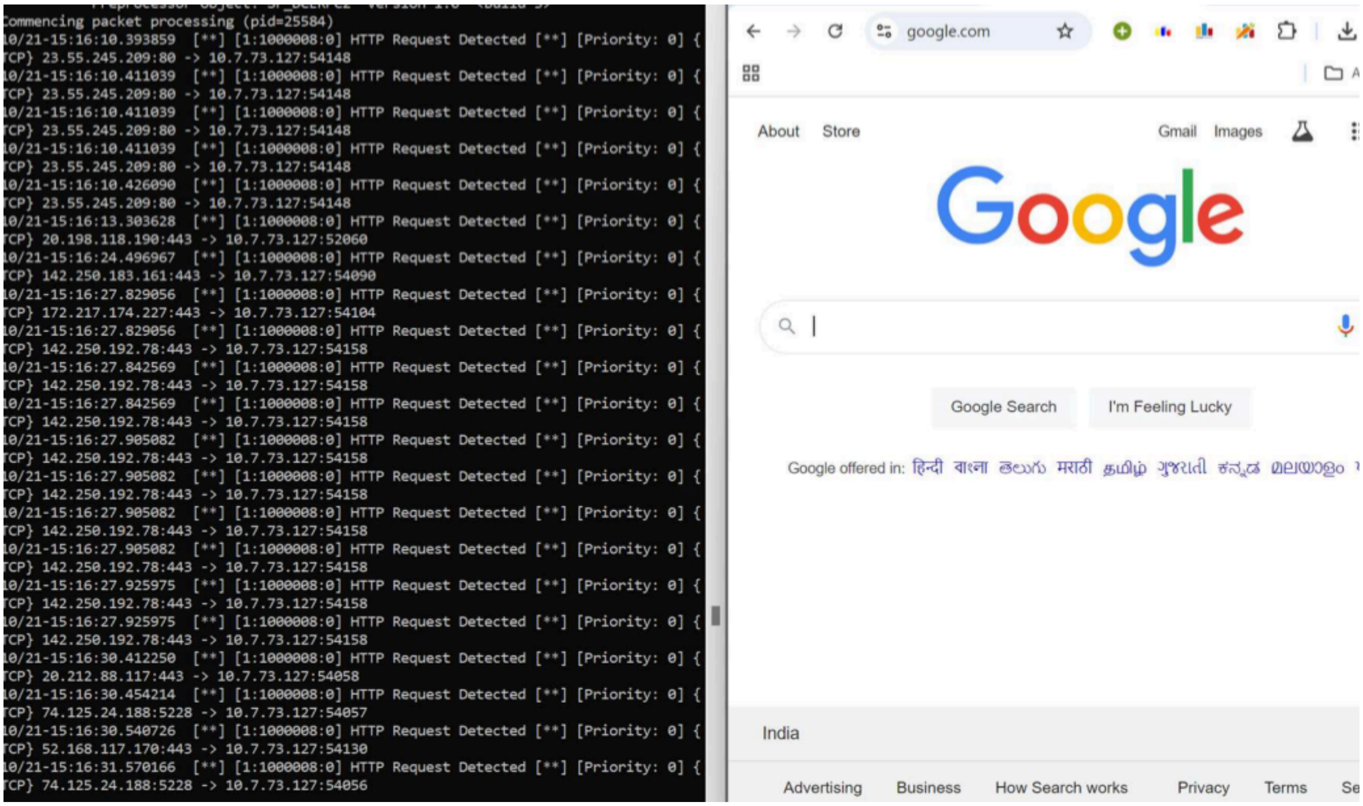
Practical - 5

Aim: IDS implementation using Snort

The following packets are shown when http request is carried out.



