Project Documentation – Network Traffic Analysis (PCAP Investigation)

1. Project Overview

This documentation outlines the steps I followed during a network traffic analysis project, where I investigated a potentially malicious PCAP file. The goal was not only to detect suspicious behavior but also to extract actionable indicators of compromise (IOCs) and understand the attacker's behavior within the network environment.

Details:

- **- Project Title:** Network Traffic Analysis of Suspicious PCAP File
- **- Date of Analysis:** 2024-11-26

2. Tools & Resources Used

To perform a proper and contextual analysis, I relied on a mix of packet analysis tools and threat intelligence platforms. Each tool had a clear purpose during my investigation:

Tool / Platform	**Purpose**
Wireshark	Packet inspection, filtering, and session reconstruction
VirusTotal	Checking domain/IP reputation and malware associations
THREAT fox	Crowdsourced threat intelligence data

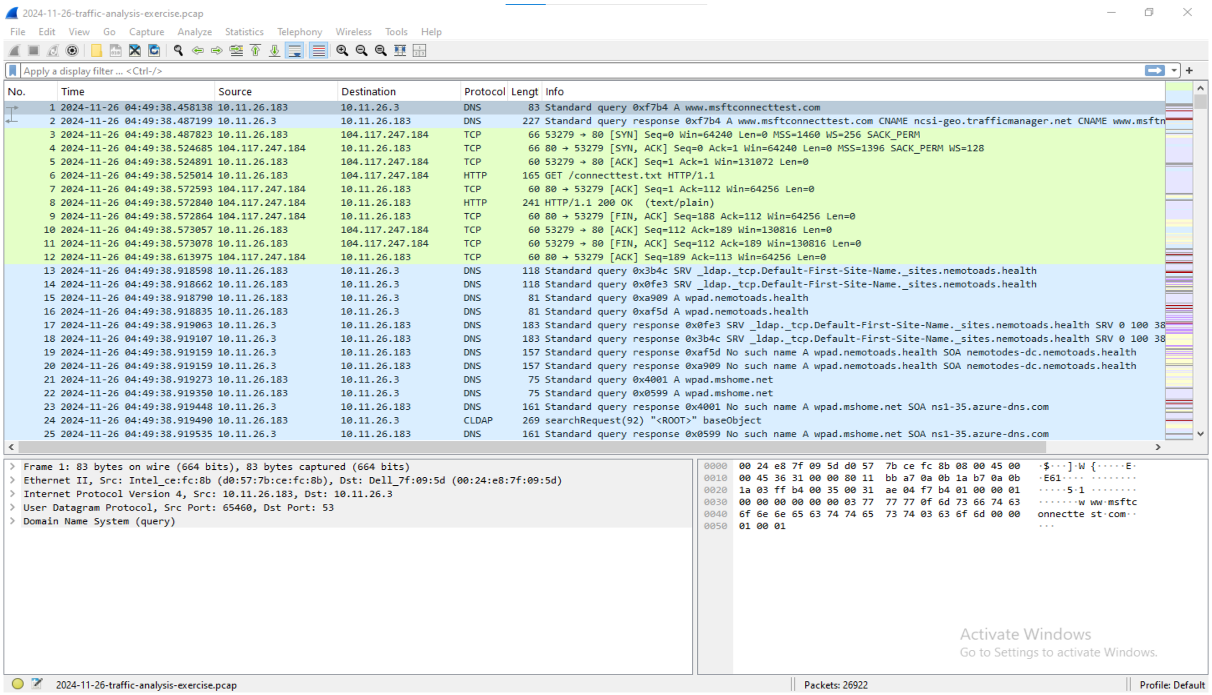
3. Step-by-Step Analysis

Here's a deep-dive walkthrough of my analysis workflow, from opening the PCAP file to extracting final IOCs:

3.1. Environment Setup

I started by opening the PCAP file in Wireshark and reviewing its metadata: the capture duration, number of packets, and time span. This initial step is crucial to get an overview of the scope.

- **Initial setup in Wireshark after loading the PCAP file for analysis**


2024-11-26-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

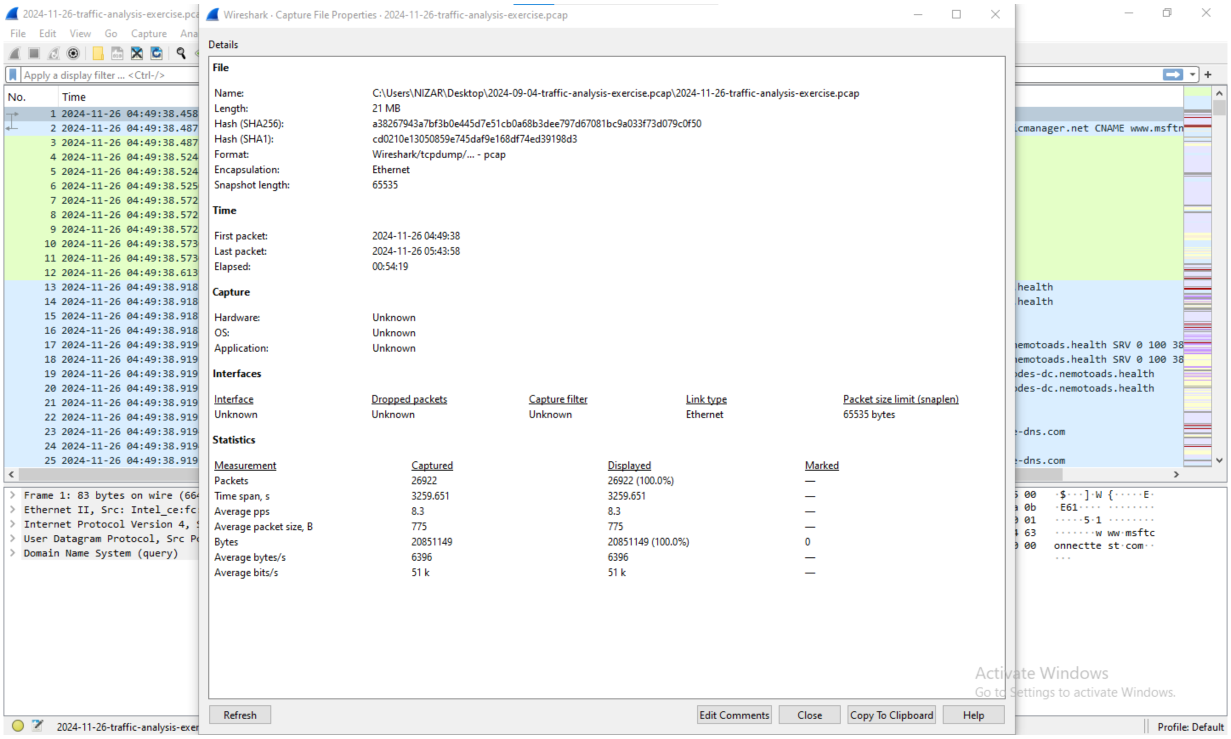
```
No.   Time                       Source          Destination     Protocol Lengt Info
    1 2024-11-26 04:49:38.458138 10.11.26.183    10.11.26.3      DNS       83 Standard query 0xf7b4 A www.msftconnecttest.com
    2 2024-11-26 04:49:38.487199 10.11.26.3      10.11.26.183    DNS      227 Standard query response 0xf7b4 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftn
    3 2024-11-26 04:49:38.487823 10.11.26.183    104.117.247.184 TCP       66 53279 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
    4 2024-11-26 04:49:38.524685 104.117.247.184 10.11.26.183    TCP       66 80 → 53279 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1396 SACK_PERM WS=128
    5 2024-11-26 04:49:38.524891 10.11.26.183    104.117.247.184 TCP       60 53279 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
    6 2024-11-26 04:49:38.525014 10.11.26.183    104.117.247.184 HTTP     165 GET /connecttest.txt HTTP/1.1
    7 2024-11-26 04:49:38.572593 104.117.247.184 10.11.26.183    TCP       60 80 → 53279 [ACK] Seq=1 Ack=112 Win=64256 Len=0
    8 2024-11-26 04:49:38.572840 104.117.247.184 10.11.26.183    HTTP     241 HTTP/1.1 200 OK  (text/plain)
    9 2024-11-26 04:49:38.572864 104.117.247.184 10.11.26.183    TCP       60 80 → 53279 [FIN, ACK] Seq=188 Ack=112 Win=64256 Len=0
   10 2024-11-26 04:49:38.573057 10.11.26.183    104.117.247.184 TCP       60 53279 → 80 [ACK] Seq=112 Ack=189 Win=130816 Len=0
   11 2024-11-26 04:49:38.573078 10.11.26.183    104.117.247.184 TCP       60 53279 → 80 [FIN, ACK] Seq=112 Ack=189 Win=130816 Len=0
   12 2024-11-26 04:49:38.613975 104.117.247.184 10.11.26.183    TCP       60 80 → 53279 [ACK] Seq=189 Ack=113 Win=64256 Len=0
   13 2024-11-26 04:49:38.918598 10.11.26.183    10.11.26.3      DNS      118 Standard query 0x3b4c SRV _ldap._tcp.Default-First-Site-Name._sites.nemotoads.health
   14 2024-11-26 04:49:38.918662 10.11.26.183    10.11.26.3      DNS      118 Standard query 0x0fe3 SRV _ldap._tcp.Default-First-Site-Name._sites.nemotoads.health
   15 2024-11-26 04:49:38.918790 10.11.26.183    10.11.26.3      DNS       81 Standard query 0xa909 A wpad.nemotoads.health
   16 2024-11-26 04:49:38.918835 10.11.26.183    10.11.26.3      DNS       81 Standard query 0xaf5d A wpad.nemotoads.health
   17 2024-11-26 04:49:38.919063 10.11.26.3      10.11.26.183    DNS      183 Standard query response 0x0fe3 SRV _ldap._tcp.Default-First-Site-Name._sites.nemotoads.health SRV 0 100 38
   18 2024-11-26 04:49:38.919107 10.11.26.3      10.11.26.183    DNS      183 Standard query response 0x3b4c SRV _ldap._tcp.Default-First-Site-Name._sites.nemotoads.health SRV 0 100 38
   19 2024-11-26 04:49:38.919159 10.11.26.3      10.11.26.183    DNS      157 Standard query response 0xaf5d No such name A wpad.nemotoads.health SOA nemotodes-dc.nemotoads.health
   20 2024-11-26 04:49:38.919159 10.11.26.3      10.11.26.183    DNS      157 Standard query response 0xa909 No such name A wpad.nemotoads.health SOA nemotodes-dc.nemotoads.health
   21 2024-11-26 04:49:38.919273 10.11.26.183    10.11.26.3      DNS       75 Standard query 0x4001 A wpad.mshome.net
   22 2024-11-26 04:49:38.919350 10.11.26.183    10.11.26.3      DNS       75 Standard query 0x0599 A wpad.mshome.net
   23 2024-11-26 04:49:38.919448 10.11.26.3      10.11.26.183    DNS      161 Standard query response 0x4001 No such name A wpad.mshome.net SOA ns1-35.azure-dns.com
   24 2024-11-26 04:49:38.919490 10.11.26.183    10.11.26.3      CLDAP    269 searchRequest(92) "<ROOT>" baseObject
   25 2024-11-26 04:49:38.919535 10.11.26.3      10.11.26.183    DNS      161 Standard query response 0x0599 No such name A wpad.mshome.net SOA ns1-35.azure-dns.com
```

```
> Frame 1: 83 bytes on wire (664 bits), 83 bytes captured (664 bits)
> Ethernet II, Src: Intel_ce:fc:8b (d0:57:7b:ce:fc:8b), Dst: Dell_7f:09:5d (00:24:e8:7f:09:5d)
> Internet Protocol Version 4, Src: 10.11.26.183, Dst: 10.11.26.3
> User Datagram Protocol, Src Port: 65460, Dst Port: 53
> Domain Name System (query)
```

```
0000  00 24 e8 7f 09 5d d0 57  7b ce fc 8b 08 00 45 00   ·$···]·W {·····E·
0010  00 45 36 31 00 00 80 11  bb a7 0a 0b 1a b7 0a 0b   ·E61···· ········
0020  1a 03 ff b4 00 35 00 31  ae 04 f7 b4 01 00 00 01   ·····5·1 ········
0030  00 00 00 00 00 00 03 77  77 77 0f 6d 73 66 74 63   ·······w ww·msftc
0040  6f 6e 6e 65 63 74 74 65  73 74 03 63 6f 6d 00 00   onnectte st·com··
0050  01 00 01                                           ···
```

