change the IP address of one A record then any Cname record pointing to that host will also change.

10.)
African Network Coordination Centre (AFRINIC): Africa
Asia-Pacific Network Coordination Centre (APNIC): Asia- pacific
American Registry for Internet Numbers (ARIN): United States, Canada, many Caribbean and North Atlantic islands
Latin American and Caribbean Internet Addresses Registry (LACNIC): Latin America and the Caribbean
Réseaux IP Européens Network Coordination Centre (RIPE NCC): Europe, the Middle East and parts of Central Asia

11.)
AFRINIC:
whois.ripe.net
whois.nic.st
whois.nic.so
whois.nic.sn
whois.nic.mu
whois.nic.mg
whois.nic.ly
whois.nic.ci
whois.nic.bj
whois.na-nic.com.na
whois.kenic.or.ke
whois.iam.net.ma
Whois.co.ug

APNIC:
whois.worldsite.ws
whois.website.ws
whois.worldnames.net
whois.nic.nu
whois.twnic.net
whois.twnic.net.tw
whois.tonic.to
whois.thnic.net
whois.nic.yt
whois.nic.wf
whois.nic.tl

whois.nic.net.sb
whois.nic.mn
whois.nic.la
whois.nic.ki
whois.nic.io
Whois.nic.fr
whois.nic.re
whois.nic.cx
whois.nic.as
whois.nic.af
whois.mynic.net.my
whois.krnic.net
whois.nic.or.kr
whois.kcce.kp
whois.jprs.jp
whois.inregistry.net
whois.hkdnr.net.hk
whois.hkirc.hk
whois.dot.tk
whois.cnnic.net.cn
whois.ck-nic.org.ck
whois.ausregistry.net
tvwhois.verisign-grs.com
srs-ak.srs.net.nz
whois.srs.net.nz
eos.nic.net.sg
whois.nic.net.sg
Ccwhois.verisign-grs.com

ARIN:
whois2.afilias-grs.net
whois.nic.ag
whois2.afilias-grs.net
whois.nic.us
whois.nic.sh
whois.nic.pr
whois.nic.pm
whois.nic.ms
whois.nic.dm
whois.dotgov.gov
whois.cira.ca
whois.ai
whois.adamsnames.tc
whois.adamsnames.tc
whois.adamsnames.com
Webhost1.capital.hm

LACNIC:
whois2.afilias-grs.net
whois.registry.gy
whois.nic.ve
whois.nic.org.uy
whois.nic.mx
whois.nic.ht

whois.nic.ec
whois.nic.br
whois.nic.bo
whois.cocca.cx
whois.nic.gs
ns.nic.do
nic.cl
whois.nic.cl
kero.yachay.pe
bzwhois.verisign-grs.co

RIPE NCC:
www.whois.lt
whois.domreg.lt
www.register.bg
whois.register.bg
www.nic.tr
whois.nic.tr
whois2.afilias-grs.net
whois01.prod.iis.se
whois.iis.se
whois.sk-nic.sk
whois.rotld.ro
whois.rnids.rs
whois.ripn.net
whois.ripe.net
whois.nic.lv
whois.norid.no
whois.nic.uk
whois.nic.tm
whois.nic.md
whois.nic.kz
whois.nic.it
whois.nic.ir
whois.nic.im
whois.nic.hu
whois.nic.fr
whois.nic.cz
whois.nic.ch
whois.nic.li
whois.nic.ch
whois.nic.at
whois.net.ua
whois.meregistry.net
whois.je
whois.gg
whois.ficora.fi
whois.eu
whois.domainregistry.ie

whois.domain.kg
whois.domain-registry.nl
whois.dns.pl
whois.dns.lu
whois.dns.be
whois.denic.de
whois.cctld.uz
whois.cctld.by
whois.arnes.si
whois.amnic.net
whois.ai
whois.aeda.net.ae
vocal.dk-hostmaster.dk
whois.dk-hostmaster.dk
register.isoc.org.il
whois.isoc.org.il
nic.net.sa
whois.saudinic.net.sa
myristaja.eenet.ee
whois.eenet.ee
min.isnic.is
whois.isnic.is
hercules.dns.pt
whois.dns.pt
online.dns.pt

12.)
The command to use is -s. It may be necessary to use this command when the domain being looked up has an ambiguous location.

