Linux Networking Basics

Naveen.M.K,
Protocol Engineering & Technology Unit,
Electrical Engineering Department,
Indian Institute of Science,
Bangalore - 12.

Outline

- Basic linux networking commands
  - ifconfig, route, ip
- Servers Setup
  - apache, ftp
- Troubleshooting
  - tcpdump and ethereal

Ifconfig

- 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.
- Options:
  - interface
  - up
  - down
  - netmask

Ifconfig

File Edit View Terminal Tabs Help

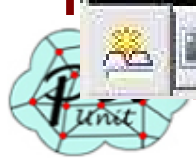
```
[satanix@pclab ~]$ /sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 00:08:A1:50:C8:94
          inet addr:10.32.21.18  Bcast:10.255.255.255  Mask:255.0.0.0
          inet6 addr: fe80::208:a1ff:fe50:c894/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1404746 errors:0 dropped:0 overruns:0 frame:0
          TX packets:125629 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:238110779 (227.0 MiB)  TX bytes:15948387 (15.2 MiB)
          Interrupt:9 Base address:0xd800

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2201 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2201 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2172968 (2.0 MiB)  TX bytes:2172968 (2.0 MiB)

[satanix@pclab ~]$
```

``ip'' command

```
[satanix@pclab network-class1]$ /sbin/ip addr
1: lo: <LOOPBACK,UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:08:a1:50:c8:94 brd ff:ff:ff:ff:ff:ff
    inet 10.32.21.18/16 brd 10.32.255.255 scope global eth0
    inet6 fe80::208:a1ff:fe50:c894/64 scope link
       valid_lft forever preferred_lft forever
3: sit0: <NOARP> mtu 1480 qdisc noop
    link/sit 0.0.0.0 brd 0.0.0.0
[satanix@pclab network-class1]$ /sbin/ip route
10.32.0.0/16 dev eth0  proto kernel  scope link  src 10.32.21.18
169.254.0.0/16 dev eth0  scope link
default via 10.32.1.1 dev eth0
[satanix@pclab network-class1]$ /sbin/ip link
1: lo: <LOOPBACK,UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:08:a1:50:c8:94 brd ff:ff:ff:ff:ff:ff
3: sit0: <NOARP> mtu 1480 qdisc noop
    link/sit 0.0.0.0 brd 0.0.0.0
[satanix@pclab network-class1]$
```



