Jan-14 Lecture

Today’s Goal

- Learning (to learn) about some of the tools available to:

  1. understand what is happening at the local host, and

  2. learning to dig into the network to see (and measure) what is happening

- Class reading for today are the man pages for most of the tools

Network Goals

- Discover information about the network

- The challenge is that it is surprisingly difficult to do
  - Layering in the protocol stack hides much of the Internet’s complexity
  - Information about conditions in the network is typically not made available to users (or to competitors)
  - What tools that do exist are less-and-less supported (for reasons of security)
    - Lots more encryption
    - Lots of disabling of services like ping (avoids scanning and DOS attacks)

- What are examples of tools people have used?

Useful Network Tools

- ifconfig* (now ip link*)
- arp* (now ip neighbor*)
- ping*
- traceroute*
- geotrace
- Bandwidth estimators
- router looking glass
- nslookup/host/dig*
- netstat/ss*
- whois/jwhois*
- Wireshark: packet-level snooping
- Firesheep: cookie snooping
- Fiddler: HTTP session snooping

Categories

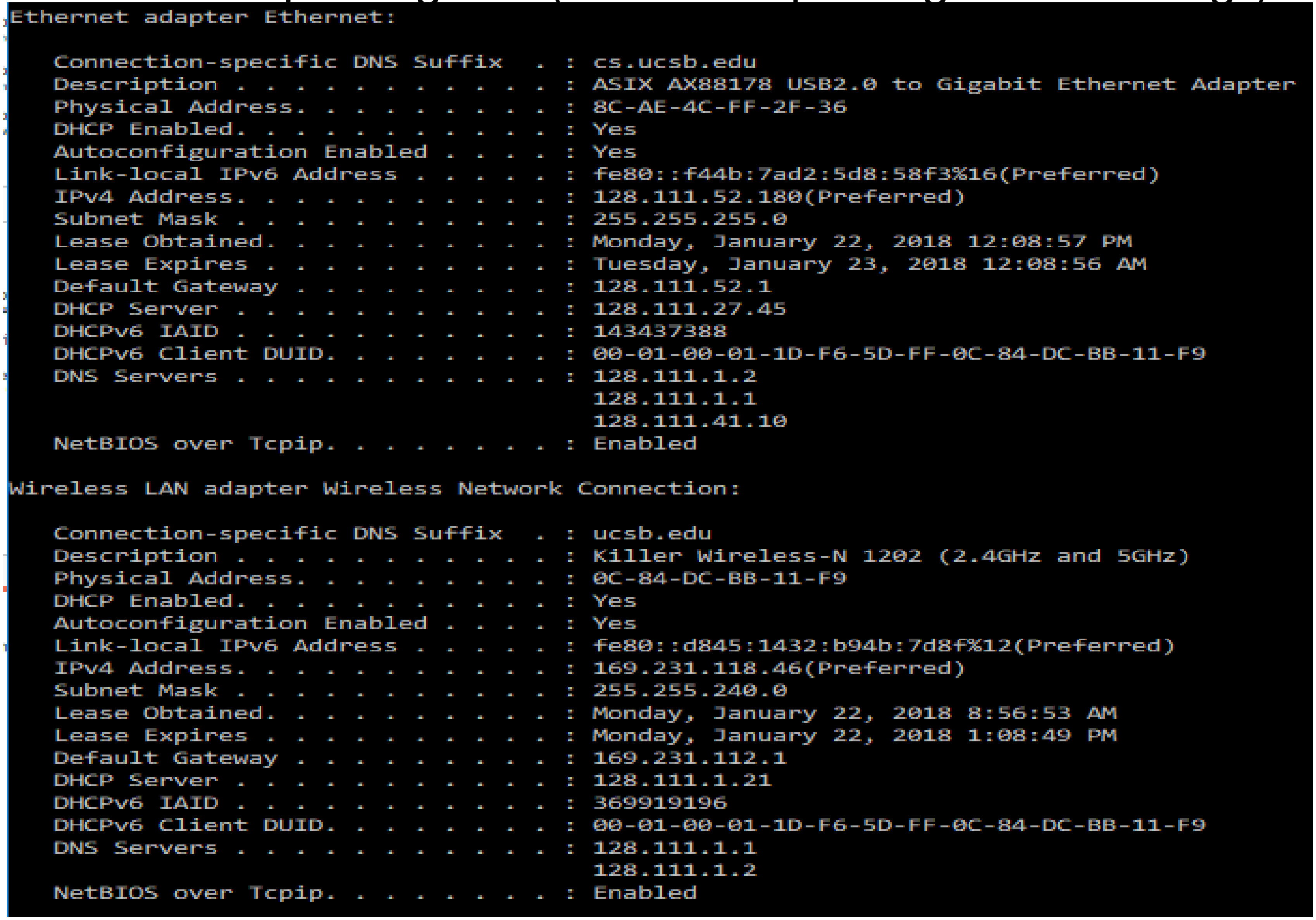
- Tools about local network interface
  - ifconfig* (now ip link*), arp* (now ip neighbor*), netstat/ss*
- Tools about network path
  - ping*, traceroute*, geotrace, bandwidth estimators
- Tools about routing
  - router looking glass
- Tools about remote hosts/networks
  - nslookup/host/dig*, whois/jwhois*
- Tools about network traffic
  - wireshark, firesheep, fiddler

ifconfig/ip link

- Information about interfaces
  - Also allows configuration of interfaces
- Varies by platform (as do most of these tools)
- The older version is “ifconfig”, the newer version is “ip” with the option of “link”

ifconfig/ip link

- Windows: ipconfig /all (note it is “ipconfig” not “ifconfig”)



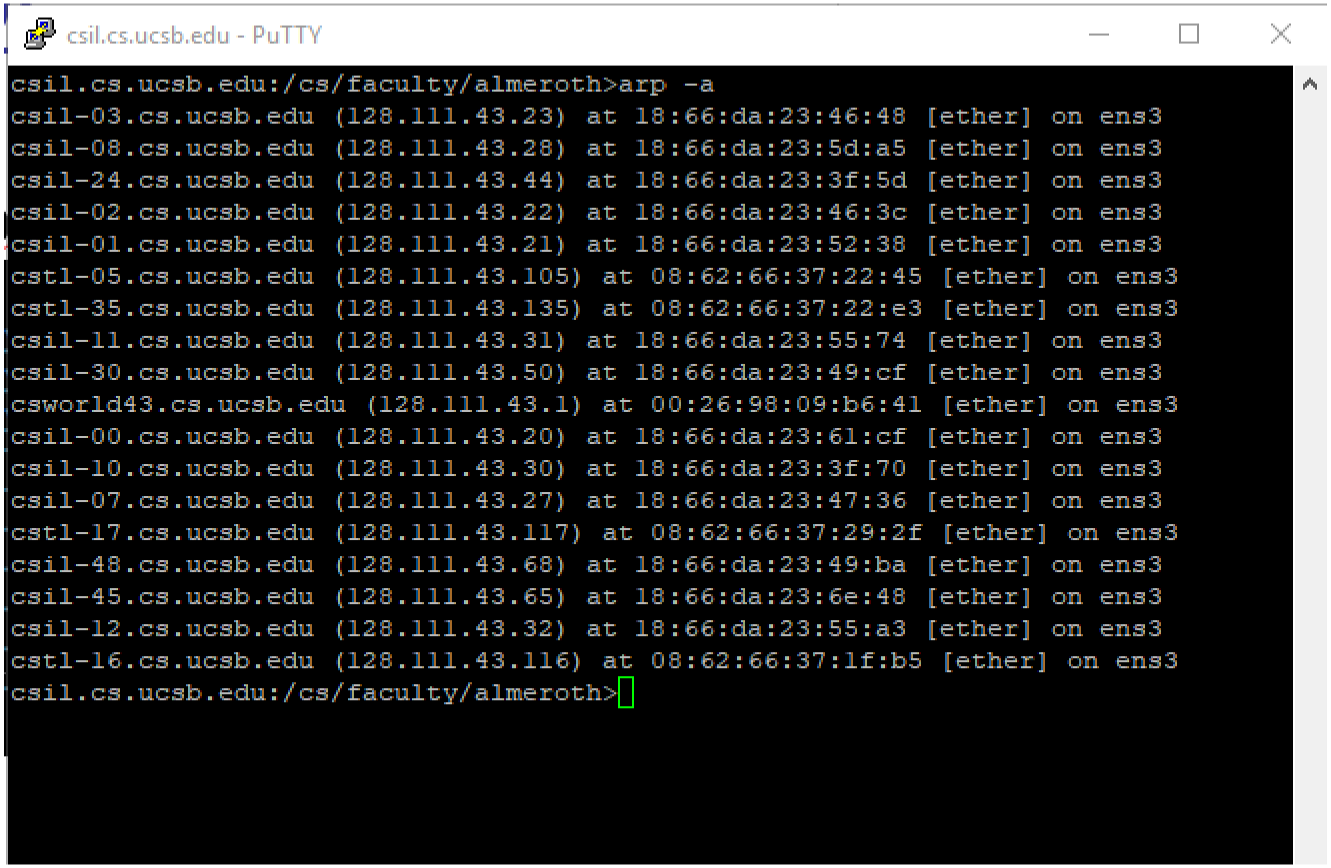
```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : cs.ucsb.edu
   Description . . . . . . . . . . . : ASIX AX88178 USB2.0 to Gigabit Ethernet Adapter
   Physical Address. . . . . . . . . : 8C-AE-4C-FF-2F-36
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::f44b:7ad2:5d8:58f3%16(Preferred)
   IPv4 Address. . . . . . . . . . . : 128.111.52.180(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, January 22, 2018 12:08:57 PM
   Lease Expires . . . . . . . . . . : Tuesday, January 23, 2018 12:08:56 AM
   Default Gateway . . . . . . . . . : 128.111.52.1
   DHCP Server . . . . . . . . . . . : 128.111.27.45
   DHCPv6 IAID . . . . . . . . . . . : 143437388
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1D-F6-5D-FF-0C-84-DC-BB-11-F9
   DNS Servers . . . . . . . . . . . : 128.111.1.2
                                       128.111.1.1
                                       128.111.41.10
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . : ucsb.edu
   Description . . . . . . . . . . . : Killer Wireless-N 1202 (2.4GHz and 5GHz)
   Physical Address. . . . . . . . . : 0C-84-DC-BB-11-F9
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d845:1432:b94b:7d8f%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 169.231.118.46(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Lease Obtained. . . . . . . . . . : Monday, January 22, 2018 8:56:53 AM
   Lease Expires . . . . . . . . . . : Monday, January 22, 2018 1:08:49 PM
   Default Gateway . . . . . . . . . : 169.231.112.1
   DHCP Server . . . . . . . . . . . : 128.111.1.21
   DHCPv6 IAID . . . . . . . . . . . : 369919196
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1D-F6-5D-FF-0C-84-DC-BB-11-F9
   DNS Servers . . . . . . . . . . . : 128.111.1.1
                                       128.111.1.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

ifconfig/ip link

- Windows: ipconfig /all (note it is “ipconfig” not “ifconfig”)
- Unix:
  - ifconfig (-v -a)
  - ip link

ip neighbor

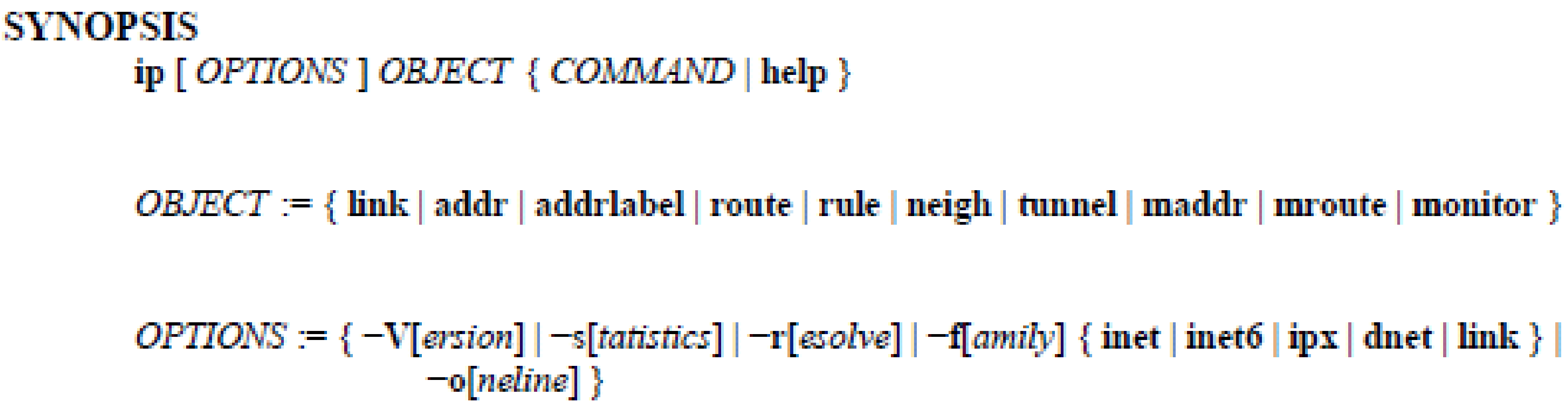
- “ip neighbor” shows ARP table (replaces “arp –a”)



