Q1 DHCP

2 Points

Show the discover, offer, request, and acknowledge packets from a *single* DCHP transaction.

Q1.1 DHCP Discover

0.5 Points

Show the "Discover" packet sent by the client to try and find DHCP servers on the LAN. (Copy and paste or show a screenshot from `tcpdump`.)

```
02:19:14.087973 02:d7:34:b9:5b:a3 > ff:ff:ff:ff:ff:ff, ethertype IPv4 (0x0800), l
ength 342: (tos 0x10, ttl 128, id 0, offset 0, flags [none], proto UDP (17), lengt
h 328)
    0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 02:d7:34:
b9:5b:a3, length 300, xid 0x6ff6d07d, Flags [none]
          Client-Ethernet-Address 02:d7:34:b9:5b:a3
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
            DHCP-Message Option 53, length 1: Discover
            Hostname Option 12, length 8: "client-1"
            Parameter-Request Option 55, length 13:
              Subnet-Mask, BR, Time-Zone, Default-Gateway
              Domain-Name, Domain-Name-Server, Option 119, Hostname
              Netbios-Name-Server, Netbios-Scope, MTU, Classless-Static-Route
              NTP
```

discover.png Download

```
02:19:14.087973 02:d7:34:b9:5b:a3 > ff:ff:ff:ff:ff:ff, ethertype IPv4 (0x0800),
length 342: (tos 0x10, ttl 128, id 0, offset 0, flags [none], proto UDP (17), le
ngth 328)
    0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 02:d7:34:b9:5b:a3,
 length 300, xid 0x6ff6d07d, Flags [none]
          Client-Ethernet-Address 02:d7:34:b9:5b:a3
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
            DHCP-Message Option 53, length 1: Discover
            Hostname Option 12, length 8: "client-1"
            Parameter-Request Option 55, length 13:
              Subnet-Mask, BR, Time-Zone, Default-Gateway
              Domain-Name, Domain-Name-Server, Option 119, Hostname
              Netbios-Name-Server, Netbios-Scope, MTU, Classless-Static-Route
              NTP
```

What are the source and destination IP addresses in this request? Why are these addresses used?

The source IP address is 0.0.0.0 since the client doesn't have an IP address yet. The destination IP address is 255.255.255.255 since the client does n ot know the address of the DHCP server, so it uses the broadcast IP addres s.

Q1.2 DHCP Offer

0.5 Points

Show the "Offer" packet sent by the server. (Copy and paste or show a screenshot from `tcpdump`.)

02:19:17.095717 02:7c:1c:03:0e:72 > 02:d7:34:b9:5b:a3, ethertype IPv4 (0x0 800), length 342: (tos 0xc0, ttl 64, id 53507, offset 0, flags [none], proto UD P (17), length 328)

192.168.100.1.67 > 192.168.100.110.68: BOOTP/DHCP, Reply, length 300, xi d 0x6ff6d07d, Flags [none]

Your-IP 192.168.100.110

Server-IP 192.168.100.1

Client-Ethernet-Address 02:d7:34:b9:5b:a3

Vendor-rfc1048 Extensions

Magic Cookie 0x63825363

DHCP-Message Option 53, length 1: Offer

Server-ID Option 54, length 4: 192.168.100.1

Lease-Time Option 51, length 4: 14400

RN Option 58, length 4: 7200

RB Option 59, length 4: 12600

Subnet-Mask Option 1, length 4: 255.255.255.0

BR Option 28, length 4: 192.168.100.255
Domain-Name-Server Option 6, length 4: 192.168.100.1
Default-Gateway Option 3, length 4: 192.168.100.1

offer.png Download

```
02:19:17.095717 02:7c:1c:03:0e:72 > 02:d7:34:b9:5b:a3, ethertype IPv4 (0x0800),
length 342: (tos 0xc0, ttl 64, id 53507, offset 0, flags [none], proto UDP (17),
 length 328)
    192.168.100.1.67 > 192.168.100.110.68: BOOTP/DHCP, Reply, length 300, xid 0x
6ff6d07d, Flags [none]
          Your-IP 192.168.100.110
          Server-IP 192.168.100.1
          Client-Ethernet-Address 02:d7:34:b9:5b:a3
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
            DHCP-Message Option 53, length 1: Offer
            Server-ID Option 54, length 4: 192.168.100.1
            Lease-Time Option 51, length 4: 14400
            RN Option 58, length 4: 7200
            RB Option 59, length 4: 12600
            Subnet-Mask Option 1, length 4: 255.255.255.0
            BR Option 28, length 4: 192.168.100.255
            Domain-Name-Server Option 6, length 4: 192.168.100.1
            Default-Gateway Option 3, length 4: 192.168.100.1
```

What IP address does the server offer in this example? What is the range of addresses that the server in our experiment may offer? (You can refer to the `dnsmasq` configuration file.)

The server offers 192.168.100.110. Base on the subnet mask 255.255.255.0. The range that the server can offer is from 192.168.100.100 to 192.168.100.199 according to the configuration file.
dhcp-range=192.168.100.100,192.168.100.199,4h

Q1.3 DHCP Request

0.5 Points

Show the "Request" packet sent by the client. (Copy and paste or show a screenshot from `tcpdump`.)

02:19:17.099449 02:d7:34:b9:5b:a3 > ff:ff:ff:ff:ff:ff, ethertype IPv4 (0x0800), length 342: (tos 0x10, ttl 128, id 0, offset 0, flags [none], proto UDP (17), length 328)
    0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 02:d7:34:b9:5b:a3, length 300, xid 0x6ff6d07d, Flags [none]
        Client-Ethernet-Address 02:d7:34:b9:5b:a3
        Vendor-rfc1048 Extensions

Magic Cookie 0x63825363
DHCP-Message Option 53, length 1: Request
Server-ID Option 54, length 4: 192.168.100.1
Requested-IP Option 50, length 4: 192.168.100.110
Hostname Option 12, length 8: "client-1"
Parameter-Request Option 55, length 13:
Subnet-Mask, BR, Time-Zone, Default-Gateway
Domain-Name, Domain-Name-Server, Option 119, Hostname
Netbios-Name-Server, Netbios-Scope, MTU, Classless-Static-Route
NTP

request.png Download

```
02:19:17.099449 02:d7:34:b9:5b:a3 > ff:ff:ff:ff:ff:ff, ethertype IPv4 (0x0800),
length 342: (tos 0x10, ttl 128, id 0, offset 0, flags [none], proto UDP (17), le
ngth 328)
    0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 02:d7:34:b9:5b:a3,
 length 300, xid 0x6ff6d07d, Flags [none]
          Client-Ethernet-Address 02:d7:34:b9:5b:a3
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
            DHCP-Message Option 53, length 1: Request
            Server-ID Option 54, length 4: 192.168.100.1
            Requested-IP Option 50, length 4: 192.168.100.110
            Hostname Option 12, length 8: "client-1"
            Parameter-Request Option 55, length 13:
              Subnet-Mask, BR, Time-Zone, Default-Gateway
              Domain-Name, Domain-Name-Server, Option 119, Hostname
              Netbios-Name-Server, Netbios-Scope, MTU, Classless-Static-Route
              NTP
```

What is the destination address in this request? Why?

The destination address is 255.255.255.255 which is a broadcast address in order to tell other DHCP servers that the client will not accept their offer.

Q1.4 DHCP ACK

0.5 Points

Show the DHCP ACK sent by the server to complete the process. (Copy and paste or show a screenshot from `tcpdump`.)

02:19:17.128901 02:7c:1c:03:0e:72 > 02:d7:34:b9:5b:a3, ethertype IPv4 (0x0800), length 344: (tos 0xc0, ttl 64, id 53510, offset 0, flags [none], proto UDP (17), length 330)
192.168.100.1.67 > 192.168.100.110.68: BOOTP/DHCP, Reply, length 302, xid 0x6ff6d07d, Flags [none]

Your-IP 192.168.100.110
Server-IP 192.168.100.1
Client-Ethernet-Address 02:d7:34:b9:5b:a3
Vendor-rfc1048 Extensions
Magic Cookie 0x63825363
DHCP-Message Option 53, length 1: ACK
Server-ID Option 54, length 4: 192.168.100.1
Lease-Time Option 51, length 4: 14400
RN Option 58, length 4: 7200
RB Option 59, length 4: 12600
Subnet-Mask Option 1, length 4: 255.255.255.0
BR Option 28, length 4: 192.168.100.255
Hostname Option 12, length 8: "client-1"
Domain-Name-Server Option 6, length 4: 192.168.100.1
Default-Gateway Option 3, length 4: 192.168.100.1

ACK.png Download

```
02:19:17.128901 02:7c:1c:03:0e:72 > 02:d7:34:b9:5b:a3, ethertype IPv4 (0x0800),
length 344: (tos 0xc0, ttl 64, id 53510, offset 0, flags [none], proto UDP (17),
 length 330)
    192.168.100.1.67 > 192.168.100.110.68: BOOTP/DHCP, Reply, length 302, xid 0x
6ff6d07d, Flags [none]
          Your-IP 192.168.100.110
          Server-IP 192.168.100.1
          Client-Ethernet-Address 02:d7:34:b9:5b:a3
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
            DHCP-Message Option 53, length 1: ACK
            Server-ID Option 54, length 4: 192.168.100.1
            Lease-Time Option 51, length 4: 14400
            RN Option 58, length 4: 7200
            RB Option 59, length 4: 12600
            Subnet-Mask Option 1, length 4: 255.255.255.0
            BR Option 28, length 4: 192.168.100.255
            Hostname Option 12, length 8: "client-1"
            Domain-Name-Server Option 6, length 4: 192.168.100.1
            Default-Gateway Option 3, length 4: 192.168.100.1
```

What command would you run at the client to verify:

- That the `eth1` interface will use the newly acquired IP address, and the `Subnet-Mask` suggested by the server?
- That the client uses the `Domain-Name-Server` suggested by the server?
- That the client uses the `Default-Gateway` suggested by the server?