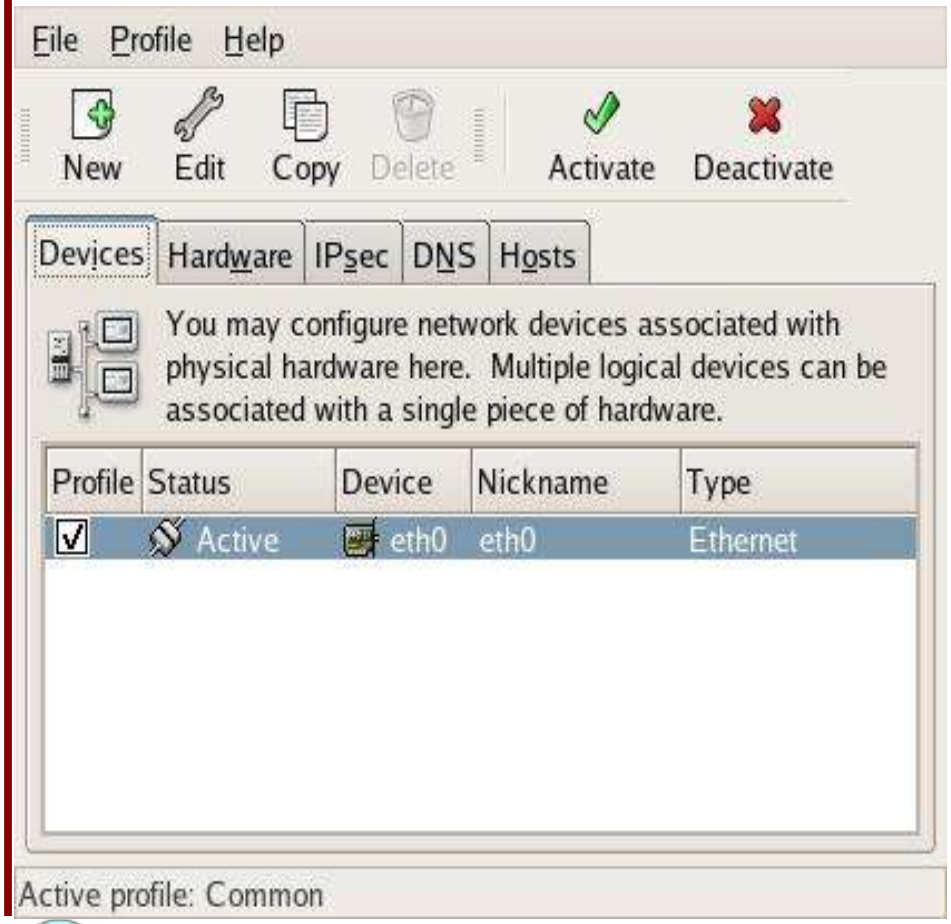
``route'' command

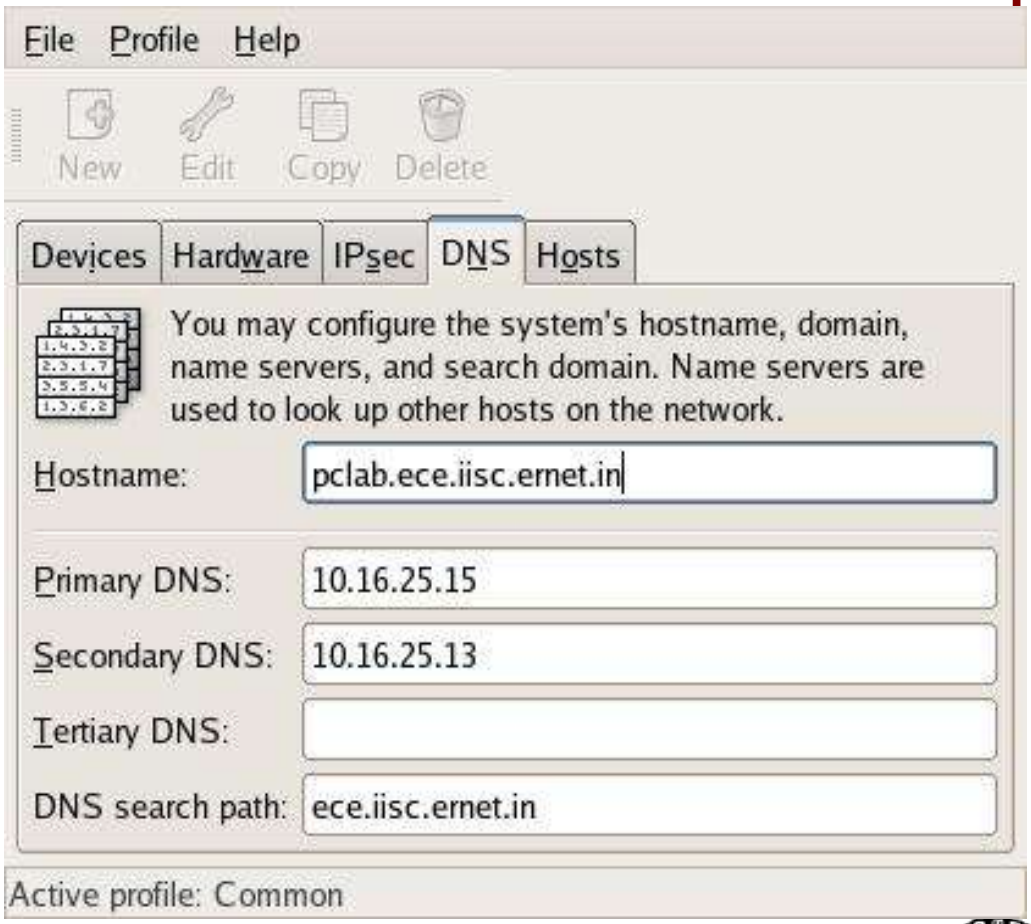
– manually configuring routes

- host route - to a single machine
  - route add –host 192.168.4.2 eth0
- network route, local - to a group of machines
  - route add –net 192.168.4.0 netmask 255.255.255.0 eth0
- network route, thru gateway - to a group of machines
  - route add –net 192.168.5.0 netmask 255.255.255.0 gw 192.168.4.1
- default route - to "any and all" else
  - route add default gw 192.168.4.1

