hw7

1. a) IPv4 has more fields and the header itself is shorter. It has fields like checksum, options, fragmenting, etc that IPv6 doesn't. IPv6 has something called Flow Label and Traffic class which IPv4 doesn't. They both have version and source/dest but the source/dest is much longer for IPv6. Both also have a payload but that is obvious
   b) Yes the router is using NAT because only one IP address is given. The router is the only one with an IP address given by the ISP so it has to be using a NAT. Because of this, the 5 devices are given a local IP address by the router that will be used within the network. These IP addresses will be chosen by the network but are usually starting with 10.0.0.0. To get these IP address, DHCP will be used between the router and the devices themselves.
2. a) From x

Step	N'	D(t) , p(t)	D(v) , p(v)	D(u) , p(u)	D(y) , p(y)	D(z) , p(z)	D(w) , p(w)
0	x	inf	3 , x	inf	6 , x	8 , x	6 , x
1	x v	7 , v	3 , x	6 , v	6 , x	8 , x	6 , x
2	x v w	7 , v	3 , x	6 , v	6 , x	8 , x	6 , x
3	x v w y	7 , v	3 , x	6 , v	6 , x	8 , x	6 , x
4	x v w y u	7 , v	3 , x	6 , v	6 , x	8 , x	6 , x
5	x v w y u t	7 , v	3 , x	6 , v	6 , x	8 , x	6 , x
6	x v w y u t z	7 , v	3 , x	6 , v	6 , x	8 , x	6 , x

```
b) From t
```

Step	N'	D(v) , p(v)	D(x) , p(x)	D(z) , p(z)	D(y) , p(y)	D(u) , p(u)	D(w) , p(w)
0	t	4 , t	inf	inf	7 , t	2 , t	inf
1	t u	4 , t	inf	inf	7 , t	2 , t	5 , u
2	t u v	4 , t	7 , v	inf	7 , t	2 , t	5 , u
3	t u v w	4 , t	7 , v	inf	7 , t	2 , t	5 , u
4	t u v w x	4 , t	7 , v	15 , x	7 , t	2 , t	5 , u

Step	N'	D(v) , p(v)	D(x) , p(x)	D(z) , p(z)	D(y) , p(y)	D(u) , p(u)	D(w) , p(w)
5	t u v w x y	4 , t	7 , v	15 , x	7 , t	2 , t	5 , u
6	t u v w x y z	4 , t	7 , v	15 , x	7 , t	2 , t	5 , u