2024-11-26-traffic-analysis-exercise.pcap | Packets: 26922 | Profile: Default

- **Capture summary showing metadata including duration, packet count, and file size**


Wireshark · Capture File Properties · 2024-11-26-traffic-analysis-exercise.pcap
Details

File

Name: C:\Users\NIZAR\Desktop\2024-09-04-traffic-analysis-exercise.pcap\2024-11-26-traffic-analysis-exercise.pcap
Length: 21 MB
Hash (SHA256): a38267943a7bf3b0e445d7e51cb0a68b3dee797d67081bc9a033f73d079c0f50
Hash (SHA1): cd0210e13050859e745daf9e168df74ed39198d3
Format: Wireshark/tcpdump/... - pcap
Encapsulation: Ethernet
Snapshot length: 65535

Time

First packet: 2024-11-26 04:49:38
Last packet: 2024-11-26 05:43:58
Elapsed: 00:54:19

Capture

Hardware: Unknown
OS: Unknown
Application: Unknown

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Unknown	Unknown	Unknown	Ethernet	65535 bytes

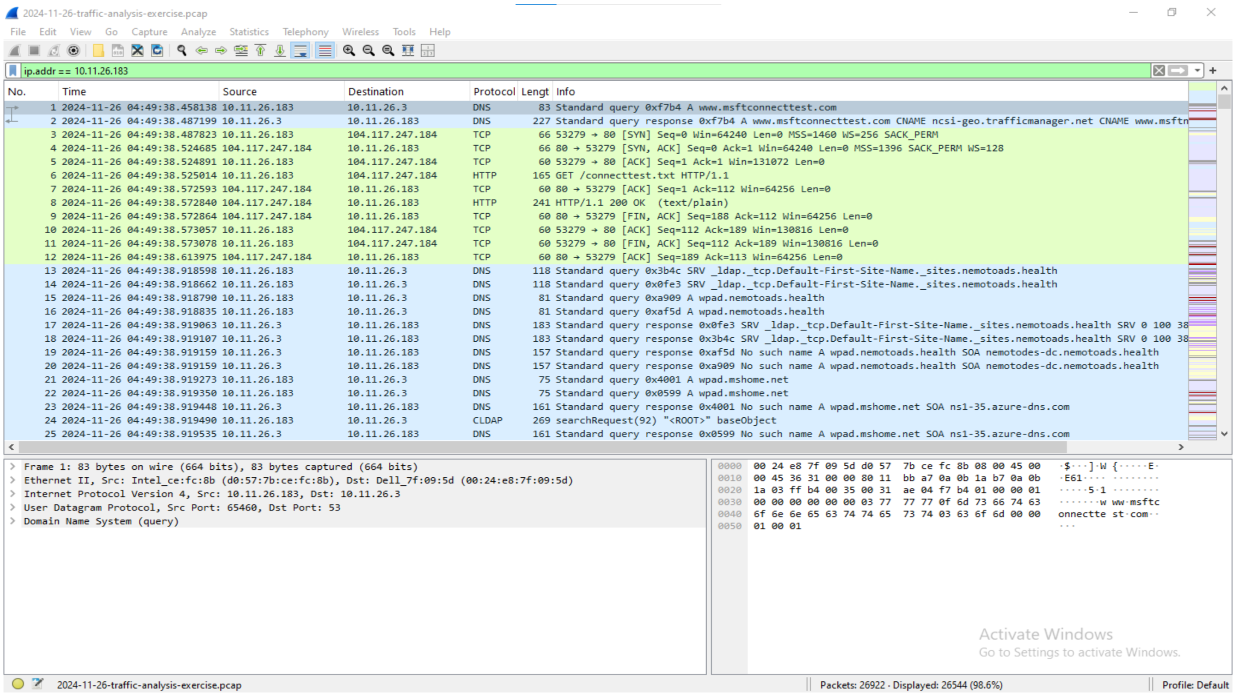
Statistics

Measurement	Captured	Displayed	Marked
Packets	26922	26922 (100.0%)	—
Time span, s	3259.651	3259.651	—
Average pps	8.3	8.3	—
Average packet size, B	775	775	—
Bytes	20851149	20851149 (100.0%)	0
Average bytes/s	6396	6396	—
Average bits/s	51 k	51 k	—

3.2. Traffic Filtering

Using display filters, I narrowed down the traffic to the host of interest: 10.11.26.183. Filters like `dns`, `http.request`, `tls.handshake`, and `ip.addr == 10.11.26.183` allowed me to isolate relevant sessions and discard noise from unrelated flows.

- **Filtered traffic showing only communications involving the internal host 10.11.26.183**



ip.addr == 10.11.26.183

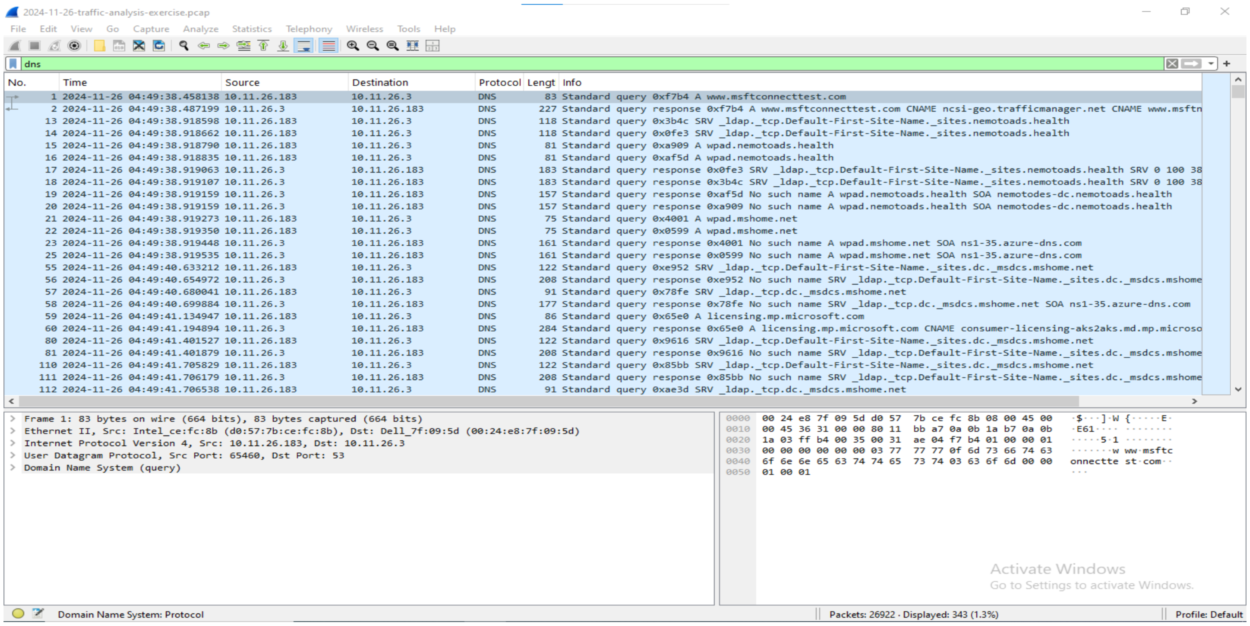
```
No.   Time                       Source          Destination     Protocol Lengt Info
    1 2024-11-26 04:49:38.458138 10.11.26.183    10.11.26.3      DNS       83 Standard query 0xf7b4 A www.msftconnecttest.com
    2 2024-11-26 04:49:38.487199 10.11.26.3      10.11.26.183    DNS      227 Standard query response 0xf7b4 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftn
    3 2024-11-26 04:49:38.487823 10.11.26.183    104.117.247.184 TCP       66 53279 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
    4 2024-11-26 04:49:38.524685 104.117.247.184 10.11.26.183    TCP       66 80 → 53279 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1396 SACK_PERM WS=128
    5 2024-11-26 04:49:38.524891 10.11.26.183    104.117.247.184 TCP       60 53279 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
    6 2024-11-26 04:49:38.525014 10.11.26.183    104.117.247.184 HTTP     165 GET /connecttest.txt HTTP/1.1
    7 2024-11-26 04:49:38.572593 104.117.247.184 10.11.26.183    TCP       60 80 → 53279 [ACK] Seq=1 Ack=112 Win=64256 Len=0
    8 2024-11-26 04:49:38.572840 104.117.247.184 10.11.26.183    HTTP     241 HTTP/1.1 200 OK  (text/plain)
    9 2024-11-26 04:49:38.572864 104.117.247.184 10.11.26.183    TCP       60 80 → 53279 [FIN, ACK] Seq=188 Ack=112 Win=64256 Len=0
   10 2024-11-26 04:49:38.573057 10.11.26.183    104.117.247.184 TCP       60 53279 → 80 [ACK] Seq=112 Ack=189 Win=130816 Len=0
   11 2024-11-26 04:49:38.573078 10.11.26.183    104.117.247.184 TCP       60 53279 → 80 [FIN, ACK] Seq=112 Ack=189 Win=130816 Len=0
   12 2024-11-26 04:49:38.613975 104.117.247.184 10.11.26.183    TCP       60 80 → 53279 [ACK] Seq=189 Ack=113 Win=64256 Len=0
   13 2024-11-26 04:49:38.918598 10.11.26.183    10.11.26.3      DNS      118 Standard query 0x3b4c SRV _ldap._tcp.Default-First-Site-Name._sites.nemotoads.health
   14 2024-11-26 04:49:38.918662 10.11.26.183    10.11.26.3      DNS      118 Standard query 0x0fe3 SRV _ldap._tcp.Default-First-Site-Name._sites.nemotoads.health
   15 2024-11-26 04:49:38.918790 10.11.26.183    10.11.26.3      DNS       81 Standard query 0xa909 A wpad.nemotoads.health
   16 2024-11-26 04:49:38.918835 10.11.26.183    10.11.26.3      DNS       81 Standard query 0xaf5d A wpad.nemotoads.health
   17 2024-11-26 04:49:38.919063 10.11.26.3      10.11.26.183    DNS      183 Standard query response 0x0fe3 SRV _ldap._tcp.Default-First-Site-Name._sites.nemotoads.health SRV 0 100 38
   18 2024-11-26 04:49:38.919107 10.11.26.3      10.11.26.183    DNS      183 Standard query response 0x3b4c SRV _ldap._tcp.Default-First-Site-Name._sites.nemotoads.health SRV 0 100 38
   19 2024-11-26 04:49:38.919159 10.11.26.3      10.11.26.183    DNS      157 Standard query response 0xaf5d No such name A wpad.nemotoads.health SOA nemotodes-dc.nemotoads.health
   20 2024-11-26 04:49:38.919159 10.11.26.3      10.11.26.183    DNS      157 Standard query response 0xa909 No such name A wpad.nemotoads.health SOA nemotodes-dc.nemotoads.health
   21 2024-11-26 04:49:38.919273 10.11.26.183    10.11.26.3      DNS       75 Standard query 0x4001 A wpad.mshome.net
   22 2024-11-26 04:49:38.919350 10.11.26.183    10.11.26.3      DNS       75 Standard query 0x0599 A wpad.mshome.net
   23 2024-11-26 04:49:38.919448 10.11.26.3      10.11.26.183    DNS      161 Standard query response 0x4001 No such name A wpad.mshome.net SOA ns1-35.azure-dns.com
   24 2024-11-26 04:49:38.919490 10.11.26.183    10.11.26.3      CLDAP    269 searchRequest(92) "<ROOT>" baseObject
   25 2024-11-26 04:49:38.919535 10.11.26.3      10.11.26.183    DNS      161 Standard query response 0x0599 No such name A wpad.mshome.net SOA ns1-35.azure-dns.com
```

```
> Frame 1: 83 bytes on wire (664 bits), 83 bytes captured (664 bits)
> Ethernet II, Src: Intel_ce:fc:8b (d0:57:7b:ce:fc:8b), Dst: Dell_7f:09:5d (00:24:e8:7f:09:5d)
> Internet Protocol Version 4, Src: 10.11.26.183, Dst: 10.11.26.3
> User Datagram Protocol, Src Port: 65460, Dst Port: 53
> Domain Name System (query)
```

```
0000  00 24 e8 7f 09 5d d0 57  7b ce fc 8b 08 00 45 00   ·$···]·W {·····E·
0010  00 45 36 31 00 00 80 11  bb a7 0a 0b 1a b7 0a 0b   ·E61···· ········
0020  1a 03 ff b4 00 35 00 31  ae 04 f7 b4 01 00 00 01   ·····5·1 ········
0030  00 00 00 00 00 00 03 77  77 77 0f 6d 73 66 74 63   ·······w ww·msftc
0040  6f 6e 6e 65 63 74 74 65  73 74 03 63 6f 6d 00 00   onnectte st·com··
0050  01 00 01                                           ···
```

