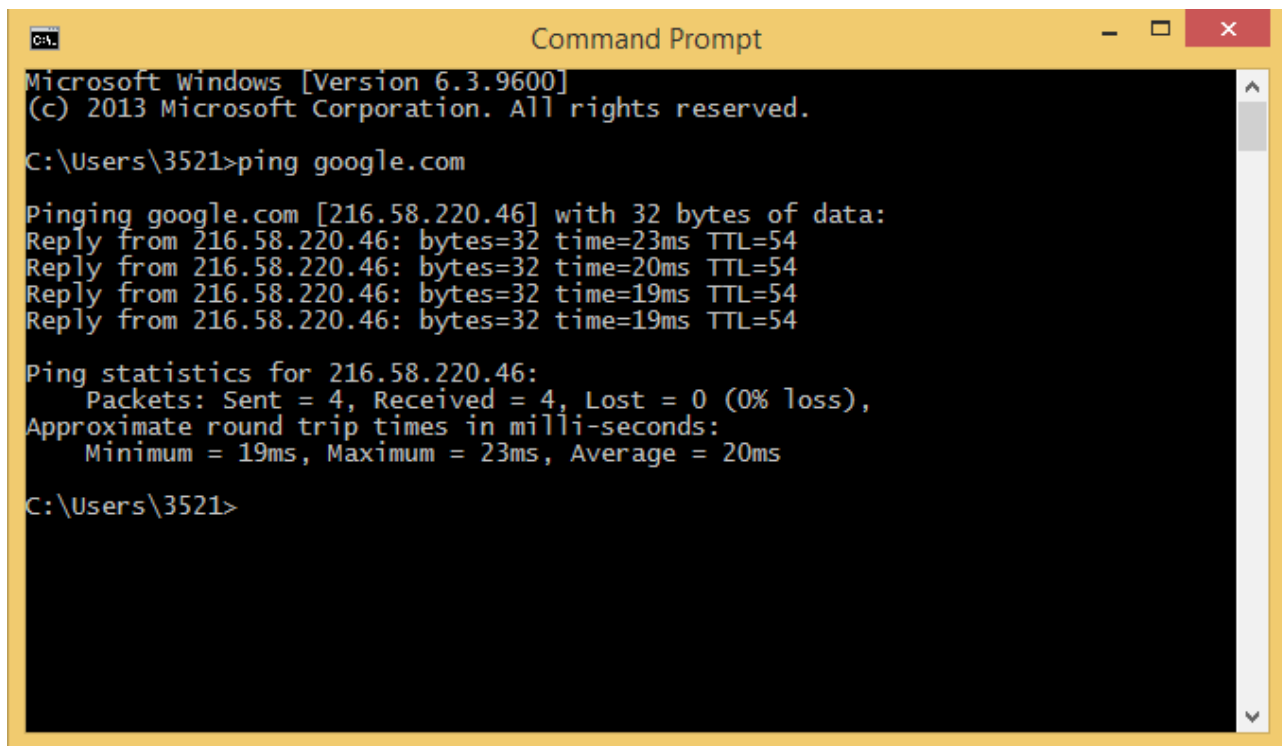


Snort showing alerts for TCP, UDP and ICMP packets :

```
Command Prompt
DP} 8.8.8.8:53 -> 10.0.0.2:65261
09/15-18:56:19.054951  [**] [1:100001:0] Testing ICMP Alert [**] [Priority: 0] {
ICMP} 10.0.0.2 -> 216.58.220.46
09/15-18:56:19.078029  [**] [1:100001:0] Testing ICMP Alert [**] [Priority: 0] {
ICMP} 216.58.220.46 -> 10.0.0.2
09/15-18:56:19.413338  [**] [1:100002:0] Testing UDP Alert [**] [Priority: 0] {U
DP} fe80:0000:0000:0000:54e2:f4b2:0a79:8d14:52308 -> ff02:0000:0000:0000:00
00:0001:0003:5355
09/15-18:56:19.413842  [**] [1:100002:0] Testing UDP Alert [**] [Priority: 0] {U
DP} 10.0.0.2:52308 -> 224.0.0.252:5355
09/15-18:56:19.479135  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 10.0.0.2:49247 -> 216.58.220.46:80
09/15-18:56:19.497833  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 216.58.220.46:80 -> 10.0.0.2:49247
09/15-18:56:19.751387  [**] [1:100002:0] Testing UDP Alert [**] [Priority: 0] {U
DP} 10.0.0.2:137 -> 10.0.0.255:137
09/15-18:56:20.074714  [**] [1:100001:0] Testing ICMP Alert [**] [Priority: 0] {
ICMP} 10.0.0.2 -> 216.58.220.46
09/15-18:56:20.094527  [**] [1:100001:0] Testing ICMP Alert [**] [Priority: 0] {
ICMP} 216.58.220.46 -> 10.0.0.2
09/15-18:56:20.310357  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 10.0.0.2:49208 -> 216.58.197.67:443
09/15-18:56:20.330831  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 216.58.197.67:443 -> 10.0.0.2:49208
09/15-18:56:20.335106  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 216.58.197.67:443 -> 10.0.0.2:49208
09/15-18:56:20.335211  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 10.0.0.2:49208 -> 216.58.197.67:443
09/15-18:56:20.336200  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 216.58.197.67:443 -> 10.0.0.2:49208
09/15-18:56:20.336575  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 10.0.0.2:49208 -> 216.58.197.67:443
09/15-18:56:20.400261  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 216.58.197.67:443 -> 10.0.0.2:49208
09/15-18:56:20.501834  [**] [1:100002:0] Testing UDP Alert [**] [Priority: 0] {U
DP} 10.0.0.2:137 -> 10.0.0.255:137
09/15-18:56:21.094448  [**] [1:100001:0] Testing ICMP Alert [**] [Priority: 0] {
ICMP} 10.0.0.2 -> 216.58.220.46
09/15-18:56:21.113985  [**] [1:100001:0] Testing ICMP Alert [**] [Priority: 0] {
ICMP} 216.58.220.46 -> 10.0.0.2
09/15-18:56:21.578046  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 10.0.0.2:49244 -> 216.58.197.74:443
09/15-18:56:21.598618  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 216.58.197.74:443 -> 10.0.0.2:49244
09/15-18:56:21.599731  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 216.58.197.74:443 -> 10.0.0.2:49244
09/15-18:56:21.649582  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 10.0.0.2:49244 -> 216.58.197.74:443
09/15-18:56:22.114059  [**] [1:100001:0] Testing ICMP Alert [**] [Priority: 0] {