```
csil.cs.ucsb.edu:/cs/faculty/almeroth>arp -a
csil-03.cs.ucsb.edu (128.111.43.23) at 18:66:da:23:46:48 [ether] on ens3
csil-08.cs.ucsb.edu (128.111.43.28) at 18:66:da:23:5d:a5 [ether] on ens3
csil-24.cs.ucsb.edu (128.111.43.44) at 18:66:da:23:3f:5d [ether] on ens3
csil-02.cs.ucsb.edu (128.111.43.22) at 18:66:da:23:46:3c [ether] on ens3
csil-01.cs.ucsb.edu (128.111.43.21) at 18:66:da:23:52:38 [ether] on ens3
cstl-05.cs.ucsb.edu (128.111.43.105) at 08:62:66:37:22:45 [ether] on ens3
cstl-35.cs.ucsb.edu (128.111.43.135) at 08:62:66:37:22:e3 [ether] on ens3
csil-11.cs.ucsb.edu (128.111.43.31) at 18:66:da:23:55:74 [ether] on ens3
csil-30.cs.ucsb.edu (128.111.43.50) at 18:66:da:23:49:cf [ether] on ens3
csworld43.cs.ucsb.edu (128.111.43.1) at 00:26:98:09:b6:41 [ether] on ens3
csil-00.cs.ucsb.edu (128.111.43.20) at 18:66:da:23:61:cf [ether] on ens3
csil-10.cs.ucsb.edu (128.111.43.30) at 18:66:da:23:3f:70 [ether] on ens3
csil-07.cs.ucsb.edu (128.111.43.27) at 18:66:da:23:47:36 [ether] on ens3
cstl-17.cs.ucsb.edu (128.111.43.117) at 08:62:66:37:29:2f [ether] on ens3
csil-48.cs.ucsb.edu (128.111.43.68) at 18:66:da:23:49:ba [ether] on ens3
csil-45.cs.ucsb.edu (128.111.43.65) at 18:66:da:23:6e:48 [ether] on ens3
csil-12.cs.ucsb.edu (128.111.43.32) at 18:66:da:23:55:a3 [ether] on ens3
cstl-16.cs.ucsb.edu (128.111.43.116) at 08:62:66:37:1f:b5 [ether] on ens3
csil.cs.ucsb.edu:/cs/faculty/almeroth>
```

- Still arp –a on Windows

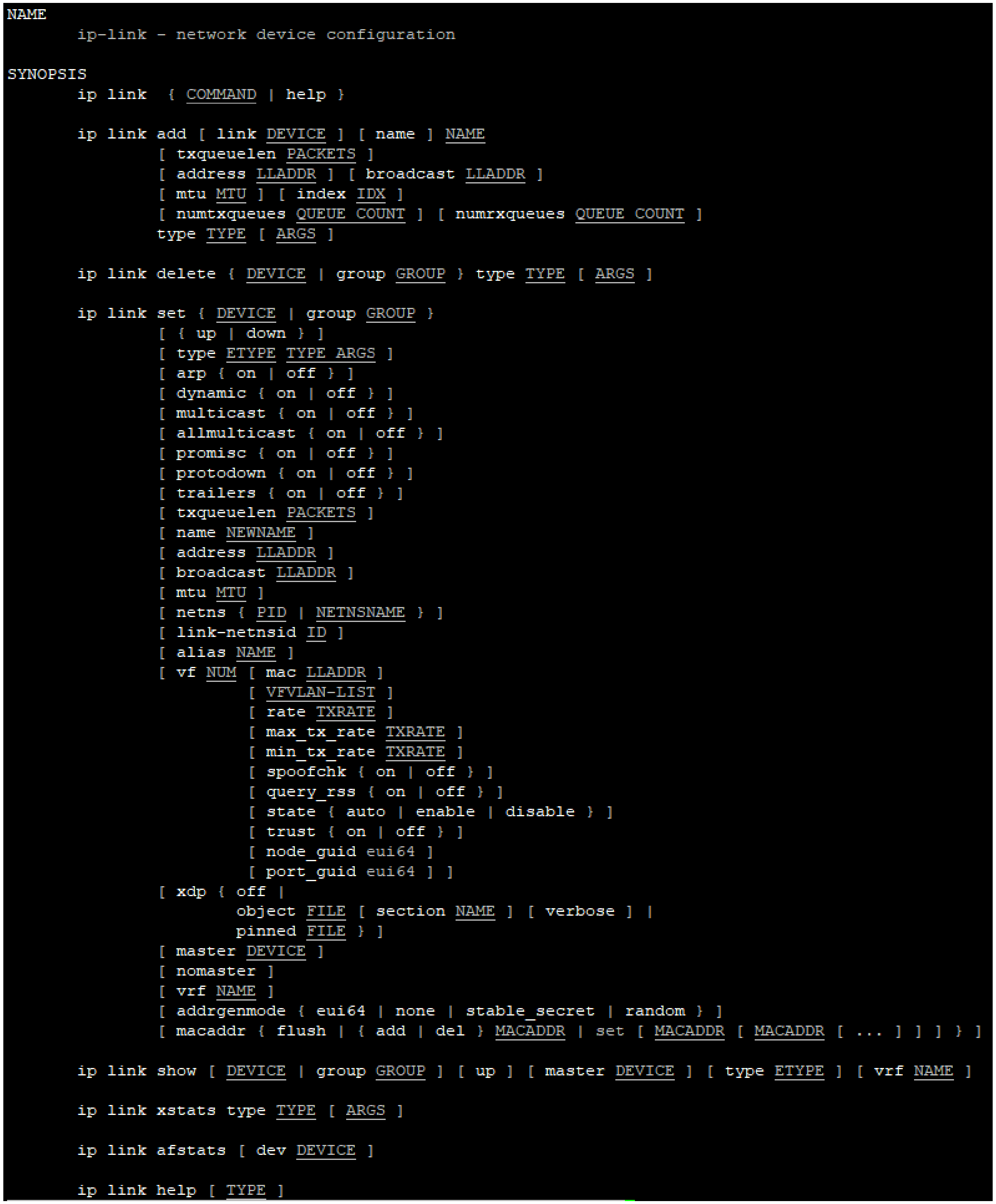
ip command



```
SYNOPSIS
       ip [ OPTIONS ] OBJECT { COMMAND | help }

       OBJECT := { link | addr | addrlabel | route | rule | neigh | tunnel | maddr | mroute | monitor }

       OPTIONS := { −V[ersion] | −s[tatistics] | −r[esolve] | −f[amily] { inet | inet6 | ipx | dnet | link } |
                    −o[neline] }
```

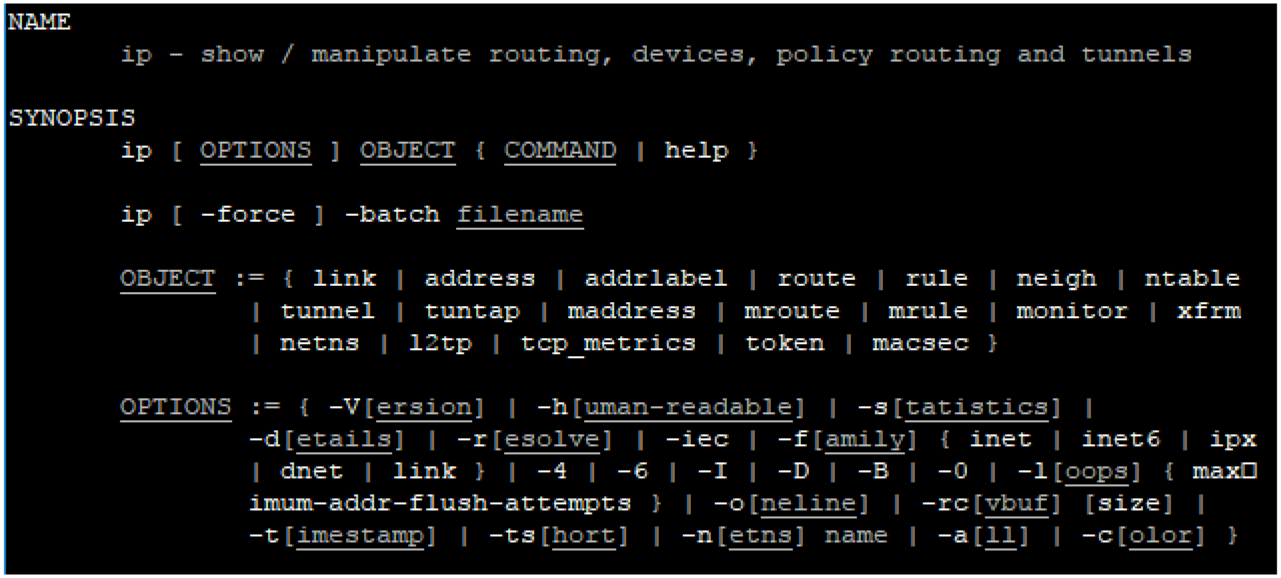
- Lots of sub-options/arguments within ip command
  - “neighbor” replaces “arp”
  - “link” replaces “ifconfig” (though without the DNS info)

ip link



```
NAME
       ip-link - network device configuration

SYNOPSIS
       ip link  { COMMAND | help }

       ip link add [ link DEVICE ] [ name ] NAME
               [ txqueuelen PACKETS ]
               [ address LLADDR ] [ broadcast LLADDR ]
               [ mtu MTU ] [ index IDX ]
               [ numtxqueues QUEUE_COUNT ] [ numrxqueues QUEUE_COUNT ]
               type TYPE [ ARGS ]

       ip link delete { DEVICE | group GROUP } type TYPE [ ARGS ]

       ip link set { DEVICE | group GROUP }
               [ { up | down } ]
               [ type ETYPE TYPE_ARGS ]
               [ arp { on | off } ]
               [ dynamic { on | off } ]
               [ multicast { on | off } ]
               [ allmulticast { on | off } ]
               [ promisc { on | off } ]
               [ protodown { on | off } ]
               [ trailers { on | off } ]
               [ txqueuelen PACKETS ]
               [ name NEWNAME ]
               [ address LLADDR ]
               [ broadcast LLADDR ]
               [ mtu MTU ]
               [ netns { PID | NETNSNAME } ]
               [ link-netnsid ID ]
               [ alias NAME ]
               [ vf NUM [ mac LLADDR ]
                        [ VFVLAN-LIST ]
                        [ rate TXRATE ]
                        [ max_tx_rate TXRATE ]
                        [ min_tx_rate TXRATE ]
                        [ spoofchk { on | off } ]
                        [ query_rss { on | off } ]
                        [ state { auto | enable | disable } ]
                        [ trust { on | off } ]
                        [ node_guid eui64 ]
                        [ port_guid eui64 ] ]
               [ xdp { off |
                       object FILE [ section NAME ] [ verbose ] |
                       pinned FILE } ]
               [ master DEVICE ]
               [ nomaster ]
               [ vrf NAME ]
               [ addrgenmode { eui64 | none | stable_secret | random } ]
               [ macaddr { flush | { add | del } MACADDR | set [ MACADDR [ MACADDR [ ... ] ] ] } ]

       ip link show [ DEVICE | group GROUP ] [ up ] [ master DEVICE ] [ type ETYPE ] [ vrf NAME ]

       ip link xstats type TYPE [ ARGS ]

       ip link afstats [ dev DEVICE ]

       ip link help [ TYPE ]
```

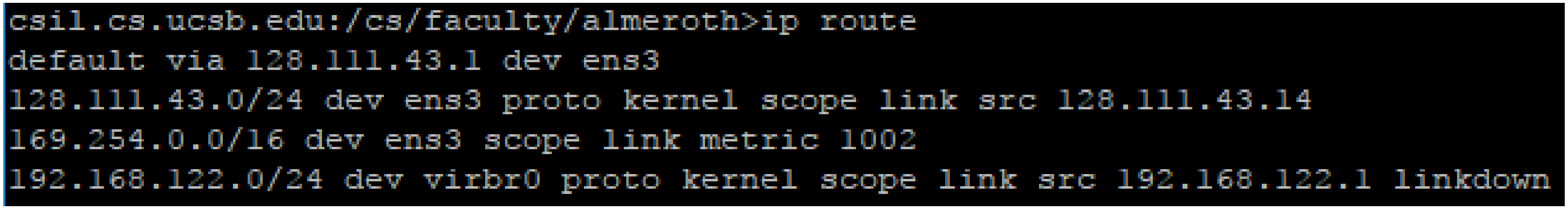
Can be used to configure a link as well as gather info about existing links



```
NAME
       ip - show / manipulate routing, devices, policy routing and tunnels

SYNOPSIS
       ip [ OPTIONS ] OBJECT { COMMAND | help }

       ip [ -force ] -batch filename

       OBJECT := { link | address | addrlabel | route | rule | neigh | ntable
               | tunnel | tuntap | maddress | mroute | mrule | monitor | xfrm
               | netns | l2tp | tcp_metrics | token | macsec }