3.

```
IFCONFIG(8)                                Linux System Administrator's Manual                                IFCONFIG(8)

NAME
       ifconfig - configure a network interface

SYNOPSIS
       ifconfig [-v] [-a] [-s] [interface]
       ifconfig [-v] interface [aftype] options | address ...

DESCRIPTION
       Ifconfig  is  used to configure the kernel-resident network interfaces.  It is used at boot time to set up interfaces as necessary.  After that, it is usually only needed when debugging or when system
       tuning is needed.

       If no arguments are given, ifconfig displays the status of the currently active interfaces.  If a single interface argument is given, it displays the status of the given interface only; if a single -a
       argument is given, it displays the status of all interfaces, even those that are down.  Otherwise, it configures an interface.

Address Families
       If  the first argument after the interface name is recognized as the name of a supported address family, that address family is used for decoding and displaying all protocol addresses.  Currently sup-
       ported address families include inet (TCP/IP, default), inet6 (IPv6), ax25 (AMPR Packet Radio), ddp (Appletalk Phase 2), ipx (Novell IPX) and netrom (AMPR Packet radio).  All numbers supplied as parts
       in IPv4 dotted decimal notation may be decimal, octal, or hexadecimal, as specified in the ISO C standard (that is, a leading 0x or 0X implies hexadecimal; otherwise, a leading '0' implies octal; oth-
       erwise, the number is interpreted as decimal). Use of hexadecimal and octal numbers is not RFC-compliant and therefore its use is discouraged.

OPTIONS
       -a     display all interfaces which are currently available, even if down

       -s     display a short list (like netstat -i)

       -v     be more verbose for some error conditions

       interface
              The name of the interface.  This is usually a driver name followed by a unit number, for example eth0 for the first Ethernet interface. If your kernel supports alias interfaces, you can specify
              them with syntax like eth0:0 for the first alias of eth0. You can use them to assign more addresses. To delete an alias interface use ifconfig eth0:0 down.  Note: for every scope (i.e. same net
              with address/netmask combination) all aliases are deleted, if you delete the first (primary).

       up     This flag causes the interface to be activated.  It is implicitly specified if an address is assigned to the interface; you can suppress this behavior when using an alias interface by appending
              an - to the alias (e.g.  eth0:0-).  It is also suppressed when using the IPv4 0.0.0.0 address as the kernel will use this to implicitly delete alias interfaces.

       down   This flag causes the driver for this interface to be shut down.

       [-]arp Enable or disable the use of the ARP protocol on this interface.

       [-]promisc
              Enable or disable the promiscuous mode of the interface.  If selected, all packets on the network will be received by the interface.

       [-]allmulti
              Enable or disable all-multicast mode.  If selected, all multicast packets on the network will be received by the interface.

       mtu N  This parameter sets the Maximum Transfer Unit (MTU) of an interface.

       dstaddr addr
              Set the remote IP address for a point-to-point link (such as PPP).  This keyword is now obsolete; use the pointopoint keyword instead.
 Manual page ifconfig(8) line 1 (press h for help or q to quit)
```

```
NETSTAT(8)                                 Linux System Administrator's Manual                                NETSTAT(8)

NAME
       netstat  -  Print network connections, routing tables, interface statistics, masquerade connections, and multi-
       cast memberships

SYNOPSIS
       netstat [address_family_options]  [--tcp|-t]  [--udp|-u]  [--udplite|-U]  [--sctp|-S]  [--raw|-w]  [--l2cap|-2]
       [--rfcomm|-f]  [--listening|-l] [--all|-a] [--numeric|-n] [--numeric-hosts] [--numeric-ports] [--numeric-users]
       [--symbolic|-N]  [--extend|-e[--extend|-e]]  [--timers|-o]  [--program|-p]   [--verbose|-v]   [--continuous|-c]
       [--wide|-W]

       netstat  {--route|-r}  [address_family_options] [--extend|-e[--extend|-e]] [--verbose|-v] [--numeric|-n] [--nu-
       meric-hosts] [--numeric-ports] [--numeric-users] [--continuous|-c]

       netstat {--interfaces|-i} [--all|-a] [--extend|-e[--extend|-e]]  [--verbose|-v]  [--program|-p]  [--numeric|-n]
       [--numeric-hosts] [--numeric-ports] [--numeric-users] [--continuous|-c]

       netstat {--groups|-g} [--numeric|-n] [--numeric-hosts] [--numeric-ports] [--numeric-users] [--continuous|-c]

       netstat  {--masquerade|-M}  [--extend|-e]  [--numeric|-n] [--numeric-hosts] [--numeric-ports] [--numeric-users]
       [--continuous|-c]

       netstat {--statistics|-s} [--tcp|-t] [--udp|-u] [--udplite|-U] [--sctp|-S] [--raw|-w]

       netstat {--version|-V}

       netstat {--help|-h}

       address_family_options:

       [-4|--inet]  [-6|--inet6]  [--protocol={inet,inet6,unix,ipx,ax25,netrom,ddp,bluetooth,  ...  }  ]   [--unix|-x]
       [--inet|--ip|--tcpip]  [--ax25]  [--x25]  [--rose] [--ash] [--bluetooth] [--ipx] [--netrom] [--ddp|--appletalk]
       [--econet|--ec]

NOTES
       This program is mostly obsolete.  Replacement for netstat is ss.  Replacement for netstat -r is ip route.   Re-
       placement for netstat -i is ip -s link.  Replacement for netstat -g is ip maddr.

DESCRIPTION
       Netstat prints information about the Linux networking subsystem.  The type of information printed is controlled
       by the first argument, as follows:

   (none)
       By default, netstat displays a list of open sockets.  If you don't specify any address families, then  the  ac-
       tive sockets of all configured address families will be printed.

   --route, -r
       Display  the  kernel routing tables. See the description in route(8) for details.  netstat -r and route -e pro-
       duce the same output.

 Manual page netstat(8) line 1 (press h for help or q to quit)
```

a)

```
~ ❯ netstat -s
Ip:
    Forwarding: 1
    96615 total packets received
    1 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    96592 incoming packets delivered
    76426 requests sent out
    20 outgoing packets dropped
    352 dropped because of missing route
    OutTransmits: 76426
Icmp:
    167 ICMP messages received
    0 input ICMP message failed
    ICMP input histogram:
        destination unreachable: 167
    233 ICMP messages sent
    0 ICMP messages failed
    OutRateLimitHost: 5
    ICMP output histogram:
        destination unreachable: 233
IcmpMsg:
        InType3: 167
        OutType3: 233
Tcp:
    2833 active connection openings
    8 passive connection openings
    38 failed connection attempts
    165 connection resets received
    5 connections established
    110264 segments received
    108152 segments sent out
    1179 segments retransmitted
    0 bad segments received
    1029 resets sent
Udp:
    35370 packets received
    238 packets to unknown port received
    0 packet receive errors
    16683 packets sent
    0 receive buffer errors
    0 send buffer errors
    IgnoredMulti: 594
UdpLite:
TcpExt:
    17 packets pruned from receive queue because of socket buffer overrun
    1783 TCP sockets finished time wait in fast timer
    1 packetes rejected in established connections because of timestamp
    1364 delayed acks sent
    2 delayed acks further delayed because of locked socket
    Quick ack mode was activated 753 times
```