2024-11-26-traffic-analysis-exercise.pcap | Packets: 26922 · Displayed: 26544 (98.6%) | Profile: Default

- **Protocol-level filters used to isolate DNS, HTTP, and TLS communications for deeper inspection**



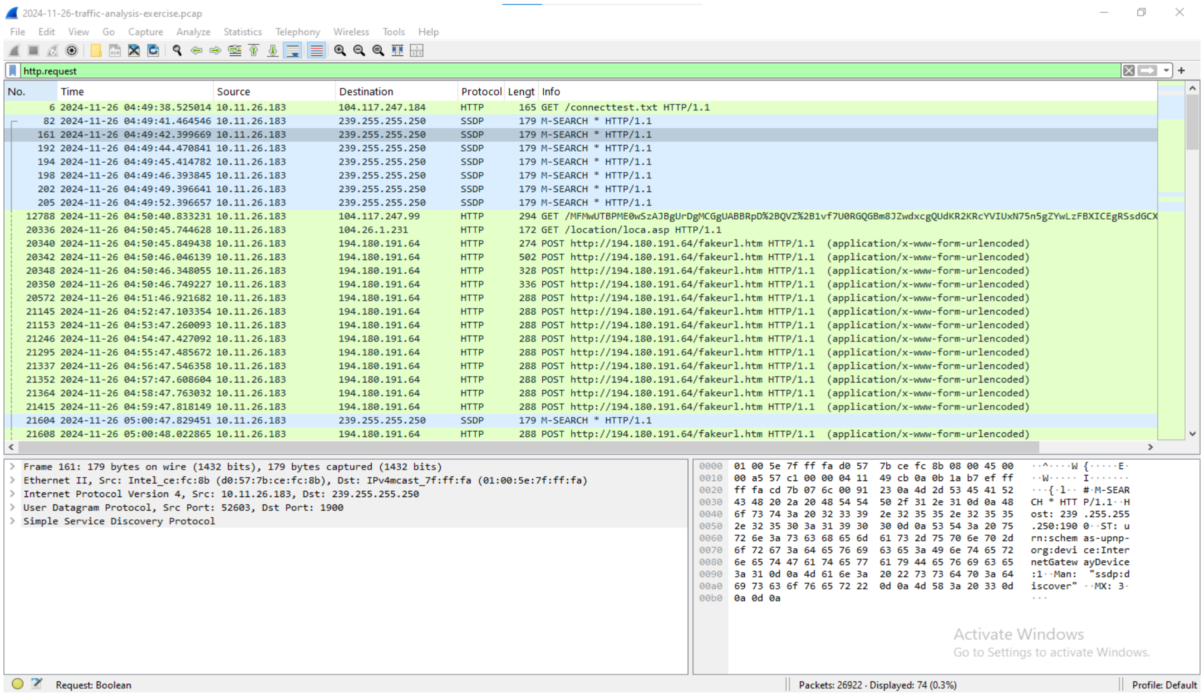
dns

```
No.   Time                       Source          Destination     Protocol Lengt Info
    1 2024-11-26 04:49:38.458138 10.11.26.183    10.11.26.3      DNS       83 Standard query 0xf7b4 A www.msftconnecttest.com
    2 2024-11-26 04:49:38.487199 10.11.26.3      10.11.26.183    DNS      227 Standard query response 0xf7b4 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftn
   13 2024-11-26 04:49:38.918598 10.11.26.183    10.11.26.3      DNS      118 Standard query 0x3b4c SRV _ldap._tcp.Default-First-Site-Name._sites.nemotoads.health
   14 2024-11-26 04:49:38.918662 10.11.26.183    10.11.26.3      DNS      118 Standard query 0x0fe3 SRV _ldap._tcp.Default-First-Site-Name._sites.nemotoads.health
   15 2024-11-26 04:49:38.918790 10.11.26.183    10.11.26.3      DNS       81 Standard query 0xa909 A wpad.nemotoads.health
   16 2024-11-26 04:49:38.918835 10.11.26.183    10.11.26.3      DNS       81 Standard query 0xaf5d A wpad.nemotoads.health
   17 2024-11-26 04:49:38.919063 10.11.26.3      10.11.26.183    DNS      183 Standard query response 0x0fe3 SRV _ldap._tcp.Default-First-Site-Name._sites.nemotoads.health SRV 0 100 38
   18 2024-11-26 04:49:38.919107 10.11.26.3      10.11.26.183    DNS      183 Standard query response 0x3b4c SRV _ldap._tcp.Default-First-Site-Name._sites.nemotoads.health SRV 0 100 38
   19 2024-11-26 04:49:38.919159 10.11.26.3      10.11.26.183    DNS      157 Standard query response 0xaf5d No such name A wpad.nemotoads.health SOA nemotodes-dc.nemotoads.health
   20 2024-11-26 04:49:38.919159 10.11.26.3      10.11.26.183    DNS      157 Standard query response 0xa909 No such name A wpad.nemotoads.health SOA nemotodes-dc.nemotoads.health
   21 2024-11-26 04:49:38.919273 10.11.26.183    10.11.26.3      DNS       75 Standard query 0x4001 A wpad.mshome.net
   22 2024-11-26 04:49:38.919350 10.11.26.183    10.11.26.3      DNS       75 Standard query 0x0599 A wpad.mshome.net
   23 2024-11-26 04:49:38.919448 10.11.26.3      10.11.26.183    DNS      161 Standard query response 0x4001 No such name A wpad.mshome.net SOA ns1-35.azure-dns.com
   25 2024-11-26 04:49:38.919535 10.11.26.3      10.11.26.183    DNS      161 Standard query response 0x0599 No such name A wpad.mshome.net SOA ns1-35.azure-dns.com
   55 2024-11-26 04:49:40.633212 10.11.26.183    10.11.26.3      DNS      122 Standard query 0xe952 SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.mshome.net
   56 2024-11-26 04:49:40.654972 10.11.26.3      10.11.26.183    DNS      208 Standard query response 0xe952 No such name SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.mshome
   57 2024-11-26 04:49:40.680041 10.11.26.183    10.11.26.3      DNS       91 Standard query 0x78fe SRV _ldap._tcp.dc._msdcs.mshome.net
   58 2024-11-26 04:49:40.699884 10.11.26.3      10.11.26.183    DNS      177 Standard query response 0x78fe No such name SRV _ldap._tcp.dc._msdcs.mshome.net SOA ns1-35.azure-dns.com
   59 2024-11-26 04:49:41.134947 10.11.26.183    10.11.26.3      DNS       86 Standard query 0x65e0 A licensing.mp.microsoft.com
   60 2024-11-26 04:49:41.194894 10.11.26.3      10.11.26.183    DNS      284 Standard query response 0x65e0 A licensing.mp.microsoft.com CNAME consumer-licensing-aks2aks.md.mp.microso
   80 2024-11-26 04:49:41.401527 10.11.26.183    10.11.26.3      DNS      122 Standard query 0x9616 SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.mshome.net
   81 2024-11-26 04:49:41.401879 10.11.26.3      10.11.26.183    DNS      208 Standard query response 0x9616 No such name SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.mshome
  110 2024-11-26 04:49:41.705829 10.11.26.183    10.11.26.3      DNS      122 Standard query 0x85bb SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.mshome.net
  111 2024-11-26 04:49:41.706179 10.11.26.3      10.11.26.183    DNS      208 Standard query response 0x85bb No such name SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.mshome
  112 2024-11-26 04:49:41.706538 10.11.26.183    10.11.26.3      DNS       91 Standard query 0xae3d SRV _ldap._tcp.dc._msdcs.mshome.net
```

```
> Frame 1: 83 bytes on wire (664 bits), 83 bytes captured (664 bits)
> Ethernet II, Src: Intel_ce:fc:8b (d0:57:7b:ce:fc:8b), Dst: Dell_7f:09:5d (00:24:e8:7f:09:5d)
> Internet Protocol Version 4, Src: 10.11.26.183, Dst: 10.11.26.3
> User Datagram Protocol, Src Port: 65460, Dst Port: 53
> Domain Name System (query)
```

```
0000  00 24 e8 7f 09 5d d0 57  7b ce fc 8b 08 00 45 00   ·$···]·W {·····E·
0010  00 45 36 31 00 00 80 11  bb a7 0a 0b 1a b7 0a 0b   ·E61···· ········
0020  1a 03 ff b4 00 35 00 31  ae 04 f7 b4 01 00 00 01   ·····5·1 ········
0030  00 00 00 00 00 00 03 77  77 77 0f 6d 73 66 74 63   ·······w ww·msftc
0040  6f 6e 6e 65 63 74 74 65  73 74 03 63 6f 6d 00 00   onnectte st·com··
0050  01 00 01                                           ···
```

Domain Name System: Protocol | Packets: 26922 · Displayed: 343 (1.3%) | Profile: Default