       OPTIONS := { -V[ersion] | -h[uman-readable] | -s[tatistics] |
                -d[etails] | -r[esolve] | -iec | -f[amily] { inet | inet6 | ipx
                | dnet | link } | -4 | -6 | -I | -D | -B | -0 | -l[oops] { max□
                imum-addr-flush-attempts } | -o[neline] | -rc[vbuf] [size] |
                -t[imestamp] | -ts[hort] | -n[etns] name | -a[ll] | -c[olor] }
```

ip show

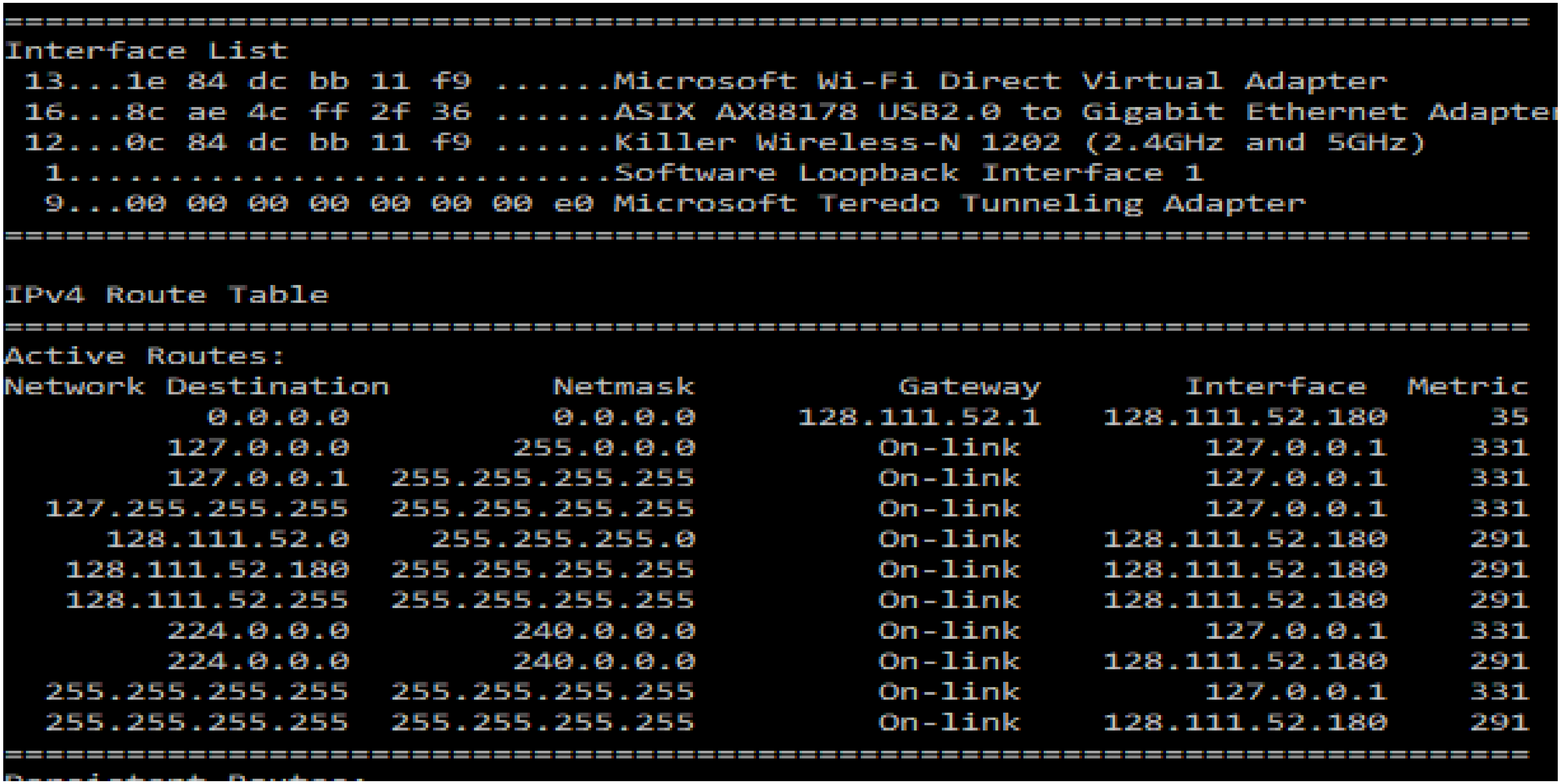
ip link
ip address
ip route
ip neigh



```
csil.cs.ucsb.edu:/cs/faculty/almeroth>ip route
default via 128.111.43.1 dev ens3
128.111.43.0/24 dev ens3 proto kernel scope link src 128.111.43.14
169.254.0.0/16 dev ens3 scope link metric 1002
192.168.122.0/24 dev virbr0 proto kernel scope link src 192.168.122.1 linkdown
```

- Not much exciting with “ip route” on a local host
  - Default route is key
  - Also a link local route

netstat -rn



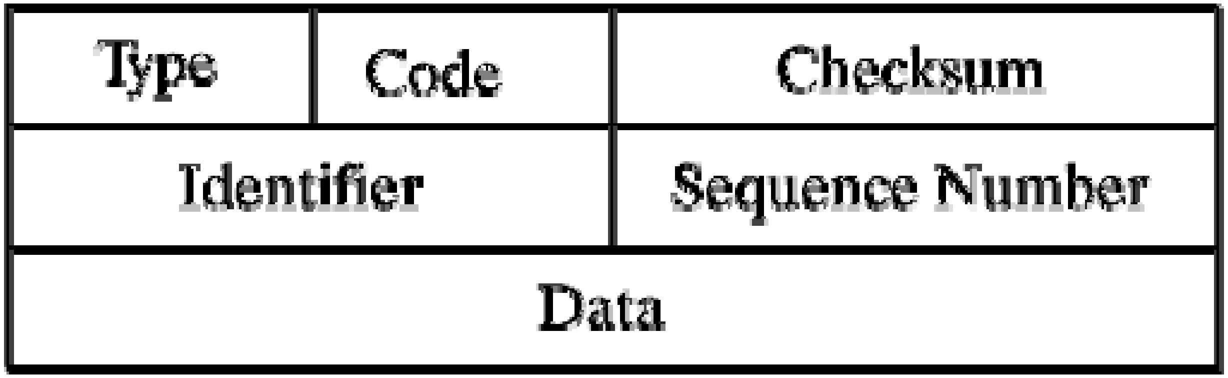
```
===========================================================================
Interface List
 13...1e 84 dc bb 11 f9 ......Microsoft Wi-Fi Direct Virtual Adapter
 16...8c ae 4c ff 2f 36 ......ASIX AX88178 USB2.0 to Gigabit Ethernet Adapter
 12...0c 84 dc bb 11 f9 ......Killer Wireless-N 1202 (2.4GHz and 5GHz)
  1...........................Software Loopback Interface 1
  9...00 00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     128.111.52.1   128.111.52.180     35
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
     128.111.52.0    255.255.255.0         On-link    128.111.52.180    291
   128.111.52.180  255.255.255.255         On-link    128.111.52.180    291
   128.111.52.255  255.255.255.255         On-link    128.111.52.180    291
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link    128.111.52.180    291
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link    128.111.52.180    291
===========================================================================
Persistent Routes:
```

Categories

- Tools about local network interface
  - ifconfig* (now ip link*), arp* (now ip neighbor*), netstat/ss*
- Tools about network path
  - ping*, traceroute*, geotrace, bandwidth estimators
- Tools about routing
  - router looking glass
- Tools about remote hosts/networks
  - nslookup/host/dig*, whois/jwhois*
- Tools about network traffic
  - wireshark, firesheep, fiddler

ping and traceroute

- Use ICMP
  - Encapsulated in IP



Type	Code	Checksum
Identifier		Sequence Number
Data		

- See man pages for interesting options
  - Packet sizes (e.g., can cause fragmentation)

ICMP Type and Code Examples

Type	Code	description
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

Traceroute Using ICMP

- Send packet with TTL=x
  - Start with x=1, then x=2, …
  - No information for non-responsive, then skip to next value
- TTL will reach 0, ICMP will be sent
  - By incrementing TTL value, responses provide a trace of the path
- Traceroute typically does each TTL value 3 times
- There is typically a setting to reverse lookup the IP addresses to try and determine host names
- Newer versions of traceroute have been developed that don't use ICMP echo request/reply
  - Concept is the same: get a host along the way to respond with some sort of message
  - Have difference performance characteristics
    - For example: ICMP is given a different priority than UDP or TCP

Online Tracing

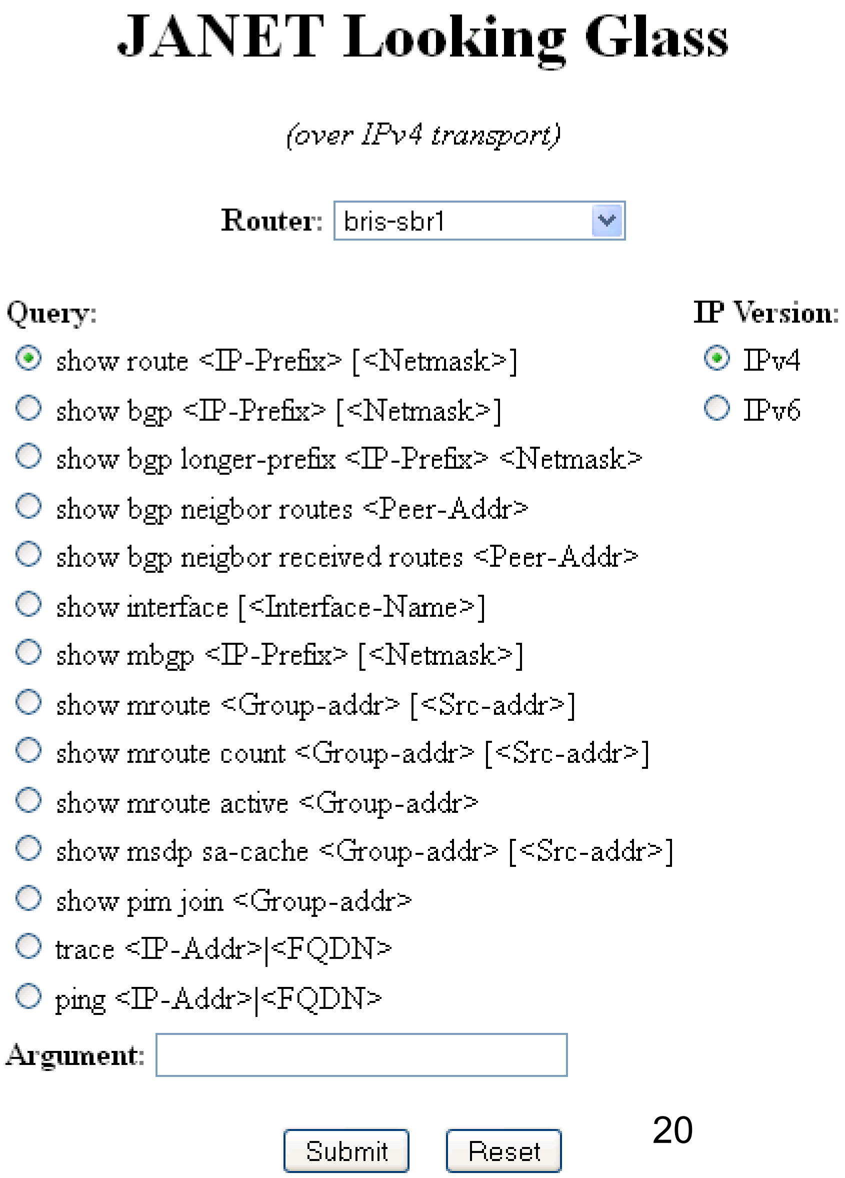
- Visual traceroute
  - https://www.monitis.com/traceroute/
  - Doesn't always work so well
  - More interesting is the source data used: basically a map between IP addresses (or ASes) and lat-long coordinates
    - See http://www.caida.org/tools/utilities/netgeo/ including alternatives at the end
  - Source code for your own project
    - See https://sourceforge.net/projects/openvisualtrace/
- Link statistics
  - http://www.visualroute.com/lite.html
- Other sites that provide bandwidth tests
  - http://www.speedtest.net/
  - Use file download and packet pair estimates

Categories

- Tools about local network interface
  - ifconfig* (now ip link*), arp* (now ip neighbor*), netstat/ss*
- Tools about network path
  - ping*, traceroute*, geotrace, bandwidth estimators
- Tools about routing
  - router looking glass
- Tools about remote hosts/networks
  - nslookup/host/dig*, whois/jwhois*
- Tools about network traffic
  - wireshark, firesheep, fiddler

Router “Looking Glass”

- Limited access to a public router
  - http://alice.ja.net/
  - https://us.ntt.net/support/looking-glass/
- JANET
  - High speed network in the UK
- Useful for checking on routes held at other routers around the Internet
- Another example, but with data archive and analysis
  - http://www.routeviews.org/
- Look up AS Numbers
  - https://www.ultratools.com/tools/asnInfo



JANET Looking Glass

(over IPv4 transport)

Router: bris-sbr1

Query:

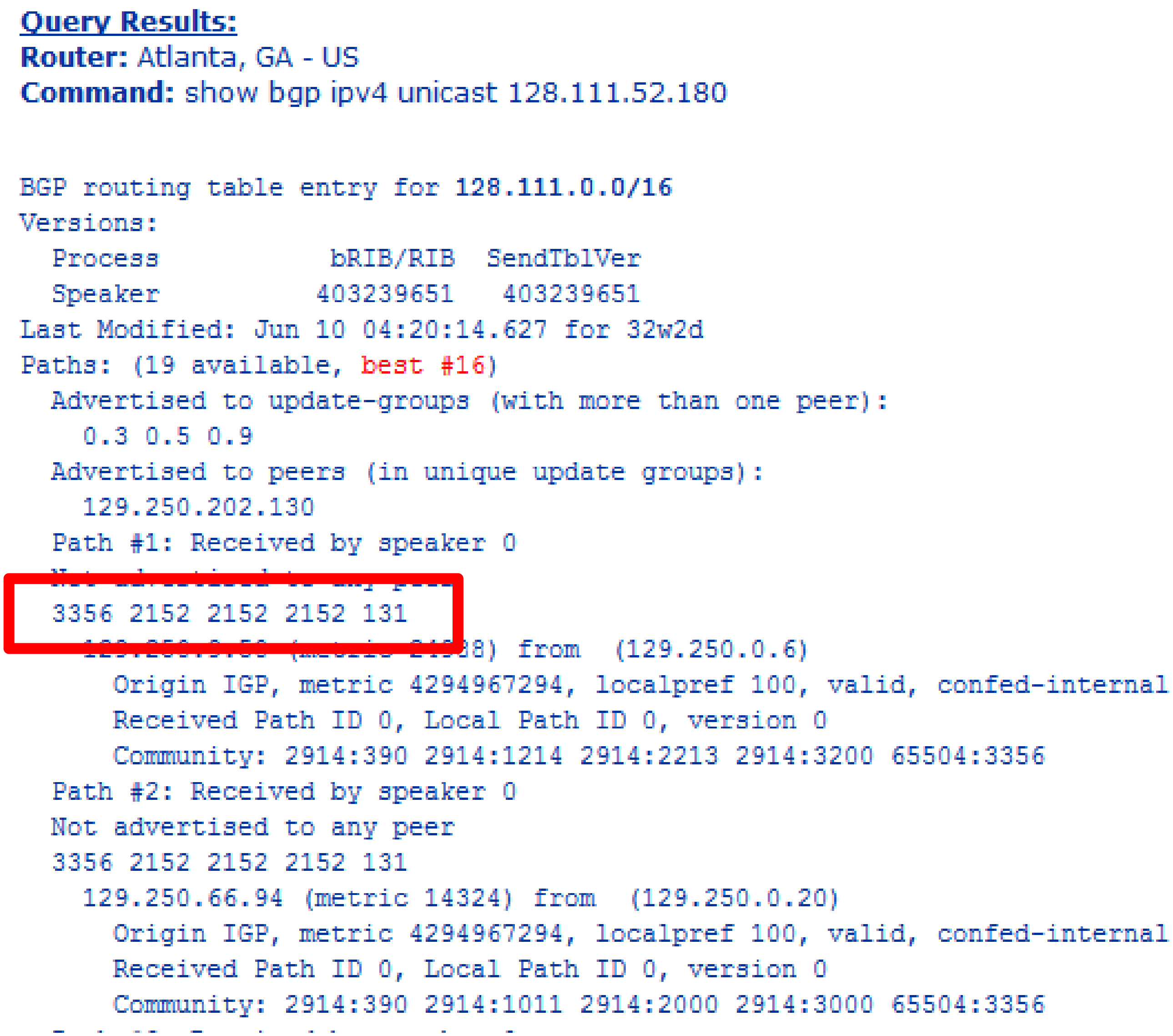
● show route <IP-Prefix> [<Netmask>]
○ show bgp <IP-Prefix> [<Netmask>]
○ show bgp longer-prefix <IP-Prefix> <Netmask>
○ show bgp neigbor routes <Peer-Addr>
○ show bgp neigbor received routes <Peer-Addr>
○ show interface [<Interface-Name>]
○ show mbgp <IP-Prefix> [<Netmask>]
○ show mroute <Group-addr> [<Src-addr>]
○ show mroute count <Group-addr> [<Src-addr>]
○ show mroute active <Group-addr>
○ show msdp sa-cache <Group-addr> [<Src-addr>]
○ show pim join <Group-addr>
○ trace <IP-Addr>|<FQDN>
○ ping <IP-Addr>|<FQDN>

IP Version:

● IPv4
○ IPv6

Argument:

https://us.ntt.net/support/looking-glass/



Query Results:
Router: Atlanta, GA - US
Command: show bgp ipv4 unicast 128.111.52.180