Upload screenshots showing the command *and* the output for each, and annotate your screenshots by drawing a circle or a box around the configuration suggested by the server in the DHCP Offer/ACK.

call "ifconfig eth1" to verify that the eth1 interface will use the newly acquire d IP address, and the Subnet-Mask suggested by the server.
call "cat /etc/resolv.conf" to verify that the client uses the Domain-Name-Se rver suggested by the server.
call "route -n" to verify that the client uses the Default-Gateway suggested by the server.

domain_name.png Download

```
ty2069@client-1:~$ cat /etc/resolv.conf
# This file is managed by man:systemd-resolved(8). Do not edit.
#
# This is a dynamic resolv.conf file for connecting local clients directly to
# all known uplink DNS servers. This file lists all configured search domains.
#
# Third party programs must not access this file directly, but only through the
# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,
# replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 192.168.100.1
nameserver 206.196.180.196
search instageni.maxgigapop.net
```

eth1.png Download

```
ty2069@client-1:~$ ifconfig eth1
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.110  netmask 255.255.255.0  broadcast 192.168.100.255
        ether 02:d7:34:b9:5b:a3  txqueuelen 1000  (Ethernet)
        RX packets 315  bytes 28327 (28.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 217  bytes 18406 (18.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

gateway.png Download

```
ty2069@client-1:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.100.1   0.0.0.0         UG    0      0        0 eth1
172.16.0.0      0.0.0.0         255.240.0.0     U     0      0        0 eth0
172.16.0.1      0.0.0.0         255.255.255.255 UH    1024   0        0 eth0
174.119.115.0   172.16.0.1      255.255.255.0   UG    0      0        0 eth0
174.119.115.23  172.16.0.1      255.255.255.255 UGH   0      0        0 eth0
192.168.100.0   0.0.0.0         255.255.255.0   U     0      0        0 eth1
```

Q2 DNS

2 Points

Q2.1 Simple DNS

1 Point

For the basic DNS resolution (not the one with `+trace`!) show the `dig` command and its output. (Either copy and paste, or upload a screenshot.)

```
ty2069@client-1:~$ dig website.lab8-ty2069.ch-geni-net.instageni.maxgiga
pop.net

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> website.lab8-ty2069.ch-geni-net.i
nstageni.maxgigapop.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13639
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 56c484c87634925f126d5ab35fb62195a27b92ae21b29db7 (goo
d)
;; QUESTION SECTION:
;website.lab8-ty2069.ch-geni-net.instageni.maxgigapop.net. IN A

;; ANSWER SECTION:
website.lab8-ty2069.ch-geni-net.instageni.maxgigapop.net. 1 IN CNAME pc
vm2-27.instageni.maxgigapop.net.
pcvm2-27.instageni.maxgigapop.net. 30 IN A      206.196.180.229

;; AUTHORITY SECTION:
instageni.maxgigapop.net. 30    IN      NS      ns.instageni.maxgigapop.net.
instageni.maxgigapop.net. 30    IN      NS      ns.emulab.net.

;; ADDITIONAL SECTION:
ns.instageni.maxgigapop.net. 30 IN      A       206.196.180.196

;; Query time: 3 msec
;; SERVER: 192.168.100.1#53(192.168.100.1)
;; WHEN: Thu Nov 19 02:41:09 EST 2020
;; MSG SIZE  rcvd: 209
```

dig.png Download

```
ty2069@client-1:~$ dig website.lab8-ty2069.ch-geni-net.instageni.maxgigapop.net

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> website.lab8-ty2069.ch-geni-net.instag
eni.maxgigapop.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13639
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 56c484c87634925f126d5ab35fb62195a27b92ae21b29db7 (good)
;; QUESTION SECTION:
;website.lab8-ty2069.ch-geni-net.instageni.maxgigapop.net. IN A

;; ANSWER SECTION:
website.lab8-ty2069.ch-geni-net.instageni.maxgigapop.net. 1 IN CNAME pcvm2-27.in
stageni.maxgigapop.net.
pcvm2-27.instageni.maxgigapop.net. 30 IN A      206.196.180.229

;; AUTHORITY SECTION:
instageni.maxgigapop.net. 30    IN      NS      ns.instageni.maxgigapop.net.
instageni.maxgigapop.net. 30    IN      NS      ns.emulab.net.

;; ADDITIONAL SECTION:
ns.instageni.maxgigapop.net. 30 IN      A       206.196.180.196

;; Query time: 3 msec
;; SERVER: 192.168.100.1#53(192.168.100.1)
;; WHEN: Thu Nov 19 02:41:09 EST 2020
;; MSG SIZE  rcvd: 209
```

Also show the DNS query and response from the `tcpdump` output (again, for the basic DNS resolution, not the one with `+trace`).

192.168.100.110.47443 > 192.168.100.1.53: 13639+ [1au] A? website.lab8-ty2069.ch-geni-net.instageni.maxgigapop.net. (97)
02:41:09.066544 IP (tos 0x0, ttl 64, id 16508, offset 0, flags [DF], proto UDP (17), length 237)
    192.168.100.1.53 > 192.168.100.110.47443: 13639* 2/2/2 website.lab8-ty2069.ch-geni-net.instageni.maxgigapop.net. CNAME pcvm2-27.instageni.maxgigapop.net., pcvm2-27.instageni.maxgigapop.net. A 206.196.180.229 (209)

tcp.png Download

```
    192.168.100.110.47443 > 192.168.100.1.53: 13639+ [1au] A? website.lab8-ty2069.
ch-geni-net.instageni.maxgigapop.net. (97)
02:41:09.066544 IP (tos 0x0, ttl 64, id 16508, offset 0, flags [DF], proto UDP (17
), length 237)
    192.168.100.1.53 > 192.168.100.110.47443: 13639* 2/2/2 website.lab8-ty2069.ch-
geni-net.instageni.maxgigapop.net. CNAME pcvm2-27.instageni.maxgigapop.net., pcvm2
-27.instageni.maxgigapop.net. A 206.196.180.229 (209)
```

Answer the following questions using the `dig` output. No explanation is required - just copy and paste the relevant word from the `dig` output for each answer.

What is the hostname that you tried to resolve?

website.nat.ch-geni-net.instageni.research.umich.edu

What is the DNS record *type* that your query relates to? (Here is a list of DNS record types.)

Address record

What is the *address* for the hostname you asked to resolve?

206.196.180.229

Give the name of an "authoritative" server listed for this name,

ns.instageni.maxgigapop.net.

and the IP address of that "authoritative" server.

206.196.180.196

What is the IP address of the server that the DNS response comes from?

192.168.100.1

Q2.2 Hierarchical DNS query

1 Point

For the hierarchical DNS resolution with `+trace`, show the `dig` command and its output. (Either copy and paste, or upload a screenshot.)

```
ty2069@gateway:~$ dig +trace website.lab8-ty2069.ch-geni-net.instageni.
maxgigapop.net

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> +trace website.lab8-ty2069.ch-ge
ni-net.instageni.maxgigapop.net
;; global options: +cmd
```

```
.                   453642  IN      NS      e.root-servers.net.
.                   453642  IN      NS      d.root-servers.net.
.                   453642  IN      NS      c.root-servers.net.
.                   453642  IN      NS      g.root-servers.net.
.                   453642  IN      NS      j.root-servers.net.
.                   453642  IN      NS      a.root-servers.net.
.                   453642  IN      NS      f.root-servers.net.
.                   453642  IN      NS      m.root-servers.net.
.                   453642  IN      NS      l.root-servers.net.
.                   453642  IN      NS      b.root-servers.net.
.                   453642  IN      NS      i.root-servers.net.
.                   453642  IN      NS      h.root-servers.net.
.                   453642  IN      NS      k.root-servers.net.
.                   453642  IN      RRSIG   NS 8 0 518400 20201201050000 20
201118040000 26116 . aL/YlhB9WF0y+CaImpUSy7UpJ1S4u7xM4j3iiTzYTjaB
ly7kbtGlwzFS 9UPosGVAWebCIx9brFPw2TVavilvUDGK1SsDOmW/zSpQCq
F8Hy4BSNKl qIaDRRWqTFXvNBQcHo6TTueLfIseoY6u1LPd2KiFjSD8gF5kiq
zN5zxK OCXuB0ewGqt4IN8jyadq7ojdF29j5B/bwfG4geULAqvryMwbfkgRis
xS HJXdITUYuIlE5qFk6nh524fs0piAnKKmouKRMEdERVfKd6tAEWzkYucl D
ageDcuGqOfu3OWSoApLYmCAICD0xgdc3Ws2DMrYg6A20QdT4u63roUN
 0R6pew==
;; Received 1125 bytes from 206.196.180.196#53(206.196.180.196) in 1 ms