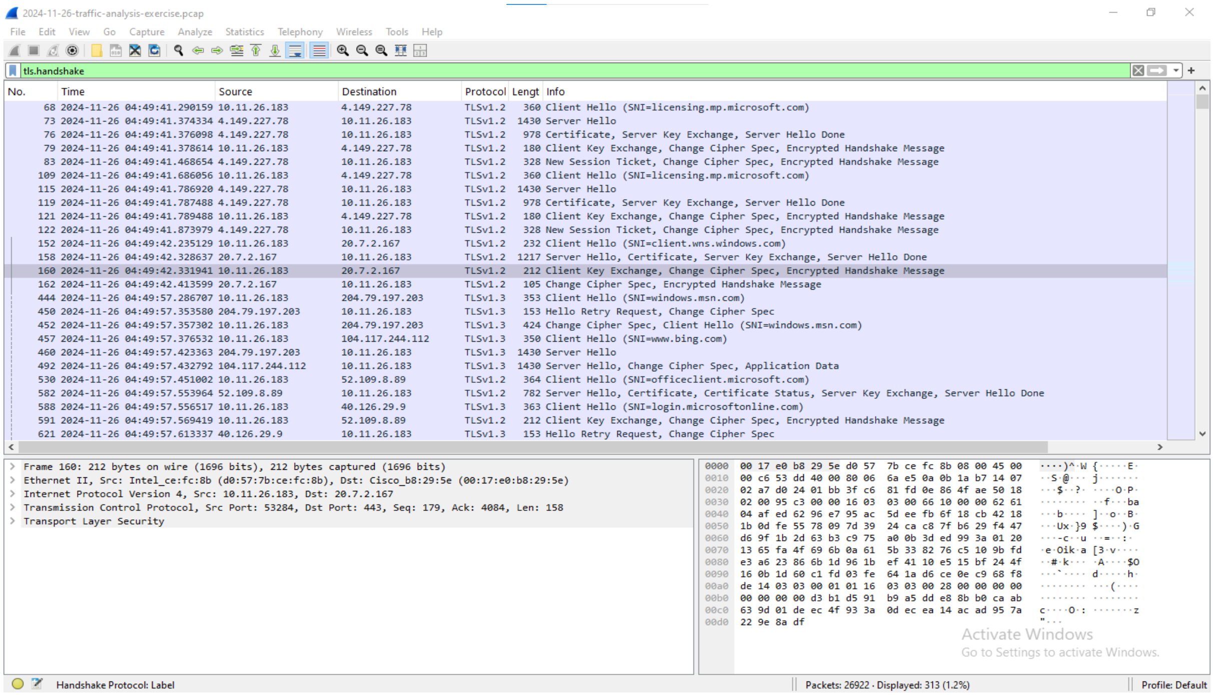
```
http.request
```

```
No.   Time                       Source        Destination      Protocol Lengt Info
    6 2024-11-26 04:49:38.525014 10.11.26.183  104.117.247.184  HTTP      165 GET /connecttest.txt HTTP/1.1
   82 2024-11-26 04:49:41.464546 10.11.26.183  239.255.255.250  SSDP      179 M-SEARCH * HTTP/1.1
  161 2024-11-26 04:49:42.399669 10.11.26.183  239.255.255.250  SSDP      179 M-SEARCH * HTTP/1.1
  192 2024-11-26 04:49:44.470841 10.11.26.183  239.255.255.250  SSDP      179 M-SEARCH * HTTP/1.1
  194 2024-11-26 04:49:45.414782 10.11.26.183  239.255.255.250  SSDP      179 M-SEARCH * HTTP/1.1
  198 2024-11-26 04:49:46.393845 10.11.26.183  239.255.255.250  SSDP      179 M-SEARCH * HTTP/1.1
  202 2024-11-26 04:49:49.396641 10.11.26.183  239.255.255.250  SSDP      179 M-SEARCH * HTTP/1.1
  205 2024-11-26 04:49:52.396657 10.11.26.183  239.255.255.250  SSDP      179 M-SEARCH * HTTP/1.1
12788 2024-11-26 04:50:40.833231 10.11.26.183  104.117.247.99   HTTP      294 GET /MFMwUTBPME0wSzAJBgUrDgMCGgUABBRpD%2BQVZ%2B1vf7U0RGQGBm8JZwdxcgQUdKR2KRcYVIUxN75n5gZYwLzFBXICEgRSsdGCX
20336 2024-11-26 04:50:45.744628 10.11.26.183  104.26.1.231     HTTP      172 GET /location/loca.asp HTTP/1.1
20340 2024-11-26 04:50:45.849438 10.11.26.183  194.180.191.64   HTTP      274 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
20342 2024-11-26 04:50:46.046139 10.11.26.183  194.180.191.64   HTTP      502 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
20348 2024-11-26 04:50:46.348055 10.11.26.183  194.180.191.64   HTTP      328 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
20350 2024-11-26 04:50:46.749227 10.11.26.183  194.180.191.64   HTTP      336 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
20572 2024-11-26 04:51:46.921682 10.11.26.183  194.180.191.64   HTTP      288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
21145 2024-11-26 04:52:47.103354 10.11.26.183  194.180.191.64   HTTP      288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
21153 2024-11-26 04:53:47.260093 10.11.26.183  194.180.191.64   HTTP      288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
21246 2024-11-26 04:54:47.427092 10.11.26.183  194.180.191.64   HTTP      288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
21295 2024-11-26 04:55:47.485672 10.11.26.183  194.180.191.64   HTTP      288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
21337 2024-11-26 04:56:47.546358 10.11.26.183  194.180.191.64   HTTP      288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
21352 2024-11-26 04:57:47.608604 10.11.26.183  194.180.191.64   HTTP      288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
21364 2024-11-26 04:58:47.763032 10.11.26.183  194.180.191.64   HTTP      288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
21415 2024-11-26 04:59:47.818149 10.11.26.183  194.180.191.64   HTTP      288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
21604 2024-11-26 05:00:47.829451 10.11.26.183  239.255.255.250  SSDP      179 M-SEARCH * HTTP/1.1
21608 2024-11-26 05:00:48.022865 10.11.26.183  194.180.191.64   HTTP      288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
```

```
> Frame 161: 179 bytes on wire (1432 bits), 179 bytes captured (1432 bits)
> Ethernet II, Src: Intel_ce:fc:8b (d0:57:7b:ce:fc:8b), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 10.11.26.183, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 52603, Dst Port: 1900
> Simple Service Discovery Protocol
```

```
0000  01 00 5e 7f ff fa d0 57  7b ce fc 8b 08 00 45 00   ··^····W {·····E·
0010  00 a5 57 c1 00 00 04 11  49 cb 0a 0b 1a b7 ef ff   ··W····· I·······
0020  ff fa cd 7b 07 6c 00 91  23 0a 4d 2d 53 45 41 52   ···{·l·· #·M-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1··H
0040  6f 73 74 3a 20 32 33 39  2e 32 35 35 2e 32 35 35   ost: 239 .255.255
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 53 54 3a 20 75   .250:190 0··ST: u
0060  72 6e 3a 73 63 68 65 6d  61 73 2d 75 70 6e 70 2d   rn:schem as-upnp-
0070  6f 72 67 3a 64 65 76 69  63 65 3a 49 6e 74 65 72   org:devi ce:Inter
0080  6e 65 74 47 61 74 65 77  61 79 44 65 76 69 63 65   netGatew ayDevice
0090  3a 31 0d 0a 4d 61 6e 3a  20 22 73 73 64 70 3a 64   :1··Man:  "ssdp:d
00a0  69 73 63 6f 76 65 72 22  0d 0a 4d 58 3a 20 33 0d   iscover" ··MX: 3·
00b0  0a 0d 0a                                           ···
```

```
Request: Boolean          Packets: 26922 · Displayed: 74 (0.3%)          Profile: Default
```



```
tls.handshake
```

```
No.   Time                       Source          Destination      Protocol Lengt Info
   68 2024-11-26 04:49:41.290159 10.11.26.183    4.149.227.78     TLSv1.2   360 Client Hello (SNI=licensing.mp.microsoft.com)
   73 2024-11-26 04:49:41.374334 4.149.227.78    10.11.26.183     TLSv1.2  1430 Server Hello
   76 2024-11-26 04:49:41.376098 4.149.227.78    10.11.26.183     TLSv1.2   978 Certificate, Server Key Exchange, Server Hello Done
   79 2024-11-26 04:49:41.378614 10.11.26.183    4.149.227.78     TLSv1.2   180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   83 2024-11-26 04:49:41.468654 4.149.227.78    10.11.26.183     TLSv1.2   328 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
  109 2024-11-26 04:49:41.686056 10.11.26.183    4.149.227.78     TLSv1.2   360 Client Hello (SNI=licensing.mp.microsoft.com)
  115 2024-11-26 04:49:41.786920 4.149.227.78    10.11.26.183     TLSv1.2  1430 Server Hello
  119 2024-11-26 04:49:41.787488 4.149.227.78    10.11.26.183     TLSv1.2   978 Certificate, Server Key Exchange, Server Hello Done
  121 2024-11-26 04:49:41.789488 10.11.26.183    4.149.227.78     TLSv1.2   180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  122 2024-11-26 04:49:41.873979 4.149.227.78    10.11.26.183     TLSv1.2   328 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
  152 2024-11-26 04:49:42.235129 10.11.26.183    20.7.2.167       TLSv1.2   232 Client Hello (SNI=client.wns.windows.com)
  158 2024-11-26 04:49:42.328637 20.7.2.167      10.11.26.183     TLSv1.2  1217 Server Hello, Certificate, Server Key Exchange, Server Hello Done
  160 2024-11-26 04:49:42.331941 10.11.26.183    20.7.2.167       TLSv1.2   212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  162 2024-11-26 04:49:42.413599 20.7.2.167      10.11.26.183     TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
  444 2024-11-26 04:49:57.286707 10.11.26.183    204.79.197.203   TLSv1.3   353 Client Hello (SNI=windows.msn.com)
  450 2024-11-26 04:49:57.353580 204.79.197.203  10.11.26.183     TLSv1.3   153 Hello Retry Request, Change Cipher Spec
  452 2024-11-26 04:49:57.357302 10.11.26.183    204.79.197.203   TLSv1.3   424 Change Cipher Spec, Client Hello (SNI=windows.msn.com)
  457 2024-11-26 04:49:57.376532 10.11.26.183    104.117.244.112  TLSv1.3   350 Client Hello (SNI=www.bing.com)
  460 2024-11-26 04:49:57.423363 204.79.197.203  10.11.26.183     TLSv1.3  1430 Server Hello
  492 2024-11-26 04:49:57.432792 104.117.244.112 10.11.26.183     TLSv1.3  1430 Server Hello, Change Cipher Spec, Application Data
  530 2024-11-26 04:49:57.451002 10.11.26.183    52.109.8.89      TLSv1.2   364 Client Hello (SNI=officeclient.microsoft.com)
  582 2024-11-26 04:49:57.553964 52.109.8.89     10.11.26.183     TLSv1.2   782 Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
  588 2024-11-26 04:49:57.556517 10.11.26.183    40.126.29.9      TLSv1.3   363 Client Hello (SNI=login.microsoftonline.com)
  591 2024-11-26 04:49:57.569419 10.11.26.183    52.109.8.89      TLSv1.2   212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  621 2024-11-26 04:49:57.613337 40.126.29.9     10.11.26.183     TLSv1.3   153 Hello Retry Request, Change Cipher Spec
```

```
> Frame 160: 212 bytes on wire (1696 bits), 212 bytes captured (1696 bits)
> Ethernet II, Src: Intel_ce:fc:8b (d0:57:7b:ce:fc:8b), Dst: Cisco_b8:29:5e (00:17:e0:b8:29:5e)
> Internet Protocol Version 4, Src: 10.11.26.183, Dst: 20.7.2.167
> Transmission Control Protocol, Src Port: 53284, Dst Port: 443, Seq: 179, Ack: 4084, Len: 158
> Transport Layer Security
```

```
0000  00 17 e0 b8 29 5e d0 57  7b ce fc 8b 08 00 45 00   ····)^·W {·····E·
0010  00 c6 53 dd 40 00 80 06  6a e5 0a 0b 1a b7 14 07   ··S·@··· j·······
0020  02 a7 d0 24 01 bb 3f c6  81 fd 0e 86 4f ae 50 18   ···$··?· ····O·P·
0030  02 00 95 c3 00 00 16 03  03 00 66 10 00 00 62 61   ········ ··f···ba
0040  04 af ed 62 96 e7 95 ac  5d ee fb 6f 18 cb 42 18   ···b···· ]··o··B·
0050  1b 0d fe 55 78 09 7d 39  24 ca c8 7f b6 29 f4 47   ···Ux·}9 $····)·G
0060  d6 9f 1b 2d 63 b3 c9 75  a0 0b 3d ed 99 3a 01 20   ···-c··u ··=··:· 
0070  13 65 fa 4f 69 6b 0a 61  5b 33 82 76 c5 10 9b fd   ·e·Oik·a [3·v····
0080  e3 a6 23 86 6b 1d 96 1b  ef 41 10 e5 15 bf 24 4f   ··#·k··· ·A····$O
0090  16 0b 1d 60 c1 fd 03 fe  64 1a d6 ce 0e c9 68 f8   ···`···· d·····h·
00a0  de 14 03 03 00 01 01 16  03 03 00 28 00 00 00 00   ········ ···(····
00b0  00 00 00 00 d3 b1 d5 91  b9 a5 dd e8 8b b0 ca ab   ········ ········
00c0  63 9d 01 de ec 4f 93 3a  0d ec ea 14 ac ad 95 7a   c····O·: ·······z
00d0  22 9e 8a df                                        "···
```

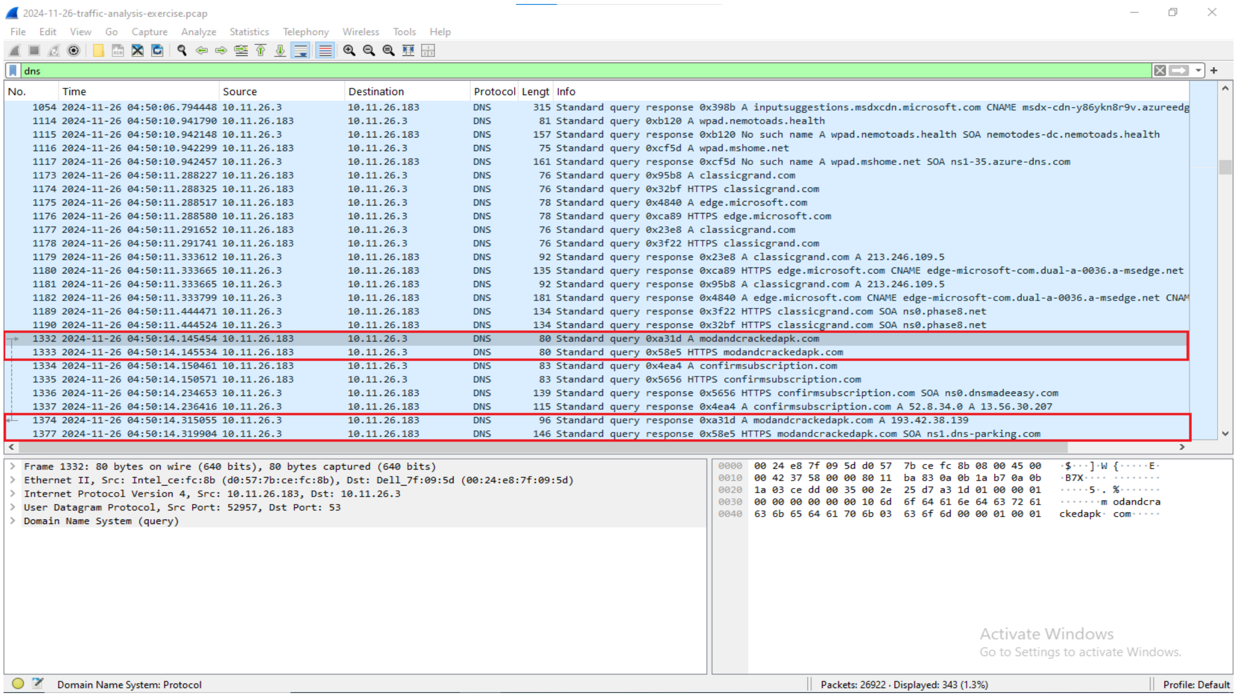
```
Handshake Protocol: Label          Packets: 26922 · Displayed: 313 (1.2%)          Profile: Default
```

3.3. Domain & DNS Analysis

I examined all domain queries made by the internal host. One domain stood out: `modandcrackedapk.com`, which hinted at potentially pirated or malicious content.