```
BGP routing table entry for 128.111.0.0/16
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker          403239651   403239651
Last Modified: Jun 10 04:20:14.627 for 32w2d
Paths: (19 available, best #16)
  Advertised to update-groups (with more than one peer):
    0.3 0.5 0.9
  Advertised to peers (in unique update groups):
    129.250.202.130
  Path #1: Received by speaker 0
  Not advertised to any peer
  3356 2152 2152 2152 131
    129.250.3.50 (metric 21388) from  (129.250.0.6)
      Origin IGP, metric 4294967294, localpref 100, valid, confed-internal
      Received Path ID 0, Local Path ID 0, version 0
      Community: 2914:390 2914:1214 2914:2213 2914:3200 65504:3356
  Path #2: Received by speaker 0
  Not advertised to any peer
  3356 2152 2152 2152 131
    129.250.66.94 (metric 14324) from  (129.250.0.20)
      Origin IGP, metric 4294967294, localpref 100, valid, confed-internal
      Received Path ID 0, Local Path ID 0, version 0
      Community: 2914:390 2914:1011 2914:2000 2914:3000 65504:3356
  Path #3: Received by speaker 0
```

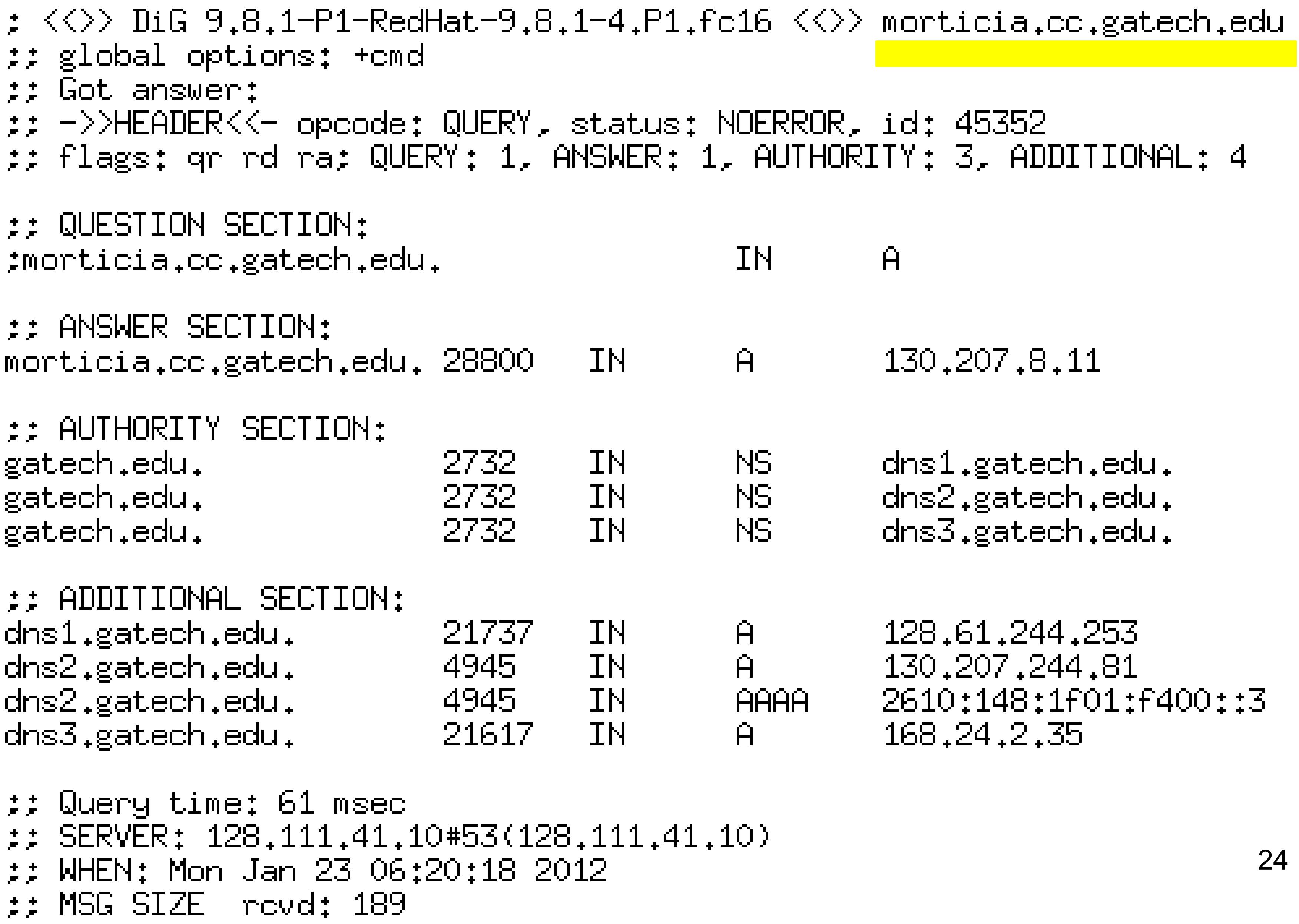
Categories

- Tools about local network interface
  - ifconfig* (now ip link*), arp* (now ip neighbor*), netstat/ss*
- Tools about network path
  - ping*, traceroute*, geotrace, bandwidth estimators
- Tools about routing
  - router looking glass
- Tools about remote hosts/networks
  - nslookup/host/dig*, whois/jwhois*
- Tools about network traffic
  - wireshark, firesheep, fiddler

dig

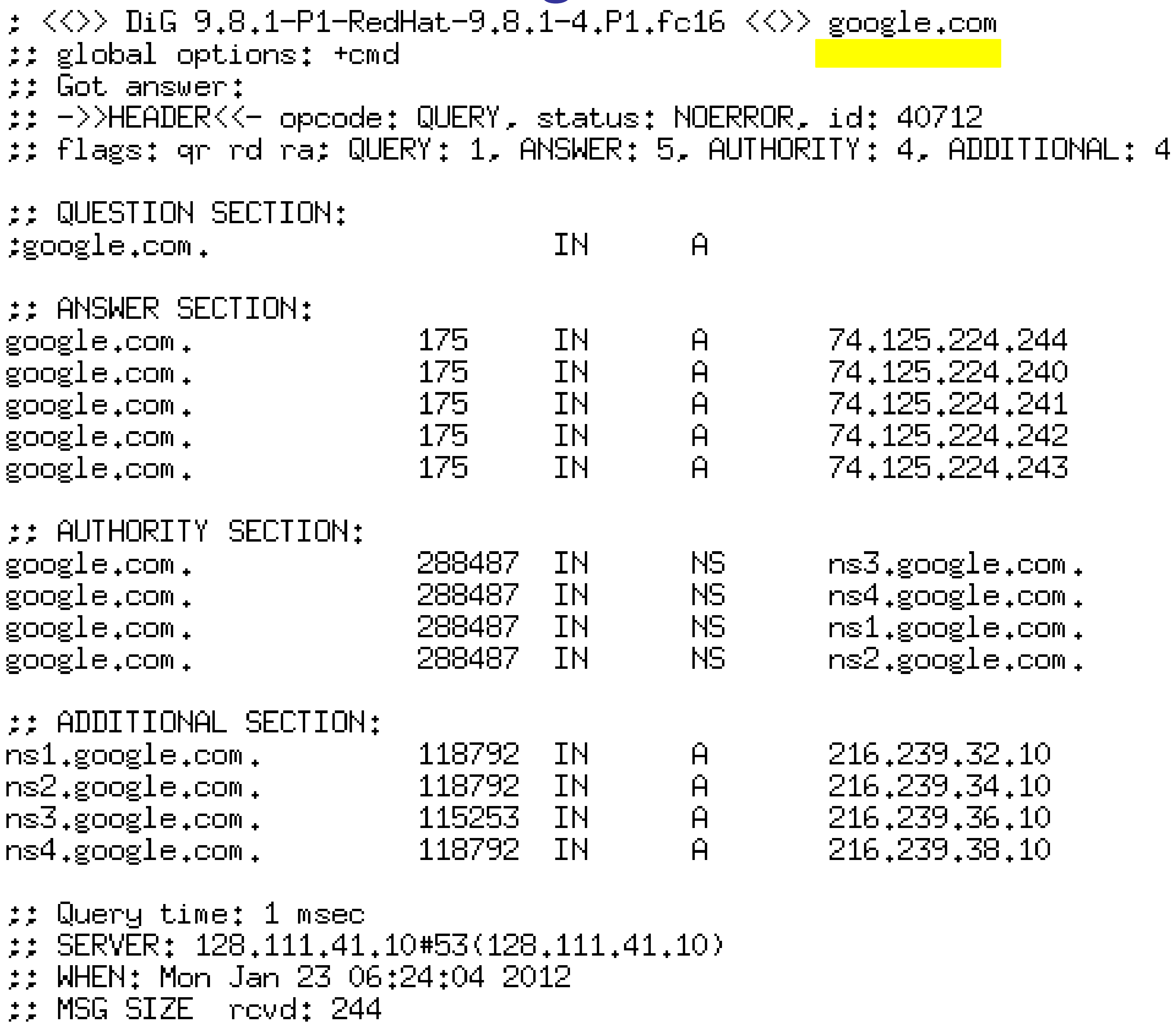
- Used to debug DNS
  - Old versions of command are nslookup and host
  - dig adds more features
  - Each also has various “verbose” modes for more info

dig #1



```
; <<>> DiG 9.8.1-P1-RedHat-9.8.1-4.P1.fc16 <<>> morticia.cc.gatech.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45352
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 4

;; QUESTION SECTION:
;morticia.cc.gatech.edu.                IN      A

;; ANSWER SECTION:
morticia.cc.gatech.edu. 28800   IN      A       130.207.8.11

;; AUTHORITY SECTION:
gatech.edu.             2732    IN      NS      dns1.gatech.edu.
gatech.edu.             2732    IN      NS      dns2.gatech.edu.
gatech.edu.             2732    IN      NS      dns3.gatech.edu.

