

Farhad Ahmed
Computer Networking
11/08/18

WireShark Lab: IP

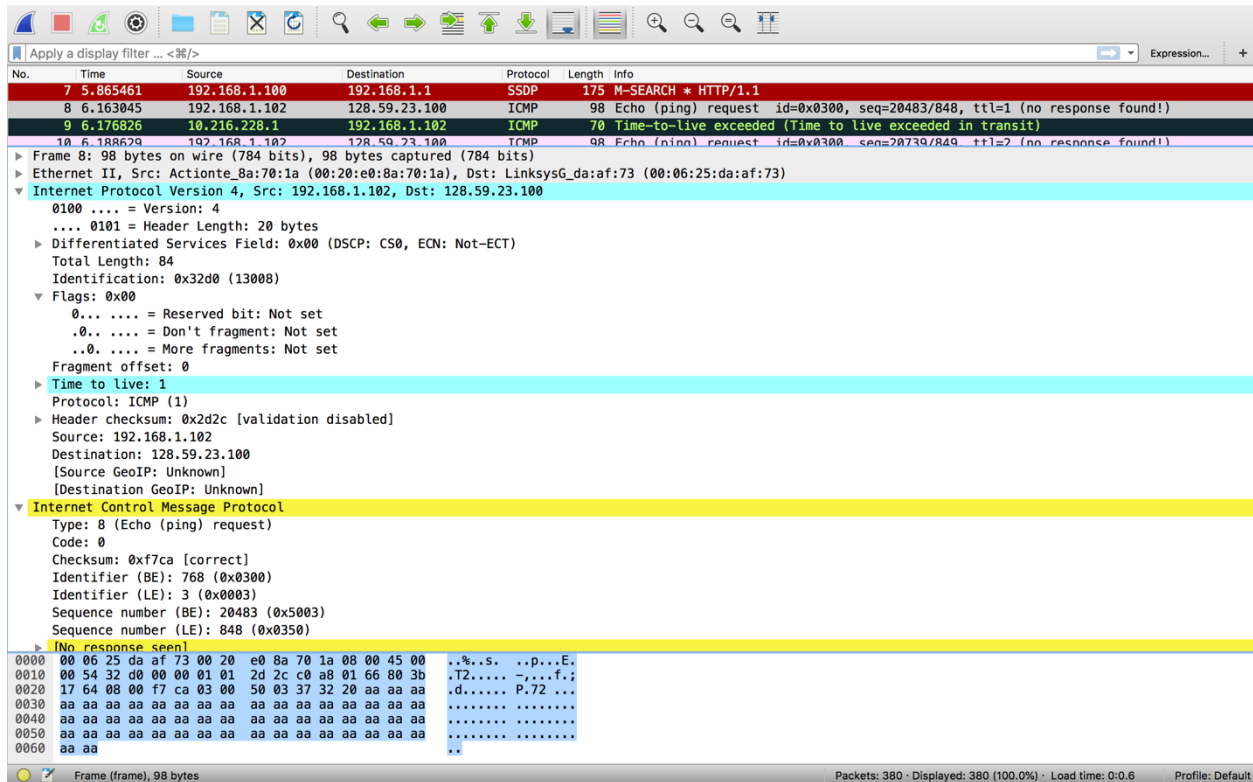
Running ifconfig:

```
farhads-MacBook-Pro:~ Farhad_Ahmed$ ipconfig
usage: ipconfig <command> <args>
where <command> is one of waitall, getifaddr, ifcount, getoption, getpacket, getv6packet, set, setverbose
farhads-MacBook-Pro:~ Farhad_Ahmed$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
    inet 127.0.0.1 netmask 0xff000000
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
    nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
XHC20: flags=0<> mtu 0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether ac:bc:32:91:a2:af
    inet6 fe80::1cef:6e2b:c794:2a4%en0 prefixlen 64 secured scopeid 0x5
    inet6 2604:2000:6aa5:4500:42f:6470:410b:b373 prefixlen 64 autoconf secured
    inet6 2604:2000:6aa5:4500:ded:14d2:7e19:68c1 prefixlen 64 autoconf temporary
    inet 192.168.0.8 netmask 0xffffffff broadcast 192.168.0.255
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect
    status: active
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
    ether 0e:bc:32:91:a2:af
    media: autoselect
    status: inactive
awd10: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1484
    ether fa:a3:79:0f:85:80
    inet6 fe80::f8a3:79ff:fe0f:8580%awd10 prefixlen 64 scopeid 0x7
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect
    status: active
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
    options=60<TS04,TS06>
    ether 4a:00:02:92:f1:80
    media: autoselect <full-duplex>
    status: inactive
en2: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
    options=60<TS04,TS06>
    ether 4a:00:02:92:f1:81
    media: autoselect <full-duplex>
    status: inactive
```

```

bridge0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
options=63<RXCSUM, TXCSUM, TS04, TS06>
ether 4a:00:02:92:f1:80
Configuration:
    id 0:0:0:0:0:0 priority 0 hellotime 0 fwddelay 0
    maxage 0 holdcnt 0 proto stp maxaddr 100 timeout 1200
    root id 0:0:0:0:0:0 priority 0 ifcost 0 port 0
    ipfilter disabled flags 0x2
member: en1 flags=3<LEARNING,DISCOVER>
    ifmaxaddr 0 port 8 priority 0 path cost 0
member: en2 flags=3<LEARNING,DISCOVER>
    ifmaxaddr 0 port 9 priority 0 path cost 0
nd6 options=201<PERFORMNUD,DAD>
media: <unknown type>
status: inactive
utun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 2000
inet6 fe80::98a3:bf24:a130:cfaa%utun0 prefixlen 64 scopeid 0xb
nd6 options=201<PERFORMNUD,DAD>
utun1: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
inet6 fe80::861f:5390:b5db:3a74%utun1 prefixlen 64 scopeid 0xc
nd6 options=201<PERFORMNUD,DAD>

