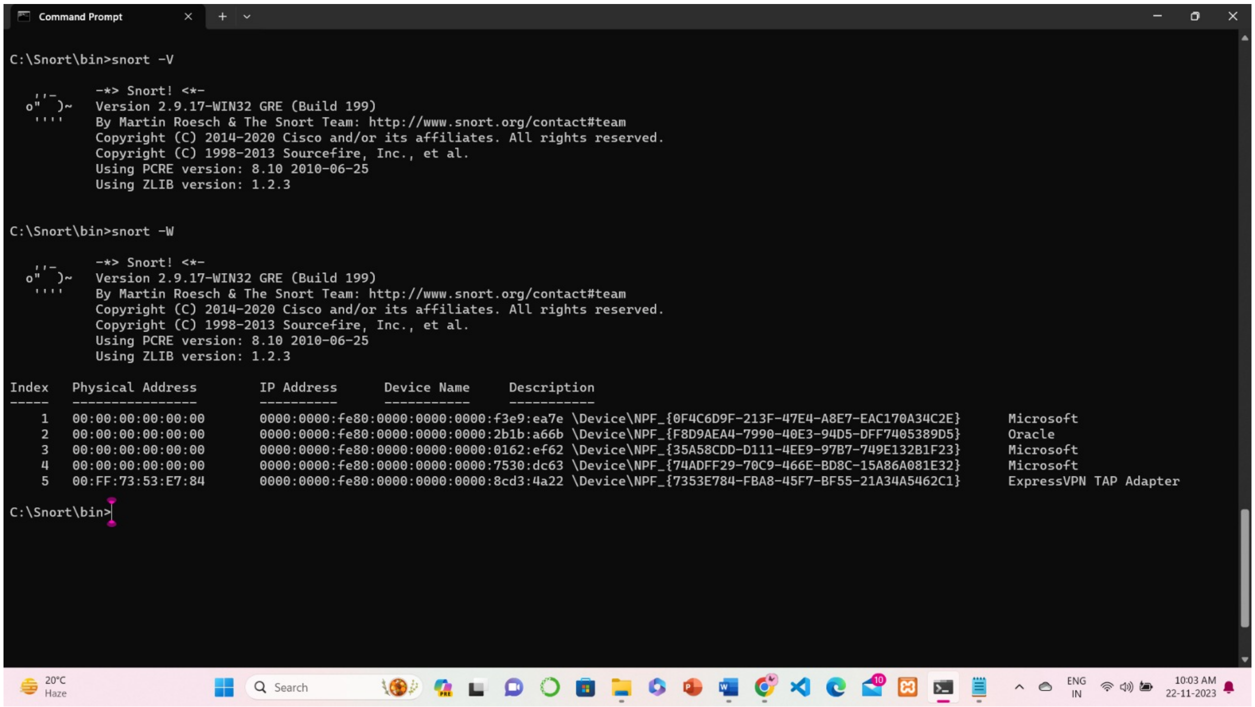
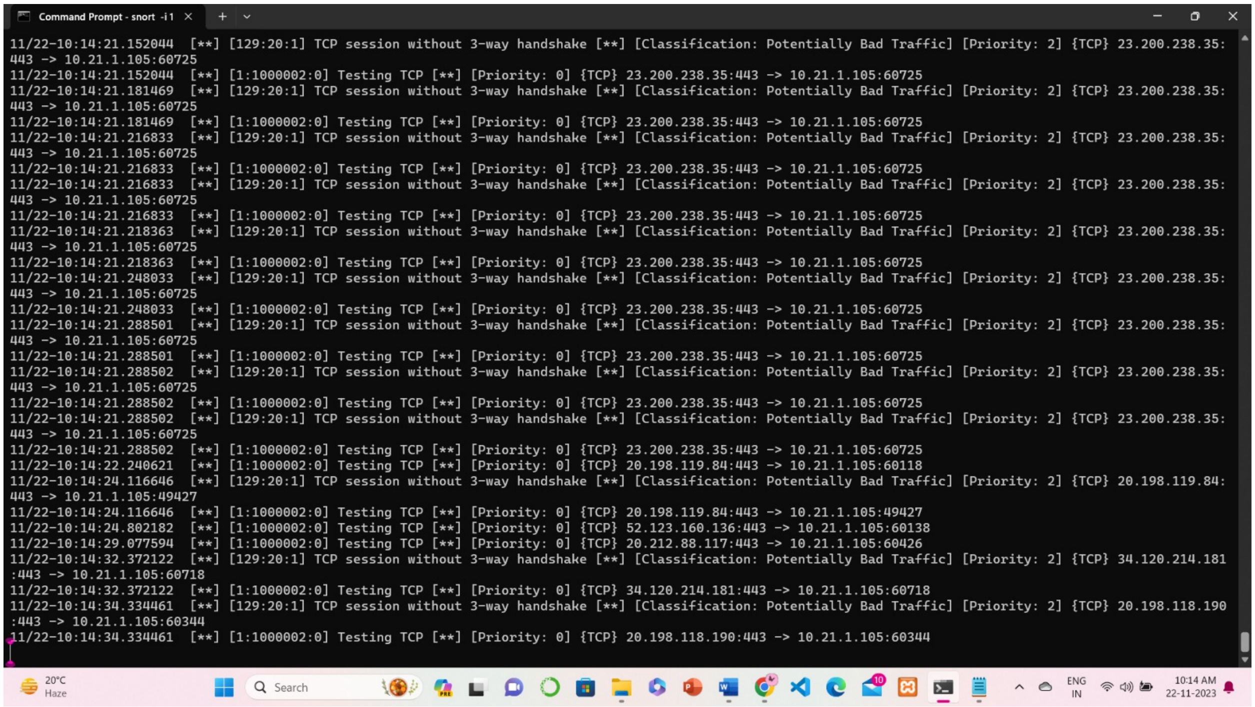
```
Microsoft Windows [Version 10.0.18362.535]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\EXAM>cd\

C:\>cd snort

C:\Snort>cd bin

C:\Snort\bin>snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15-WIN32 GRE (Build 7)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 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: 1.2.3
C:\Snort\bin>snort -W

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15-WIN32 GRE (Build 7)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 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: 1.2.3

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   24:BE:05:0F:AC:E1       0000:0000:fe80:0000:0000:0000:d882:861b
\Device\NPF_{F22D1C40-BF2A-4B59-B2BB-EB386E967426}      Intel(R) 82579LM Gigabit
Network Connection

C:\Snort\bin>snort -i 1 -c C:\Snort\etc\snort.conf -T
Running in Test mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "C:\Snort\etc\snort.conf"
```

```
Detection:
  Search-Method = AC-Full-Q
   Split Any/Any group = enabled
   Search-Method-Optimizations = enabled
   Maximum pattern length = 20
Tagged Packet Limit: 256
        IIS Unicode Map Filename: C:\Snort\etc\unicode.map
     IIS Unicode Map Codepage: 1252
     Memcap used for logging URI and Hostname: 150994944
     Max Gzip Memory: 838860
     Max Gzip Sessions: 2688
     Gzip Compress Depth: 65535
     Gzip Decompress Depth: 65535
   DEFAULT SERVER CONFIG:
     Server profile: All
     Ports (PAF): 80 81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128
3702 4343 4848 5250 6988 7000 7001 7144 7145 7510 7777 7779 8000 8008 8014 8028 8080
8085 8088 8090 8118 8123 8180 8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090
9091 9443 9999 11371 34443 34444 41080 50002 55555
    Ignore Data: No
   Ignore TLS Data: No
   Ignore SMTP Alerts: No
   Max Command Line Length: 512
   Max auth Command Line Length: 1000
   Max Specific Command Line Length:
          MaxClientBytes: 19600 (Default)
   Ports:
       22
DCE/RPC 2 Preprocessor Configuration
  Global Configuration
   DCE/RPC Defragmentation: Enabled
   Memcap: 102400 KB
   Events: co
   SMB Fingerprint policy: Disabled
  Server Default Configuration
   Policy: WinXP
   Detect ports (PAF)
     SMB: 139 445
     TCP: 135
     UDP: 135
     RPC over HTTP server: 593
     RPC over HTTP proxy: None
   Autodetect ports (PAF)
   SMB: None
   TCP: 1025-65535
   UDP: 1025-65535
   RPC over HTTP server: 1025-65535
   RPC over HTTP proxy: None
  Invalid SMB shares: C$ D$ ADMIN$
  Maximum SMB command chaining: 3 commands
  SMB file inspection: Disabled
DNS config:
  DNS Client rdata txt Overflow Alert: ACTIVE
  Obsolete DNS RR Types Alert: INACTIVE
  Experimental DNS RR Types Alert: INACTIVE
  Ports: 53
SSLPP config:
  Encrypted packets: not inspected
  Ports:
   443   465   563   636   989
   992   993   994   995  7801
  7802  7900  7901  7902  7903