;; ADDITIONAL SECTION:
dns1.gatech.edu.        21737   IN      A       128.61.244.253
dns2.gatech.edu.        4945    IN      A       130.207.244.81
dns2.gatech.edu.        4945    IN      AAAA    2610:148:1f01:f400::3
dns3.gatech.edu.        21617   IN      A       168.24.2.35

;; Query time: 61 msec
;; SERVER: 128.111.41.10#53(128.111.41.10)
;; WHEN: Mon Jan 23 06:20:18 2012
;; MSG SIZE  rcvd: 189
```

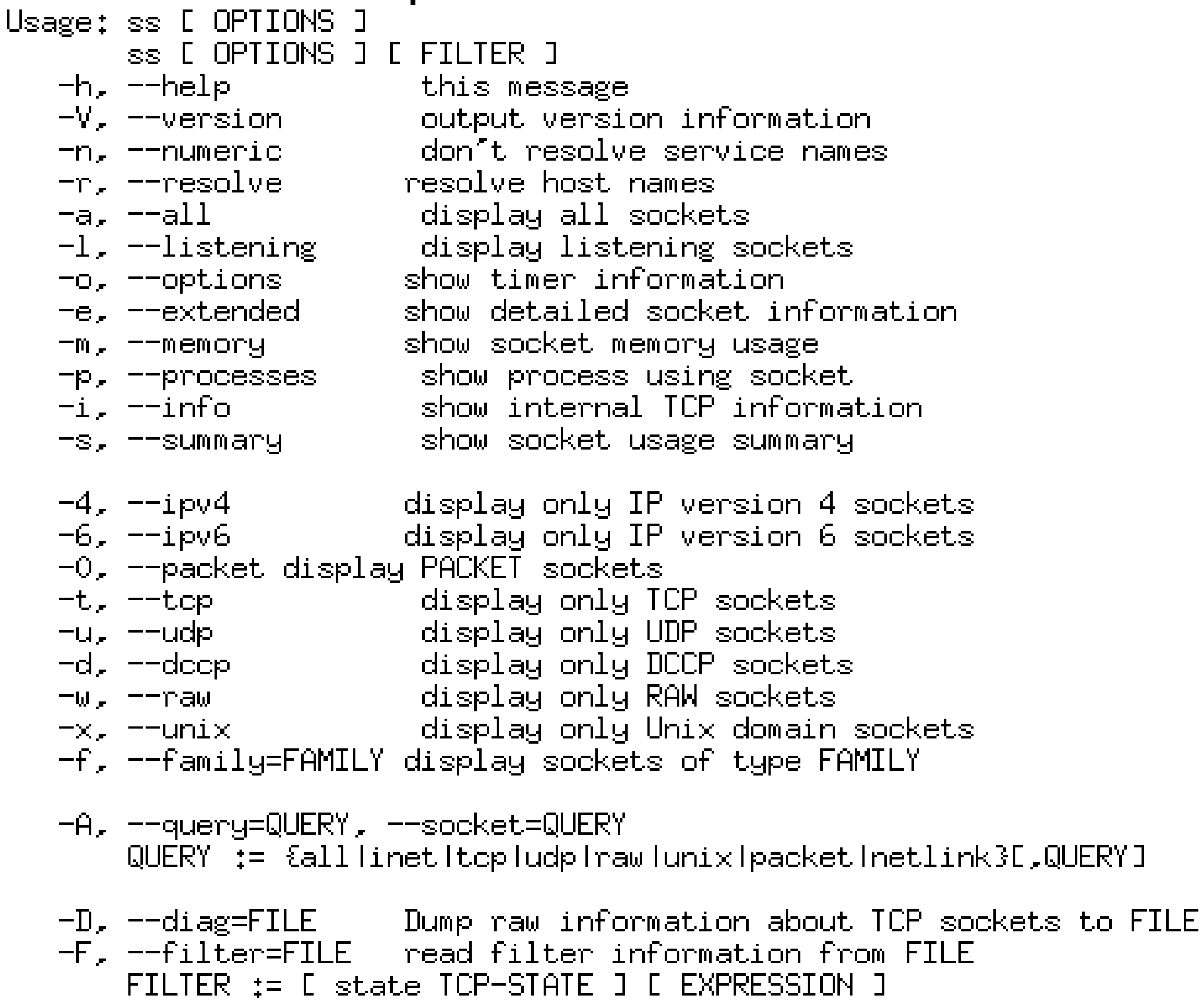
dig #2



```
; <<>> DiG 9.8.1-P1-RedHat-9.8.1-4.P1.fc16 <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40712
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             175     IN      A       74.125.224.244
google.com.             175     IN      A       74.125.224.240
google.com.             175     IN      A       74.125.224.241
google.com.             175     IN      A       74.125.224.242
google.com.             175     IN      A       74.125.224.243

;; AUTHORITY SECTION:
google.com.             288487  IN      NS      ns3.google.com.
google.com.             288487  IN      NS      ns4.google.com.
google.com.             288487  IN      NS      ns1.google.com.
google.com.             288487  IN      NS      ns2.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.         118792  IN      A       216.239.32.10
ns2.google.com.         118792  IN      A       216.239.34.10
ns3.google.com.         115253  IN      A       216.239.36.10
ns4.google.com.         118792  IN      A       216.239.38.10

;; Query time: 1 msec
;; SERVER: 128.111.41.10#53(128.111.41.10)
;; WHEN: Mon Jan 23 06:24:04 2012
;; MSG SIZE  rcvd: 244
```

netstat or ss

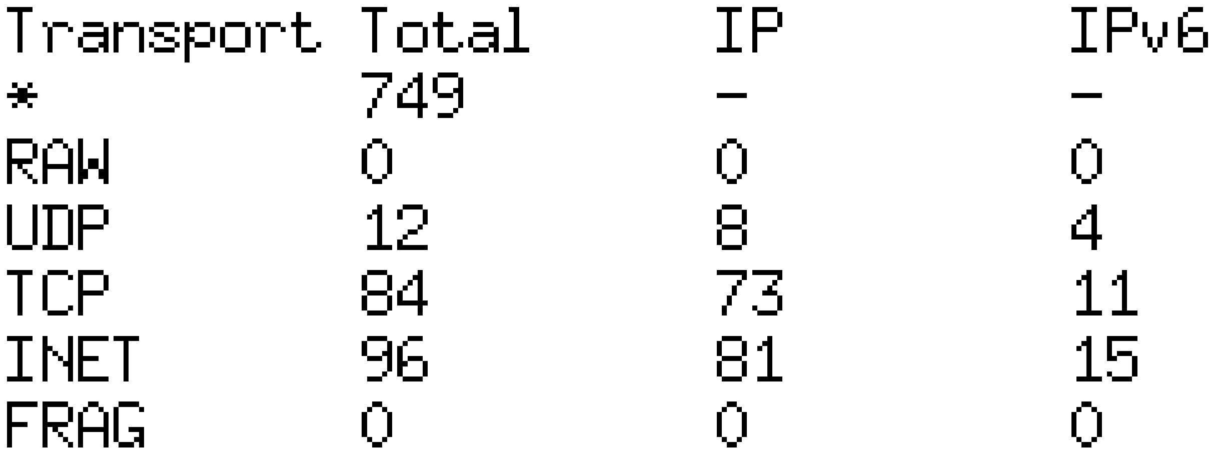
- Information about open connections



```
Usage: ss [ OPTIONS ]
       ss [ OPTIONS ] [ FILTER ]
   -h, --help           this message
   -V, --version        output version information
   -n, --numeric        don't resolve service names
   -r, --resolve       resolve host names
   -a, --all            display all sockets
   -l, --listening      display listening sockets
   -o, --options       show timer information
   -e, --extended      show detailed socket information
   -m, --memory        show socket memory usage
   -p, --processes      show process using socket
   -i, --info           show internal TCP information
   -s, --summary        show socket usage summary

   -4, --ipv4          display only IP version 4 sockets
   -6, --ipv6          display only IP version 6 sockets
   -0, --packet display PACKET sockets
   -t, --tcp            display only TCP sockets
   -u, --udp            display only UDP sockets
   -d, --dccp           display only DCCP sockets
   -w, --raw            display only RAW sockets
   -x, --unix           display only Unix domain sockets
   -f, --family=FAMILY display sockets of type FAMILY

   -A, --query=QUERY, --socket=QUERY
       QUERY := {all|inet|tcp|udp|raw|unix|packet|netlink}[,QUERY]

   -D, --diag=FILE     Dump raw information about TCP sockets to FILE
   -F, --filter=FILE   read filter information from FILE
       FILTER := [ state TCP-STATE ] [ EXPRESSION ]
```

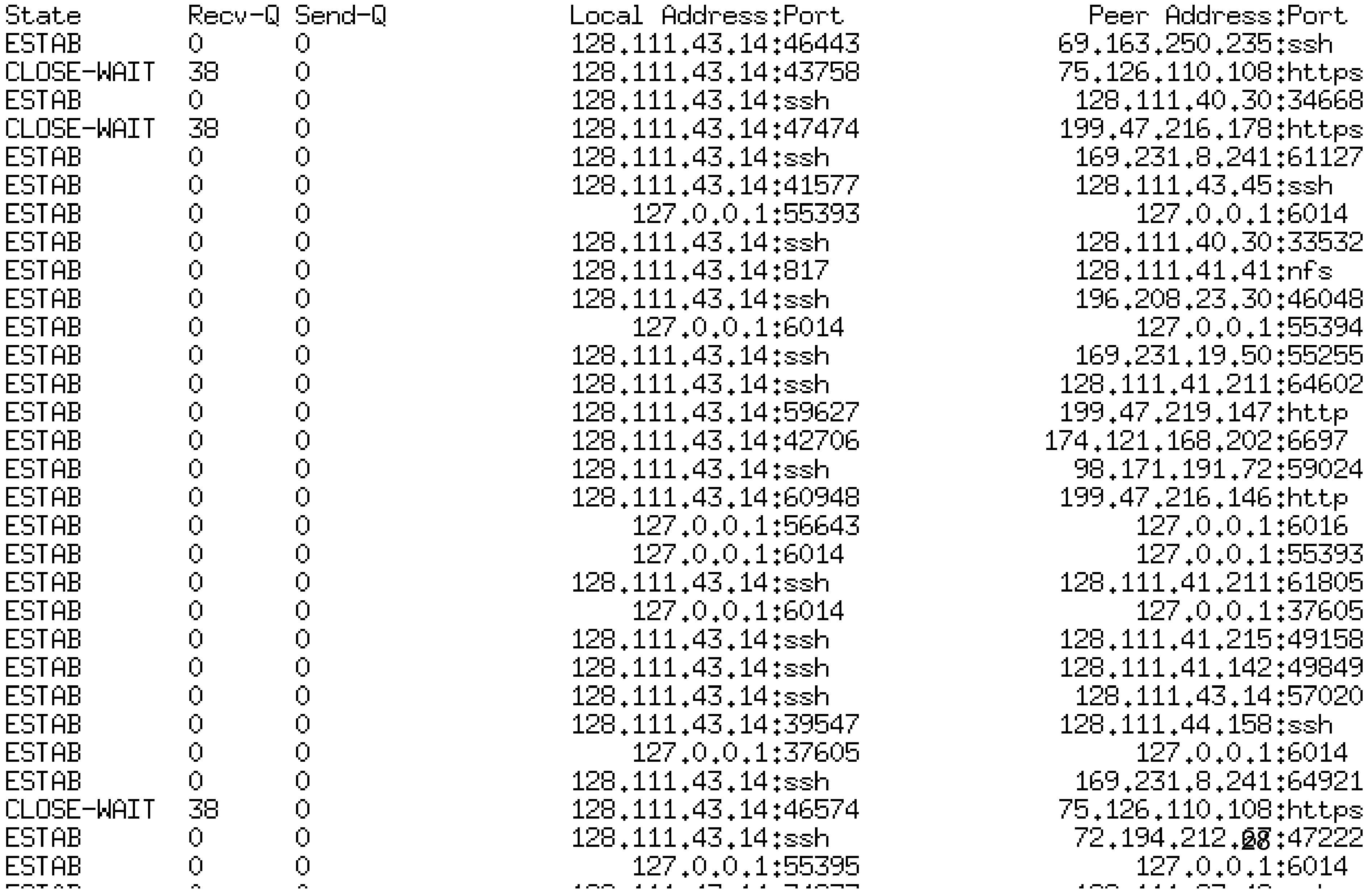
ss –s (summary display)

- An “ss –s” (summary) for csil.cs.ucsb.edu:



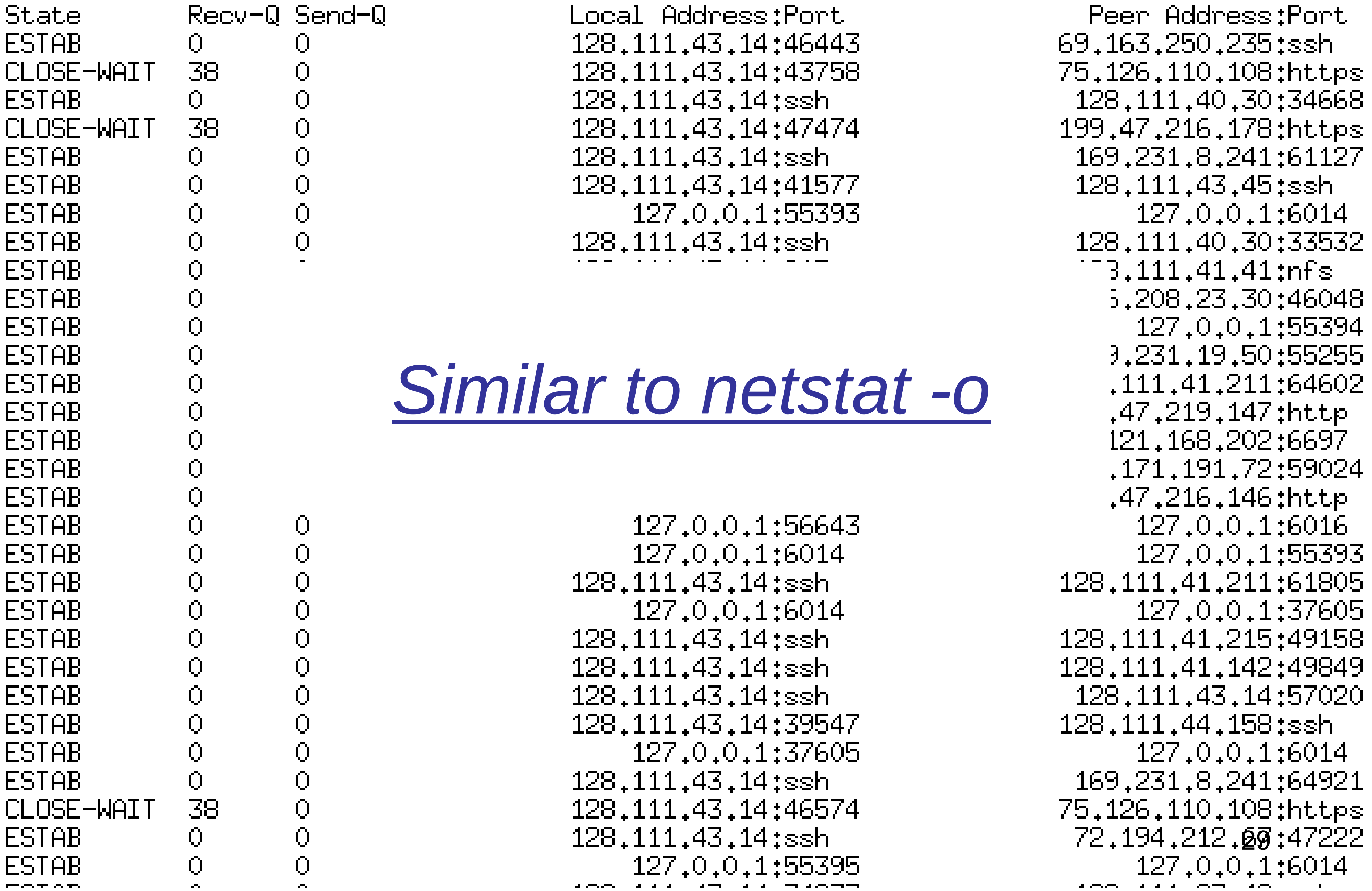
```
Transport Total      IP         IPv6
*         749        -          -
RAW       0          0          0
UDP       12         8          4
TCP       84         73         11
INET      96         81         15
FRAG      0          0          0
```

ss –e (extended display)