```



1. The IP Address of my computer is 192.168.1.102.
2. The value in the upper layer protocol field is ICMP.

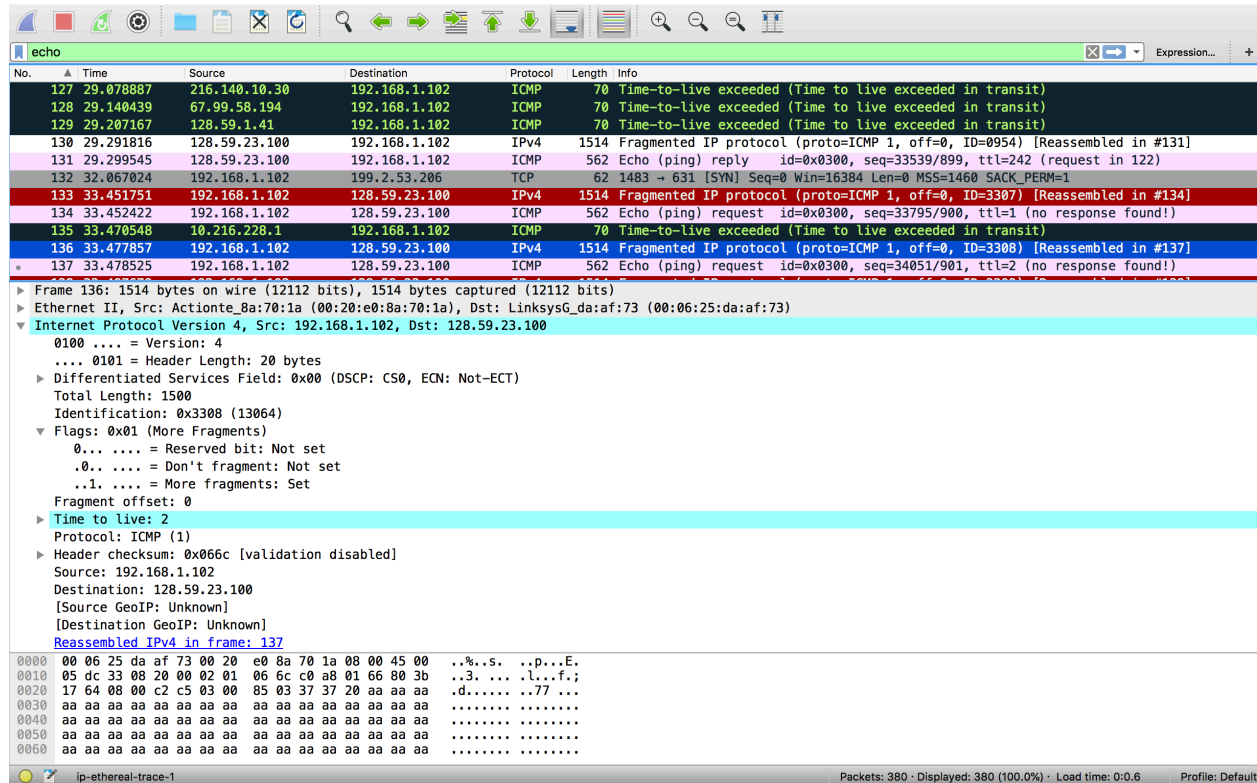
3. There are 20 bytes in the header and a total length of 84 bytes, so the payload of the IP data gram is 64 bytes.
4. The more fragments bit has a value of 0 so thus the data is not fragmented.
5. Identification, Time to live and Header checksum always change between datagrams.
6. The fields that stay constant across IP datagrams are Version, header length, source IP, destination IP, differentiated services, and upper layer protocol. The fields that must stay constant are Version, header length, source ip, destination ip, differentiated services, upper layer protocol. The fields that must change are identification, time to live, and header checksum.
7. The pattern is the IP header identification fields are incremented with the ICMP echo ping request.