```

```
Command Prompt
CP} 10.0.0.2:49244 -> 216.58.197.74:443
09/15-18:56:22.114059  [**] [1:100001:0] Testing ICMP Alert [**] [Priority: 0] {
ICMP} 10.0.0.2 -> 216.58.220.46
09/15-18:56:22.133536  [**] [1:100001:0] Testing ICMP Alert [**] [Priority: 0] {
ICMP} 216.58.220.46 -> 10.0.0.2
09/15-18:56:22.579486  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 10.0.0.2:49225 -> 216.58.220.33:443
09/15-18:56:22.598944  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 216.58.220.33:443 -> 10.0.0.2:49225
09/15-18:56:22.600065  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 216.58.220.33:443 -> 10.0.0.2:49225
09/15-18:56:22.650231  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 10.0.0.2:49225 -> 216.58.220.33:443
09/15-18:56:24.191626  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 74.125.200.189:443 -> 10.0.0.2:49254
09/15-18:56:24.232319  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 10.0.0.2:49254 -> 74.125.200.189:443
09/15-18:56:24.912701  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 10.0.0.2:49201 -> 216.58.220.46:80
09/15-18:56:24.933922  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 216.58.220.46:80 -> 10.0.0.2:49201
09/15-18:56:26.582322  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 10.0.0.2:49235 -> 216.58.220.46:443
09/15-18:56:26.605642  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 216.58.220.46:443 -> 10.0.0.2:49235
09/15-18:56:26.605644  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 216.58.220.46:443 -> 10.0.0.2:49235
09/15-18:56:26.655908  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 10.0.0.2:49235 -> 216.58.220.46:443
09/15-18:56:27.001986  [**] [1:100002:0] Testing UDP Alert [**] [Priority: 0] {U
DP} 10.0.0.2:137 -> 10.0.0.255:137
09/15-18:56:27.003300  [**] [1:100002:0] Testing UDP Alert [**] [Priority: 0] {U
DP} fe80:0000:0000:0000:54e2:f4b2:0a79:8d14:50619 -> ff02:0000:0000:0000:00
00:0001:0003:5355
09/15-18:56:27.003873  [**] [1:100002:0] Testing UDP Alert [**] [Priority: 0] {U
DP} 10.0.0.2:50619 -> 224.0.0.252:5355
09/15-18:56:27.414618  [**] [1:100002:0] Testing UDP Alert [**] [Priority: 0] {U
DP} fe80:0000:0000:0000:54e2:f4b2:0a79:8d14:50619 -> ff02:0000:0000:0000:00
00:0001:0003:5355
09/15-18:56:27.415117  [**] [1:100002:0] Testing UDP Alert [**] [Priority: 0] {U
DP} 10.0.0.2:50619 -> 224.0.0.252:5355
09/15-18:56:27.449670  [**] [1:100002:0] Testing UDP Alert [**] [Priority: 0] {U
DP} fe80:0000:0000:0000:54e2:f4b2:0a79:8d14:546 -> ff02:0000:0000:0000:0000
:0001:0002:547
09/15-18:56:27.583839  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 10.0.0.2:49231 -> 216.58.197.78:443
09/15-18:56:27.619485  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 216.58.197.78:443 -> 10.0.0.2:49231
09/15-18:56:27.622249  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
```