NIC Configuration

- **/etc/init.d/network start/stop** command
- **system-config-network** command

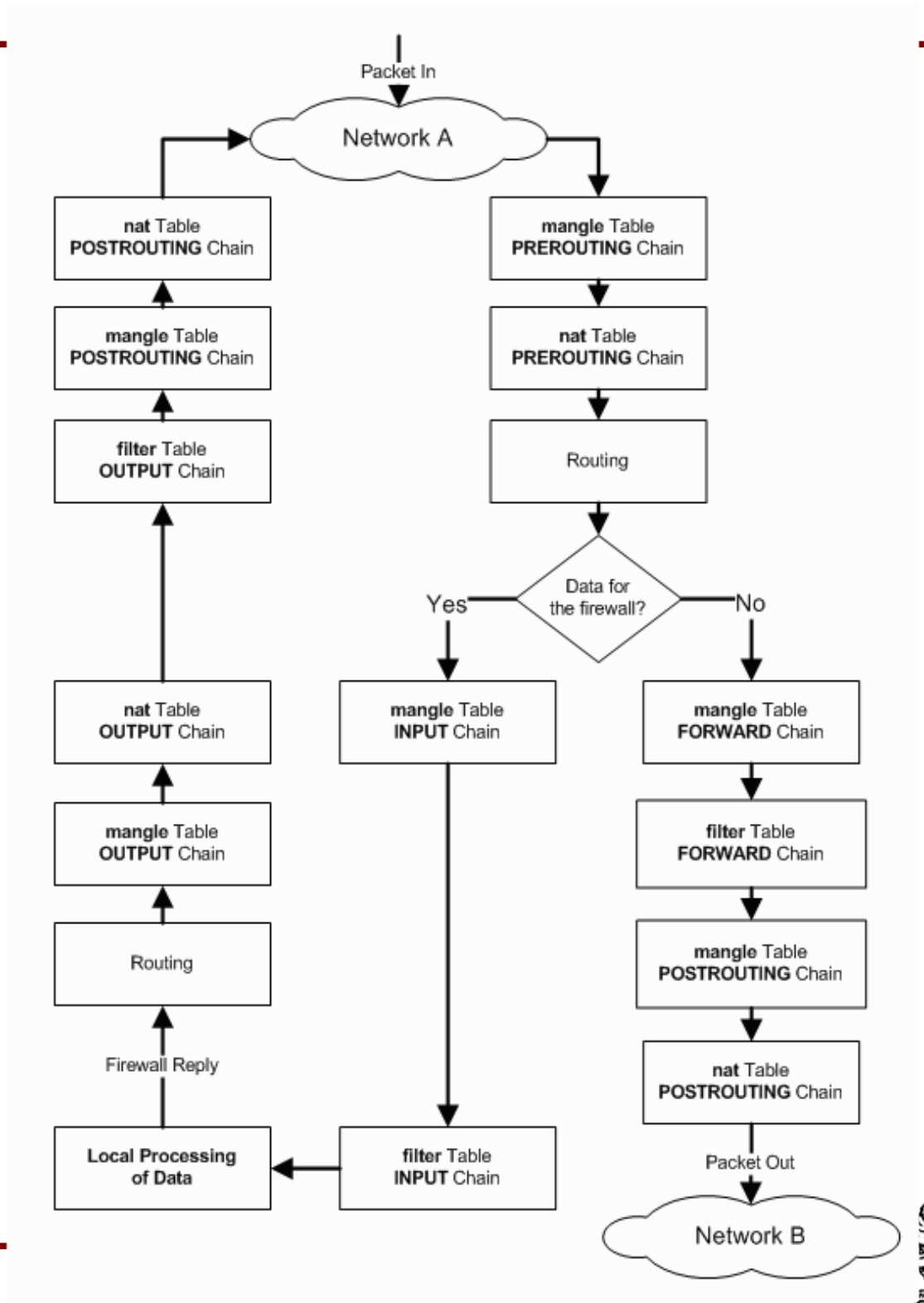




Linux Firewall Configuration

- Using ``**iptables**'' and ``**system-config-securitylevel**''
  - Stateful packet inspection
  - Filtering packets based on a MAC address and the values of the flags in the TCP header
  - System logging that provides the option of adjusting the level of detail of the reporting
  - Better network address translation
  - Support for transparent integration with such Web proxy programs as Squid
  - A rate limiting feature helps iptables block some types of denial of service (DoS) attacks.

iptables execution



Linux Firewall Configuration

- Using ``iptables''
  - ACCEPT
  - DROP
  - REJECT
  - LOG
  - DNAT
  - SNAT
  - MASQUERADE: Used to SNAT.

ipchains rules examples

- **iptables -A INPUT -s 0/0 -i eth0 -d 192.168.1.1 -p TCP -j ACCEPT**
- iptables is being configured to allow the firewall to accept TCP packets coming in on interface eth0 from any IP address destined for the firewall's IP address of 192.168.1.1. The 0/0 representation of an IP address means any.

- **iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.1.58 -o eth1 -p TCP --sport 1024:65535 --dport 80 -j ACCEPT**
- iptables is being configured to allow the firewall to accept TCP packets for routing when they enter on interface eth0 from any IP address and are destined for an IP address of 192.168.1.58 that is reachable via interface eth1. The source port is in the range 1024 to 65535 and the destination port is port 80 (www/http).

SERVERS

WEB, FTP, DHCP.

Apache Web Server

- Download and install: http://httpd.apache.org/
- Configuration files
- httpd.conf, access.conf. and srm.conf

```
<Directory /var/www/html>
order deny,allow
deny from all
allow from 10.10.64
</Directory>
```

```
ErrorDocument 404 /error.html
```

```
DocumentRoot /var/www/html
```

FTP Server

- Using ``vsftpd''

- The vsftpd.conf File
  - VSFTPD runs as an anonymous FTP server.
  - VSFTPD allows only anonymous FTP downloads to remote users, not uploads from them
  - VSFTPD doesn't allow anonymous users to create directories on your FTP server
  - VSFTPD logs FTP access to the /var/log/vsftpd.log log file
  - By default VSFTPD expects files for anonymous FTP to be placed in the /var/ftp directory.
  - Limiting the maximum number of client connections (max_clients)

DHCP: dhcpd and dhclient

- **dhcpd** - Dynamic Host Configuration Protocol Server
- Implements the Dynamic Host Configuration Protocol (DHCP) and the Internet Bootstrap Protocol (BOOTP). DHCP allows hosts on a TCP/IP network to request and be assigned IP addresses, and also to discover information about the network to which they are attached.
- **#[PATH-TO-DHCPD]dhcpd {start|stop|restart|status}**

dhcpd and **dhclient**

- DHCP Client, ***dhclient***, provides a means for configuring one or more network interfaces using the Dynamic Host Configuration Protocol, BOOTP protocol, or if these protocols fail, by statically assigning an address.