net.                172800  IN      NS      c.gtld-servers.net.
net.                172800  IN      NS      d.gtld-servers.net.
net.                172800  IN      NS      e.gtld-servers.net.
net.                172800  IN      NS      a.gtld-servers.net.
net.                172800  IN      NS      k.gtld-servers.net.
net.                172800  IN      NS      j.gtld-servers.net.
net.                172800  IN      NS      g.gtld-servers.net.
net.                172800  IN      NS      i.gtld-servers.net.
net.                172800  IN      NS      l.gtld-servers.net.
net.                172800  IN      NS      m.gtld-servers.net.
net.                172800  IN      NS      h.gtld-servers.net.
net.                172800  IN      NS      b.gtld-servers.net.
net.                172800  IN      NS      f.gtld-servers.net.
net.                86400   IN      DS      35886 8 2 7862B27F5F516EBE19680
444D4CE5E762981931842C465F00236401D 8BD973EE
net.                86400   IN      RRSIG   DS 8 1 86400 20201202050000 20
201119040000 26116 . oO6mbv7hyGaKkXTk4opN6b7VDkUeYnW6k09vyv
```

Qcen+m2ZOgnYukeeie +MYwRN+4vID5ToDsIs1X/paiE8fewzsi5SwFff579ac
e799phIx5NvU4 oanF/q8JET94LhiAeZoGWgpZsKGezGcSGPmcTe492UHq
cDGY0hFAbYXi gvS1o1++82SqmwdYs/1fkH1H4oagi5G/c6m6RU3EBPpHiYpl
5djBymja qc8DmDqieqQkJRQzCgTAKJUJ4I9bipzpTKGLW7jTFpamzT1XOa9
cJ4DK ri9rFaNTptqRYLhVill+Ig6OewBacCWKI0i1qlkG9IffXz7KcVjXBp/s djvv
8w==
;; Received 1213 bytes from 192.203.230.10#53(e.root-servers.net) in 92 ms

maxgigapop.net. 172800 IN NS ns1.maxgigapop.net.
maxgigapop.net. 172800 IN NS ns2.maxgigapop.net.
maxgigapop.net. 172800 IN NS ns3.maxgigapop.net.
A1RT98BS5QGC9NFI51S9HCI47ULJG6JH.net. 86400 IN NSEC3 1 1 0 - A1R
UUFFJKCT2Q54P78F8EJGJ8JBK7I8B NS SOA RRSIG DNSKEY NSEC3PAR
AM
A1RT98BS5QGC9NFI51S9HCI47ULJG6JH.net. 86400 IN RRSIG NSEC3 8 2
86400 20201125081320 20201118070320 15314 net. JS5Yc/Aw8sTfIFGbIR
JlQyechka7Bd0BMssel25JJGdCPOMUVtLvET+f vtlWZ0dINdKoCbiUB9Gxs
qP1zU3e6FNKz81Z32IVypFKs5LS0QbJgJch FANGK8Dujsuo2MA6SHxe1x8
Wh5qz/PQoyotaWFTWvNqLxLdKcgpcRpq8 uYUcPmoBKyXgMo90BsCFQZr
zI4a23tYFwAQNwmCJVpWnwA==
T65H8UARFKQ4JV3TU96QKI8HR2IIV054.net. 86400 IN NSEC3 1 1 0 - T65
PLQFL06MUN6GBOC536BKFVRCL5HRD NS DS RRSIG
T65H8UARFKQ4JV3TU96QKI8HR2IIV054.net. 86400 IN RRSIG NSEC3 8 2
86400 20201125080744 20201118065744 15314 net. cLO1X8NYWHL2NhO
TrmawTFoDtmUGmzcq2AdTxyCuRk4OtmVRX6IMqDvz WH563y94ioqsIqnL
7z24D0KQ3sQZNBFOhyLCRnDmfmaeUHnyatTSiqdx S5QOUQVHcVrqQdi
ULXMEWW6aqHw9GPlw4apDfAIdVNjLLAEjSXu7ZgIK /3OyRfYv9XY4u3rad
uFzVOTSGWRpMDQoU2hysmZgoDJDew==
;; Received 820 bytes from 192.52.178.30#53(k.gtld-servers.net) in 16 ms

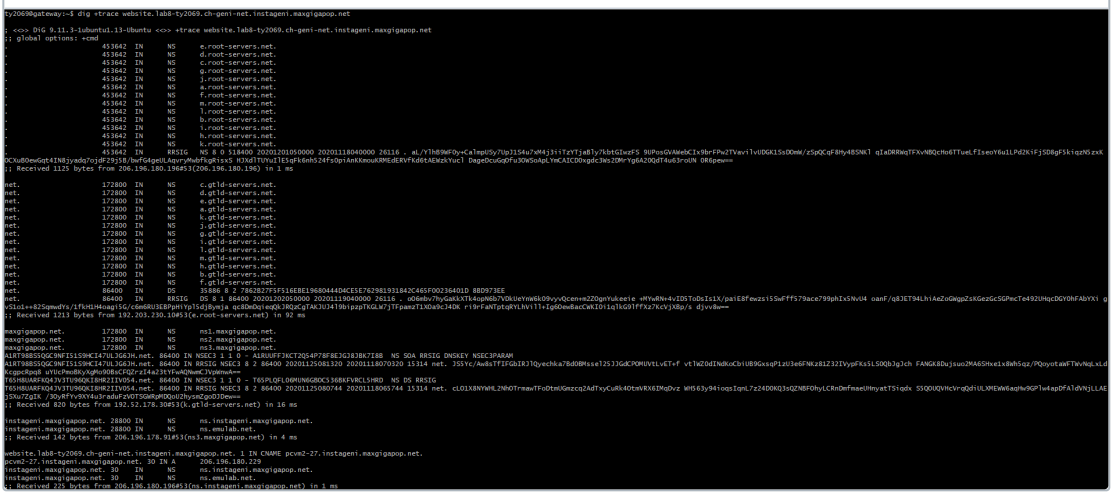
instageni.maxgigapop.net. 28800 IN NS ns.instageni.maxgigapop.ne
t.
instageni.maxgigapop.net. 28800 IN NS ns.emulab.net.
;; Received 142 bytes from 206.196.178.91#53(ns3.maxgigapop.net) in 4 ms

website.lab8-ty2069.ch-geni-net.instageni.maxgigapop.net. 1 IN CNAME pc
vm2-27.instageni.maxgigapop.net.
pcvm2-27.instageni.maxgigapop.net. 30 IN A 206.196.180.229
instageni.maxgigapop.net. 30 IN NS ns.instageni.maxgigapop.net.
instageni.maxgigapop.net. 30 IN NS ns.emulab.net.

;; Received 225 bytes from 206.196.180.196#53(ns.instageni.maxgigapop.net) in 1 ms

dig_trace+.png

Download



```
ty2069@gateway:~$ dig +trace website.lab8-ty2069.ch-geni-net.instageni.maxgigapop.net

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> +trace website.lab8-ty2069.ch-geni-net.instageni.maxgigapop.net
;; global options: +cmd
.                       453642  IN      NS      e.root-servers.net.
.                       453642  IN      NS      d.root-servers.net.
.                       453642  IN      NS      c.root-servers.net.
.                       453642  IN      NS      g.root-servers.net.
.                       453642  IN      NS      j.root-servers.net.
.                       453642  IN      NS      a.root-servers.net.
.                       453642  IN      NS      f.root-servers.net.
.                       453642  IN      NS      m.root-servers.net.
.                       453642  IN      NS      l.root-servers.net.
.                       453642  IN      NS      b.root-servers.net.
.                       453642  IN      NS      i.root-servers.net.
.                       453642  IN      NS      h.root-servers.net.
.                       453642  IN      NS      k.root-servers.net.
.                       453642  IN      RRSIG   NS 8 0 518400 20201210105000 20201118040000 26116 . mL/Y7h0WFOy+CaImpU5y/Ubj15Ku7xM4j3iiTzYTjaBly7kbtGlwzF5 NUPesGVAWebCIv9brFPw2TVavilvUDGK15sDXmW/z5pQCqF8Hy4BSNKl qIeDRRWqTFXvNBQcHo6TTueLfIseoY6u1LPdZKiFjSD8gF5kiqzNGzxK
DCXuBOewGqt4IN8jyadq7ojdF2918/bmfG4geULAqvryMwbFkgB1sxS H3XdlTUVuIE1qFk6nh524fsOpiAnKKmouKRMEdERVFkd6tAEWzkYucl DageDcyGpFu3OWSoApLYmCA2CDXgdc3WsZOMrYg6A2OQdT4u63roUN OR6pew==
;; Received 1125 bytes from 206.196.180.196#53(206.196.180.196) in 1 ms

net.                    172800  IN      NS      c.gtld-servers.net.
net.                    172800  IN      NS      d.gtld-servers.net.
net.                    172800  IN      NS      e.gtld-servers.net.
net.                    172800  IN      NS      a.gtld-servers.net.
net.                    172800  IN      NS      k.gtld-servers.net.
net.                    172800  IN      NS      j.gtld-servers.net.
net.                    172800  IN      NS      g.gtld-servers.net.
net.                    172800  IN      NS      i.gtld-servers.net.
net.                    172800  IN      NS      l.gtld-servers.net.
net.                    172800  IN      NS      m.gtld-servers.net.
net.                    172800  IN      NS      h.gtld-servers.net.
net.                    172800  IN      NS      b.gtld-servers.net.
net.                    172800  IN      NS      f.gtld-servers.net.
net.                    86400   IN      DS      35886 8 2 7062B273F5F516EBE196804444D4CE5E7629819318142C46LF002364O1D 8BD973EE
net.                    86400   IN      RRSIG   DS 8 1 86400 20201202050000 20201110040000 26116 . oO6mbv7hyGaKkXTk4opN6b7VDkUeYnW6k09vyvQcen+m2ZOgnYukeeie +MYwRNn4vIDSToDsIsiX/paiE8fewzsiSwFffS79ace799phIxSNvU4 oanF/q8JET94LhiAeZoGWgpZsKGezGc5GPmcTe492UHqcDGYOhFAbYXi g
vSIoi++82SqmwdYs/1fkH14oagiSG/c6m6RUSEBPpHiYpI5dj8ymja qcdOmOdqieqQk3RQzCgTAKJU3419bipzpTKGLW7jTFpamzTiXDa9cJ4DK ri9rFaNTptqRYLhViTl+Ig6DemBacCwKIOiiqlkG9fffXz7KcVjXBp/s djvv8w==
;; Received 1213 bytes from 192.203.230.10#53(e.root-servers.net) in 92 ms