The -s flag shows statistics of the protocol including information like packet type and amount received, dropped packets, etc. In the screenshot, we can see different protocols like Ip, TCP, UDP, and more and each line has different statistics about the protocol. Like for example there are 2833 active TCP connections.

```
unix  3      [ ]         STREAM     CONNECTED     90373    @/home/ajain/.cache/ibus/dbus-1IplxVFL
unix  3      [ ]         STREAM     CONNECTED     22721
unix  3      [ ]         STREAM     CONNECTED     19101
unix  3      [ ]         STREAM     CONNECTED     17334    /run/systemd/journal/stdout
unix  2      [ ]         SEQPACKET  CONNECTED     74325
unix  3      [ ]         STREAM     CONNECTED     13423    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     281450
unix  3      [ ]         STREAM     CONNECTED     20387
unix  3      [ ]         STREAM     CONNECTED     25649    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     20267
unix  2      [ ]         DGRAM                    257364
unix  3      [ ]         STREAM     CONNECTED     23992
unix  3      [ ]         STREAM     CONNECTED     23845
unix  3      [ ]         STREAM     CONNECTED     17215    @/tmp/dbus-GiXo5BtY
unix  3      [ ]         STREAM     CONNECTED     284106
unix  3      [ ]         STREAM     CONNECTED     251087
unix  3      [ ]         STREAM     CONNECTED     174100
unix  3      [ ]         STREAM     CONNECTED     89805    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     22718    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     20266    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     21706
unix  3      [ ]         STREAM     CONNECTED     8968     /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     247690
unix  3      [ ]         STREAM     CONNECTED     20367
unix  3      [ ]         STREAM     CONNECTED     21935    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     46357    /run/user/1000/pulse/native
unix  3      [ ]         STREAM     CONNECTED     23873
unix  3      [ ]         STREAM     CONNECTED     24805
unix  3      [ ]         STREAM     CONNECTED     92953
unix  3      [ ]         STREAM     CONNECTED     91265    /run/user/1000/gvfsd/socket-dESBqQqs
unix  3      [ ]         STREAM     CONNECTED     257623   /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     174102
unix  3      [ ]         STREAM     CONNECTED     24797    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     21711
unix  3      [ ]         STREAM     CONNECTED     12216
unix  3      [ ]         STREAM     CONNECTED     15383    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     20371
unix  3      [ ]         STREAM     CONNECTED     25741    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     19202    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     248526
unix  3      [ ]         STREAM     CONNECTED     101504   /run/user/1000/at-spi/bus_0
unix  3      [ ]         STREAM     CONNECTED     18568    /run/systemd/journal/stdout
unix  2      [ ]         STREAM     CONNECTED     263362
unix  3      [ ]         STREAM     CONNECTED     40492
unix  3      [ ]         STREAM     CONNECTED     284103
unix  3      [ ]         STREAM     CONNECTED     22658    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     285019
unix  3      [ ]         STREAM     CONNECTED     169603
unix  3      [ ]         STREAM     CONNECTED     93959
unix  3      [ ]         STREAM     CONNECTED     22055    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     20276    /run/user/1000/bus
```

The -c flag shows the network connections but updates it every second so the information it is giving is in real time and not out of date. Other than that the info is the same as just regular netstat which shows active internet and local connections

```
~ ❯ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG        0 0          0 wlo1
10.109.0.0      0.0.0.0         255.255.128.0   U         0 0          0 wlo1
link-local      0.0.0.0         255.255.0.0     U         0 0          0 wlo1
172.17.0.0      0.0.0.0         255.255.0.0     U         0 0          0 docker0
172.18.0.0      0.0.0.0         255.255.0.0     U         0 0          0 br-fb96648c4518
~ ❯
```

The -r flag shows the routing table for the kernel which essentially just tells the computer where to route traffic. Looking at the last entry, the address 172.18.0.0 is the network for the route (in this case I think it is a doker container), the gateway is none, the mask is for the size of the network (/16), the flag is U which means active. The next 2 are for max segment/window size (not used). irtt is round trip estimate (not used). And the last one is the network interface which according to google is a docker bridge.