13.)
The default local DNS server is 146.187.224.191
dig ewu.edu

```
; <<>> DiG 9.11.16-2-Debian <<>> ewu.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7961
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;ewu.edu.                       IN      A

;; ANSWER SECTION:
ewu.edu.                1800    IN      A       146.187.224.191

;; Query time: 55 msec
;; SERVER: 75.75.75.75#53(75.75.75.75)
;; WHEN: Tue Apr 07 03:26:31 PDT 2020
```

```
;; MSG SIZE  rcvd: 52
```

14.)

dig (no arguments)

The names are on the left column and IP addresses on the right

```
m.root-servers.net.     375027  IN      A       202.12.27.33
b.root-servers.net.     407612  IN      A       199.9.14.201
c.root-servers.net.     452230  IN      A       192.33.4.12
d.root-servers.net.     474263  IN      A       199.7.91.13
e.root-servers.net.     433841  IN      A       192.203.230.10
f.root-servers.net.     429611  IN      A       192.5.5.241
g.root-servers.net.     434329  IN      A       192.112.36.4
h.root-servers.net.     401843  IN      A       198.97.190.53
i.root-servers.net.     396813  IN      A       192.36.148.17
a.root-servers.net.     374957  IN      A       198.41.0.4
j.root-servers.net.     406815  IN      A       192.58.128.30
k.root-servers.net.     424644  IN      A       193.0.14.129
l.root-servers.net.     396096  IN      A       199.7.83.42
```

15.)

dig 8.8.4.4

```
; <<>> DiG 9.11.16-2-Debian <<>> 8.8.4.4
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 13039
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;8.8.4.4.                       IN      A

;; AUTHORITY SECTION:
.                       10800   IN      SOA     a.root-servers.net.
nstld.verisign-grs.com. 2020040701 1800 900 604800 86400

;; Query time: 47 msec
;; SERVER: 75.75.75.75#53(75.75.75.75)
```

```
;; WHEN: Tue Apr 07 11:06:14 PDT 2020
;; MSG SIZE  rcvd: 111
```

Based on this information, I can make an educated guess that this is google's DNS server

16.)
The hostname of the default nameserver is cdns01.comcast.net

```
austin@kali:~$ dig ewu.edu

; <<>> DiG 9.11.16-2-Debian <<>> ewu.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24942
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;ewu.edu.                       IN      A

;; ANSWER SECTION:
ewu.edu.                1800    IN      A       146.187.224.191

;; Query time: 54 msec
;; SERVER: 75.75.75.75#53(75.75.75.75)
;; WHEN: Tue Apr 07 11:21:31 PDT 2020
;; MSG SIZE  rcvd: 52



austin@kali:~$ dig -x 75.75.75.75

; <<>> DiG 9.11.16-2-Debian <<>> -x 75.75.75.75
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58443
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;75.75.75.75.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
75.75.75.75.in-addr.arpa. 6787  IN      PTR     cdns01.comcast.net.

;; Query time: 30 msec
```

```
;; SERVER: 75.75.75.75#53(75.75.75.75)
;; WHEN: Tue Apr 07 11:21:55 PDT 2020
;; MSG SIZE  rcvd: 85
```

17.)

```
austin@kali:~$ dig +recurse @e.root-servers.net google.com

; <<>> DiG 9.11.16-2-Debian <<>> +recurse @e.root-servers.net google.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64601
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 27
;; WARNING: recursion requested but not available
```

When adding the +recurse option and requesting a response from a root name server, there is a warning that recursion is not available and isn't done. This is because the root server doesn't have anything to recursively search through, it's the search result/ the beginning of the search and all searches begin with it.