maxgigapop.net.         172800  IN      NS      ns1.maxgigapop.net.
maxgigapop.net.         172800  IN      NS      ns2.maxgigapop.net.
maxgigapop.net.         172800  IN      NS      ns3.maxgigapop.net.
AIRT988SSQGC9NFIS1S9HCI47ULJG6JH.net. 86400 IN NSEC3 1 1 0 - AIRUUFFJKCT2QS4P78F8EJG38JBK7I8B  NS SOA RRSIG DNSKEY NSEC3PARAM
AIRT988SSQGC9NFIS1S9HCI47ULJG6JH.net. 86400 IN RRSIG NSEC3 8 2 86400 20201125081320 20201118070320 15314 net. JSSYe/Aw8sTfIFGbIRJ1Qyechka78dO8Msse125JJGdCPOMUVtLvET+f vtlWZOdIWdKoCbiUB9GxsqP1zU3e6FNKz81232IVypFKs5LSDQbJgJch FANGK8Dujsuo2MA6SHxe1x8Wh5qz/PQoyotaWFTWvNqLxLd
KcgpcRqq8 uYUcPmdBsyXgRu9OBsCFQZrzI4a3t5YFwAQNqmKJVpWnwA==
T65HBUABFKQ4JVJTU96QKIBHR2IIVO54.net. 86400 IN NSEC3 1 1 0 - T65PLQFLO6MHUN6GBOCS36BKFVBCL5HBD  NS DS RRSIG
T65HBUABFKQ4JVJTU96QKIBHR2IIVO54.net. 86400 IN RRSIG NSEC3 8 2 86400 20201125080744 20201118065744 15314 net. cLO1X8NYWHL2NhOTrmxwTFoDtmUGmzcqZAdTxyCuRk4OtmVRX6IMqDvz WH563y94ioqsIqnL7z24DOKQ3sQZNBFOhyLCRnDmfmaeUHnyatTSiqdx S5QOUQVHcVrqQdiULXMEWV6aqHw9GPlw4apDFAldVNjLLAE
jSXu7ZgIK /3OyRFYv9XY4u3radufzVOTSWRpMDQoU2hysmZgoDJDew==
;; Received 820 bytes from 192.52.178.30#53(k.gtld-servers.net) in 16 ms

instageni.maxgigapop.net. 28800 IN      NS      ns.instageni.maxgigapop.net.
instageni.maxgigapop.net. 28800 IN      NS      ns.emulab.net.
;; Received 142 bytes from 206.196.178.91#53(ns3.maxgigapop.net) in 4 ms

website.lab8-ty2069.ch-geni-net.instageni.maxgigapop.net. 1 IN CNAME pcvm2-27.instageni.maxgigapop.net.
pcvm2-27.instageni.maxgigapop.net. 30 IN A      206.196.180.229
instageni.maxgigapop.net. 30    IN      NS      ns.instageni.maxgigapop.net.
instageni.maxgigapop.net. 30    IN      NS      ns.emulab.net.
;; Received 225 bytes from 206.196.180.196#53(ns.instageni.maxgigapop.net) in 1 ms
```

Draw a diagram showing how the hostname was resolved recursively, starting from the implied `.` at the end and moving toward the beginning.

- At the top, show the nameservers for the root domain. Highlight the one that you queried for the top-level domain (as shown in the `dig +trace` output).
- At the next level, show the nameservers for the top-level domain. Highlight the one that you queried for the second-level domain.
- At the next level, show the nameservers for the second-level domain. Highlight the one that you queried for the subdomain.
- Repeat until you have shown how the complete hostname is resolved.

level.png

Download

Root domain	. e.root-servers.net. d.root-servers.net. c.root-servers.net. g.root-servers.net. j.root-servers.net. a.root-servers.net. f.root-servers.net. m.root-servers.net. l.root-servers.net. b.root-servers.net. i.root-servers.net. h.root-servers.net. k.root-servers.net.
Top level domains	net. c.gtld-servers.net. d.gtld-servers.net. e.gtld-servers.net. a.gtld-servers.net. k.gtld-servers.net. j.gtld-servers.net. g.gtld-servers.net. i.gtld-servers.net. l.gtld-servers.net. m.gtld-servers.net. h.gtld-servers.net. b.gtld-servers.net. f.gtld-servers.net.
Second level domains	maxgigapop.net. ns1.maxgigapop.net. ns2.maxgigapop.net. ns3.maxgigapop.net.
subdomain	instageni.maxgigapop.net. ns.instageni.maxgigapop.net. ns.emulab.net.

Q3 NAT

1 Point

Q3.1 NAT rewriting

1 Point

Show the three-way TCP handshake for a connection between client and website as seen by `tcpdump` at the website:

```
03:31:12.960916 IP 172.17.3.35.53138 > 206.196.180.229.80: Flags [S], seq 17
23065109, win 64240, options [mss 1460,sackOK,TS val 3071958563 ecr 0,
nop,wscale 7], length 0
03:31:12.961004 IP 206.196.180.229.80 > 172.17.3.35.53138: Flags [S.], seq 2
97424244, ack 1723065110, win 65160, options [mss 1460,sackOK,TS val 3
909723916 ecr 3071958563,nop,wscale 7], length 0
03:31:13.658366 IP 172.17.3.35.53138 > 206.196.180.229.80: Flags [.], ack 1,
 win 502, options [nop,nop,TS val 3071959466 ecr 3909723916], length 0
```

web_3ways.png Download

```
03:31:12.960916 IP 172.17.3.35.53138 > 206.196.180.229.80: Flags [S], seq 172306
5109, win 64240, options [mss 1460,sackOK,TS val 3071958563 ecr 0,nop,wscale 7],
 length 0
03:31:12.961004 IP 206.196.180.229.80 > 172.17.3.35.53138: Flags [S.], seq 29742
4244, ack 1723065110, win 65160, options [mss 1460,sackOK,TS val 3909723916 ecr
3071958563,nop,wscale 7], length 0
03:31:13.658366 IP 172.17.3.35.53138 > 206.196.180.229.80: Flags [.], ack 1, win
 502, options [nop,nop,TS val 3071959466 ecr 3909723916], length 0
```

and as seen by `tcpdump` at the gateway (on the LAN):

```
03:31:12.754569 IP 192.168.100.110.53138 > 206.196.180.229.80: Flags [S], se
q 1723065109, win 64240, options [mss 1460,sackOK,TS val 3071958563 e
cr 0,nop,wscale 7], length 0
03:31:13.656814 IP 206.196.180.229.80 > 192.168.100.110.53138: Flags [S.], se
q 297424244, ack 1723065110, win 65160, options [mss 1460,sackOK,TS va
l 3909723916 ecr 3071958563,nop,wscale 7], length 0
03:31:13.657413 IP 192.168.100.110.53138 > 206.196.180.229.80: Flags [.], ack
 1, win 502, options [nop,nop,TS val 3071959466 ecr 3909723916], length 0
```

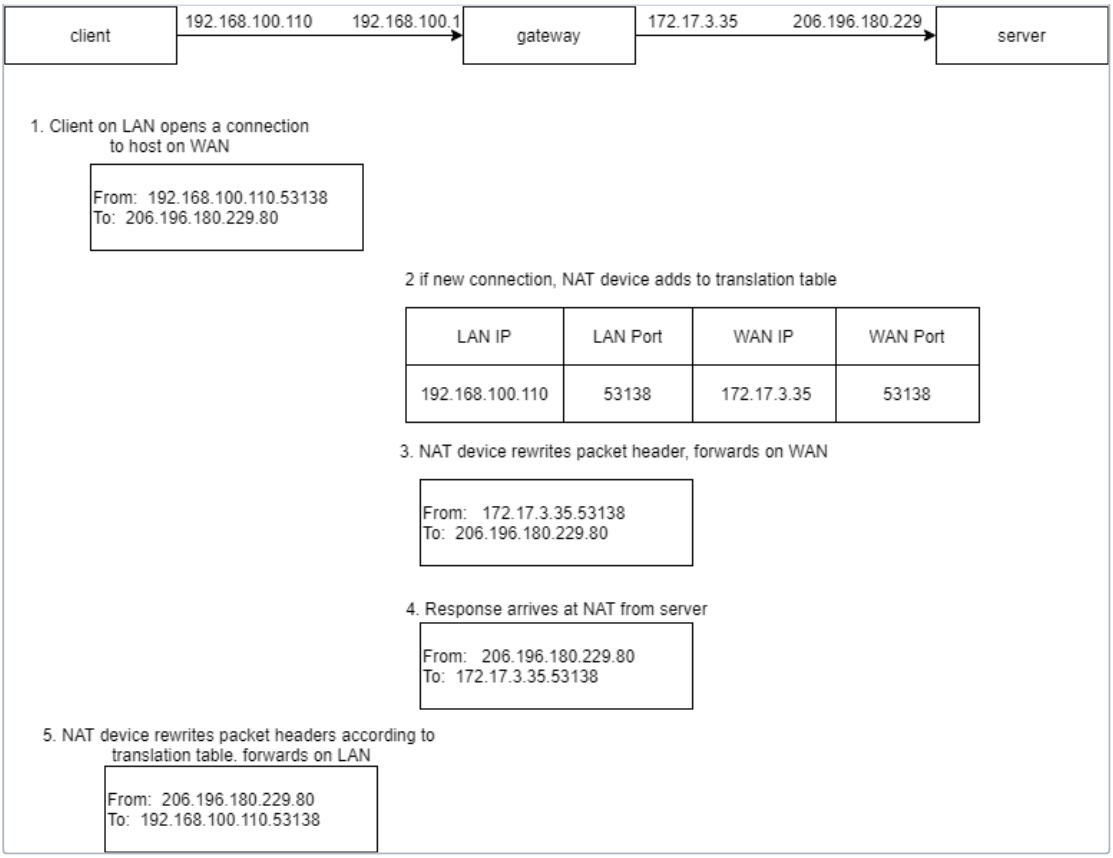
gateway_3ways.png Download