- **#[PATH-TO-dhclient]dhclient**

dhclient output

File Edit View Terminal Tabs Help

```
[root@rajata ~]# dhclient
Internet Systems Consortium DHCP Client V3.0.1
Copyright 2004 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/products/DHCP

sit0: unknown hardware address type 776
sit0: unknown hardware address type 776
Listening on LPF/sit0/
Sending on   LPF/sit0/
Listening on LPF/eth1/00:0c:f1:00:0a:11
Sending on   LPF/eth1/00:0c:f1:00:0a:11
Listening on LPF/eth0/00:00:f0:87:26:b3
Sending on   LPF/eth0/00:00:f0:87:26:b3
Listening on LPF/lo/
Sending on   LPF/lo/
Sending on   Socket/fallback
DHCPDISCOVER on lo to 255.255.255.255 port 67 interval 8
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 6
DHCPDISCOVER on sit0 to 255.255.255.255 port 67 interval 3
DHCPREQUEST on eth1 to 255.255.255.255 port 67
DHCPACK from 192.168.1.1
bound to 192.168.1.102 -- renewal in 34386 seconds.
[root@rajata ~]#
```

dhcpd.conf and **dhclient.conf**

- ***dhcpd.conf*** file contains configuration information for **dhcpd**
- Keywords:
  - default-lease-time, max-lease-time
  - subnet, netmask, range, routers
  - domain-name, domain-name-servers

dhcpd.conf and **dhclient.conf**

- ***dhclient.conf*** file can be used to configure the behaviour of the client in a wide variety of ways:
- protocol timing, information requested from the server
- information required of the server
- defaults to use if the server does not provide certain information
- values with which to override information provided by the server,
- values to prepend or append to information provided by the server. The configuration file can also be preinitialized with addresses to use on networks that don't have DHCP servers.

dhcpd.conf and dhclient.conf

File Edit View Search Tools Documents Help

dhcpd.conf

```
# Set some defaults for least time and DNS update method
# ddns-update-style ad-hoc;
default-lease-time 1200;
max-lease-time 9200;

# set the subnet mask here for the wireless IP network
option subnet-mask 255.255.255.0;

# set the broadcast address here
option broadcast-address 172.18.64.255;

# set the router address.
# This will be 172.x.x.1 - the address of your wireless interface WLAN0
# (the AP In this case )
option routers 172.18.64.1;

# set Name Server address. This will be the same as your ethernet DNS address
# (check ur /etc/resolv.conf file)
option domain-name-servers 10.16.25.15;

# Set default domain name for the clients in the wless network
option domain-name "ece.iisc.ernet.in";

# Address 172.18.64.1 to 172.16.64.10 is admin numbers
# Address 172.18.64.11 to 172.18.64.20 is for AP's

# Added 20 hosts.
subnet 172.18.64.0 netmask 255.255.255.0 {
range 172.18.64.21 172.18.64.40;
option routers 172.18.64.1;
}
```

Ln 8, Col 34 INS

dhcpd.conf and dhclient.conf

File Edit View Search Tools Documents Help

dhclient.conf ×

```
send host-name "samsung.x10";
#send dhcp-client-identifier 1:0:a0:24:ab:fb:9c;
send dhcp-lease-time 3600;
supersede domain-name "ece.iisc.ernet.in mobile.com";
#prepend domain-name-servers 127.0.0.1;
request subnet-mask, broadcast-address, time-offset, routers,
        domain-name, domain-name-servers, host-name;
require subnet-mask, domain-name-servers;
timeout 60;
retry 60;
reboot 10;
select-timeout 5;
initial-interval 2;
script "/etc/dhclient-script";
# reject 192.33.137.209;
alias {
  interface "ep0";
  fixed-address 192.5.5.213;
  option subnet-mask 255.255.255.255;
}
lease {
  interface "eth1";
  fixed-address 172.18.64.21;
  option host-name "x10.samsung.com";
  option subnet-mask 255.255.255.0;
  option broadcast-address 172.18.64..255;
  option routers 172.18.64.1;
  option domain-name-servers 10.16.25.15;
}
```

Ln 8, Col 42 INS

Troubleshooting

- Tcpdump
  - Tcpdump prints out the headers of packets on a network interface that match the boolean expression.