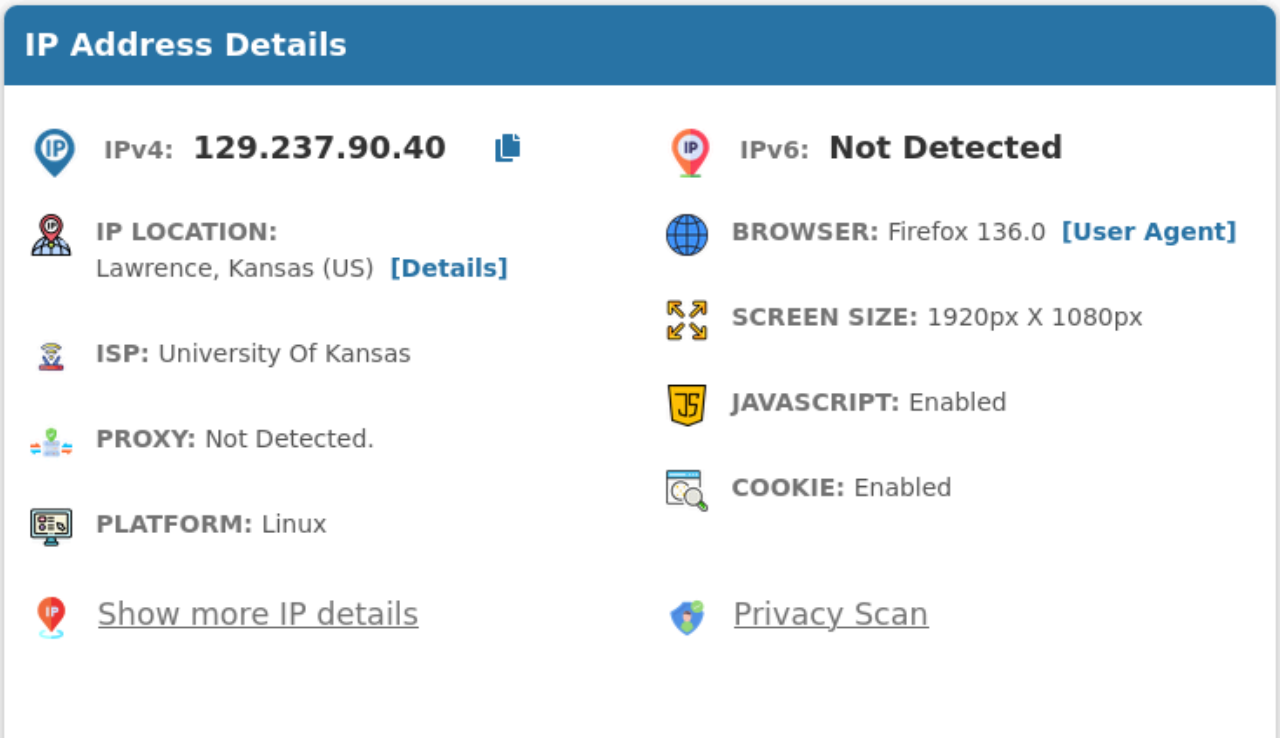
b)

```
~ ❯ sudo cat /var/lib/dhcp/dhclient.leases

lease {
  interface "wlo1";
  fixed-address 10.109.108.146;
  option subnet-mask 255.255.128.0;
  option routers 10.109.127.254;
  option dhcp-lease-time 480;
  option dhcp-message-type 5;
  option domain-name-servers 164.113.207.250,164.113.221.250;
  option dhcp-server-identifier 129.237.32.1;
  option domain-search "ku.edu.";
  option broadcast-address 10.109.127.255;
  renew 1 2025/04/28 18:31:26;
  rebind 1 2025/04/28 18:31:26;
  expire 1 2025/04/28 18:31:26;
}
lease {
  interface "wlo1";
  fixed-address 10.109.108.146;
  option subnet-mask 255.255.128.0;
  option routers 10.109.127.254;
  option dhcp-lease-time 468;
  option dhcp-message-type 5;
  option domain-name-servers 164.113.207.250,164.113.221.250;
  option dhcp-server-identifier 129.237.32.1;
  option domain-search "ku.edu.";
  option broadcast-address 10.109.127.255;
  renew 1 2025/04/28 18:34:47;
  rebind 1 2025/04/28 18:38:19;
  expire 1 2025/04/28 18:39:18;
}
```