```
03:31:12.754569 IP 192.168.100.110.53138 > 206.196.180.229.80: Flags [S], seq 1723
065109, win 64240, options [mss 1460,sackOK,TS val 3071958563 ecr 0,nop,wscale 7],
 length 0
03:31:13.656814 IP 206.196.180.229.80 > 192.168.100.110.53138: Flags [S.], seq 297
424244, ack 1723065110, win 65160, options [mss 1460,sackOK,TS val 3909723916 ecr
3071958563,nop,wscale 7], length 0
03:31:13.657413 IP 192.168.100.110.53138 > 206.196.180.229.80: Flags [.], ack 1, w
in 502, options [nop,nop,TS val 3071959466 ecr 3909723916], length 0
```

(Make sure these show the IP addresses and port numbers used in the connection!)

Then, draw a diagram showing how NAT is used between client and website, similar to this diagram but with the IP addresses, hostnames, and ports from *your* experiment.

NAT_rerwite.png Download



Q4 8.7 HTTP exercises

3 Points

Q4.1 Write and send an HTTP request (Exercise 2)

1 Point

Show the HTTP request and response *headers* that you captured.

GET /index.html HTTP/1.0
From: guest@client
User-Agent: HTTPTool/1.0

HTTP/1.1 200 OK
Date: Thu, 19 Nov 2020 08:55:49 GMT
Server: Apache/2.4.29 (Ubuntu)
Last-Modified: Thu, 19 Nov 2020 08:29:42 GMT
ETag: "2aa6-5b471878d62a5"
Accept-Ranges: bytes
Content-Length: 10918
Vary: Accept-Encoding

Connection: close
Content-Type: text/html

req_resp.png Download