  7904  7905  7906  7907  7908
  7909  7910  7911  7912  7913
  7914  7915  7916  7917  7918
  7919  7920
  Server side data is trusted
  Maximum SSL Heartbeat length: 0
Sensitive Data preprocessor config:
  Global Alert Threshold: 25
  Masked Output: DISABLED
SIP config:
  Max number of sessions: 40000
  Max number of dialogs in a session: 4 (Default)
  Status: ENABLED
  Ignore media channel: DISABLED
  Max URI length: 512
  Max Call ID length: 80
  Max Request name length: 20 (Default)
  Max From length: 256 (Default)
  Max To length: 256 (Default)
  Max Via length: 1024 (Default)
  Max Contact length: 512
  Max Content length: 2048
  Ports:
    5060  5061  5600
    Methods:
          invite cancel ack bye register options refer subscribe update join info message notify
benotify do qauth sprack publish service unsubscribe prack
IMAP Config:
    Ports: 143
    POP Config:
  Modbus config:
    Ports:
        502
DNP3 config:
    Memcap: 262144
    Check Link-Layer CRCs: ENABLED
    Ports:
        20000
Reputation config:

+-------------------[Rule Port Counts]--------------------------------------
|            tcp     udp    icmp      ip
|     src    4084      24       0       0
|     dst    7669      89       0       0
|     any     833       7       4       0
|      nc     453       0       0       0
|     s+d       3       2       0       0
+----------------------------------------------------------------------------
|
[ Port Based Pattern Matching Memory ]
+- [ Aho-Corasick Summary ] -------------------------------------
| Storage Format    : Full-Q
| Finite Automaton  : DFA
| Alphabet Size     : 256 Chars
| Sizeof State      : Variable (1,2,4 bytes)
| Instances         : 309
|     1 byte states : 293
|     2 byte states : 14
|     4 byte states : 2
| Characters        : 262242
| States            : 204489
| Transitions       : 34964857
| State Density     : 66.8%
| Patterns          : 12444
| Match States      : 13080
| Memory (MB)       : 173.38
|   Patterns        : 1.07
|   Match Lists     : 1.81
|   DFA
|     1 byte states : 1.84
|     2 byte states : 26.61
|     4 byte states : 141.74
+-------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 682 ]
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{F22D1C40-BF2A-4B59-B2BB-EB386E967426}".

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15-WIN32 GRE (Build 7)
   ""    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 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: 1.2.3

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.1  <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>

C:\Snort\bin>snort -i 1 -c C:\Snort\etc\snort.conf -A console

Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "C:\Snort\etc\snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301
2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000
8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899
9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