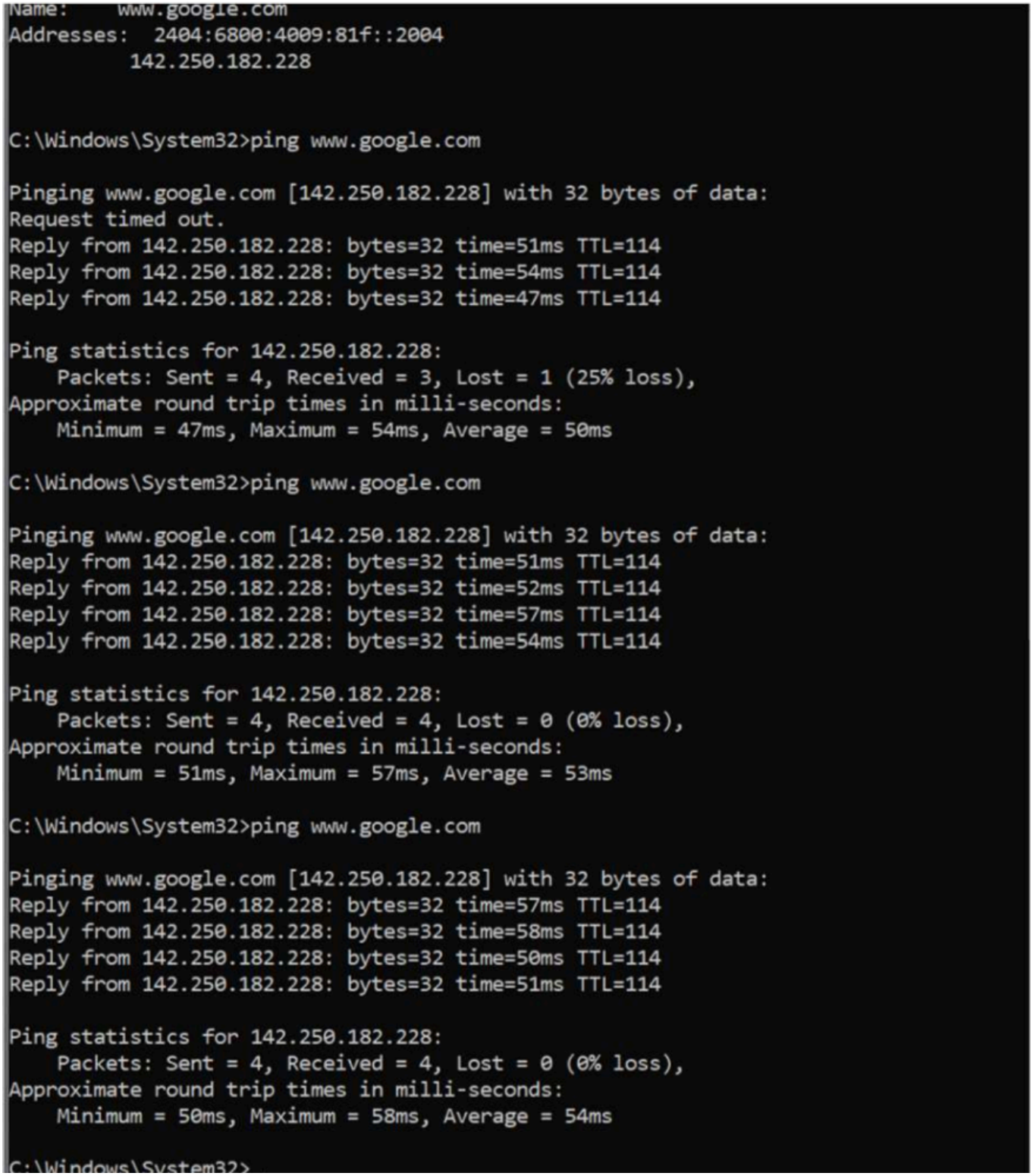
Rule:
alert tcp any any -> any any (msg:"HTTP Request Detected"; sid:1000008;)