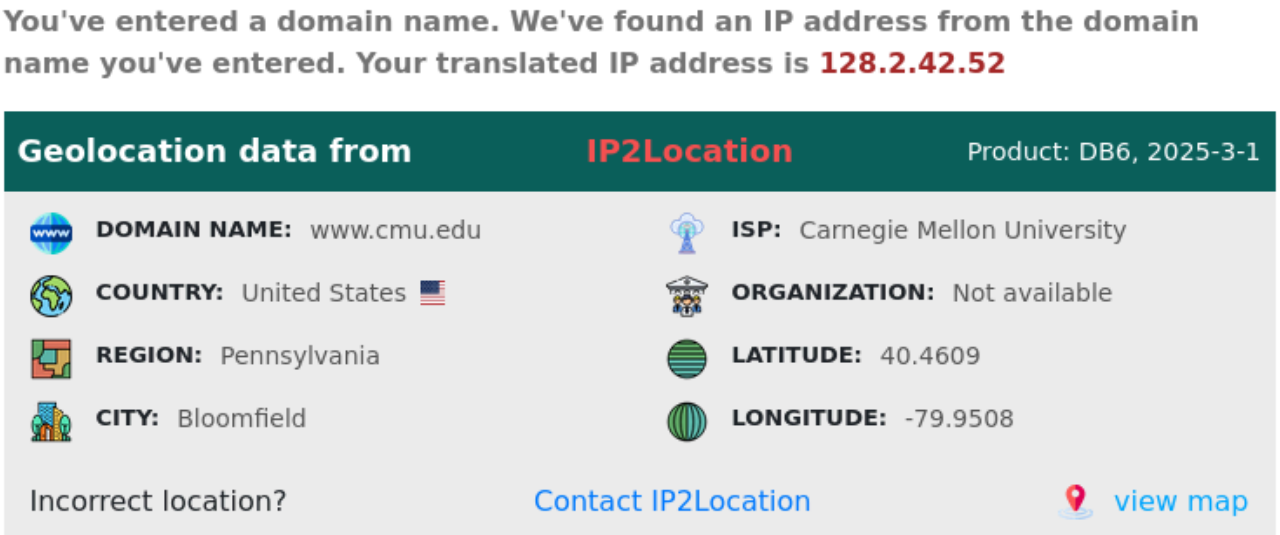
This is for KU. The first lease was replaced by the second entry when I forced my computer to renew the lease (I wasn't sure if I did it right). It is cool to see a history of the leases. The mask is /17 and The lease length is 8 mins which is not very long. The DHCP broadcast address is 10.109.127.255 which is the highest address for /17

```
~ ❯ sudo cat /var/lib/dhcp/dhclient.leases

lease {
  interface "wlo1";
  fixed-address 10.108.66.160;
  option subnet-mask 255.255.128.0;
  option routers 10.108.127.254;
  option dhcp-lease-time 7182;
  option dhcp-message-type 5;
  option domain-name-servers 164.113.207.250,164.113.221.250;
  option dhcp-server-identifier 129.237.32.1;
  option domain-search "ku.edu.";
  option broadcast-address 10.108.127.255;
  renew 2 2025/04/29 23:31:42;
  rebind 2 2025/04/29 23:31:42;
  expire 2 2025/04/29 23:31:42;
}
lease {
  interface "wlo1";
  fixed-address 192.168.1.227;
  option subnet-mask 255.255.255.0;
  option routers 192.168.1.1;
  option dhcp-lease-time 43200;
  option dhcp-message-type 5;
  option domain-name-servers 192.168.1.1;
  option dhcp-server-identifier 192.168.1.1;
  option dhcp-renewal-time 21600;
  option broadcast-address 192.168.1.255;
  option dhcp-rebinding-time 37800;
  option host-name "ajain-HP-ENVY-x360-Convertible-15-bp1xx";
  option domain-name "home.local";
  renew 3 2025/04/30 04:55:01;
  rebind 3 2025/04/30 10:01:48;
  expire 3 2025/04/30 11:31:48;
}
~ ❯
```

This is at my apartment. The top one is ku (once again) and then the bottom one is my apartment. Here we can see that the duration for the lease at my house is a lot more than the one at my university. We can also see that my network is /24 which is different. An interesting aspect is that the DNS here is the same as the router which according to a google search means that the router will help fetch the IP address and then give it to the user.

4. 

School, accurate



Different university (CMU), accurate

Geolocation data from IP2Location Product: DB6, 2025-3-1

DOMAIN NAME: aniketh.dev
ISP: CloudFlare Inc.
COUNTRY: United States
ORGANIZATION: Not available
REGION: California
LATITUDE: 37.7757
CITY: San Francisco
LONGITUDE: -122.3952

Incorrect location? Contact IP2Location view map

Geolocation data from ipinfo.io Product: API, real-time

Friend's website hosted with cloudflare, also accurate because cloudflare is based in SF.

Geolocation data from IP2Location Product: DB6, 2025-3-1

DOMAIN NAME: ethz.ch
ISP: Federal Institute of Technology Zurich
COUNTRY: Switzerland
ORGANIZATION: Not available
REGION: Zurich
LATITUDE: 47.3668
CITY: Zurich
LONGITUDE: 8.5498