**Pinging google to create ICMP packets to check if Snort alerts us of those packets :**

A screenshot of a Windows Command Prompt window. The title bar is yellow and says "Command Prompt". The window has standard Windows window controls (minimize, maximize, close) on the right. The background is black, and the text is white. The text shows the command prompt at "C:\Users\3521>", the command "ping google.com", and the output of the ping command. The output shows four successful replies from 216.58.220.46 with varying times and TTL values. It also shows ping statistics for 216.58.220.46, indicating 0% loss and average round trip times. The prompt ends with "C:\Users\3521>".

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\3521>ping google.com

Pinging google.com [216.58.220.46] with 32 bytes of data:
Reply from 216.58.220.46: bytes=32 time=23ms TTL=54
Reply from 216.58.220.46: bytes=32 time=20ms TTL=54
Reply from 216.58.220.46: bytes=32 time=19ms TTL=54
Reply from 216.58.220.46: bytes=32 time=19ms TTL=54

Ping statistics for 216.58.220.46:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 19ms, Maximum = 23ms, Average = 20ms

C:\Users\3521>
```

Snort showing packet analysis results :

```
Command Prompt
CP} 216.58.220.46:80 -> 10.0.0.2:49247
*** Caught Int-Signal
09/15-18:56:33.007217  [**] [1:100002:0] Testing UDP Alert [**] [Priority: 0] {U
DP} 10.0.0.2:137 -> 10.0.0.255:137
=====
Run time for packet processing was 143.682000 seconds
Snort processed 7427 packets.
Snort ran for 0 days 0 hours 2 minutes 23 seconds
  Pkts/min:      3713
  Pkts/sec:       51
=====
Packet I/O Totals:
  Received:      7421
  Analyzed:      7427 (100.081%)
  Dropped:       0 ( 0.000%)
  Filtered:      0 ( 0.000%)
  Outstanding:  0 ( 0.000%)
  Injected:      0
=====
Breakdown by protocol (includes rebuilt packets):
  Eth:           7431 (100.000%)
  VLAN:          0 ( 0.000%)
  IP4:           7378 ( 99.287%)
  Frag:          0 ( 0.000%)
  ICMP:          8 ( 0.108%)
  UDP:           185 ( 2.490%)
  TCP:           7185 ( 96.690%)
  IP6:           41 ( 0.552%)
  IP6 Ext:       41 ( 0.552%)
  IP6 Opts:      0 ( 0.000%)
  Frag6:         0 ( 0.000%)
  ICMP6:         0 ( 0.000%)
  UDP6:          41 ( 0.552%)
  TCP6:          0 ( 0.000%)
  Teredo:        0 ( 0.000%)
  ICMP-IP:       0 ( 0.000%)
  EAPOL:         0 ( 0.000%)
  IP4/IP4:       0 ( 0.000%)
  IP4/IP6:       0 ( 0.000%)
  IP6/IP4:       0 ( 0.000%)
  IP6/IP6:       0 ( 0.000%)
  GRE:           0 ( 0.000%)
  GRE Eth:       0 ( 0.000%)
  GRE VLAN:     0 ( 0.000%)
  GRE IP4:       0 ( 0.000%)
  GRE IP6:       0 ( 0.000%)
  GRE IP6 Ext:  0 ( 0.000%)
  GRE PPTP:      0 ( 0.000%)
  GRE ARP:       0 ( 0.000%)
```