```
GET /index.html HTTP/1.0
From: guest@client
User-Agent: HTTPTool/1.0

HTTP/1.1 200 OK
Date: Thu, 19 Nov 2020 08:55:49 GMT
Server: Apache/2.4.29 (Ubuntu)
Last-Modified: Thu, 19 Nov 2020 08:29:42 GMT
ETag: "2aa6-5b471878d62a5"
Accept-Ranges: bytes
Content-Length: 10918
Vary: Accept-Encoding
Connection: close
Content-Type: text/html
```

Q4.2 HTTP with KeepAlive on (Exercise 3)

1 Point

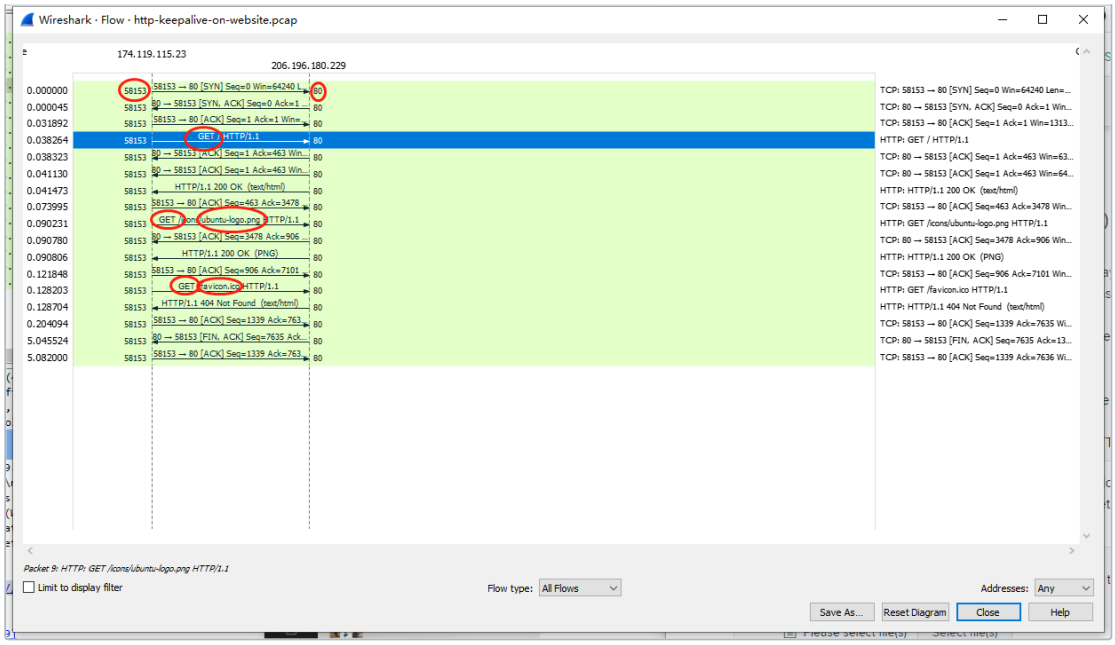
In Wireshark, use the "Statistics > Flow Graph" display to analyze your TCP connection with KeepAlive *enabled*. Use it to answer these questions:

- With the KeepAlive directive enabled (default case), how many HTTP GET requests were sent?
- Which files were requested?
- How many TCP connections were used to retrieve the page and linked assets?
- How many SYN packets did you observe?
- What were the TCP port numbers used for the HTTP request and response for each file?

Three HTTP GET requests were sent and ubuntu-logo.png and favicon.ico were requested.
One TCP connection was used and two SYN packets observed.
port 58153 for HTTP request and 80 for HTTP response.

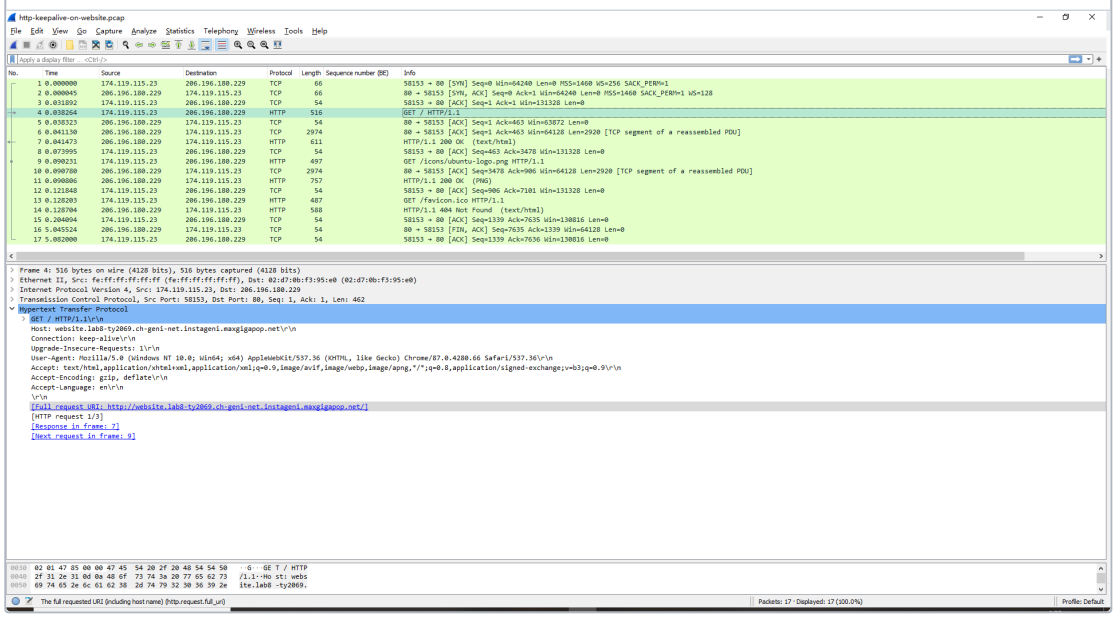
Annotate your flow graph to show where you found the answer to each of these questions, and upload it here.

keepalive_on.png Download

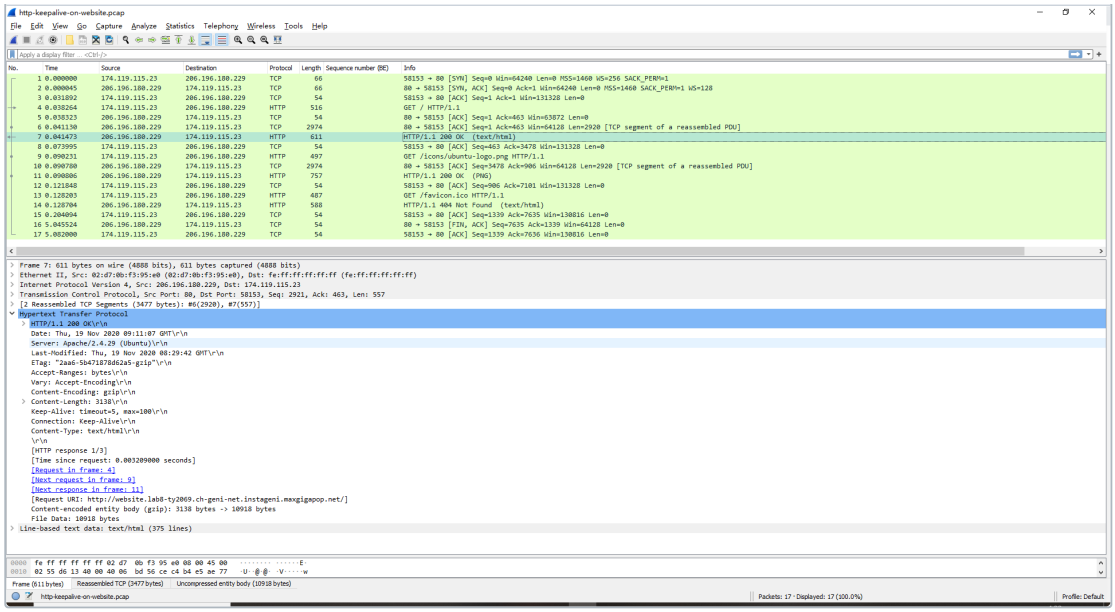


Also show your HTTP request and response *headers*, annotated to highlight any reference to the KeepAlive directive.

▾ req_header.png Download



▾ resp_header.png Download



Q4.3 HTTP with KeepAlive off (Exercise 3)

1 Point

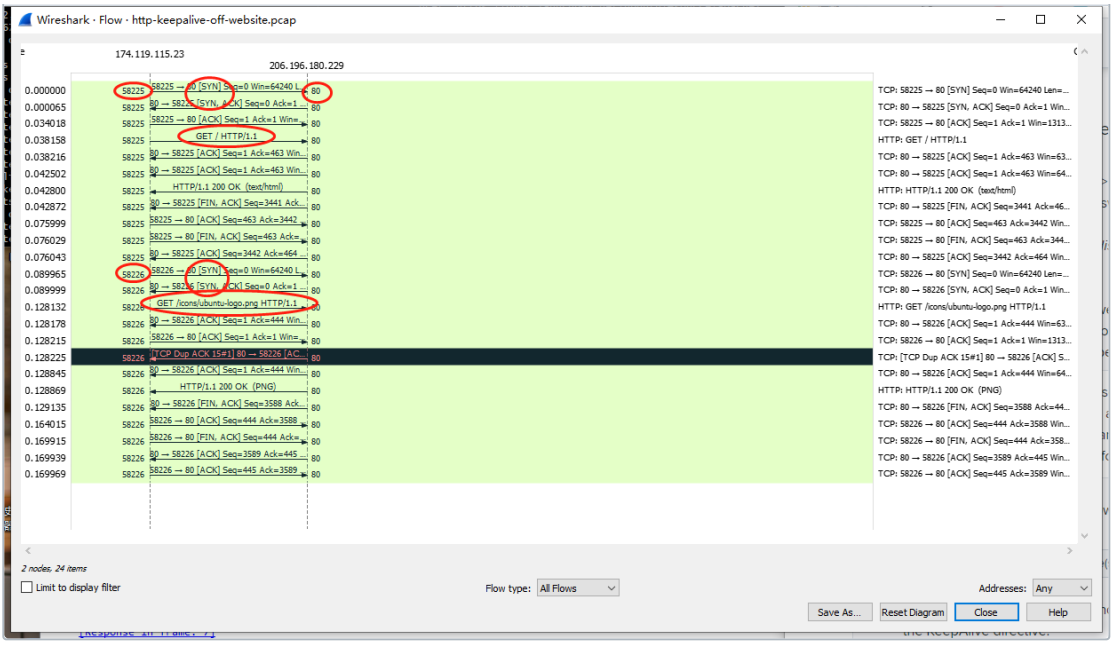
In Wireshark, use the "Statistics > Flow Graph" display to analyze your TCP connection with KeepAlive *disabled*. Use it to answer these questions:

- With the KeepAlive directive *disabled* (default case), how many HTTP GET requests were sent?
- Which files were requested?
- How many TCP connections were used to retrieve the page and linked assets?
- How many SYN packets did you observe?
- What were the TCP port numbers used for the HTTP request and response for each file?

two HTTP GET requests were sent and ubuntu-logo.png was requested.
two TCP connection was used and four SYN packets observed.
port 58225 for HTTP request and 80 for HTTP response for the first conne ction and port 58226 for HTTP request and 80 for HTTP response for the s econd.

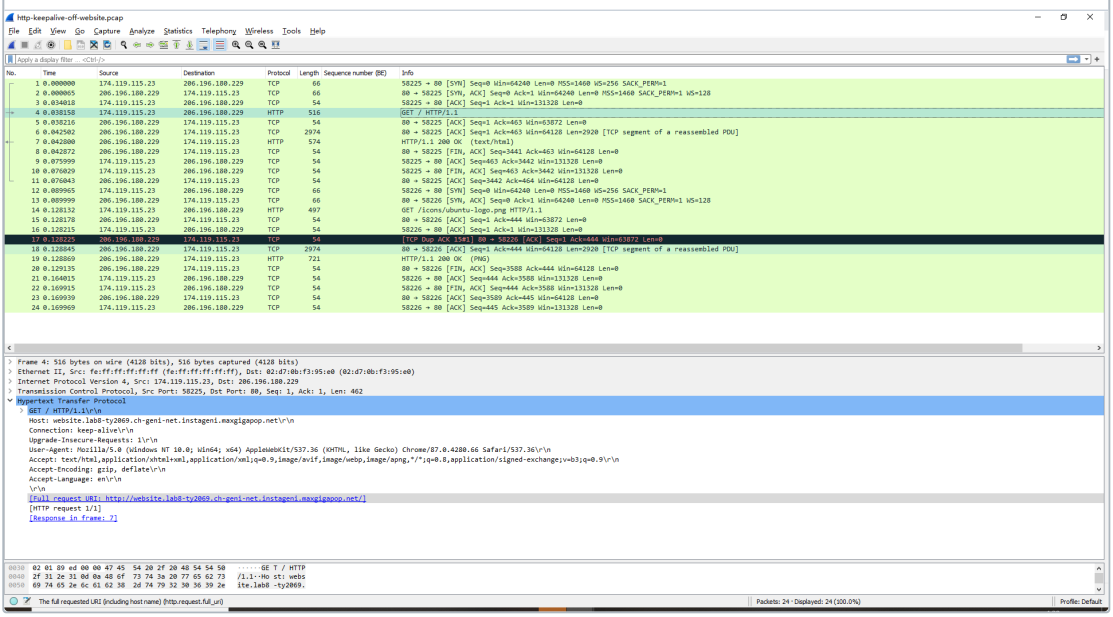
Annotate your flow graph to show where you found the answer to each of these questions, and upload it here.

keepalive_off.png Download

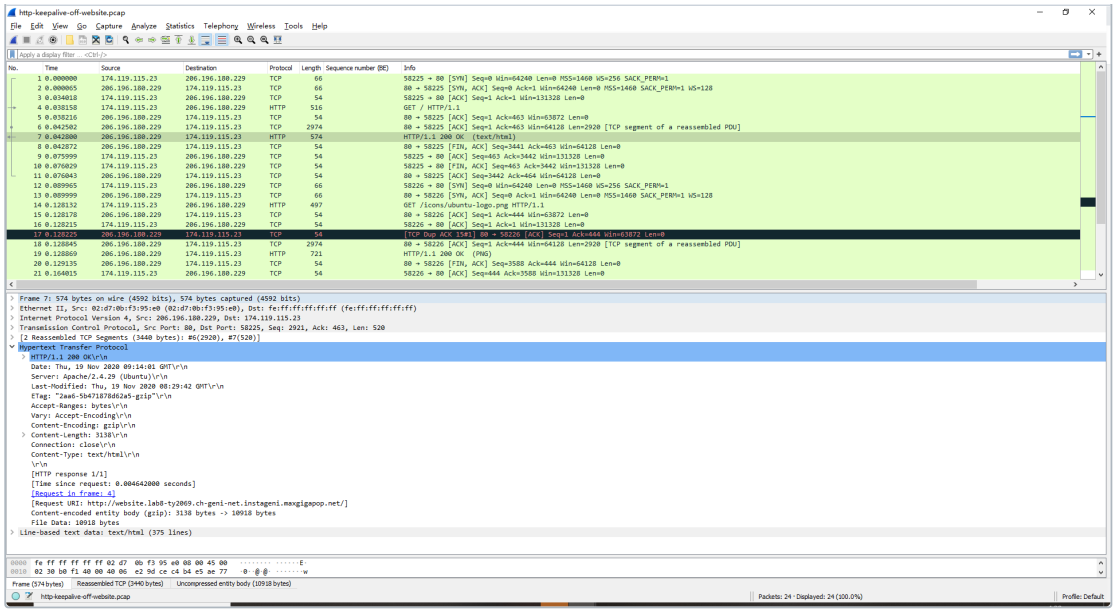


Also show your HTTP request and response *headers*, annotated to highlight any reference to the KeepAlive directive.

▾ req_header2.png Download



▾ resp_header2.png Download



What is different between this HTTP response header and the previous one?

This response header doesn't have the Next request and Next response.

Q5 8.9 NTP exercises

2 Points

Q5.1 NTP servers (Exercise 7)

0.5 Points

Answer the following questions about your experiment:

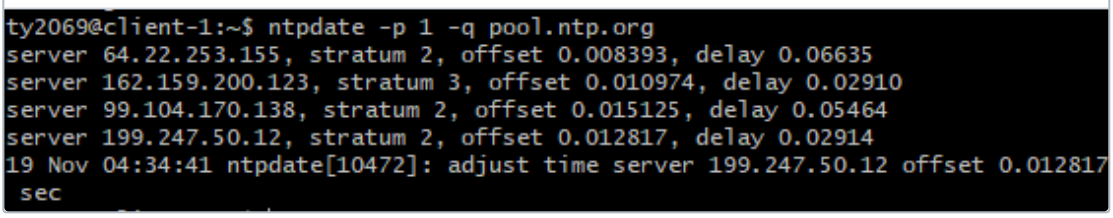
- How many NTP servers did the client receive a response from?
- What stratum did each server belong to, and what is the significance of the "stratum"?

the client receives a response from 4 servers.
They belong to stratum 2 3 2 2.
Stratum can reduce server load and enable more hosts to synchronize time

Upload the `ntpdate` output to support your answer.