Incorrect location? Contact IP2Location view map

Geolocation data from ipinfo.io Product: API, real-time

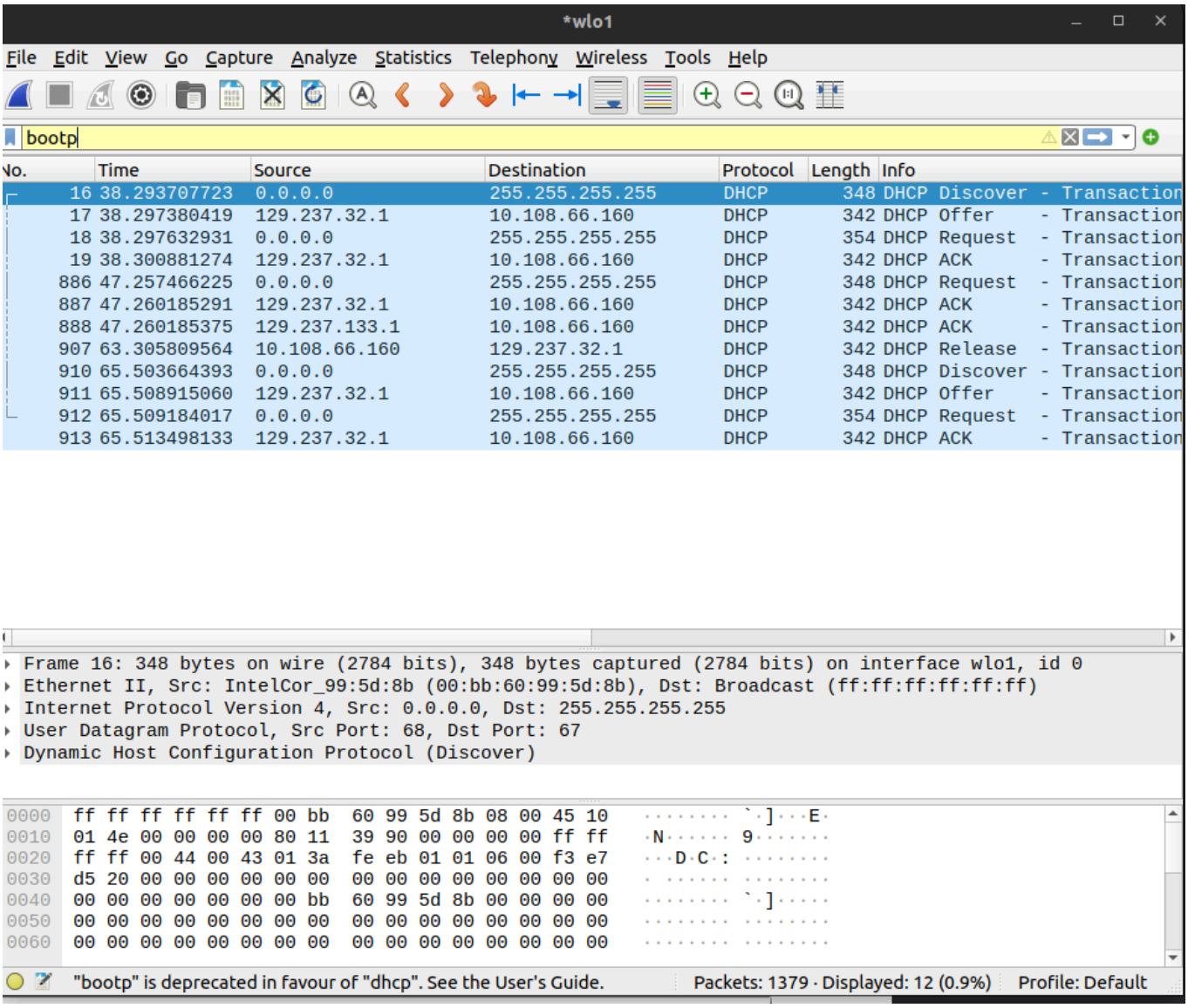
Zurich website, also accurate

All of the websites were accurate when it came to finding the city of hosting.

b) One use case is for services to target info to people living in certain areas. There is no point in showing news articles about a city in China to someone living in North Dakota so being able to target the user with information that is closer (literally) to them is useful. The other is to track malicious users. If there is someone committing crimes on the internet then you can find where they are and respond with law enforcement in that city.