```
Command Prompt

GRE ARP: 0 ( 0.000%)
GRE IPX: 0 ( 0.000%)
GRE Loop: 0 ( 0.000%)
MPLS: 0 ( 0.000%)
ARP: 12 ( 0.161%)
IPX: 0 ( 0.000%)
Eth Loop: 0 ( 0.000%)
Eth Disc: 0 ( 0.000%)
IP4 Disc: 0 ( 0.000%)
IP6 Disc: 0 ( 0.000%)
TCP Disc: 0 ( 0.000%)
UDP Disc: 0 ( 0.000%)
ICMP Disc: 0 ( 0.000%)
All Discard: 0 ( 0.000%)
Other: 0 ( 0.000%)
Bad Chk Sum: 0 ( 0.000%)
Bad TTL: 0 ( 0.000%)
S5 G 1: 3 ( 0.040%)
S5 G 2: 1 ( 0.013%)
Total: 7431

=====
Action Stats:
Alerts: 7419 ( 99.839%)
Logged: 7419 ( 99.839%)
Passed: 0 ( 0.000%)
Limits:
Match: 0
Queue: 0
Log: 0
Event: 0
Alert: 147
Verdicts:
Allow: 727 ( 9.797%)
Block: 0 ( 0.000%)
Replace: 0 ( 0.000%)
Whitelist: 6700 ( 90.284%)
Blacklist: 0 ( 0.000%)
Ignore: 0 ( 0.000%)
(null): 0 ( 0.000%)

=====
Frag3 statistics:
Total Fragments: 0
Frag3 Reassembled: 0
Discards: 0
Memory Faults: 0
Timeouts: 0
Overlaps: 0
Anomalies: 0
Alerts: 0
```

```
Command Prompt

Alerts: 0
Drops: 0
FragTrackers Added: 0
FragTrackers Dumped: 0
FragTrackers Auto Freed: 0
Frag Nodes Inserted: 0
Frag Nodes Deleted: 0
=====
Stream statistics:
  Total sessions: 109
    TCP sessions: 39
    UDP sessions: 70
    ICMP sessions: 0
    IP sessions: 0
      TCP Prunes: 0
      UDP Prunes: 0
      ICMP Prunes: 0
      IP Prunes: 0
TCP StreamTrackers Created: 39
TCP StreamTrackers Deleted: 39
  TCP Timeouts: 0
  TCP Overlaps: 0
    TCP Segments Queued: 229
    TCP Segments Released: 229
    TCP Rebuilt Packets: 147
    TCP Segments Used: 206
    TCP Discards: 39
    TCP Gaps: 9
  UDP Sessions Created: 70
  UDP Sessions Deleted: 70
    UDP Timeouts: 0
    UDP Discards: 0
    Events: 4
  Internal Events: 0
  TCP Port Filter
    Filtered: 0
    Inspected: 0
    Tracked: 7181
  UDP Port Filter
    Filtered: 0
    Inspected: 0
    Tracked: 70
=====
HTTP Inspect - encodings (Note: stream-reassembled packets included):
  POST methods: 2
  GET methods: 0
  HTTP Request Headers extracted: 3
  HTTP Request cookies extracted: 0
```



```
Command Prompt

HTTP Request Headers extracted: 3
HTTP Request cookies extracted: 0
Post parameters extracted: 3
HTTP Response Headers extracted: 5
HTTP Response cookies extracted: 0
Unicode: 0
Double unicode: 0
Non-ASCII representable: 0
Directory traversals: 0
Extra slashes ("//"): 0
Self-referencing paths ("./"): 0
HTTP Response Gzip packets extracted: 0
Gzip Compressed Data Processed: n/a
Gzip Decompressed Data Processed: n/a
Total packets processed: 44
=====
SMTP Preprocessor Statistics
  Total sessions : 0
  Max concurrent sessions : 0
=====
dcerpc2 Preprocessor Statistics
  Total sessions: 0
=====
SSL Preprocessor:
  SSL packets decoded: 366
    Client Hello: 48
    Server Hello: 48
    Certificate: 48
    Server Done: 143
  Client Key Exchange: 50
  Server Key Exchange: 45
  Change Cipher: 98
  Finished: 0
  Client Application: 46
  Server Application: 51
  Alert: 7
  Unrecognized records: 74
  Completed handshakes: 0
  Bad handshakes: 0
  Sessions ignored: 30
  Detection disabled: 26
=====
SIP Preprocessor Statistics
  Total sessions: 0
=====
Reputation Preprocessor Statistics
  Total Memory Allocated: 0
=====
Snort exiting
```