A lookup on VirusTotal revealed that the domain had a high threat score.

- **DNS query observed for suspicious domain modandcrackedapk.com**



2024-11-26-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

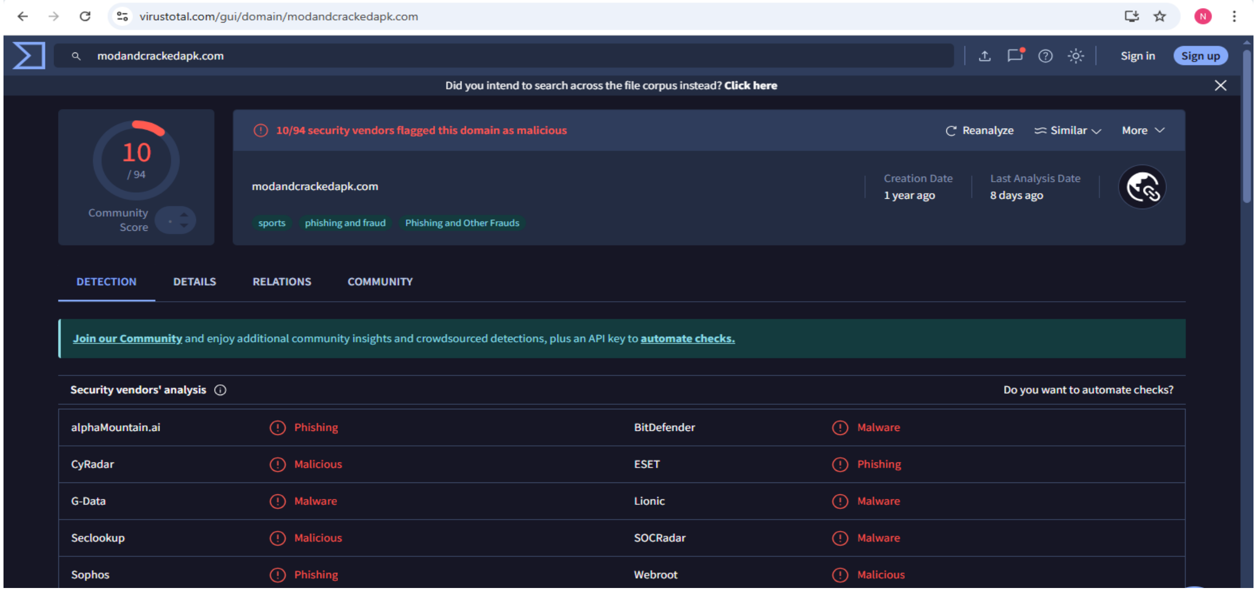
```
No.   Time                       Source        Destination   Protocol Lengt Info
 1054 2024-11-26 04:50:06.794448 10.11.26.3    10.11.26.183  DNS   315 Standard query response 0x398b A inputsuggestions.msdxcdn.microsoft.com CNAME msdx-cdn-y86ykn8r9v.azureedg
 1114 2024-11-26 04:50:10.941790 10.11.26.183  10.11.26.3    DNS    81 Standard query 0xb120 A wpad.nemotoads.health
 1115 2024-11-26 04:50:10.942148 10.11.26.3    10.11.26.183  DNS   157 Standard query response 0xb120 No such name A wpad.nemotoads.health SOA nemotodes-dc.nemotoads.health
 1116 2024-11-26 04:50:10.942299 10.11.26.183  10.11.26.3    DNS    75 Standard query 0xcf5d A wpad.mshome.net
 1117 2024-11-26 04:50:10.942457 10.11.26.3    10.11.26.183  DNS   161 Standard query response 0xcf5d No such name A wpad.mshome.net SOA ns1-35.azure-dns.com
 1173 2024-11-26 04:50:11.288227 10.11.26.183  10.11.26.3    DNS    76 Standard query 0x95b8 A classicgrand.com
 1174 2024-11-26 04:50:11.288325 10.11.26.183  10.11.26.3    DNS    76 Standard query 0x32bf HTTPS classicgrand.com
 1175 2024-11-26 04:50:11.288517 10.11.26.183  10.11.26.3    DNS    78 Standard query 0x4840 A edge.microsoft.com
 1176 2024-11-26 04:50:11.288580 10.11.26.183  10.11.26.3    DNS    78 Standard query 0xca89 HTTPS edge.microsoft.com
 1177 2024-11-26 04:50:11.291652 10.11.26.183  10.11.26.3    DNS    76 Standard query 0x23e8 A classicgrand.com
 1178 2024-11-26 04:50:11.291741 10.11.26.183  10.11.26.3    DNS    76 Standard query 0x3f22 HTTPS classicgrand.com
 1179 2024-11-26 04:50:11.333612 10.11.26.3    10.11.26.183  DNS    92 Standard query response 0x23e8 A classicgrand.com A 213.246.109.5
 1180 2024-11-26 04:50:11.333665 10.11.26.3    10.11.26.183  DNS   135 Standard query response 0xca89 HTTPS edge.microsoft.com CNAME edge-microsoft-com.dual-a-0036.a-msedge.net
 1181 2024-11-26 04:50:11.333665 10.11.26.3    10.11.26.183  DNS    92 Standard query response 0x95b8 A classicgrand.com A 213.246.109.5
 1182 2024-11-26 04:50:11.333799 10.11.26.3    10.11.26.183  DNS   181 Standard query response 0x4840 A edge.microsoft.com CNAME edge-microsoft-com.dual-a-0036.a-msedge.net CNAM
 1189 2024-11-26 04:50:11.444471 10.11.26.3    10.11.26.183  DNS   134 Standard query response 0x3f22 HTTPS classicgrand.com SOA ns0.phase8.net
 1190 2024-11-26 04:50:11.444524 10.11.26.3    10.11.26.183  DNS   134 Standard query response 0x32bf HTTPS classicgrand.com SOA ns0.phase8.net
 1332 2024-11-26 04:50:14.145454 10.11.26.183  10.11.26.3    DNS    80 Standard query 0xa31d A modandcrackedapk.com
 1333 2024-11-26 04:50:14.145534 10.11.26.183  10.11.26.3    DNS    80 Standard query 0x58e5 HTTPS modandcrackedapk.com
 1334 2024-11-26 04:50:14.150461 10.11.26.183  10.11.26.3    DNS    83 Standard query 0x4ea4 A confirmsubscription.com
 1335 2024-11-26 04:50:14.150571 10.11.26.183  10.11.26.3    DNS    83 Standard query 0x5656 HTTPS confirmsubscription.com
 1336 2024-11-26 04:50:14.234653 10.11.26.3    10.11.26.183  DNS   139 Standard query response 0x5656 HTTPS confirmsubscription.com SOA ns0.dnsmadeeasy.com
 1337 2024-11-26 04:50:14.236416 10.11.26.3    10.11.26.183  DNS   115 Standard query response 0x4ea4 A confirmsubscription.com A 52.8.34.0 A 13.56.30.207
 1374 2024-11-26 04:50:14.315055 10.11.26.3    10.11.26.183  DNS    96 Standard query response 0xa31d A modandcrackedapk.com A 193.42.38.139
 1377 2024-11-26 04:50:14.319904 10.11.26.3    10.11.26.183  DNS   146 Standard query response 0x58e5 HTTPS modandcrackedapk.com SOA ns1.dns-parking.com
```

```
> Frame 1332: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
> Ethernet II, Src: Intel_ce:fc:8b (d0:57:7b:ce:fc:8b), Dst: Dell_7f:09:5d (00:24:e8:7f:09:5d)
> Internet Protocol Version 4, Src: 10.11.26.183, Dst: 10.11.26.3
> User Datagram Protocol, Src Port: 52957, Dst Port: 53
> Domain Name System (query)
```

```
0000  00 24 e8 7f 09 5d d0 57  7b ce fc 8b 08 00 45 00   ·$···]·W {·····E·
0010  00 42 37 58 00 00 80 11  ba 83 0a 0b 1a b7 0a 0b   ·B7X···· ········
0020  1a 03 ce dd 00 35 00 2e  25 d7 a3 1d 01 00 00 01   ·····5·. %·······
0030  00 00 00 00 00 00 10 6d  6f 64 61 6e 64 63 72 61   ·······m odandcra
0040  63 6b 65 64 61 70 6b 03  63 6f 6d 00 00 01 00 01   ckedapk· com·····
```

Activate Windows
Go to Settings to activate Windows.
Domain Name System: Protocol
Packets: 26922 · Displayed: 343 (1.3%)
Profile: Default

- **VirusTotal results confirming high threat score queried domain**



virustotal.com/gui/domain/modandcrackedapk.com
modandcrackedapk.com
Sign in
Sign up
Did you intend to search across the file corpus instead? Click here
10
/ 94
Community Score
Reanalyze
Similar
More
DETECTION
DETAILS
RELATIONS
COMMUNITY

10/94 security vendors flagged this domain as malicious

modandcrackedapk.com

sports | phishing and fraud | Phishing and Other Frauds

Creation Date: 1 year ago

Last Analysis Date: 8 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

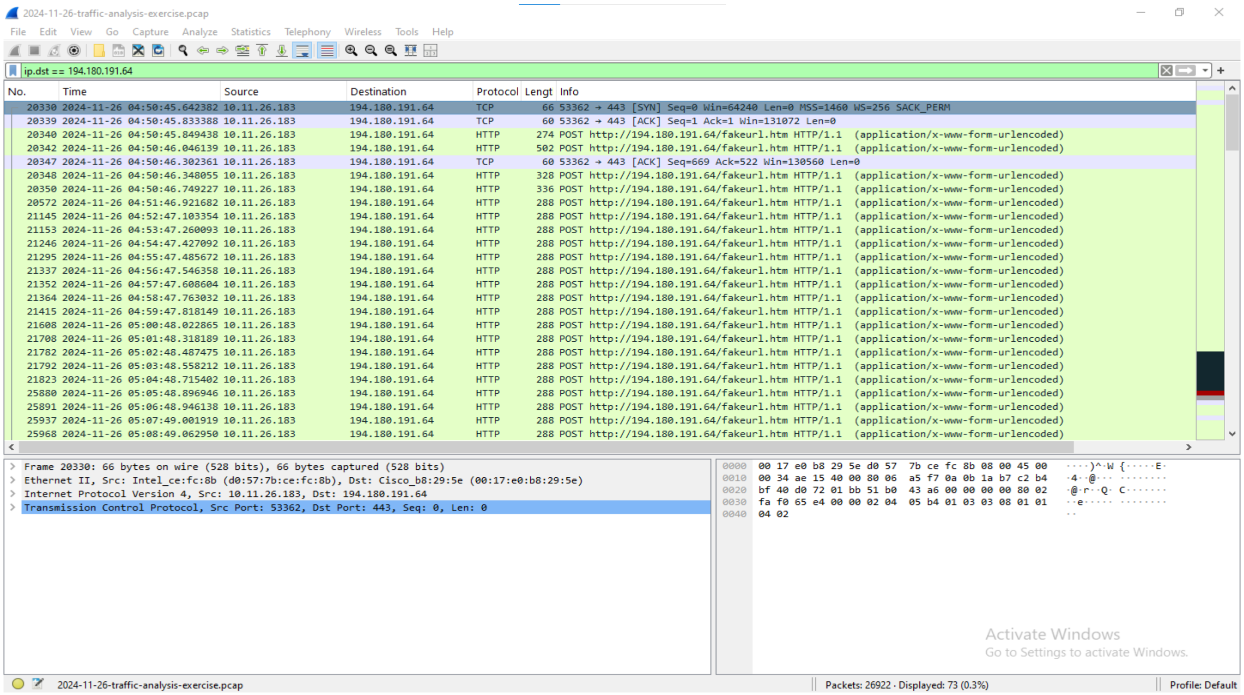
Do you want to automate checks?