  Server Default Configuration
    Policy: WinXP
    Detect ports (PAF)
      SMB: 139 445
      TCP: 135
      UDP: 135
      RPC over HTTP server: 593
      RPC over HTTP proxy: None
    Autodetect ports (PAF)
      SMB: None
      TCP: 1025-65535
      UDP: 1025-65535
      RPC over HTTP server: 1025-65535
      RPC over HTTP proxy: None
    Invalid SMB shares: C$ D$ ADMIN$
    Maximum SMB command chaining: 3 commands
    SMB file inspection: Disabled
DNS config:
    DNS Client rdata txt Overflow Alert: ACTIVE
    Obsolete DNS RR Types Alert: INACTIVE
    Experimental DNS RR Types Alert: INACTIVE
    Ports: 53
SSLPP config:
    Encrypted packets: not inspected
    Ports:
      443      465      563      636      989
      992      993      994      995     7801
     7802     7900     7901     7902     7903
     7904     7905     7906     7907     7908
     7909     7910     7911     7912     7913
     7914     7915     7916     7917     7918
     7919     7920
    Server side data is trusted
    Maximum SSL Heartbeat length: 0
Sensitive Data preprocessor config:
    Global Alert Threshold: 25
    Masked Output: DISABLED
SIP config:
    Max number of sessions: 40000
    Max number of dialogs in a session: 4 (Default)
    Status: ENABLED
    Ignore media channel: DISABLED
    Max URI length: 512
    Max Call ID length: 80
    Max Request name length: 20 (Default)
    Max From length: 256 (Default)
    Max To length: 256 (Default)
```

```
   Max Via length: 1024 (Default)
   Max Contact length: 512
   Max Content length: 2048
   Ports:
      5060    5061    5600
   Methods:
        invite cancel ack bye register options refer subscribe update join info message notify
benotify do qauth sprack publish service unsubscribe prack
IMAP Config:
   Ports: 143
   IMAP Memcap: 838860
   MIME Max Mem: 838860
   Base64 Decoding: Enabled
   Base64 Decoding Depth: Unlimited
   Quoted-Printable Decoding: Enabled
   Quoted-Printable Decoding Depth: Unlimited
   Unix-to-Unix Decoding: Enabled
   Unix-to-Unix Decoding Depth: Unlimited
   Non-Encoded MIME attachment Extraction: Enabled
   Non-Encoded MIME attachment Extraction Depth: Unlimited
POP Config:
   Ports: 110
   POP Memcap: 838860
   MIME Max Mem: 838860
   Base64 Decoding: Enabled
   Base64 Decoding Depth: Unlimited
   Quoted-Printable Decoding: Enabled
   Quoted-Printable Decoding Depth: Unlimited
   Unix-to-Unix Decoding: Enabled
   Unix-to-Unix Decoding Depth: Unlimited
   Non-Encoded MIME attachment Extraction: Enabled
   Non-Encoded MIME attachment Extraction Depth: Unlimited
Modbus config:
   Ports:
      502
DNP3 config:
   Memcap: 262144
   Check Link-Layer CRCs: ENABLED
   Ports:


+++++++++++++++++++++++++++++++++++++++++++++++++++
+-------------------[Rule Port Counts]---------------------------------------
|           tcp     udp    icmp      ip
|     src    4084      24       0       0
|     dst    7669      89       0       0