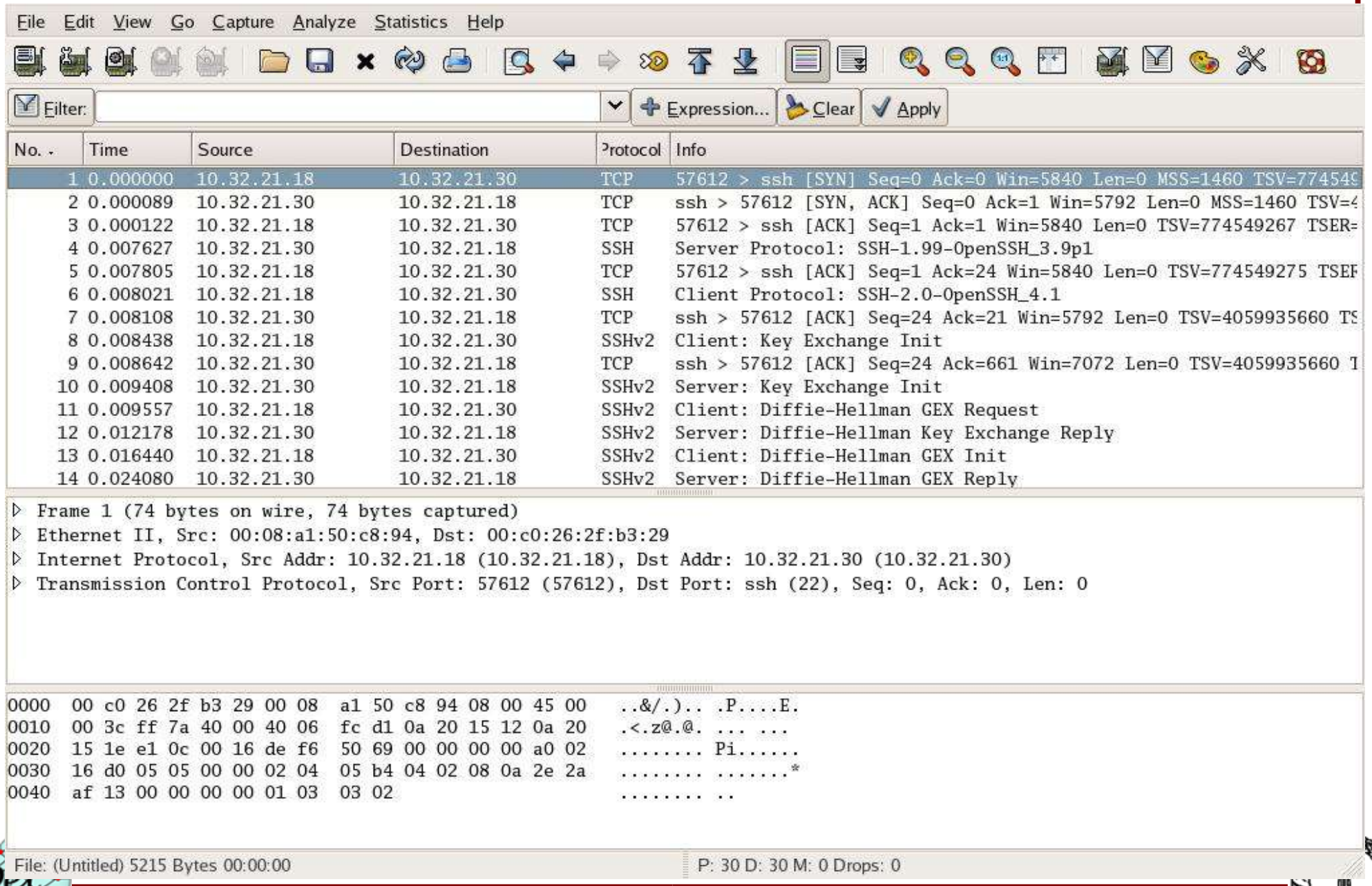
- Ethereal
  - Protocol analyzer, or "packet sniffer" software, used for network troubleshooting, analysis, software and protocol development, and education. It has all of the standard features of a protocol analyzer.