alphaMountain.ai	Phishing	BitDefender	Malware
CyRadar	Malicious	ESET	Phishing
G-Data	Malware	Lionic	Malware
Seclookup	Malicious	SOCRadar	Malware
Sophos	Phishing	Webroot	Malicious

3.4. IP Address Correlation

External IPs the host communicated with were listed. The IP `194.180.191.64` appeared multiple times and was cross-checked against ThreatFox and VirusTotal. Its reputation showed associations with RAT (NetSupport RAT) infrastructure, particularly C2 servers. The internal host attempted to contact geo.supportsoftware.com, which is known to be part of the NetSupport Remote Access Trojan

- **Repeated communication observed with suspicious external IP : 194.180.191.64**



2024-11-26-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.dst == 194.180.191.64

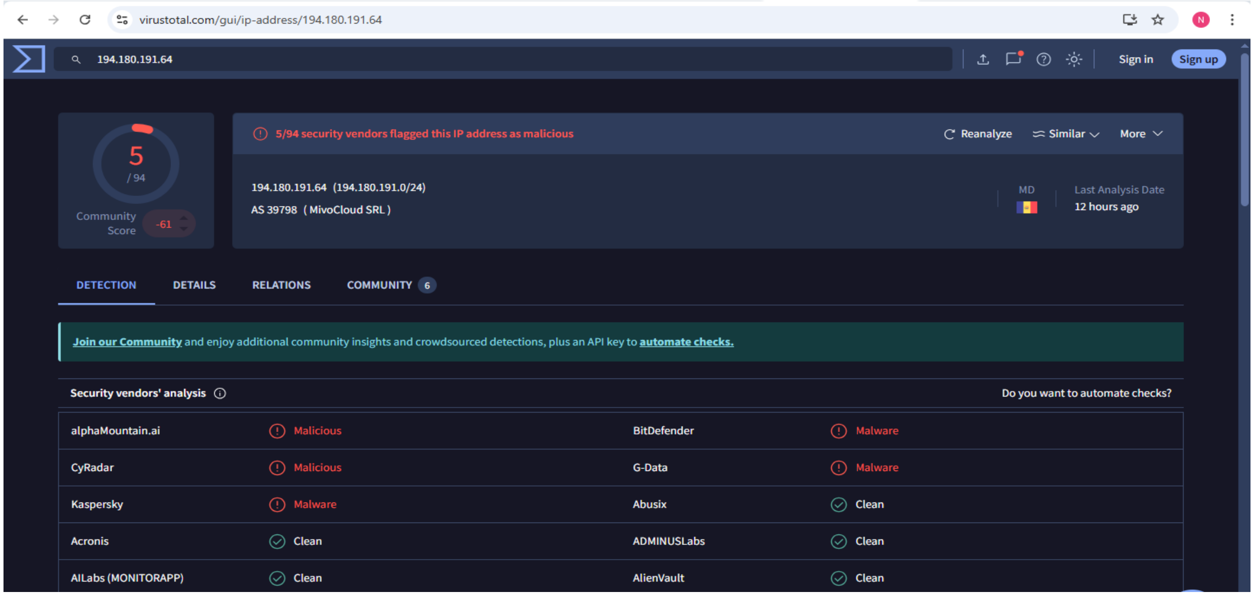
```
No.   Time                       Source        Destination     Protocol Lengt Info
20330 2024-11-26 04:50:45.642382 10.11.26.183  194.180.191.64  TCP       66 53362 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
20339 2024-11-26 04:50:45.833388 10.11.26.183  194.180.191.64  TCP       60 53362 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
20340 2024-11-26 04:50:45.849438 10.11.26.183  194.180.191.64  HTTP     274 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
20342 2024-11-26 04:50:46.046139 10.11.26.183  194.180.191.64  HTTP     502 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
20347 2024-11-26 04:50:46.302361 10.11.26.183  194.180.191.64  TCP       60 53362 → 443 [ACK] Seq=669 Ack=522 Win=130560 Len=0
20348 2024-11-26 04:50:46.348055 10.11.26.183  194.180.191.64  HTTP     328 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
20350 2024-11-26 04:50:46.749227 10.11.26.183  194.180.191.64  HTTP     336 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
20572 2024-11-26 04:51:46.921682 10.11.26.183  194.180.191.64  HTTP     288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
21145 2024-11-26 04:52:47.103354 10.11.26.183  194.180.191.64  HTTP     288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
21153 2024-11-26 04:53:47.260093 10.11.26.183  194.180.191.64  HTTP     288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
21246 2024-11-26 04:54:47.427092 10.11.26.183  194.180.191.64  HTTP     288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
21295 2024-11-26 04:55:47.485672 10.11.26.183  194.180.191.64  HTTP     288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
21337 2024-11-26 04:56:47.546358 10.11.26.183  194.180.191.64  HTTP     288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
21352 2024-11-26 04:57:47.608604 10.11.26.183  194.180.191.64  HTTP     288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
21364 2024-11-26 04:58:47.763032 10.11.26.183  194.180.191.64  HTTP     288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
21415 2024-11-26 04:59:47.818149 10.11.26.183  194.180.191.64  HTTP     288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
21608 2024-11-26 05:00:48.022865 10.11.26.183  194.180.191.64  HTTP     288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
21708 2024-11-26 05:01:48.318189 10.11.26.183  194.180.191.64  HTTP     288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
21782 2024-11-26 05:02:48.487475 10.11.26.183  194.180.191.64  HTTP     288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
21792 2024-11-26 05:03:48.558212 10.11.26.183  194.180.191.64  HTTP     288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
21823 2024-11-26 05:04:48.715402 10.11.26.183  194.180.191.64  HTTP     288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
25880 2024-11-26 05:05:48.896946 10.11.26.183  194.180.191.64  HTTP     288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
25891 2024-11-26 05:06:48.946138 10.11.26.183  194.180.191.64  HTTP     288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
25937 2024-11-26 05:07:49.001919 10.11.26.183  194.180.191.64  HTTP     288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
25968 2024-11-26 05:08:49.062950 10.11.26.183  194.180.191.64  HTTP     288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1  (application/x-www-form-urlencoded)
```

```
> Frame 20330: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: Intel_ce:fc:8b (d0:57:7b:ce:fc:8b), Dst: Cisco_b8:29:5e (00:17:e0:b8:29:5e)
> Internet Protocol Version 4, Src: 10.11.26.183, Dst: 194.180.191.64
> Transmission Control Protocol, Src Port: 53362, Dst Port: 443, Seq: 0, Len: 0
```

```
0000  00 17 e0 b8 29 5e d0 57  7b ce fc 8b 08 00 45 00   ····)^·W {·····E·
0010  00 34 ae 15 40 00 80 06  a5 f7 0a 0b 1a b7 c2 b4   ·4··@··· ········
0020  bf 40 d0 72 01 bb 51 b0  43 a6 00 00 00 00 80 02   ·@·r··Q· C·······
0030  fa f0 65 e4 00 00 02 04  05 b4 01 03 03 08 01 01   ··e····· ········
0040  04 02                                              ··
```

2024-11-26-traffic-analysis-exercise.pcap | Packets: 26922 · Displayed: 73 (0.3%) | Profile: Default

- **VirusTotal confirms the IP address is malicious**



virustotal.com/gui/ip-address/194.180.191.64

194.180.191.64

5 / 94

Community Score -61

5/94 security vendors flagged this IP address as malicious

194.180.191.64 (194.180.191.0/24)
AS 39798 (MivoCloud SRL)

MD

Last Analysis Date
12 hours ago

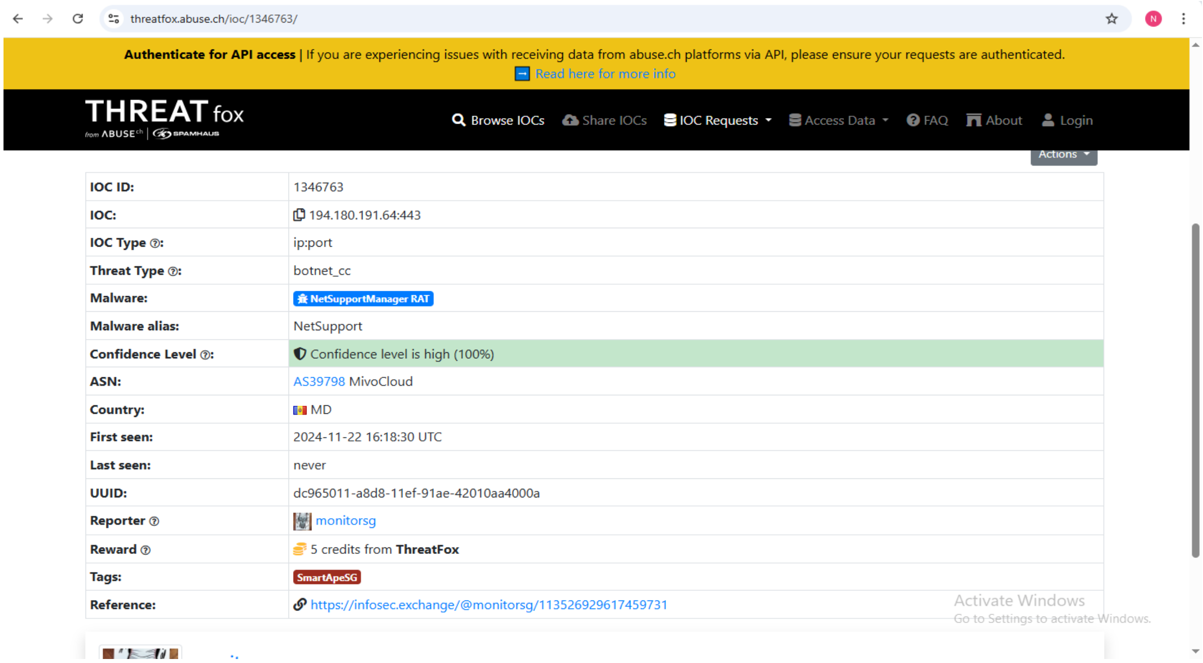
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

alphaMountain.ai	Malicious	BitDefender	Malware
CyRadar	Malicious	G-Data	Malware
Kaspersky	Malware	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean

- **Threat Intelligence lookup confirms the IP is linked to known RAT infrastructure**

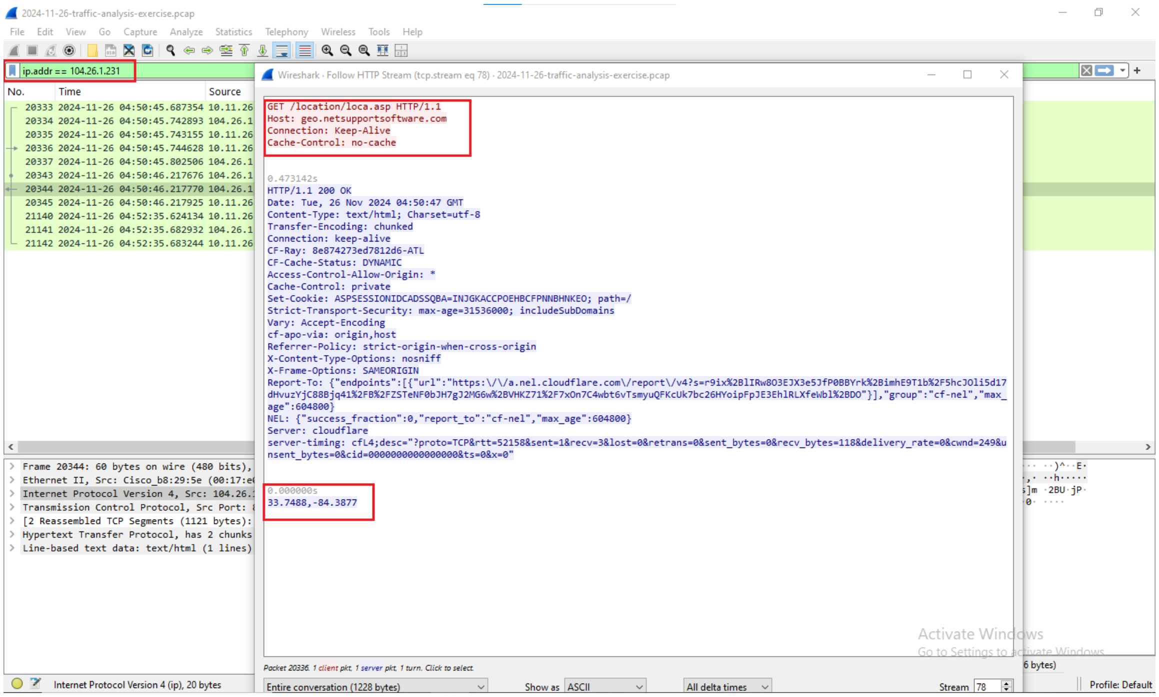


threatfox.abuse.ch/ioc/1346763/

Authenticate for API access | If you are experiencing issues with receiving data from abuse.ch platforms via API, please ensure your requests are authenticated.
Read here for more info