```
State       Recv-Q Send-Q            Local Address:Port             Peer Address:Port
ESTAB       0      0             128.111.43.14:46443           69.163.250.235:ssh
CLOSE-WAIT  38     0             128.111.43.14:43758           75.126.110.108:https
ESTAB       0      0             128.111.43.14:ssh              128.111.40.30:34668
CLOSE-WAIT  38     0             128.111.43.14:47474           199.47.216.178:https
ESTAB       0      0             128.111.43.14:ssh              169.231.8.241:61127
ESTAB       0      0             128.111.43.14:41577            128.111.43.45:ssh
ESTAB       0      0                 127.0.0.1:55393                127.0.0.1:6014
ESTAB       0      0             128.111.43.14:ssh              128.111.40.30:33532
ESTAB       0      0             128.111.43.14:817              128.111.41.41:nfs
ESTAB       0      0             128.111.43.14:ssh              196.208.23.30:46048
ESTAB       0      0                 127.0.0.1:6014                 127.0.0.1:55394
ESTAB       0      0             128.111.43.14:ssh              169.231.19.50:55255
ESTAB       0      0             128.111.43.14:ssh             128.111.41.211:64602
ESTAB       0      0             128.111.43.14:59627           199.47.219.147:http
ESTAB       0      0             128.111.43.14:42706          174.121.168.202:6697
ESTAB       0      0             128.111.43.14:ssh              98.171.191.72:59024
ESTAB       0      0             128.111.43.14:60948           199.47.216.146:http
ESTAB       0      0                 127.0.0.1:56643                127.0.0.1:6016
ESTAB       0      0                 127.0.0.1:6014                 127.0.0.1:55393
ESTAB       0      0             128.111.43.14:ssh             128.111.41.211:61805
ESTAB       0      0                 127.0.0.1:6014                 127.0.0.1:37605
ESTAB       0      0             128.111.43.14:ssh             128.111.41.215:49158
ESTAB       0      0             128.111.43.14:ssh             128.111.41.142:49849
ESTAB       0      0             128.111.43.14:ssh              128.111.43.14:57020
ESTAB       0      0             128.111.43.14:39547           128.111.44.158:ssh
ESTAB       0      0                 127.0.0.1:37605                127.0.0.1:6014
ESTAB       0      0             128.111.43.14:ssh              169.231.8.241:64921
CLOSE-WAIT  38     0             128.111.43.14:46574           75.126.110.108:https
ESTAB       0      0             128.111.43.14:ssh              72.194.212.[illegible]:47222
ESTAB       0      0                 127.0.0.1:55395                127.0.0.1:6014
```

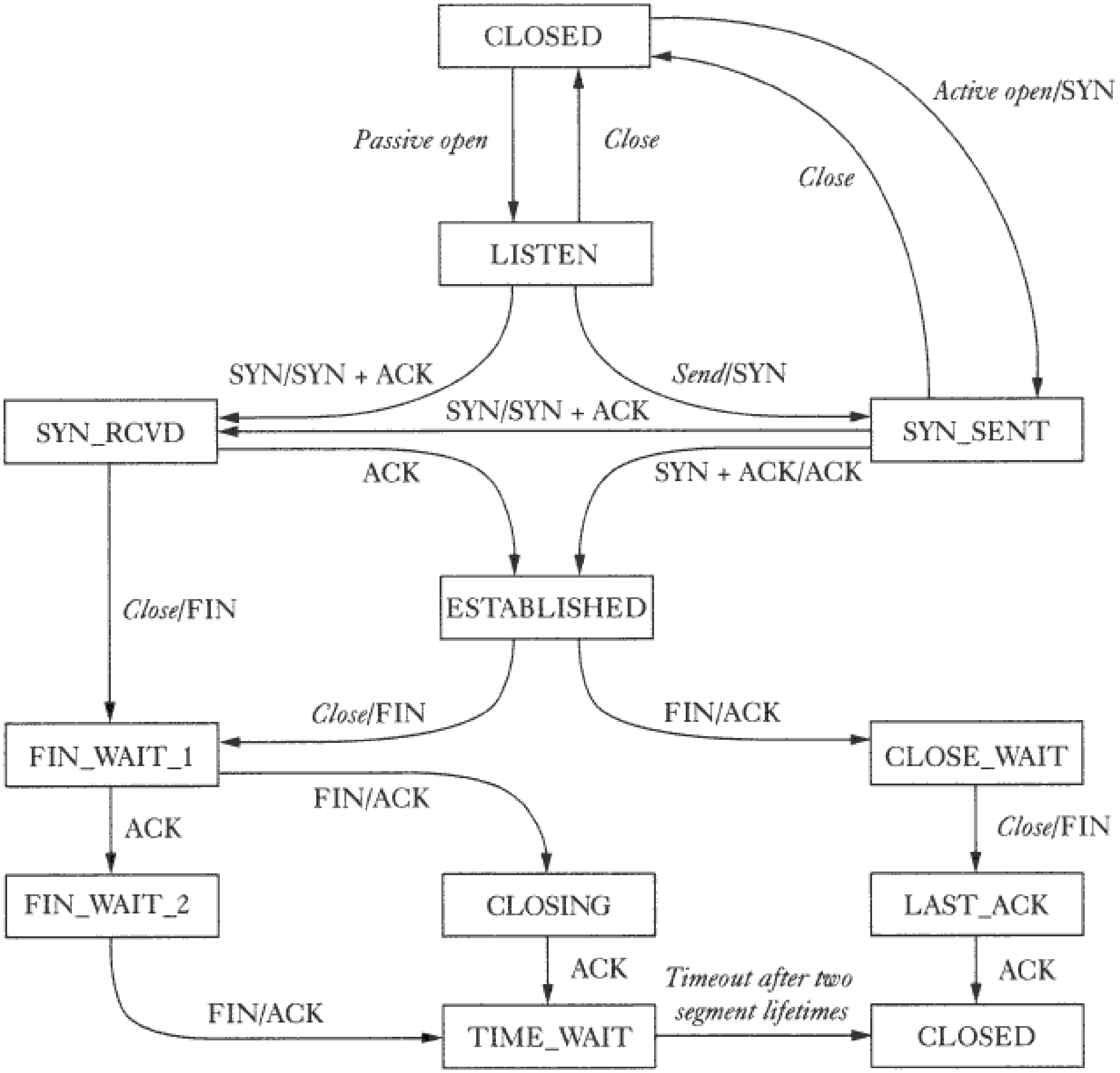
ss –e (extended display)