18.)

```
austin@kali:~$ whois beer
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

domain:       BEER

organisation: Minds + Machines Group Limited
address:      Craigmuir Chambers, Road Town Tortola VG 1110
address:      Virgin Islands, British

contact:      administrative
name:         Admin Contact
organisation: Minds + Machines Ltd
address:      32 Nassau St, Dublin 2
address:      Ireland
phone:        +1-877-734-4783
e-mail:       ops@mmx.co

contact:      technical
name:         TLD Registry Services Technical
organisation: Nominet
address:      Minerva House,
address:      Edmund Halley Road,
address:      Oxford Science Park,
address:      Oxford,
```

```
address:        OX4 4DQ
address:        United Kingdom
phone:          +44.1865332211
e-mail:         registrytechnical@nominet.uk

nserver:        DNS1.NIC.BEER 213.248.217.15 2a01:618:401:0:0:0:0:15
nserver:        DNS2.NIC.BEER 103.49.81.15 2401:fd80:401:0:0:0:0:15
nserver:        DNS3.NIC.BEER 213.248.221.15 2a01:618:405:0:0:0:0:15
nserver:        DNS4.NIC.BEER 2401:fd80:405:0:0:0:0:15 43.230.49.15
nserver:        DNSA.NIC.BEER 156.154.100.3 2001:502:ad09:0:0:0:0:3
nserver:        DNSB.NIC.BEER 156.154.101.3
nserver:        DNSC.NIC.BEER 156.154.102.3
nserver:        DNSD.NIC.BEER 156.154.103.3
ds-rdata:       56125 8 2
C674B8966CB78A79E67A2ED674917CF39F96ED6C7E5460425C61EAFBAD7E2A87

whois:          whois.nic.beer
status:         ACTIVE
remarks:        Registration information: http://mm-registry.com

created:        2014-03-13
changed:        2019-08-22
source:         IANA
```

The TLD name servers for the .beer domain are in bold above. It is owned by Minds + Machines Group Limited. The technical point of contact is `name:TLD Registry Services Technical, organisation: Nominet.` Also shown in bold above.

19.)

Autonomous System Numbers are the registered addresses of an ISP to use the Autonomous System for use in BGP routing and uniquely identifies each network on the internet. The Autonomous System is a collection of connected IP routing prefixes controlled by an entity or organization that presents a clearly defined routing policy to the internet.

20.)

ASNumber 8 has OrgName: Rice University, OrgID: RICEUN, ASName: Rice-As, ASHandle: AS8

```
austin@kali:~$ whois as8
ASNumber:       8
ASName:         RICE-AS
ASHandle:       AS8
RegDate:        1984-03-26
Updated:        1997-11-10
Ref:            https://rdap.arin.net/registry/autnum/8
```

```
OrgName:        Rice University
OrgId:          RICEUN
Address:        Networking MS 119
Address:        6100 Main Street
City:           Houston
StateProv:      TX
PostalCode:     77005
Country:        US
RegDate:        1983-12-02
Updated:        2018-07-03
Ref:            https://rdap.arin.net/registry/entity/RICEUN


OrgAbuseHandle: RUH-ORG-ARIN
OrgAbuseName:   Rice University Networking
OrgAbusePhone:  +1-713-348-4989
OrgAbuseEmail:  ipadmin@rice.edu
OrgAbuseRef:    https://rdap.arin.net/registry/entity/RUH-ORG-ARIN

OrgTechHandle: RUH-ORG-ARIN
OrgTechName:   Rice University Networking
OrgTechPhone:  +1-713-348-4989
OrgTechEmail:  ipadmin@rice.edu
OrgTechRef:    https://rdap.arin.net/registry/entity/RUH-ORG-ARIN

RTechHandle: RUH-ORG-ARIN
RTechName:   Rice University Networking
RTechPhone:  +1-713-348-4989
RTechEmail:  ipadmin@rice.edu
RTechRef:    https://rdap.arin.net/registry/entity/RUH-ORG-ARIN
```

21.)

The IP address range for ewu is 146.187.0.0 to 146.187.255.255

```
austin@kali:~$ dig ewu.edu +short
146.187.224.191
austin@kali:~$ whois 146.187.224.191

NetRange:       146.187.0.0 - 146.187.255.255
CIDR:           146.187.0.0/16
NetName:        EWU
NetHandle:      NET-146-187-0-0-1
Parent:         NET146 (NET-146-0-0-0-0)
NetType:        Direct Assignment
OriginAS:       AS3935
Organization:   Eastern Washington University (EWU)
RegDate:        1991-02-25
Updated:        2017-04-19
Comment:        http://www.ewu.edu
Ref:            https://rdap.arin.net/registry/ip/146.187.0.0
```

…
…
…

22.)
The IP address is 146.187.134.27

```
austin@kali:~$ dig penguin.ewu.edu +short
146.187.134.27
```