TCPDUMP

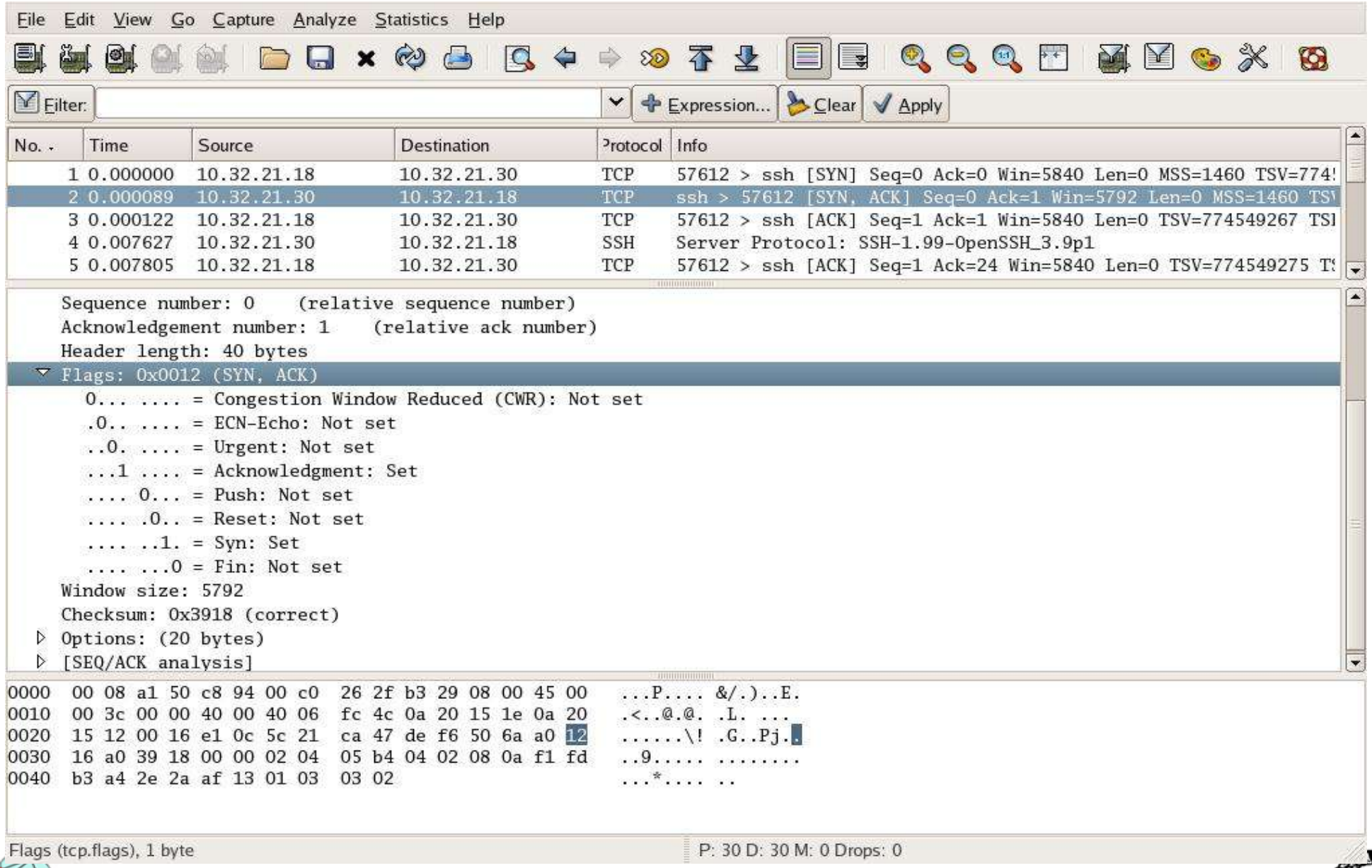
```
[root@pclab ~]# tcpdump -vv icmp
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
17:38:00.721659 IP (tos 0x0, ttl  64, id 0, offset 0, flags [DF], proto 1, length: 84) kaveri > pclab: icmp 64: echo request s
eq 0
17:38:00.722570 IP (tos 0x0, ttl  64, id 64771, offset 0, flags [none], proto 1, length: 84) pclab > kaveri: icmp 64: echo rep
ly seq 0
17:38:01.721996 IP (tos 0x0, ttl  64, id 1, offset 0, flags [DF], proto 1, length: 84) kaveri > pclab: icmp 64: echo request s
eq 1
17:38:01.722035 IP (tos 0x0, ttl  64, id 64772, offset 0, flags [none], proto 1, length: 84) pclab > kaveri: icmp 64: echo rep
ly seq 1
17:38:02.722832 IP (tos 0x0, ttl  64, id 2, offset 0, flags [DF], proto 1, length: 84) kaveri > pclab: icmp 64: echo request s
eq 2
17:38:02.722888 IP (tos 0x0, ttl  64, id 64773, offset 0, flags [none], proto 1, length: 84) pclab > kaveri: icmp 64: echo rep
ly seq 2
17:38:03.723653 IP (tos 0x0, ttl  64, id 3, offset 0, flags [DF], proto 1, length: 84) kaveri > pclab: icmp 64: echo request s
eq 3
17:38:03.723694 IP (tos 0x0, ttl  64, id 64774, offset 0, flags [none], proto 1, length: 84) pclab > kaveri: icmp 64: echo rep
ly seq 3
17:38:04.723476 IP (tos 0x0, ttl  64, id 4, offset 0, flags [DF], proto 1, length: 84) kaveri > pclab: icmp 64: echo request s
eq 4
17:38:04.723516 IP (tos 0x0, ttl  64, id 64775, offset 0, flags [none], proto 1, length: 84) pclab > kaveri: icmp 64: echo rep
ly seq 4

10 packets captured
10 packets received by filter
0 packets dropped by kernel
[root@pclab ~]#
```