```
State        Recv-Q Send-Q              Local Address:Port                Peer Address:Port
ESTAB        0      0                128.111.43.14:46443              69.163.250.235:ssh
CLOSE-WAIT   38     0                128.111.43.14:43758              75.126.110.108:https
ESTAB        0      0                128.111.43.14:ssh                 128.111.40.30:34668
CLOSE-WAIT   38     0                128.111.43.14:47474              199.47.216.178:https
ESTAB        0      0                128.111.43.14:ssh                 169.231.8.241:61127
ESTAB        0      0                128.111.43.14:41577               128.111.43.45:ssh
ESTAB        0      0                    127.0.0.1:55393                   127.0.0.1:6014
ESTAB        0      0                128.111.43.14:ssh                 128.111.40.30:33532
ESTAB        0                                                           3.111.41.41:nfs
ESTAB        0                                                          5.208.23.30:46048
ESTAB        0                                                           127.0.0.1:55394
ESTAB        0                                                          9.231.19.50:55255
ESTAB        0                                                         .111.41.211:64602
ESTAB        0                                                         .47.219.147:http
ESTAB        0                                                         121.168.202:6697
ESTAB        0                                                         .171.191.72:59024
ESTAB        0                                                         .47.216.146:http
ESTAB        0      0                    127.0.0.1:56643                   127.0.0.1:6016
ESTAB        0      0                    127.0.0.1:6014                    127.0.0.1:55393
ESTAB        0      0                128.111.43.14:ssh                128.111.41.211:61805
ESTAB        0      0                    127.0.0.1:6014                    127.0.0.1:37605
ESTAB        0      0                128.111.43.14:ssh                128.111.41.215:49158
ESTAB        0      0                128.111.43.14:ssh                128.111.41.142:49849
ESTAB        0      0                128.111.43.14:ssh                 128.111.43.14:57020
ESTAB        0      0                128.111.43.14:39547              128.111.44.158:ssh
ESTAB        0      0                    127.0.0.1:37605                   127.0.0.1:6014
ESTAB        0      0                128.111.43.14:ssh                 169.231.8.241:64921
CLOSE-WAIT   38     0                128.111.43.14:46574              75.126.110.108:https
ESTAB        0      0                128.111.43.14:ssh                 72.194.212.57:47222
ESTAB        0      0                    127.0.0.1:55395                   127.0.0.1:6014
```

Similar to netstat -o

TCP State Diagram



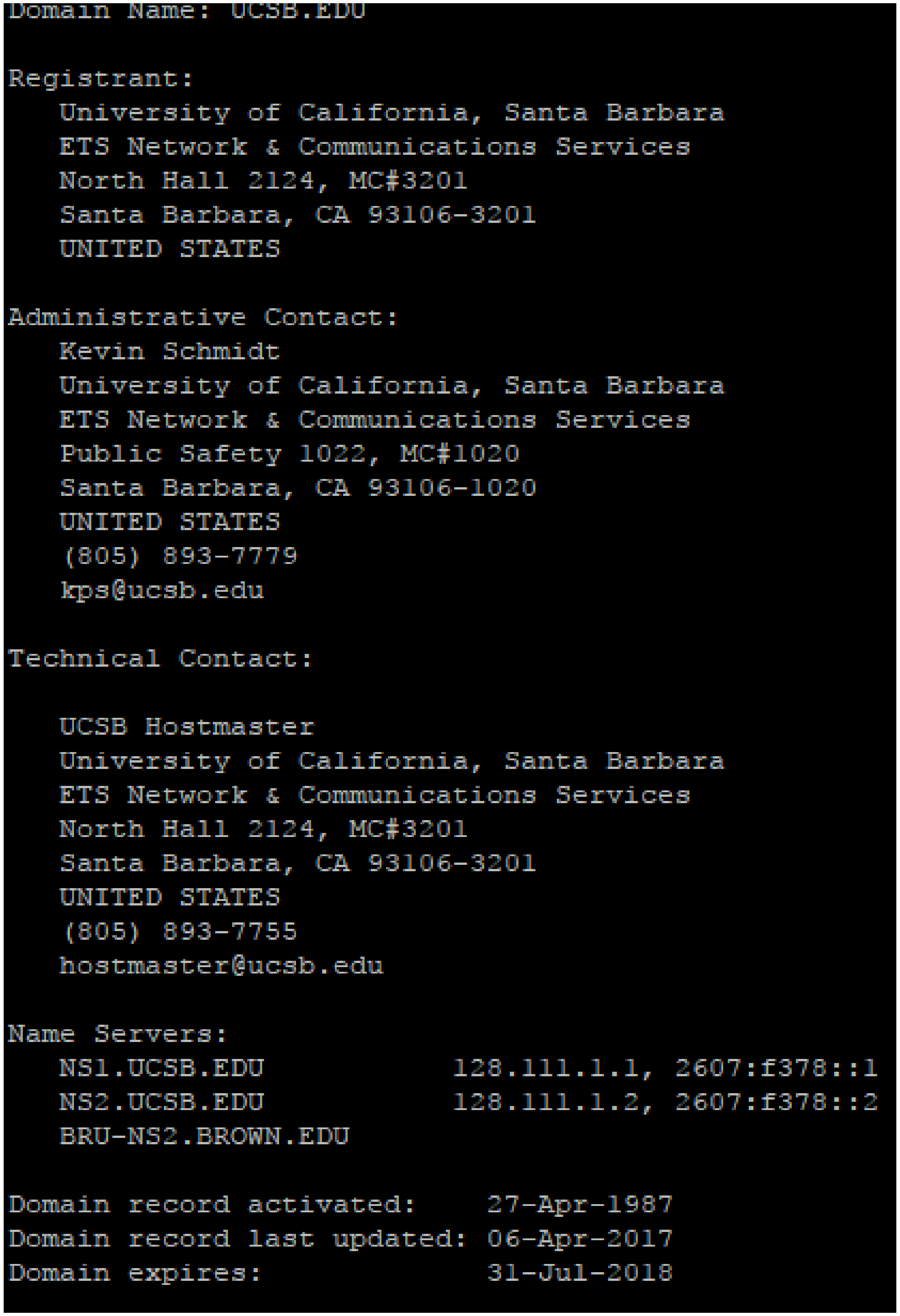
whois

- Used to gather information associated with DNS records

- Examples
  - prompt> whois ucsb.edu
  - prompt> whois google.com
  - prompt> whois 128.111.52.1
  - prompt> whois ieee-icnp.org
  - prompt> whois whitehouse.gov

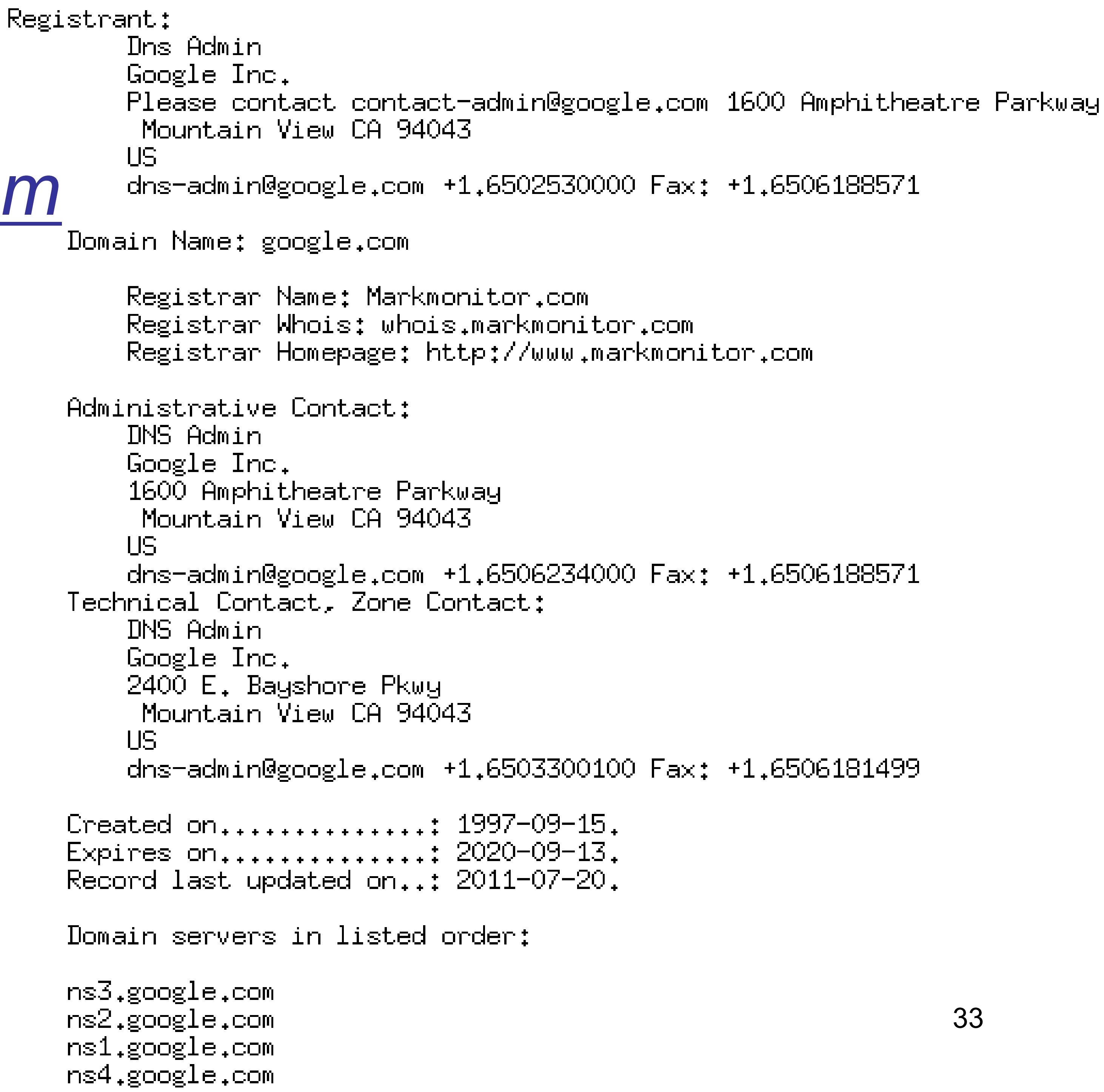
- Check out some of the options (man pages)

whois ucsb.edu



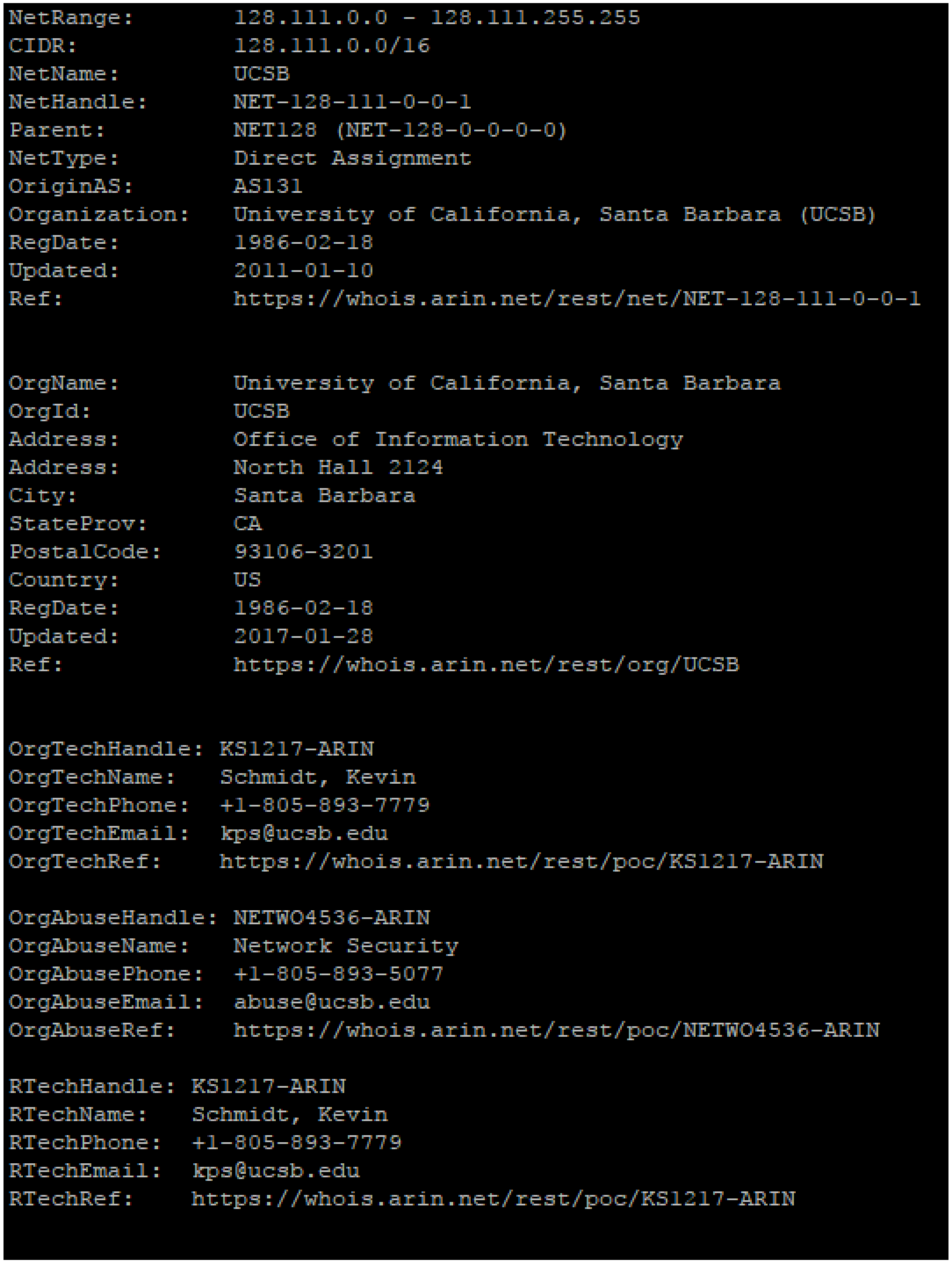
```
Domain Name: UCSB.EDU

Registrant:
   University of California, Santa Barbara
   ETS Network & Communications Services
   North Hall 2124, MC#3201
   Santa Barbara, CA 93106-3201
   UNITED STATES

Administrative Contact:
   Kevin Schmidt
   University of California, Santa Barbara
   ETS Network & Communications Services
   Public Safety 1022, MC#1020
   Santa Barbara, CA 93106-1020
   UNITED STATES
   (805) 893-7779
   kps@ucsb.edu

Technical Contact:

   UCSB Hostmaster
   University of California, Santa Barbara
   ETS Network & Communications Services
   North Hall 2124, MC#3201
   Santa Barbara, CA 93106-3201
   UNITED STATES
   (805) 893-7755
   hostmaster@ucsb.edu

Name Servers:
   NS1.UCSB.EDU           128.111.1.1, 2607:f378::1
   NS2.UCSB.EDU           128.111.1.2, 2607:f378::2
   BRU-NS2.BROWN.EDU

Domain record activated:    27-Apr-1987
Domain record last updated: 06-Apr-2017
Domain expires:             31-Jul-2018
```

whois google.com



```
Registrant:
        Dns Admin
        Google Inc.
        Please contact contact-admin@google.com 1600 Amphitheatre Parkway
         Mountain View CA 94043
        US
        dns-admin@google.com +1.6502530000 Fax: +1.6506188571
    Domain Name: google.com

        Registrar Name: Markmonitor.com
        Registrar Whois: whois.markmonitor.com
        Registrar Homepage: http://www.markmonitor.com

    Administrative Contact:
        DNS Admin
        Google Inc.
        1600 Amphitheatre Parkway
         Mountain View CA 94043
        US
        dns-admin@google.com +1.6506234000 Fax: +1.6506188571
    Technical Contact, Zone Contact:
        DNS Admin
        Google Inc.
        2400 E. Bayshore Pkwy
         Mountain View CA 94043
        US
        dns-admin@google.com +1.6503300100 Fax: +1.6506181499

    Created on..............: 1997-09-15.
    Expires on..............: 2020-09-13.
    Record last updated on..: 2011-07-20.