No.	Time	Source	Destination	Protocol	Length	Info
9	6.176826	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
40	11.174495	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
65	16.179649	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
94	28.462264	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
135	33.470548	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
179	38.491817	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
219	43.485786	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
274	48.493873	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
330	53.501082	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
21	6.334320	12.122.10.22	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)
52	11.332109	12.122.10.22	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)

▶ Frame 9: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
 ▶ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
 ▼ Internet Protocol Version 4, Src: 10.216.228.1, Dst: 192.168.1.102
 0100 = Version: 4
 0101 = Header Length: 20 bytes
 ▶ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
 Total Length: 56
 Identification: 0x9d7c (40316)
 ▼ Flags: 0x00
 0... = Reserved bit: Not set
 .0.. = Don't fragment: Not set
 ..0. = More fragments: Not set
 Fragment offset: 0
 Time to live: 255
 Protocol: ICMP (1)
 ▶ Header checksum: 0x6ca0 [validation disabled]
 Source: 10.216.228.1
 Destination: 192.168.1.102
 [Source GeoIP: Unknown]
 [Destination GeoIP: Unknown]
 ▼ Internet Control Message Protocol
 0000 00 20 e0 8a 70 1a 00 06 25 da af 73 08 00 45 c0 ...p...%.s..E.
 0010 00 38 9d 7c 00 00 ff 01 6c a0 0a d8 e4 01 c0 a8 .8.|....l.....
 0020 01 66 0b 00 d9 46 00 00 00 00 45 00 00 54 32 d0 .f...F...E..T2.
 0030 00 00 01 01 f6 16 c0 a8 01 66 80 3b 17 64 08 00 f.;.d..
 0040 f7 ca 03 00 50 03 P.

8. The Identification field has 40316 and the TTL is 255.

9. The identification fields changes since it is supposed to be a unique id value. Two or more datagrams having the same id field means that they are part of the same datagram. The TTL field is the same since the TTL for the first hop router is always the same.