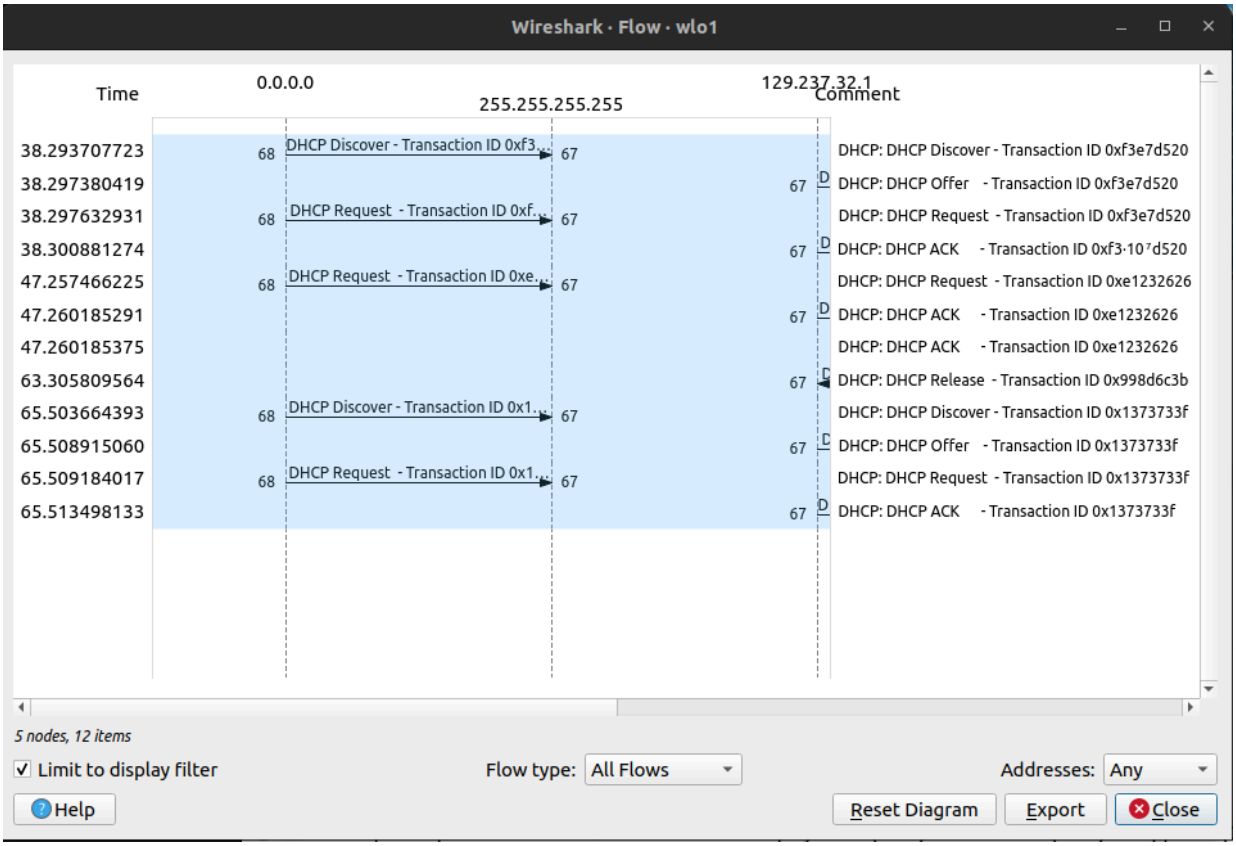
Lab

```
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/wlo1/00:bb:60:99:5d:8b
Sending on   LPF/wlo1/00:bb:60:99:5d:8b
Sending on   Socket/fallback
DHCPDISCOVER on wlo1 to 255.255.255.255 port 67 interval 3 (xid=0xf3e7d520)
DHCPOFFER of 10.108.66.160 from 129.237.32.1
DHCPREQUEST for 10.108.66.160 on wlo1 to 255.255.255.255 port 67 (xid=0x20d5e7f3)
DHCPACK of 10.108.66.160 from 129.237.32.1 (xid=0xf3e7d520)
bound to 10.108.66.160 -- renewal in 2787 seconds.
~ ❯ sudo dhclient -v wlo1
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/wlo1/00:bb:60:99:5d:8b
Sending on   LPF/wlo1/00:bb:60:99:5d:8b
Sending on   Socket/fallback
DHCPREQUEST for 10.108.66.160 on wlo1 to 255.255.255.255 port 67 (xid=0x262623e1)
DHCPACK of 10.108.66.160 from 129.237.32.1 (xid=0xe1232626)
Error: ipv4: Address already assigned.
bound to 10.108.66.160 -- renewal in 2813 seconds.
~ ❯ sudo dhclient -v -r wlo1
Killed old client process
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/wlo1/00:bb:60:99:5d:8b
Sending on   LPF/wlo1/00:bb:60:99:5d:8b
Sending on   Socket/fallback
DHCPRELEASE of 10.108.66.160 on wlo1 to 129.237.32.1 port 67 (xid=0x5da40e3d)
~ ❯ sudo dhclient -v wlo1
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/wlo1/00:bb:60:99:5d:8b
Sending on   LPF/wlo1/00:bb:60:99:5d:8b
Sending on   Socket/fallback
DHCPDISCOVER on wlo1 to 255.255.255.255 port 67 interval 3 (xid=0x1373733f)
DHCPOFFER of 10.108.66.160 from 129.237.32.1
DHCPREQUEST for 10.108.66.160 on wlo1 to 255.255.255.255 port 67 (xid=0x3f737313)
DHCPACK of 10.108.66.160 from 129.237.32.1 (xid=0x1373733f)
bound to 10.108.66.160 -- renewal in 3102 seconds.
~ ❯
```



1. UDP
2. The process of DHCP has 4 steps
    1. First, DHCP Discover is used to send a message to the network that it is looking for an IP address
    2. Second, the DHCP server sends a message with an IP (and other info sometimes). This IP is what the client can use (DHCP offer)
    3. Third, the user then asks to use that available IP address (DHCP request)

4. And lastly, the DHCP confirms that client is using that IP with DHCP ACK



3.