    Domain servers in listed order:

    ns3.google.com
    ns2.google.com
    ns1.google.com
    ns4.google.com
```

whois 128.111.52.1



```
NetRange:       128.111.0.0 - 128.111.255.255
CIDR:           128.111.0.0/16
NetName:        UCSB
NetHandle:      NET-128-111-0-0-1
Parent:         NET128 (NET-128-0-0-0-0)
NetType:        Direct Assignment
OriginAS:       AS131
Organization:   University of California, Santa Barbara (UCSB)
RegDate:        1986-02-18
Updated:        2011-01-10
Ref:            https://whois.arin.net/rest/net/NET-128-111-0-0-1


OrgName:        University of California, Santa Barbara
OrgId:          UCSB
Address:        Office of Information Technology
Address:        North Hall 2124
City:           Santa Barbara
StateProv:      CA
PostalCode:     93106-3201
Country:        US
RegDate:        1986-02-18
Updated:        2017-01-28
Ref:            https://whois.arin.net/rest/org/UCSB


OrgTechHandle: KS1217-ARIN
OrgTechName:   Schmidt, Kevin
OrgTechPhone:  +1-805-893-7779
OrgTechEmail:  kps@ucsb.edu
OrgTechRef:    https://whois.arin.net/rest/poc/KS1217-ARIN

OrgAbuseHandle: NETWO4536-ARIN
OrgAbuseName:   Network Security
OrgAbusePhone:  +1-805-893-5077
OrgAbuseEmail:  abuse@ucsb.edu
OrgAbuseRef:    https://whois.arin.net/rest/poc/NETWO4536-ARIN

RTechHandle: KS1217-ARIN
RTechName:   Schmidt, Kevin
RTechPhone:  +1-805-893-7779
RTechEmail:  kps@ucsb.edu
RTechRef:    https://whois.arin.net/rest/poc/KS1217-ARIN
```

Categories

- Tools about local network interface
  - ifconfig* (now ip link*), arp* (now ip neighbor*), netstat/ss*
- Tools about network path
  - ping*, traceroute*, geotrace, bandwidth estimators
- Tools about routing
  - router looking glass
- Tools about remote hosts/networks
  - nslookup/host/dig*, whois/jwhois*
- Tools about network traffic
  - wireshark, firesheep, fiddler

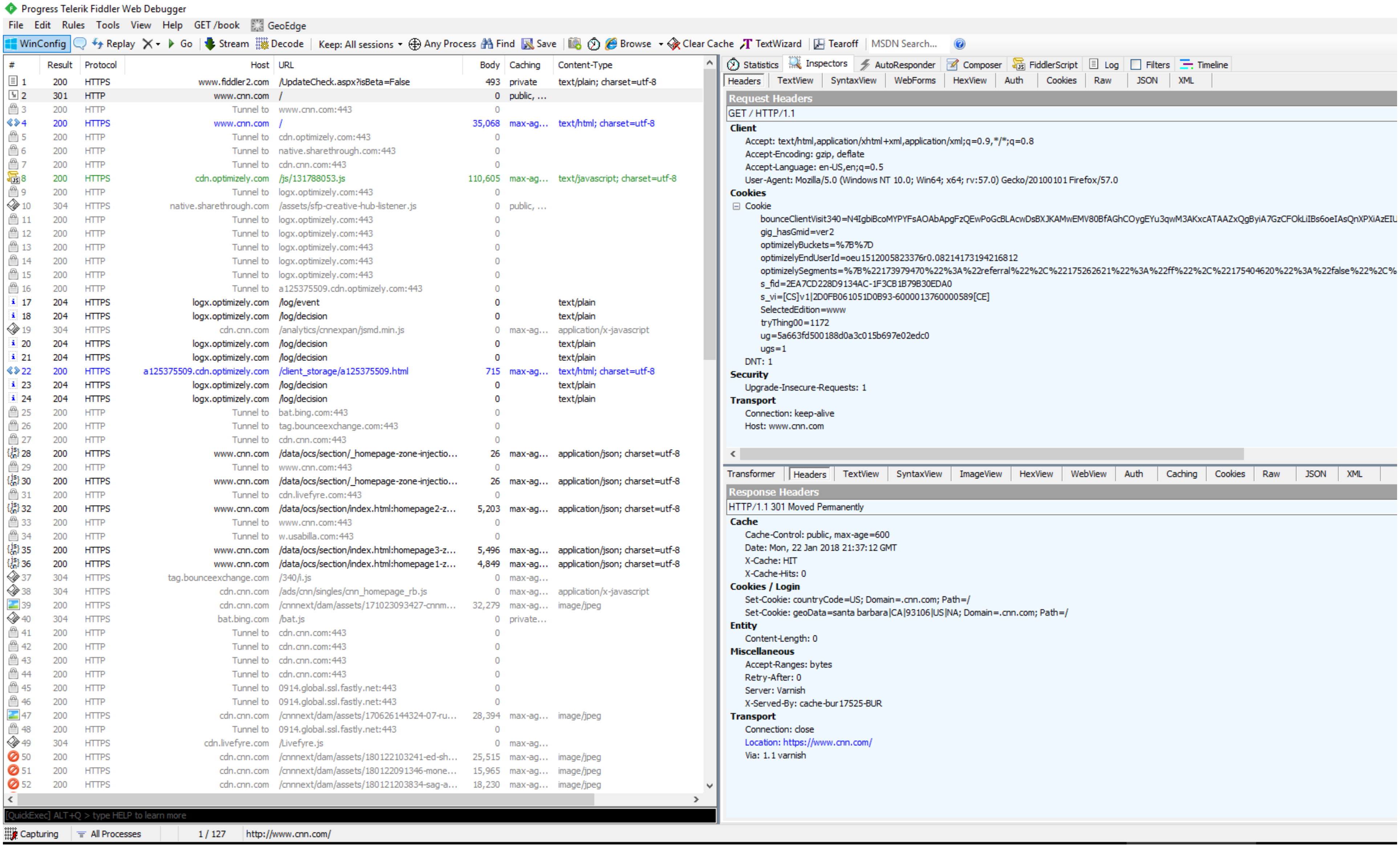
Wireshark

- Available from: http://www.wireshark.org/
  - Requires "libpcap" or "WinPcap" to be installed (included in distribution)
- Great tool for sniffing packets
- Wireshark has a flexible and deep set of analysis tools
- Wireshark + Windows + WLAN != promiscuous capture
  - http://wiki.wireshark.org/CaptureSetup/WLAN

"Unfortunately, changing the 802.11 capture modes is very platform/network adapter/driver/libpcap dependent, and might not be possible at all (Windows is very limited here)."

Fiddler

- Available from: http://www.telerik.com/fiddler
- Great tool for re-constructing HTTP sessions
  - Better than wireshark for displaying application-layer contents
  - Can install add-ons that show “transformation” from raw data to HTML data
- Inserts itself into the packet flow by creating a process that acts as a browser proxy
  - Packets flow: browser<->proxy<->Internet
  - Allows session keys to be used to decrypt session data
- Unlike wireshark, only works for sessions on a particular device


Progress Telerik Fiddler Web Debugger
File Edit Rules Tools View Help GET /book GeoEdge
WinConfig Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff MSDN Search...
Statistics Inspectors AutoResponder Composer FiddlerScript Log Filters Timeline
Headers TextView SyntaxView WebForms HexView Auth Cookies Raw JSON XML
Transformer Headers TextView SyntaxView ImageView HexView WebView Auth Caching Cookies Raw JSON XML

#	Result	Protocol	Host	URL	Body	Caching	Content-Type
1	200	HTTPS	www.fiddler2.com	/UpdateCheck.aspx?isBeta=False	493	private	text/plain; charset=utf-8
2	301	HTTP	www.cnn.com	/	0	public, ...	
3	200	HTTP	Tunnel to	www.cnn.com:443	0		
4	200	HTTPS	www.cnn.com	/	35,068	max-ag...	text/html; charset=utf-8
5	200	HTTP	Tunnel to	cdn.optimizely.com:443	0		
6	200	HTTP	Tunnel to	native.sharethrough.com:443	0		
7	200	HTTP	Tunnel to	cdn.cnn.com:443	0		
8	200	HTTPS	cdn.optimizely.com	/js/131788053.js	110,605	max-ag...	text/javascript; charset=utf-8
9	200	HTTP	Tunnel to	logx.optimizely.com:443	0		
10	304	HTTPS	native.sharethrough.com	/assets/sfp-creative-hub-listener.js	0	public, ...	
11	200	HTTP	Tunnel to	logx.optimizely.com:443	0		
12	200	HTTP	Tunnel to	logx.optimizely.com:443	0		
13	200	HTTP	Tunnel to	logx.optimizely.com:443	0		
14	200	HTTP	Tunnel to	logx.optimizely.com:443	0		
15	200	HTTP	Tunnel to	logx.optimizely.com:443	0		
16	200	HTTP	Tunnel to	a125375509.cdn.optimizely.com:443	0		
17	204	HTTPS	logx.optimizely.com	/log/event	0		text/plain
18	204	HTTPS	logx.optimizely.com	/log/decision	0		text/plain
19	304	HTTPS	cdn.cnn.com	/analytics/cnnexpan/jsmd.min.js	0	max-ag...	application/x-javascript
20	204	HTTPS	logx.optimizely.com	/log/decision	0		text/plain
21	204	HTTPS	logx.optimizely.com	/log/decision	0		text/plain
22	200	HTTPS	a125375509.cdn.optimizely.com	/client_storage/a125375509.html	715	max-ag...	text/html; charset=utf-8
23	204	HTTPS	logx.optimizely.com	/log/decision	0		text/plain
24	204	HTTPS	logx.optimizely.com	/log/decision	0		text/plain
25	200	HTTP	Tunnel to	bat.bing.com:443	0		
26	200	HTTP	Tunnel to	tag.bounceexchange.com:443	0		
27	200	HTTP	Tunnel to	cdn.cnn.com:443	0		
28	200	HTTPS	www.cnn.com	/data/ocs/section/_homepage-zone-injectio...	26	max-ag...	application/json; charset=utf-8
29	200	HTTP	Tunnel to	www.cnn.com:443	0		
30	200	HTTPS	www.cnn.com	/data/ocs/section/_homepage-zone-injectio...	26	max-ag...	application/json; charset=utf-8
31	200	HTTP	Tunnel to	cdn.livefyre.com:443	0		
32	200	HTTPS	www.cnn.com	/data/ocs/section/index.html:homepage2-z...	5,203	max-ag...	application/json; charset=utf-8
33	200	HTTP	Tunnel to	www.cnn.com:443	0		
34	200	HTTP	Tunnel to	w.usabilla.com:443	0		
35	200	HTTPS	www.cnn.com	/data/ocs/section/index.html:homepage3-z...	5,496	max-ag...	application/json; charset=utf-8
36	200	HTTPS	www.cnn.com	/data/ocs/section/index.html:homepage1-z...	4,849	max-ag...	application/json; charset=utf-8
37	304	HTTPS	tag.bounceexchange.com	/340/i.js	0	max-ag...	
38	304	HTTPS	cdn.cnn.com	/ads/cnn/singles/cnn_homepage_rb.js	0	max-ag...	application/x-javascript
39	200	HTTPS	cdn.cnn.com	/cnnnext/dam/assets/171023093427-cnnm...	32,279	max-ag...	image/jpeg
40	304	HTTPS	bat.bing.com	/bat.js	0	private...	
41	200	HTTP	Tunnel to	cdn.cnn.com:443	0		
42	200	HTTP	Tunnel to	cdn.cnn.com:443	0		
43	200	HTTP	Tunnel to	cdn.cnn.com:443	0		
44	200	HTTP	Tunnel to	cdn.cnn.com:443	0		
45	200	HTTP	Tunnel to	0914.global.ssl.fastly.net:443	0		
46	200	HTTP	Tunnel to	0914.global.ssl.fastly.net:443	0		
47	200	HTTPS	cdn.cnn.com	/cnnnext/dam/assets/170626144324-07-ru...	28,394	max-ag...	image/jpeg
48	200	HTTP	Tunnel to	0914.global.ssl.fastly.net:443	0		
49	304	HTTPS	cdn.livefyre.com	/Livefyre.js	0	max-ag...	
50	200	HTTPS	cdn.cnn.com	/cnnnext/dam/assets/180122103241-ed-sh...	25,515	max-ag...	image/jpeg
51	200	HTTPS	cdn.cnn.com	/cnnnext/dam/assets/180122091346-mone...	15,965	max-ag...	image/jpeg
52	200	HTTPS	cdn.cnn.com	/cnnnext/dam/assets/180121203834-sag-a...	18,230	max-ag...	image/jpeg

```
[QuickExec] ALT+Q > type HELP to learn more
```

Capturing | All Processes | 1 / 127 | http://www.cnn.com/

Request Headers

```
GET / HTTP/1.1
Client
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
    Accept-Encoding: gzip, deflate
    Accept-Language: en-US,en;q=0.5
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0
Cookies
  ⊟ Cookie
        bounceClientVisit340=N4IgbiBcoMYPYFsAOAbApgFzQEwPoGcBLAcwDsBXJKAMwEMV80BfAGhCOygEYu3qwM3AKxcATAAZxQgByiA7GzCFOkLiIBs6oeIAsQnXPXiAzEIU
        gig_hasGmid=ver2
        optimizelyBuckets=%7B%7D
        optimizelyEndUserId=oeu1512005823376r0.08214173194216812
        optimizelySegments=%7B%22173979470%22%3A%22referral%22%2C%22175262621%22%3A%22ff%22%2C%22175404620%22%3A%22false%22%2C%
        s_fid=2EA7CD228D9134AC-1F3CB1B79B30EDA0
        s_vi=[CS]v1|2D0FB061051D0B93-6000013760000589[CE]
        SelectedEdition=www
        tryThing00=1172
        ug=5a663fd500188d0a3c015b697e02edc0
        ugs=1
    DNT: 1
Security
    Upgrade-Insecure-Requests: 1
Transport
    Connection: keep-alive
    Host: www.cnn.com
```

Response Headers

```
HTTP/1.1 301 Moved Permanently
Cache
    Cache-Control: public, max-age=600
    Date: Mon, 22 Jan 2018 21:37:12 GMT
    X-Cache: HIT
    X-Cache-Hits: 0
Cookies / Login
    Set-Cookie: countryCode=US; Domain=.cnn.com; Path=/
    Set-Cookie: geoData=santa barbara|CA|93106|US|NA; Domain=.cnn.com; Path=/
Entity
    Content-Length: 0
Miscellaneous
    Accept-Ranges: bytes
    Retry-After: 0
    Server: Varnish
    X-Served-By: cache-bur17525-BUR
Transport
    Connection: close
    Location: https://www.cnn.com/
    Via: 1.1 varnish
```

Firesheep

- ***WARNING: Use of Firesheep in a public network is very likely illegal***
  - While an excellent tool from which to learn (good demonstration of HTTP hijacking attack), it must be used with great care
  - http://codebutler.com/firesheep
  - http://en.wikipedia.org/wiki/Firesheep
- Mostly worked with older versions of Firefox
- Source code is available, worth a look if you are interested
- Basic idea
  - Many sites use cookies to maintain low-maintenance sessions
  - Firesheep sniffs the cookie and then installs it as your own
  - When visiting to a site, the new cookie will allow you to impersonate the cookie owner
- Easy solution is to use HTTPS