The following snapshots show the processing packets when DNS and ICMP packets are generated.

```
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{743A80F6-BFE3-457F-819F-04352E0FA752}".

Decoding Ethernet

       --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20-WIN64 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.

           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.2  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
Commencing packet processing (pid=4804)
10/14-15:43:47.376904  [**] [1:1000005:0] DNS Query Detected [**] [Priority: 0] {UDP
} 10.7.82.87:57621 -> 10.7.127.255:57621
10/14-15:43:48.301722  [**] [1:1000005:0] DNS Query Detected [**] [Priority: 0] {UDP
} 10.7.91.201:137 -> 10.7.127.255:137
10/14-15:43:49.218350  [**] [1:1000005:0] DNS Query Detected [**] [Priority: 0] {UDP
} 10.7.112.140:137 -> 10.7.127.255:137
10/14-15:43:49.527968  [**] [1:1000005:0] DNS Query Detected [**] [Priority: 0] {UDP
} 10.7.109.129:137 -> 10.7.127.255:137
*** Caught Int-Signal
===============================================================================
Run time for packet processing was 3.708000 seconds
Snort processed 143 packets.
Snort ran for 0 days 0 hours 0 minutes 3 seconds
```

```
C:\Windows\System32>ping 10.7.84.165

Pinging 10.7.84.165 with 32 bytes of data:
Reply from 10.7.84.165: bytes=32 time<1ms TTL=128
Reply from 10.7.84.165: bytes=32 time<1ms TTL=128
Reply from 10.7.84.165: bytes=32 time<1ms TTL=128
Reply from 10.7.84.165: bytes=32 time<1ms TTL=128

Ping statistics for 10.7.84.165:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Windows\System32>nslookup www.google.com
Server:  uniboxadmin.wifi-soft.com
Address:  10.7.61.5

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:6800:4009:81f::2004
          142.250.182.228


C:\Windows\System32>nslookup www.google.com
Server:  uniboxadmin.wifi-soft.com
Address:  10.7.61.5

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:6800:4009:81f::2004
          142.250.182.228


C:\Windows\System32>
```

```
10/14-15:46:21.366625  [**] [1:1000005:0] DNS Query Detected [**] [Priority: 0] {UDP
} 10.7.94.175:137 -> 10.7.127.255:137
10/14-15:46:21.366625  [**] [1:1000005:0] DNS Query Detected [**] [Priority: 0] {UDP
} 10.7.94.175:137 -> 10.7.127.255:137
10/14-15:46:21.459724  [**] [1:1000005:0] DNS Query Detected [**] [Priority: 0] {UDP
} 10.7.61.5:53 -> 10.7.84.165:56692
10/14-15:46:21.459724  [**] [1:1000005:0] DNS Query Detected [**] [Priority: 0] {UDP
} 10.7.61.5:53 -> 10.7.84.165:51525
10/14-15:46:21.499770  [**] [1:1000005:0] DNS Query Detected [**] [Priority: 0] {UDP
} 10.7.61.5:53 -> 10.7.84.165:51742
10/14-15:46:21.499770  [**] [1:1000005:0] DNS Query Detected [**] [Priority: 0] {UDP
} 10.7.61.5:53 -> 10.7.84.165:64105
10/14-15:46:21.776666  [**] [1:1000005:0] DNS Query Detected [**] [Priority: 0] {UDP
} 10.7.114.52:137 -> 10.7.127.255:137
10/14-15:46:22.094651  [**] [1:1000005:0] DNS Query Detected [**] [Priority: 0] {UDP
} 10.7.61.5:53 -> 10.7.84.165:54409
10/14-15:46:22.094651  [**] [1:1000005:0] DNS Query Detected [**] [Priority: 0] {UDP
} 10.7.61.5:53 -> 10.7.84.165:56599
10/14-15:46:22.187597  [**] [1:1000005:0] DNS Query Detected [**] [Priority: 0] {UDP
} 10.7.94.175:137 -> 10.7.127.255:137
10/14-15:46:22.694020  [**] [1:1000005:0] DNS Query Detected [**] [Priority: 0] {UDP
} 10.7.89.188:137 -> 10.7.127.255:137
10/14-15:46:22.897903  [**] [1:1000005:0] DNS Query Detected [**] [Priority: 0] {UDP
} 10.7.104.241:57621 -> 10.7.127.255:57621
10/14-15:46:23.002413  [**] [1:1000005:0] DNS Query Detected [**] [Priority: 0] {UDP
} 10.7.112.140:137 -> 10.7.127.255:137
10/14-15:46:23.259303  [**] [1:10000001:1] ICMP traffic detected [**] [Priority: 0]
{ICMP} 142.250.182.228 -> 10.7.84.165
10/14-15:46:23.413878  [**] [1:1000005:0] DNS Query Detected [**] [Priority: 0] {UDP
} 10.7.89.188:137 -> 10.7.127.255:137
10/14-15:46:23.722226  [**] [1:1000005:0] DNS Query Detected [**] [Priority: 0] {UDP
} 10.7.112.140:137 -> 10.7.127.255:137
10/14-15:46:23.829130  [**] [1:1000005:0] DNS Query Detected [**] [Priority: 0] {UDP
} 10.7.102.217:54915 -> 10.7.127.255:54915
10/14-15:46:24.285722  [**] [1:10000001:1] ICMP traffic detected [**] [Priority: 0]
{ICMP} 142.250.182.228 -> 10.7.84.165
10/14-15:46:24.843055  [**] [1:1000005:0] DNS Query Detected [**] [Priority: 0] {UDP
} 10.7.102.217:54915 -> 10.7.127.255:54915
10/14-15:46:25.302782  [**] [1:10000001:1] ICMP traffic detected [**] [Priority: 0]
{ICMP} 142.250.182.228 -> 10.7.84.165
10/14-15:46:25.764542  [**] [1:1000005:0] DNS Query Detected [**] [Priority: 0] {UDP
} 10.7.96.171:57621 -> 10.7.127.255:57621
10/14-15:46:26.328883  [**] [1:10000001:1] ICMP traffic detected [**] [Priority: 0]
{ICMP} 142.250.182.228 -> 10.7.84.165
```



Rules:

#alert icmp any any -> $HOME_NET any (msg: "ICMP traffic detected"; sid:10000001;)

#alert udp any any -> $HOME_NET any (msg:"DNS Query Detected"; sid:1000005;)