Packet	Source IP	Source Port	Dest IP	Dest port
DHCP Discover	0.0.0.0	68	255.255.255.255	67
DHCP Offer	129.237.32.1	67	10.108.66.160	68
DHCP Request	0.0.0.0	68	255.255.255.255	67
DHCP ACK	129.237.32.1	67	10.108.66.160	68

4. There are a couple differentiating factors. The most important is in the options 53 field where value of 1 is for discover and value of 3 is Request. Secondly reqest has another field 54 for a server identifier which checks out because now we know what the server is Discover:

```
    Client MAC address: IntelCor_99:5d:8b (00:bb:60:99:5d:8b)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▾ Option: (53) DHCP Message Type (Discover)
      Length: 1
      DHCP: Discover (1)
  ▸ Option: (50) Requested IP Address (10.108.66.160)
  ▸ Option: (12) Host Name
  ▸ Option: (55) Parameter Request List
  ▸ Option: (255) End
```

DHCP/BOOTP option type ...p.option.type), 3 bytes Packets: 1379 · Displa

Request:

```
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▾ Option: (53) DHCP Message Type (Request)
      Length: 1
      DHCP: Request (3)
  ▸ Option: (54) DHCP Server Identifier (129.237.32.1)
  ▸ Option: (50) Requested IP Address (10.108.66.160)
  ▸ Option: (12) Host Name
  ▸ Option: (55) Parameter Request List
  ▸ Option: (255) End
```

DHCP/BOOTP option type ...p.option.type), 3 bytes Packets: 1379 · Displa

5. The transaction IDs are as follows:

No.	Time	Info
16	38.293707723	DHCP Discover - Transaction ID 0xf3e7d520
17	38.297380419	DHCP Offer - Transaction ID 0xf3e7d520
18	38.297632931	DHCP Request - Transaction ID 0xf3e7d520
19	38.300881274	DHCP ACK - Transaction ID 0xf3e7d520
886	47.257466225	DHCP Request - Transaction ID 0xe1232626
887	47.260185291	DHCP ACK - Transaction ID 0xe1232626
888	47.260185375	DHCP ACK - Transaction ID 0xe1232626
907	63.305809564	DHCP Release - Transaction ID 0x998d6c3b
910	65.503664393	DHCP Discover - Transaction ID 0x1373733f
911	65.508915060	DHCP Offer - Transaction ID 0x1373733f
912	65.509184017	DHCP Request - Transaction ID 0x1373733f
913	65.513498133	DHCP ACK - Transaction ID 0x1373733f

They exist in order to keep track of which DHCP request chain each message belongs to. If a server gives 2 DHCP messages to the same laptop, it can help differentiate which it belongs to. The first set has transaction ID 0xf3e7d520 and the second set has 0xe1232626

6. The DHCP server is 129.237.32.1. This is found in two places, first the source of the offer and ack packets. Secondly it can be found in Option 54 of the DHCP request packet. The pictures are above
7. Again the IP is 129.237.32.1. Found in Option 54

```
▸ Option: (53) DHCP Message Type (Offer)
▸ Option: (54) DHCP Server Identifier (129.237.32.1)
▸ Option: (51) IP Address Lease Time
▸ Option: (1) Subnet Mask (255.255.128.0)
▸ Option: (28) Broadcast Address (10.108.127.255)
▸ Option: (3) Router
▸ Option: (6) Domain Name Server
▸ Option: (119) Domain Search
▸ Option: (255) End
  Padding: 000000000000
```

8. The lease time is like a check-in to make sure you are still there. After a certain amount of time, if the lease is expired and the user is gone, we can forgo the connection so that we don't sustain connections that are gone. The IP is now freed up and can be used by someone else. If the user wishes to stay connected, they simply renew the lease and then nothing changes.
   For us, the lease time is 7200s or 2 hours which makes sense as students enter and leave campus frequently (I am on campus)

```
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
▸ Option: (53) DHCP Message Type (Offer)
▸ Option: (54) DHCP Server Identifier (129.237.32.1)
▾ Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: (7200s) 2 hours
▸ Option: (1) Subnet Mask (255.255.128.0)
▸ Option: (28) Broadcast Address (10.108.127.255)
▸ Option: (3) Router
▾ Option: (6) Domain Name Server
```