IOC ID:	1346763
IOC:	194.180.191.64:443
IOC Type ⓘ**:**	ip:port
Threat Type ⓘ**:**	botnet_cc
Malware:	NetSupportManager RAT
Malware alias:	NetSupport
Confidence Level ⓘ**:**	Confidence level is high (100%)
ASN:	AS39798 MivoCloud
Country:	MD
First seen:	2024-11-22 16:18:30 UTC
Last seen:	never
UUID:	dc965011-a8d8-11ef-91ae-42010aa4000a
Reporter ⓘ	monitorsg
Reward ⓘ	5 credits from **ThreatFox**
Tags:	SmartApeSG
Reference:	https://infosec.exchange/@monitorsg/113526929617459731

- **Suspicious request to geo.supportsoftware.com, an endpoint commonly used by NetSupport RAT for victim geolocation.**



2024-11-26-traffic-analysis-exercise.pcap

ip.addr == 104.26.1.231

```
No.    Time                       Source
20333 2024-11-26 04:50:45.687354 10.11.26
20334 2024-11-26 04:50:45.742893 104.26.1
20335 2024-11-26 04:50:45.743155 10.11.26
20336 2024-11-26 04:50:45.744628 10.11.26
20337 2024-11-26 04:50:45.802506 104.26.1
20343 2024-11-26 04:50:46.217676 104.26.1
20344 2024-11-26 04:50:46.217770 104.26.1
20345 2024-11-26 04:50:46.217925 10.11.26
21140 2024-11-26 04:52:35.624134 10.11.26
21141 2024-11-26 04:52:35.682932 104.26.1
21142 2024-11-26 04:52:35.683244 10.11.26
```

```
> Frame 20344: 60 bytes on wire (480 bits),
> Ethernet II, Src: Cisco_b8:29:5e (00:17:e
> Internet Protocol Version 4, Src: 104.26.
> Transmission Control Protocol, Src Port:
> [2 Reassembled TCP Segments (1121 bytes):
> Hypertext Transfer Protocol, has 2 chunks
> Line-based text data: text/html (1 lines)
```

Wireshark · Follow HTTP Stream (tcp.stream eq 78) · 2024-11-26-traffic-analysis-exercise.pcap

```
GET /location/loca.asp HTTP/1.1
Host: geo.netsupportsoftware.com
Connection: Keep-Alive
Cache-Control: no-cache

0.473142s
HTTP/1.1 200 OK
Date: Tue, 26 Nov 2024 04:50:47 GMT
Content-Type: text/html; Charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
CF-Ray: 8e874273ed7812d6-ATL
CF-Cache-Status: DYNAMIC
Access-Control-Allow-Origin: *
Cache-Control: private
Set-Cookie: ASPSESSIONIDCADSSQBA=INJGKACCPOEHBCFPNNBHNKEO; path=/
Strict-Transport-Security: max-age=31536000; includeSubDomains
Vary: Accept-Encoding
cf-apo-via: origin,host
Referrer-Policy: strict-origin-when-cross-origin
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?s=r9ix%2BlIRw8O3EJX3e5JfP0BBYrk%2BimhE9T1b%2F5hcJOli5d17
dHvuzYjC88Bjq41%2FB%2FZSTeNF0bJH7gJ2MG6w%2BVHKZ71%2F7xOn7C4wbt6vTsmyuQFKcUk7bc26HYoipFpJE3EhlRLXfeWbl%2BDO"}],"group":"cf-nel","max_
age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
server-timing: cfL4;desc="?proto=TCP&rtt=52158&sent=1&recv=3&lost=0&retrans=0&sent_bytes=0&recv_bytes=118&delivery_rate=0&cwnd=249&u
nsent_bytes=0&cid=0000000000000000&ts=0&x=0"

0.000000s
33.7488,-84.3877
```

Packet 20336. 1 client pkt, 1 server pkt, 1 turn. Click to select.

Entire conversation (1228 bytes) Show as ASCII All delta times Stream 78

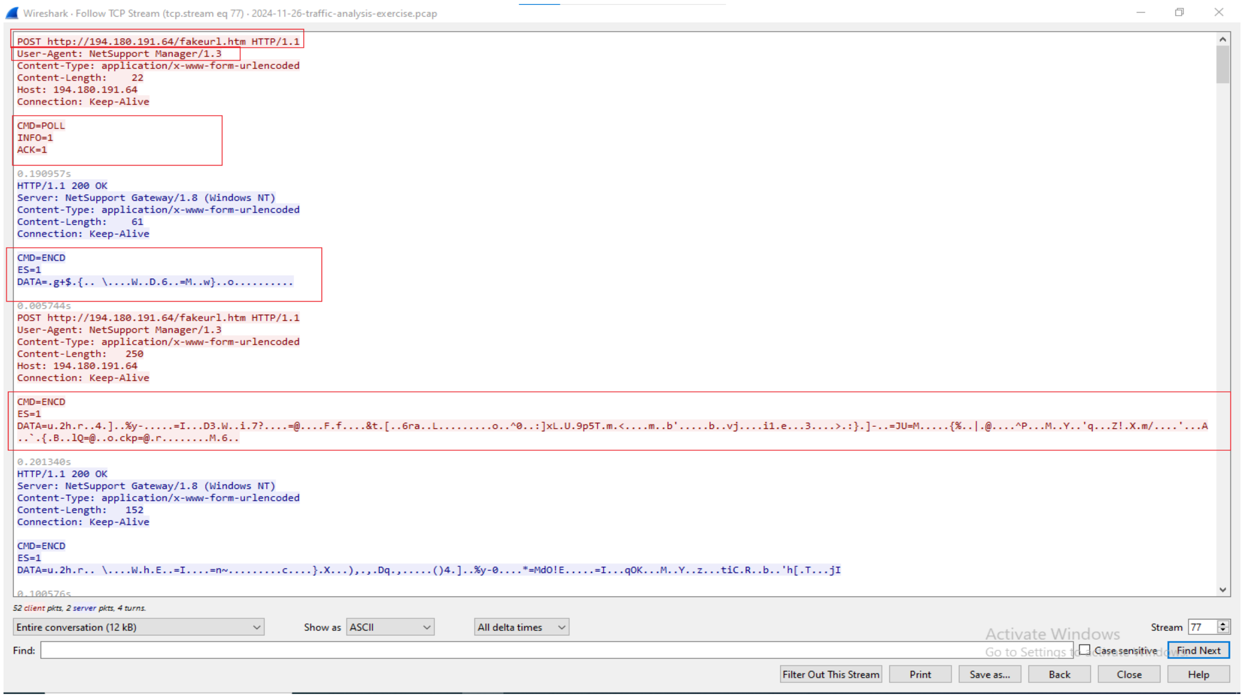
Internet Protocol Version 4 (ip), 20 bytes

Profile: Default

3.5. HTTP / POST Traffic Review

I identified a POST request sent over HTTP (not HTTPS) to the IP mentioned below. The User-Agent string looked generic but suspicious (often used by downloaders or scripts). The URL path and parameters suggested possible data exfiltration or beaconing behavior.

- ➢ **Unencrypted HTTP POST request made to suspicious IP, indicating potential data exfiltration.**
- ➢ **Suspicious User-Agent and URL path used in outbound POST request**



Wireshark · Follow TCP Stream (tcp.stream eq 77) · 2024-11-26-traffic-analysis-exercise.pcap

```
POST http://194.180.191.64/fakeurl.htm HTTP/1.1
User-Agent: NetSupport Manager/1.3
Content-Type: application/x-www-form-urlencoded
Content-Length:    22
Host: 194.180.191.64
Connection: Keep-Alive

CMD=POLL
INFO=1
ACK=1

0.190957s
HTTP/1.1 200 OK
Server: NetSupport Gateway/1.8 (Windows NT)
Content-Type: application/x-www-form-urlencoded
Content-Length:    61
Connection: Keep-Alive

CMD=ENCD
ES=1
DATA=.g+$.{.. \....W..D.6..=M..w}..o.........

0.005744s
POST http://194.180.191.64/fakeurl.htm HTTP/1.1
User-Agent: NetSupport Manager/1.3
Content-Type: application/x-www-form-urlencoded
Content-Length:   250
Host: 194.180.191.64
Connection: Keep-Alive

CMD=ENCD
ES=1
DATA=u.2h.r..4.]..%y-.....=I...D3.W..i.7?....=@....F.f....&t.[..6ra..L.........o..^0..:]xL.U.9p5T.m.<....m..b'.....b..vj....i1.e...3....>.:}.]-..=JU=M.....{%..|.@....^P...M..Y..'q...Z!.X.m/....'...A
..`.{.B..lQ=@..o.ckp=@.r........M.6..

0.201340s
HTTP/1.1 200 OK
Server: NetSupport Gateway/1.8 (Windows NT)
Content-Type: application/x-www-form-urlencoded
Content-Length:   152
Connection: Keep-Alive

CMD=ENCD
ES=1
DATA=u.2h.r.. \....W.h.E..=I....=n~.........c....}.X...),.,.Dq.,.....()4.]..%y-0....*=MdO!E.....=I...qOK...M..Y..z...tiC.R..b..'h[.T...jI

0.100576s
```

52 client pkts, 2 server pkts, 4 turns.

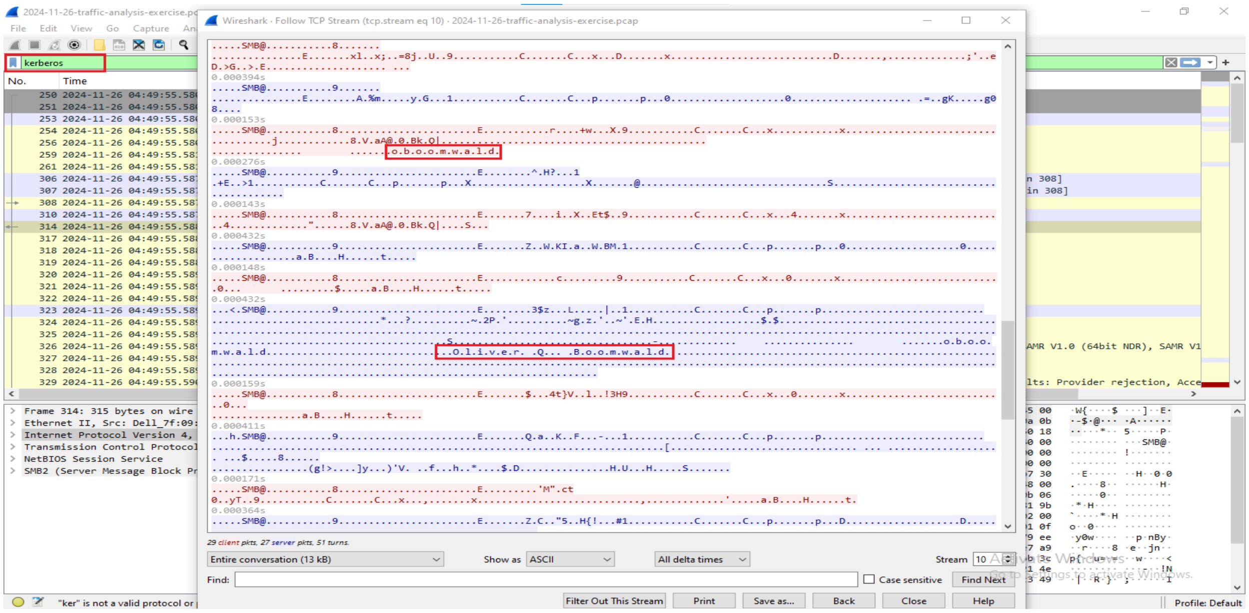
Entire conversation (12 kB) Show as ASCII All delta times Stream 77

Find: ☐ Case sensitive

3.6. Victim Profiling

From internal metadata and traffic patterns, I was able to extract partial victim profiling data such as hostname, MAC address, internal IP, and hints of the system username. This helped assess the impact scope and identify the potentially compromised asset.