|     any     834       7       5       0
|      nc     454       0       1       0
|     s+d       3       2       0       0
+----------------------------------------------------------------------------

----

| States           : 204489
| Transitions       : 34964857
| State Density     : 66.8%
| Patterns         : 12444
| Match States      : 13080
| Memory (MB)       : 173.38
|   Patterns        : 1.07
|   Match Lists     : 1.81
|   DFA
|     1 byte states : 1.84
|     2 byte states : 26.61
|     4 byte states : 141.74
+----------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 682 ]
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{F22D1C40-BF2A-4B59-B2BB-EB386E967426}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15-WIN32 GRE (Build 7)
   ""    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 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: 1.2.3

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.1  <Build 1>
```



```
C:\Snort\bin>snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.17-WIN32 GRE (Build 199)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2020 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: 1.2.3


C:\Snort\bin>snort -W

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.17-WIN32 GRE (Build 199)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2020 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: 1.2.3

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:f3e9:ea7e \Device\NPF_{0F4C6D9F-213F-47E4-A8E7-EAC170A34C2E}      Microsoft
    2   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:2b1b:a66b \Device\NPF_{F8D9AEA4-7990-40E3-94D5-DFF7405389D5}      Oracle
    3   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:0162:ef62 \Device\NPF_{35A58CDD-D111-4EE9-97B7-749E132B1F23}      Microsoft
    4   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:7530:dc63 \Device\NPF_{74ADFF29-70C9-466E-BD8C-15A86A081E32}      Microsoft
    5   00:FF:73:53:E7:84       0000:0000:fe80:0000:0000:0000:8cd3:4a22 \Device\NPF_{7353E784-FBA8-45F7-BF55-21A34A5462C1}      ExpressVPN TAP Adapter

C:\Snort\bin>
```



```
11/22-10:14:21.152044  [**] [129:20:1] TCP session without 3-way handshake [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 23.200.238.35:
443 -> 10.21.1.105:60725
11/22-10:14:21.152044  [**] [1:1000002:0] Testing TCP [**] [Priority: 0] {TCP} 23.200.238.35:443 -> 10.21.1.105:60725
11/22-10:14:21.181469  [**] [129:20:1] TCP session without 3-way handshake [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 23.200.238.35:
443 -> 10.21.1.105:60725
11/22-10:14:21.181469  [**] [1:1000002:0] Testing TCP [**] [Priority: 0] {TCP} 23.200.238.35:443 -> 10.21.1.105:60725
11/22-10:14:21.216833  [**] [129:20:1] TCP session without 3-way handshake [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 23.200.238.35:
443 -> 10.21.1.105:60725
11/22-10:14:21.216833  [**] [1:1000002:0] Testing TCP [**] [Priority: 0] {TCP} 23.200.238.35:443 -> 10.21.1.105:60725