```
ty2069@client-1:~$ ntpdate -p 1 -q pool.ntp.org
server 64.22.253.155, stratum 2, offset 0.008393, delay 0.06635
server 162.159.200.123, stratum 3, offset 0.010974, delay 0.02910
server 99.104.170.138, stratum 2, offset 0.015125, delay 0.05464
server 199.247.50.12, stratum 2, offset 0.012817, delay 0.02914
19 Nov 04:34:41 ntpdate[10472]: adjust time server 199.247.50.12 offset 0.01
2817 sec
```

▾ ntpdate.png Download



Q5.2 NTP request and response (Exercise 7)

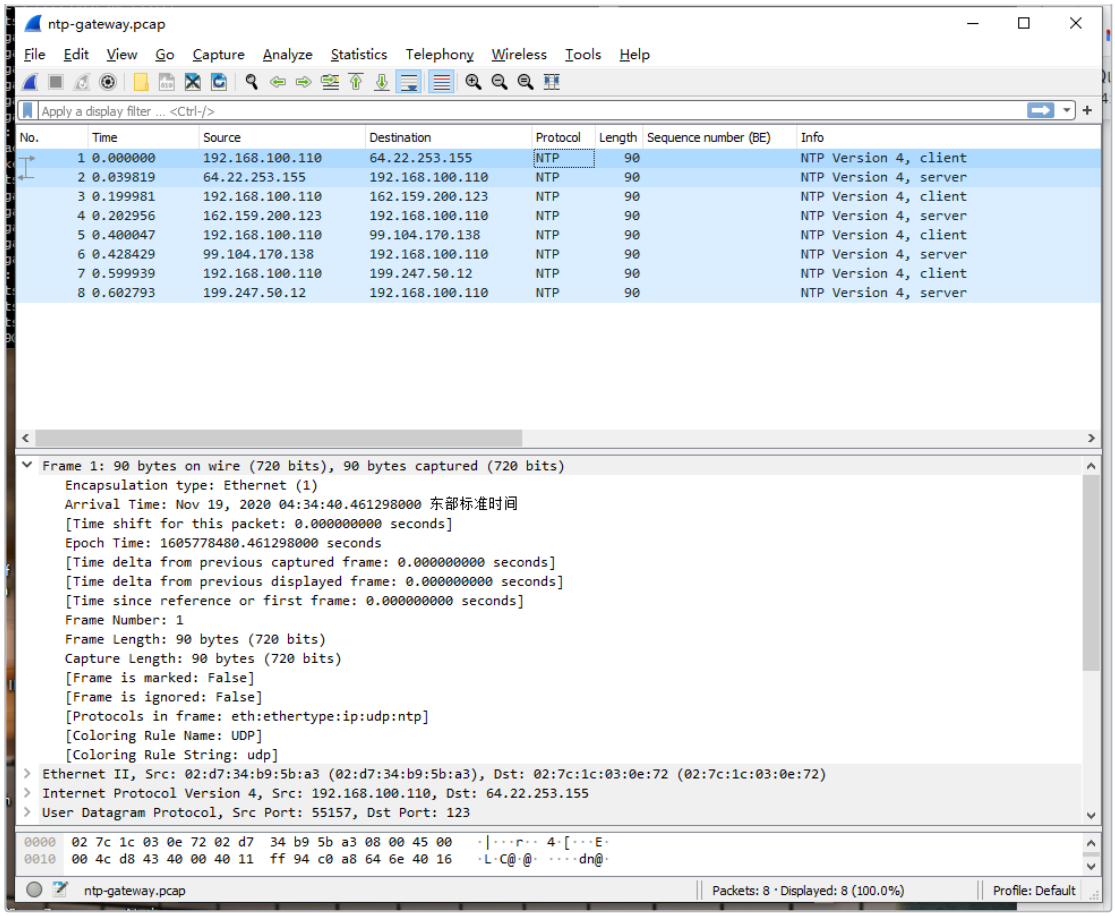
1 Point

In Wireshark, select *one* NTP request and its associated response from your packet capture.

Upload the NTP request and response, but *annotate* the response - draw a circle or a box around the values for **T1**, **T2**, **T3**, and **T4**, and label them so that it is apparent which is which.

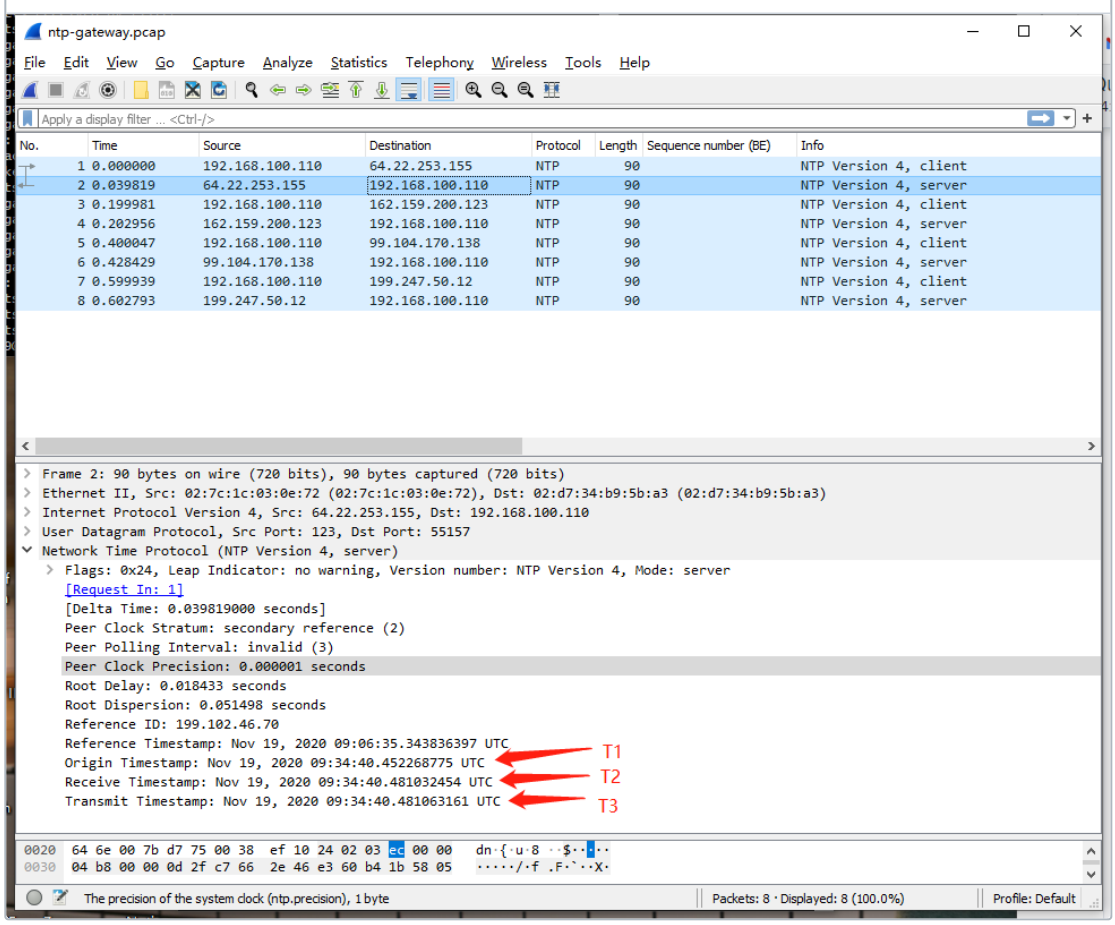
*(Note: **T4** is not included in the packet, since this is a time measured by the client when the NTP reply is received. You can use the "Arrival Time" in the frame header in Wireshark as approximately equal to **T4**. This timestamp is actually a bit smaller than the true **T4**, since it represents the time at which the frame is received by the OS's networking system but not yet received by the NTP process.)*

▾ request_ntp.png Download

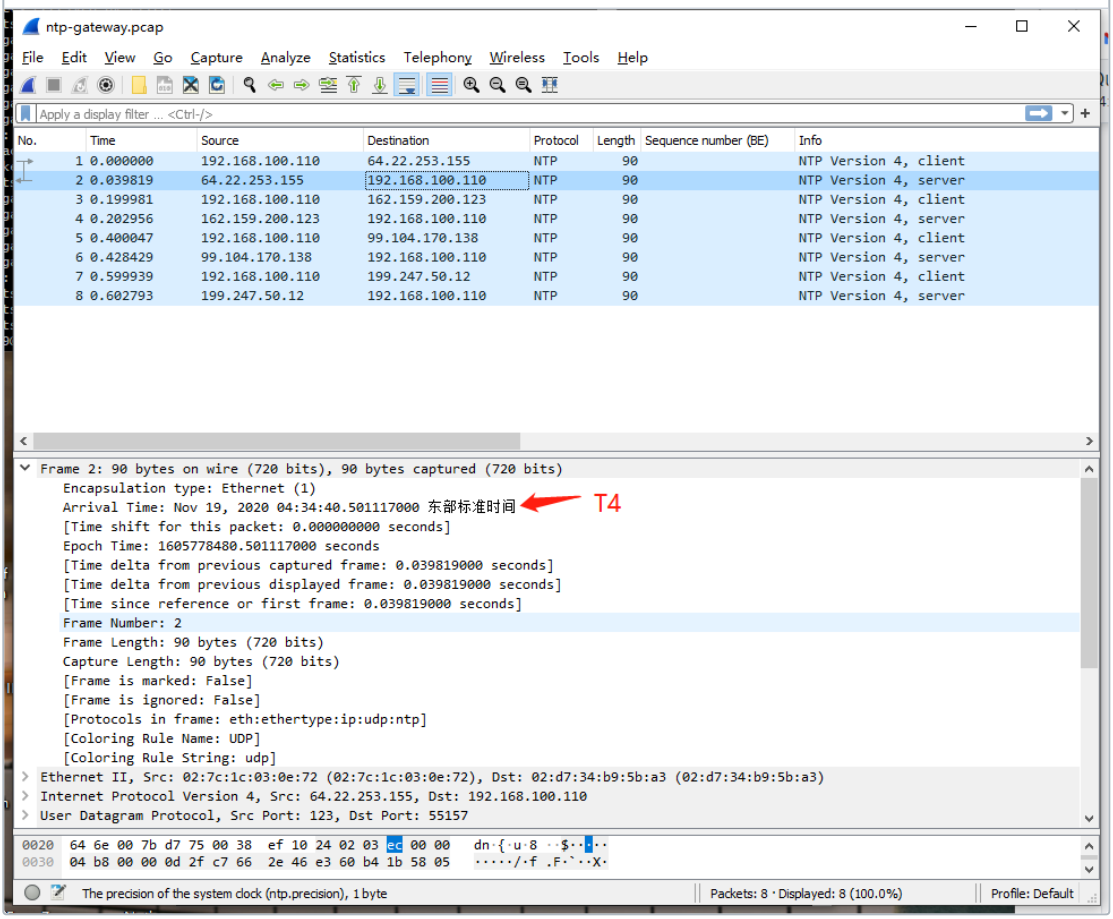


response_ntp.png

Download



response_ntp2.png Download

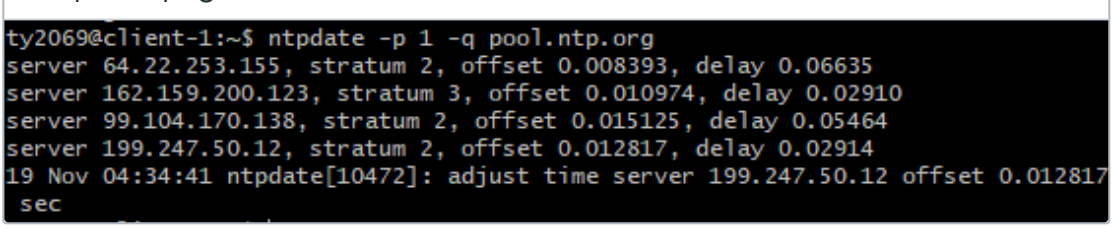


What is the delay δ and offset θ? Show how you compute this value.

delay = (T4 - T1) - (T3 - T2) = 0.048817518

offset = 1/2[(T2-T1) + (T3-T4)] = 0.00435492

ntpdate.png Download



Show the line of `ntpdate` output for this server, and compare the values you compute to those reported in the `ntpdate` output. Are they similar?

Yes they are

ntpdate.png Download