No.	Time	Source	Destination	Protocol	Length	Info
127	29.078887	216.140.10.30	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
128	29.140439	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
129	29.207167	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
130	29.291816	128.59.23.100	192.168.1.102	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0954) [Reassembled in #131]
131	29.299545	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=0x0300, seq=33539/899, ttl=242 (request in 122)
132	32.067024	192.168.1.102	199.2.53.206	TCP	62	1483 → 631 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
133	33.451751	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3307) [Reassembled in #134]
134	33.452422	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=33795/900, ttl=1 (no response found!)
135	33.470548	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
136	33.477857	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3308) [Reassembled in #137]
137	33.478525	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=34051/901, ttl=2 (no response found!)

Frame 136: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)

Ethernet II, Src: Actionte_Ba:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)

Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100

0100 = Version: 4
.... 0101 = Header Length: 20 bytes
► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0x3308 (13064)
▼ Flags: 0x01 (More Fragments)
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..1. = More fragments: Set
Fragment offset: 0
► Time to live: 2
Protocol: ICMP (1)
► Header checksum: 0x066c [validation disabled]
Source: 192.168.1.102
Destination: 128.59.23.100
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Reassembled IPv4 in frame: 137

0000 00 06 25 da af 73 00 20 e0 8a 70 1a 08 00 45 00 ..%.s. .p...E.
0010 05 dc 33 08 20 00 02 01 06 6c c0 a8 01 66 80 3b ..3. ...l...f.;
0020 17 64 08 00 c2 c5 03 00 85 03 37 37 20 aa aa aa .d.....77 ...
0030 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0040 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0050 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0060 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa

10. This packet was fragmented across more than one ip datagram.

11. Under the flags section, the more fragments bit is set to 1. The fragment offset being 0 denotes that this is the first fragment. The first datagram has a total length of 1500.

12. It is clear that this is the second fragment from looking at the fragment offset which is 1480 here. We know this is the last fragment since the more fragments flag is not set to 1.

13. The fields that changed are total length, flags, fragment offset, and checksum.

No.	Time	Source	Destination	Protocol	Length	Info
210	39.098928	216.140.10.30	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
211	39.164169	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
212	39.227649	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
213	39.314263	128.59.23.100	192.168.1.102	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0956) [Reassembled in #214]
214	39.322566	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=0x0300, seq=40195/925, ttl=242 (request in #205)
215	41.038658	192.168.1.102	199.2.53.206	TCP	62	[TCP Retransmission] 1483 → 631 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
216	43.466136	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
217	43.466808	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #218]
218	43.467629	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=40451/926, ttl=1 (no response found!)
219	43.485786	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
220	43.492284	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3324) [Reassembled in #222]
▶ Frame 216: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)						
▶ Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)						
▼ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100						
0100 = Version: 4						
.... 0101 = Header Length: 20 bytes						
▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
Total Length: 1500						
Identification: 0x3323 (13091)						
▼ Flags: 0x01 (More Fragments)						
0... = Reserved bit: Not set						
.0.. = Don't fragment: Not set						
..1. = More fragments: Set						
Fragment offset: 0						
▶ Time to live: 1						
Protocol: ICMP (1)						
▶ Header checksum: 0x0751 [validation disabled]						
Source: 192.168.1.102						
Destination: 128.59.23.100						
[Source GeoIP: Unknown]						
[Destination GeoIP: Unknown]						
Reassembled IPv4 in frame: 218						
0000	00 06 25 da af 73 00 20	e0 8a 70 1a 00 00 45 00	..%.s. .p...E.			
0010	05 dc 33 23 20 00 01 01	07 51 c0 a0 01 66 00 3b	..3#... .Q...f.;			
0020	17 64 00 00 a9 c3 03 00	9e 03 37 39 20 aa aa aa	..d..... .79 ...			
0030	aa aa aa aa aa aa aa aa	aa aa aa aa aa aa aa aa			
0040	aa aa aa aa aa aa aa aa	aa aa aa aa aa aa aa aa			
0050	aa aa aa aa aa aa aa aa	aa aa aa aa aa aa aa aa			
0060	aa aa aa aa aa aa aa aa	aa aa aa aa aa aa aa aa			

14. Switching the packet size to 3500 yielded 3 packets from the original datagram.

15. The fields that changed between all packets are fragment offset and checksum. In the first two packets and the last packets there's a change in total length and the flags that are set.