11/22-10:14:21.216833  [**] [129:20:1] TCP session without 3-way handshake [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 23.200.238.35:
443 -> 10.21.1.105:60725
11/22-10:14:21.216833  [**] [1:1000002:0] Testing TCP [**] [Priority: 0] {TCP} 23.200.238.35:443 -> 10.21.1.105:60725
11/22-10:14:21.218363  [**] [129:20:1] TCP session without 3-way handshake [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 23.200.238.35:
443 -> 10.21.1.105:60725
11/22-10:14:21.218363  [**] [1:1000002:0] Testing TCP [**] [Priority: 0] {TCP} 23.200.238.35:443 -> 10.21.1.105:60725
11/22-10:14:21.248033  [**] [129:20:1] TCP session without 3-way handshake [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 23.200.238.35:
443 -> 10.21.1.105:60725
11/22-10:14:21.248033  [**] [1:1000002:0] Testing TCP [**] [Priority: 0] {TCP} 23.200.238.35:443 -> 10.21.1.105:60725
11/22-10:14:21.288501  [**] [129:20:1] TCP session without 3-way handshake [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 23.200.238.35:
443 -> 10.21.1.105:60725
11/22-10:14:21.288501  [**] [1:1000002:0] Testing TCP [**] [Priority: 0] {TCP} 23.200.238.35:443 -> 10.21.1.105:60725
11/22-10:14:21.288502  [**] [129:20:1] TCP session without 3-way handshake [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 23.200.238.35:
443 -> 10.21.1.105:60725
11/22-10:14:21.288502  [**] [1:1000002:0] Testing TCP [**] [Priority: 0] {TCP} 23.200.238.35:443 -> 10.21.1.105:60725
11/22-10:14:21.288502  [**] [129:20:1] TCP session without 3-way handshake [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 23.200.238.35:
443 -> 10.21.1.105:60725
11/22-10:14:21.288502  [**] [1:1000002:0] Testing TCP [**] [Priority: 0] {TCP} 23.200.238.35:443 -> 10.21.1.105:60725
11/22-10:14:22.240621  [**] [1:1000002:0] Testing TCP [**] [Priority: 0] {TCP} 20.198.119.84:443 -> 10.21.1.105:60118
11/22-10:14:24.116646  [**] [129:20:1] TCP session without 3-way handshake [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 20.198.119.84:
443 -> 10.21.1.105:49427
11/22-10:14:24.116646  [**] [1:1000002:0] Testing TCP [**] [Priority: 0] {TCP} 20.198.119.84:443 -> 10.21.1.105:49427
11/22-10:14:24.802182  [**] [1:1000002:0] Testing TCP [**] [Priority: 0] {TCP} 52.123.160.136:443 -> 10.21.1.105:60138
11/22-10:14:29.077594  [**] [1:1000002:0] Testing TCP [**] [Priority: 0] {TCP} 20.212.88.117:443 -> 10.21.1.105:60426
11/22-10:14:32.372122  [**] [129:20:1] TCP session without 3-way handshake [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 34.120.214.181
:443 -> 10.21.1.105:60718
11/22-10:14:32.372122  [**] [1:1000002:0] Testing TCP [**] [Priority: 0] {TCP} 34.120.214.181:443 -> 10.21.1.105:60718
11/22-10:14:34.334461  [**] [129:20:1] TCP session without 3-way handshake [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 20.198.118.190
:443 -> 10.21.1.105:60344
11/22-10:14:34.334461  [**] [1:1000002:0] Testing TCP [**] [Priority: 0] {TCP} 20.198.118.190:443 -> 10.21.1.105:60344
```