```
ty2069@client-1:~$ ntpdate -p 1 -q pool.ntp.org
server 64.22.253.155, stratum 2, offset 0.008393, delay 0.06635
server 162.159.200.123, stratum 3, offset 0.010974, delay 0.02910
server 99.104.170.138, stratum 2, offset 0.015125, delay 0.05464
server 199.247.50.12, stratum 2, offset 0.012817, delay 0.02914
19 Nov 04:34:41 ntpdate[10472]: adjust time server 199.247.50.12 offset 0.012817
 sec
```

Q5.3 Synchronizing hosts on a LAN with NTP (Exercise 8)

0.5 Points

Show a screenshot of your client hosts' time, side by side,

- before synchronizing with NTP, when there is a time offset, and
- after synchronizing with NTP.

screenshot

after.png Download

```
ty2069@client-2:~$ timedatectl
                      Local time: Thu 2020-11-19 03:01:01 MST
                  Universal time: Thu 2020-11-19 10:01:01 UTC
                        RTC time: n/a
                       Time zone: America/Denver (MST, -0700)
       System clock synchronized: yes
systemd-timesyncd.service active: no
                 RTC in local TZ: no
```

```
ty2069@client-1:~$ timedatectl
                      Local time: Thu 2020-11-19 03:01:01 MST
                  Universal time: Thu 2020-11-19 10:01:01 UTC
                        RTC time: n/a
                       Time zone: America/Denver (MST, -0700)
       System clock synchronized: no
systemd-timesyncd.service active: no
                 RTC in local TZ: no
```

before.png Download

```
ty2069@client-2:~$ timedatectl
                      Local time: Thu 2020-11-19 02:59:29 MST
                  Universal time: Thu 2020-11-19 09:59:29 UTC
                        RTC time: n/a
                       Time zone: America/Denver (MST, -0700)
       System clock synchronized: yes
systemd-timesyncd.service active: no
                 RTC in local TZ: no
```

```
ty2069@client-1:~$ timedatectl
                      Local time: Thu 2020-11-19 02:59:31 MST
                  Universal time: Thu 2020-11-19 09:59:31 UTC
                        RTC time: n/a
                       Time zone: America/Denver (MST, -0700)
       System clock synchronized: yes
systemd-timesyncd.service active: no
                 RTC in local TZ: no
```

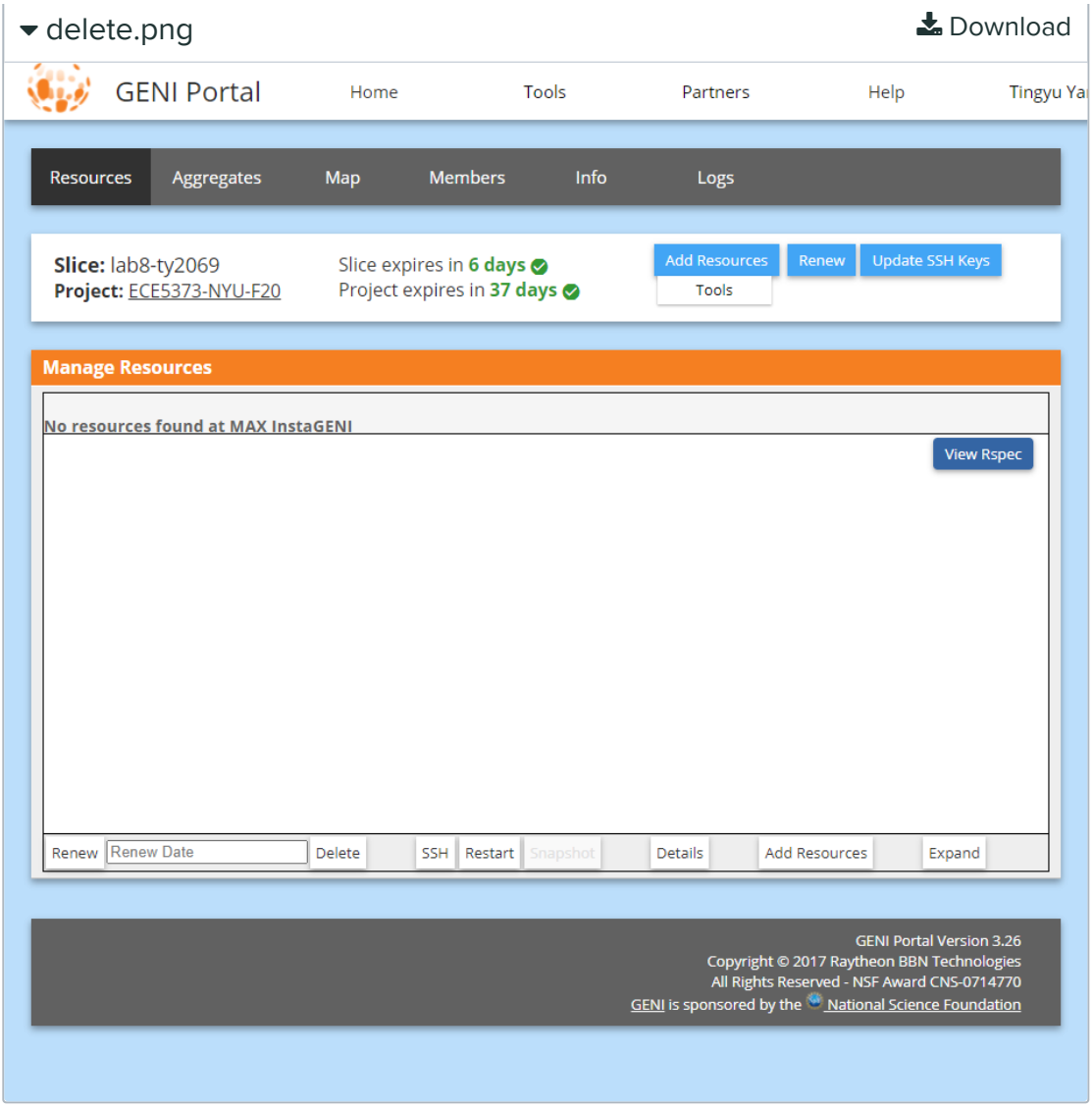
Q6 Delete your resources, please

0 Points

Did you delete your resources in the GENI Portal? After you have finished submitting your answers to the questions above, delete your resources so that they will be available to other experimenters.

- [x] Yes, I deleted my resources.

Upload a screenshot of the slice page for each of the slices that you used for lab 5. Your screenshots should show that there are no resources left in your slice.



Lab 8: The Web, DHCP, NTP and NAT

UNGRADED

STUDENT

Tingyu Yang

TOTAL POINTS

- / 10 pts

QUESTION 1

DHCP		2 pts
1.1	DHCP Discover	0.5 pts
1.2	DHCP Offer	0.5 pts
1.3	DHCP Request	0.5 pts
1.4	DHCP ACK	0.5 pts

QUESTION 2

DNS		2 pts
2.1	Simple DNS	1 pt
2.2	Hierarchical DNS query	1 pt

QUESTION 3

NAT		1 pt
3.1	NAT rewriting	1 pt

QUESTION 4

8.7 HTTP exercises		3 pts
4.1	Write and send an HTTP request (Exercise 2)	1 pt
4.2	HTTP with KeepAlive on (Exercise 3)	1 pt
4.3	HTTP with KeepAlive off (Exercise 3)	1 pt

QUESTION 5

8.9 NTP exercises		2 pts
5.1	NTP servers (Exercise 7)	0.5 pts
5.2	NTP request and response (Exercise 7)	1 pt
5.3	Synchronizing hosts on a LAN with NTP (Exercise 8)	0.5 pts

QUESTION 6

Delete your resources, please	0 pts