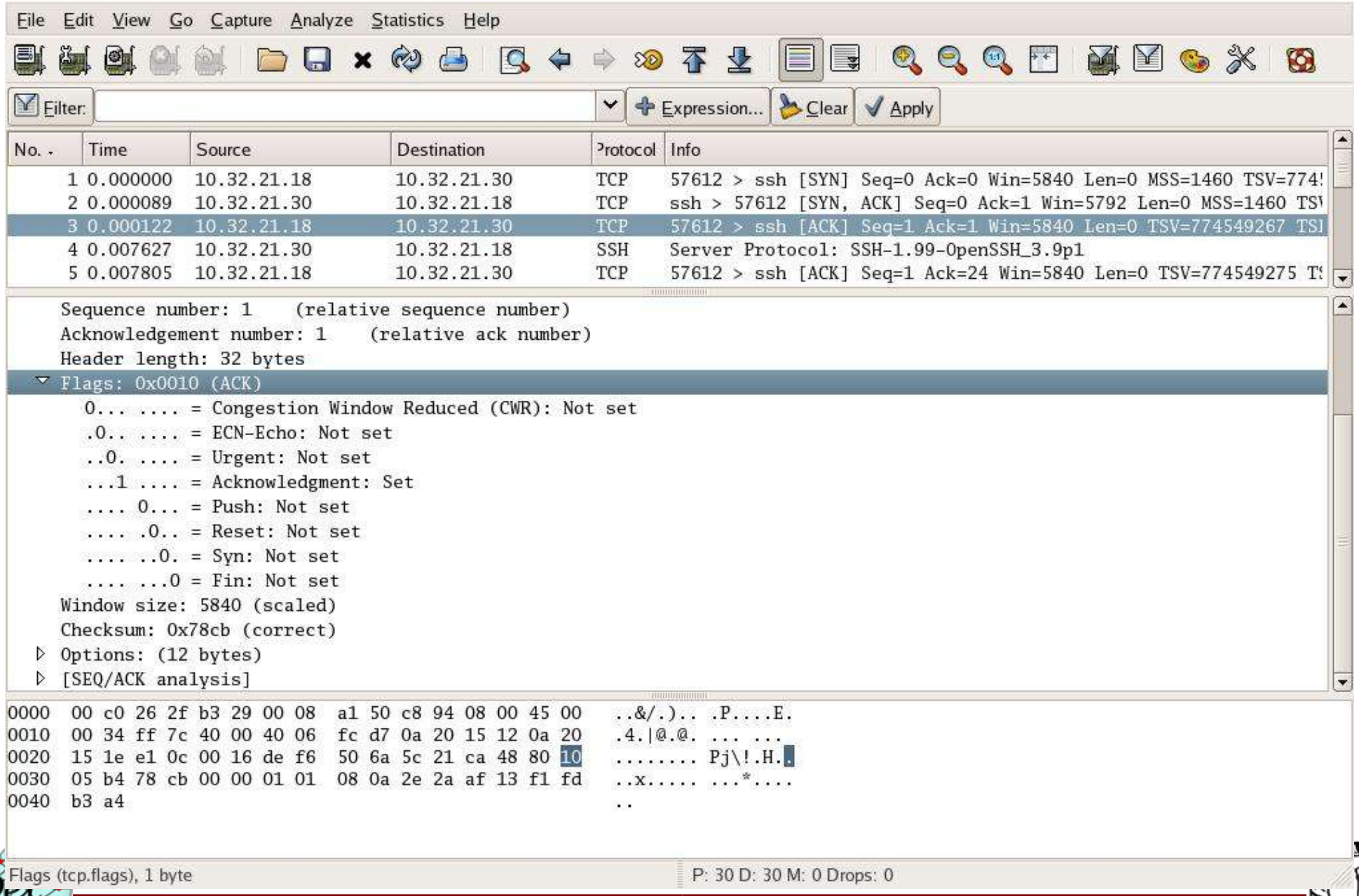
Ethereal


File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 10.32.21.18 10.32.21.30 TCP 57612 > ssh [SYN] Seq=0 Ack=0 Win=5840 Len=0 MSS=1460 TSV=774549
2 0.000089 10.32.21.30 10.32.21.18 TCP ssh > 57612 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=
3 0.000122 10.32.21.18 10.32.21.30 TCP 57612 > ssh [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=774549267 TSER=
4 0.007627 10.32.21.30 10.32.21.18 SSH Server Protocol: SSH-1.99-OpenSSH_3.9p1
5 0.007805 10.32.21.18 10.32.21.30 TCP 57612 > ssh [ACK] Seq=1 Ack=24 Win=5840 Len=0 TSV=774549275 TSEF
6 0.008021 10.32.21.18 10.32.21.30 SSH Client Protocol: SSH-2.0-OpenSSH_4.1
7 0.008108 10.32.21.30 10.32.21.18 TCP ssh > 57612 [ACK] Seq=24 Ack=21 Win=5792 Len=0 TSV=4059935660 TS
8 0.008438 10.32.21.18 10.32.21.30 SSHv2 Client: Key Exchange Init
9 0.008642 10.32.21.30 10.32.21.18 TCP ssh > 57612 [ACK] Seq=24 Ack=661 Win=7072 Len=0 TSV=4059935660 T
10 0.009408 10.32.21.30 10.32.21.18 SSHv2 Server: Key Exchange Init
11 0.009557 10.32.21.18 10.32.21.30 SSHv2 Client: Diffie-Hellman GEX Request
12 0.012178 10.32.21.30 10.32.21.18 SSHv2 Server: Diffie-Hellman Key Exchange Reply
13 0.016440 10.32.21.18 10.32.21.30 SSHv2 Client: Diffie-Hellman GEX Init
14 0.024080 10.32.21.30 10.32.21.18 SSHv2 Server: Diffie-Hellman GEX Reply
Frame 1 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:08:a1:50:c8:94, Dst: 00:c0:26:2f:b3:29
Internet Protocol, Src Addr: 10.32.21.18 (10.32.21.18), Dst Addr: 10.32.21.30 (10.32.21.30)
Transmission Control Protocol, Src Port: 57612 (57612), Dst Port: ssh (22), Seq: 0, Ack: 0, Len: 0
0000 00 c0 26 2f b3 29 00 08 a1 50 c8 94 08 00 45 00 ..&/.).. .P....E.
0010 00 3c ff 7a 40 00 40 06 fc d1 0a 20 15 12 0a 20 .<.z@.@. ... ...
0020 15 1e e1 0c 00 16 de f6 50 69 00 00 00 00 a0 02 .... Pi......
0030 16 d0 05 05 00 00 02 04 05 b4 04 02 08 0a 2e 2a ....*
0040 af 13 00 00 00 00 01 03 03 02 ....
File: (Untitled) 5215 Bytes 00:00:00
P: 30 D: 30 M: 0 Drops: 0

Ethereal


File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 10.32.21.18 10.32.21.30 TCP 57612 > ssh [SYN] Seq=0 Ack=0 Win=5840 Len=0 MSS=1460 TSV=774
2 0.000089 10.32.21.30 10.32.21.18 TCP ssh > 57612 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TS
3 0.000122 10.32.21.18 10.32.21.30 TCP 57612 > ssh [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=774549267 TS
4 0.007627 10.32.21.30 10.32.21.18 SSH Server Protocol: SSH-1.99-OpenSSH_3.9p1
5 0.007805 10.32.21.18 10.32.21.30 TCP 57612 > ssh [ACK] Seq=1 Ack=24 Win=5840 Len=0 TSV=774549275 T
Sequence number: 0 (relative sequence number)
Acknowledgement number: 1 (relative ack number)
Header length: 40 bytes
Flags: 0x0012 (SYN, ACK)
0... .... = Congestion Window Reduced (CWR): Not set
.0.. .... = ECN-Echo: Not set
..0. .... = Urgent: Not set
...1 .... = Acknowledgment: Set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
.... ..1. = Syn: Set
....0 = Fin: Not set
Window size: 5792
Checksum: 0x3918 (correct)
Options: (20 bytes)
[SEQ/ACK analysis]
0000 00 08 a1 50 c8 94 00 c0 26 2f b3 29 08 00 45 00 ...P.... &/.)..E.
0010 00 3c 00 00 40 00 40 06 fc 4c 0a 20 15 1e 0a 20 .<..@.@. .L. ...
0020 15 12 00 16 e1 0c 5c 21 ca 47 de f6 50 6a a0 12 ......\! .G..Pj..
0030 16 a0 39 18 00 00 02 04 05 b4 04 02 08 0a f1 fd ..9..... ....
0040 b3 a4 2e 2a af 13 01 03 03 02 ...*.... ..
Flags (tcp.flags), 1 byte
P: 30 D: 30 M: 0 Drops: 0

Ethereal


File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 10.32.21.18 10.32.21.30 TCP 57612 > ssh [SYN] Seq=0 Ack=0 Win=5840 Len=0 MSS=1460 TSV=774
2 0.000089 10.32.21.30 10.32.21.18 TCP ssh > 57612 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TS
3 0.000122 10.32.21.18 10.32.21.30 TCP 57612 > ssh [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=774549267 TS
4 0.007627 10.32.21.30 10.32.21.18 SSH Server Protocol: SSH-1.99-OpenSSH_3.9p1
5 0.007805 10.32.21.18 10.32.21.30 TCP 57612 > ssh [ACK] Seq=1 Ack=24 Win=5840 Len=0 TSV=774549275 T
Sequence number: 1 (relative sequence number)
Acknowledgement number: 1 (relative ack number)
Header length: 32 bytes
Flags: 0x0010 (ACK)
0... .... = Congestion Window Reduced (CWR): Not set
.0.. .... = ECN-Echo: Not set
..0. .... = Urgent: Not set
...1 .... = Acknowledgment: Set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
.... ..0. = Syn: Not set
....0 = Fin: Not set
Window size: 5840 (scaled)
Checksum: 0x78cb (correct)
Options: (12 bytes)
[SEQ/ACK analysis]
0000 00 c0 26 2f b3 29 00 08 a1 50 c8 94 08 00 45 00 ..&/.).. .P....E.
0010 00 34 ff 7c 40 00 40 06 fc d7 0a 20 15 12 0a 20 .4.|@.@. ... ...
0020 15 1e e1 0c 00 16 de f6 50 6a 5c 21 ca 48 80 10 .... Pj\!.H..
0030 05 b4 78 cb 00 00 01 01 08 0a 2e 2a af 13 f1 fd ..x..... ...*....
0040 b3 a4 ..
Flags (tcp.flags), 1 byte
P: 30 D: 30 M: 0 Drops: 0