- **Extracting host profiling data including internal IP, MAC address, and hostname**



2024-11-26-traffic-analysis-exercise.pc

Filter: kerberos

```
No.  Time
 250 2024-11-26 04:49:55.58
 251 2024-11-26 04:49:55.58
 253 2024-11-26 04:49:55.58
 254 2024-11-26 04:49:55.58
 256 2024-11-26 04:49:55.58
 259 2024-11-26 04:49:55.58
 261 2024-11-26 04:49:55.58
 306 2024-11-26 04:49:55.58
 307 2024-11-26 04:49:55.58
 308 2024-11-26 04:49:55.58
 310 2024-11-26 04:49:55.58
 314 2024-11-26 04:49:55.58
 317 2024-11-26 04:49:55.58
 318 2024-11-26 04:49:55.58
 319 2024-11-26 04:49:55.58
 320 2024-11-26 04:49:55.58
 321 2024-11-26 04:49:55.58
 322 2024-11-26 04:49:55.58
 323 2024-11-26 04:49:55.58
 324 2024-11-26 04:49:55.58
 325 2024-11-26 04:49:55.58
 326 2024-11-26 04:49:55.58
 327 2024-11-26 04:49:55.58
 328 2024-11-26 04:49:55.58
 329 2024-11-26 04:49:55.59

> Frame 314: 315 bytes on wire
> Ethernet II, Src: Dell_7f:09:
> Internet Protocol Version 4,
> Transmission Control Protocol
> NetBIOS Session Service
> SMB2 (Server Message Block Pr
```

"ker" is not a valid protocol or

Wireshark · Follow TCP Stream (tcp.stream eq 10) · 2024-11-26-traffic-analysis-exercise.pcap

```
.....SMB@..........8.......
...............E.......xl..x;..=8j..U..9..........C.......C...x...D.......x.........................D.......,.............;'..e
D.>G..>.E...................  ...
0.000394s
.....SMB@..........9.......
...............E........A.%m.....y.G...1..........C.......C...p.......p...0...................0....................  .=..gK.....g0
8....
0.000153s
.....SMB@..........8.......................E...........r....+w...X.9..........C.......C...x..........x.......................
..........j............8.V.aA@.0.Bk.Q|..............................................
...............          ......o.b.o.o.m.w.a.l.d.
0.000276s
.....SMB@..........9.......................E........^.H?...1
.+E..>1...........C.......C...p.......p...X...................X.......@..............................S.......................
...........
0.000143s
.....SMB@..........8.......................E.......7....i..X..Et$..9..........C.......C...x...4.......x.......................
..4.............".......8.V.aA@.0.Bk.Q|....S...
0.000432s
.....SMB@..........9.......................E.......Z..W.KI.a..W.BM.1..........C.......C...p.......p...0...................0.....
..............a.B....H......t.....
0.000148s
.....SMB@..........8.......................E............c.........9..........C.......C...x...0.......x.......................
.0...       .........$.....a.B....H......t.....
0.000432s
...<.SMB@..........9.......................E........3$z...L.....|..1..........C.......C...p.......p.........................
..........................*...?..........~.2P.'..........~g.z.'..~'.E.H.................$.$.................................
.............................................................................................................................
..........................S.............................-...........      .............        .......o.b.o.o.
m.w.a.l.d...........................O.l.i.v.e.r. .Q...  .B.o.o.m.w.a.l.d.................................................
.............................................................................................................................
.............................................................
0.000159s
.....SMB@..........8.......................E.......$...4t}V..l..!3H9..........C.......C...x...0.......x.......................
..0...
..............a.B....H......t.....
0.000411s
...h.SMB@..........9.......................E.......Q.a..K..F...-...1..........C.......C...p.......p.........................
.......................................................................[.......................  ...  ......................
.  ...$.....8......
...............(g!>....]y...)'V.  ..f...h..*....$.D..............H.U...H.....S.......
0.000171s
.....SMB@..........8.......................E.........'M".ct
0..yT..9..........C.......C...x..,.........x.........................,...............'.....a.B....H......t.
0.000364s
.....SMB@..........9.......................E.......Z.C.."5..H{!...#1..........C.......C...p.......p...D.................D.....
```

29 client pkts, 27 server pkts, 51 turns.

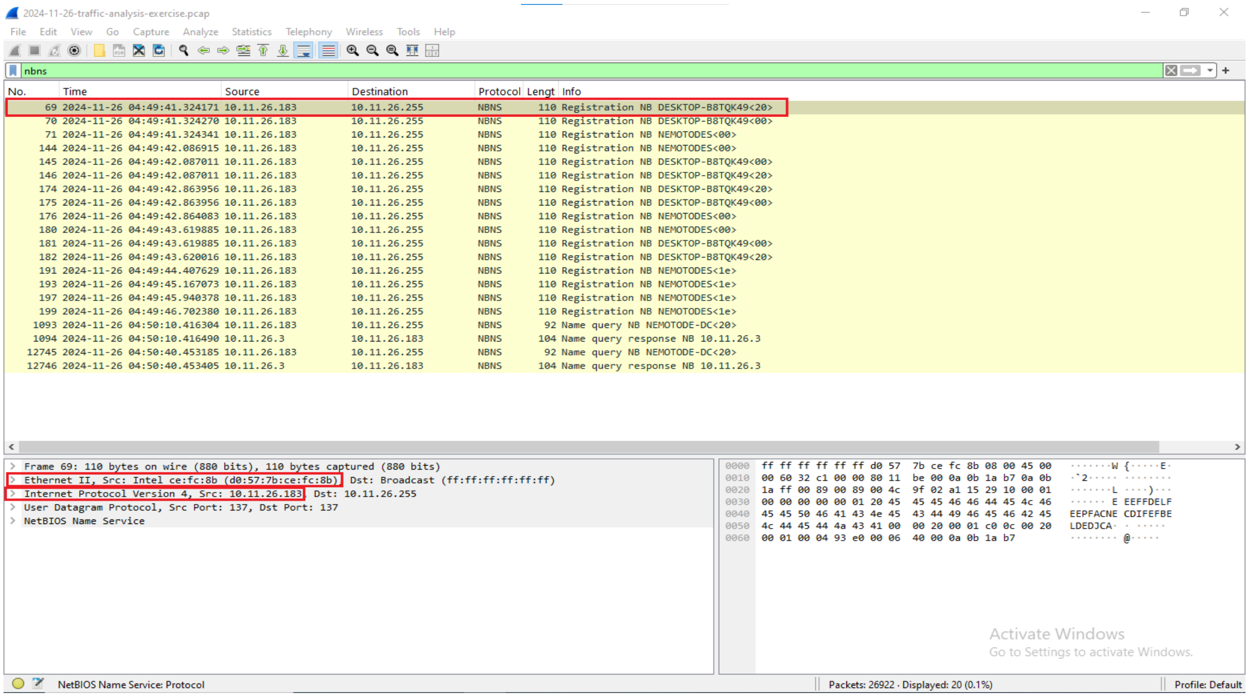
Entire conversation (13 kB) | Show as ASCII | All delta times | Stream 10

Find: | ☐ Case sensitive | Find Next

Filter Out This Stream | Print | Save as… | Back | Close | Help

```
n 308]
in 308]
AMR V1.0 (64bit NDR), SAMR V1
lts: Provider rejection, Acce
```

Profile: Default



2024-11-26-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: nbns

```
No.   Time                       Source        Destination   Protocol Lengt Info
   69 2024-11-26 04:49:41.324171 10.11.26.183  10.11.26.255  NBNS     110 Registration NB DESKTOP-B8TQK49<20>
   70 2024-11-26 04:49:41.324270 10.11.26.183  10.11.26.255  NBNS     110 Registration NB DESKTOP-B8TQK49<00>
   71 2024-11-26 04:49:41.324341 10.11.26.183  10.11.26.255  NBNS     110 Registration NB NEMOTODES<00>
  144 2024-11-26 04:49:42.086915 10.11.26.183  10.11.26.255  NBNS     110 Registration NB NEMOTODES<00>
  145 2024-11-26 04:49:42.087011 10.11.26.183  10.11.26.255  NBNS     110 Registration NB DESKTOP-B8TQK49<00>
  146 2024-11-26 04:49:42.087011 10.11.26.183  10.11.26.255  NBNS     110 Registration NB DESKTOP-B8TQK49<20>
  174 2024-11-26 04:49:42.863956 10.11.26.183  10.11.26.255  NBNS     110 Registration NB DESKTOP-B8TQK49<20>
  175 2024-11-26 04:49:42.863956 10.11.26.183  10.11.26.255  NBNS     110 Registration NB DESKTOP-B8TQK49<00>
  176 2024-11-26 04:49:42.864083 10.11.26.183  10.11.26.255  NBNS     110 Registration NB NEMOTODES<00>
  180 2024-11-26 04:49:43.619885 10.11.26.183  10.11.26.255  NBNS     110 Registration NB NEMOTODES<00>
  181 2024-11-26 04:49:43.619885 10.11.26.183  10.11.26.255  NBNS     110 Registration NB DESKTOP-B8TQK49<00>
  182 2024-11-26 04:49:43.620016 10.11.26.183  10.11.26.255  NBNS     110 Registration NB DESKTOP-B8TQK49<20>
  191 2024-11-26 04:49:44.407629 10.11.26.183  10.11.26.255  NBNS     110 Registration NB NEMOTODES<1e>
  193 2024-11-26 04:49:45.167073 10.11.26.183  10.11.26.255  NBNS     110 Registration NB NEMOTODES<1e>
  197 2024-11-26 04:49:45.940378 10.11.26.183  10.11.26.255  NBNS     110 Registration NB NEMOTODES<1e>
  199 2024-11-26 04:49:46.702380 10.11.26.183  10.11.26.255  NBNS     110 Registration NB NEMOTODES<1e>
 1093 2024-11-26 04:50:10.416304 10.11.26.183  10.11.26.255  NBNS      92 Name query NB NEMOTODE-DC<20>
 1094 2024-11-26 04:50:10.416490 10.11.26.3    10.11.26.183  NBNS     104 Name query response NB 10.11.26.3
12745 2024-11-26 04:50:40.453185 10.11.26.183  10.11.26.255  NBNS      92 Name query NB NEMOTODE-DC<20>
12746 2024-11-26 04:50:40.453405 10.11.26.3    10.11.26.183  NBNS     104 Name query response NB 10.11.26.3
```

```
> Frame 69: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
> Ethernet II, Src: Intel ce:fc:8b (d0:57:7b:ce:fc:8b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 10.11.26.183, Dst: 10.11.26.255
> User Datagram Protocol, Src Port: 137, Dst Port: 137
> NetBIOS Name Service
```

```
0000  ff ff ff ff ff ff d0 57  7b ce fc 8b 08 00 45 00   ·······W {·····E·
0010  00 60 32 c1 00 00 80 11  be 00 0a 0b 1a b7 0a 0b   ·`2····· ········
0020  1a ff 00 89 00 89 00 4c  9f 02 a1 15 29 10 00 01   ·······L ····)···
0030  00 00 00 00 00 01 20 45  45 45 46 46 44 45 4c 46   ······ E EEFFDELF
0040  45 45 50 46 41 43 4e 45  43 44 49 46 45 46 42 45   EEPFACNE CDIFEFBE
0050  4c 44 45 44 4a 43 41 00  00 20 00 01 c0 0c 00 20   LDEDJCA· · ······
0060  00 01 00 04 93 e0 00 06  40 00 0a 0b 1a b7         ········ @·····
```

NetBIOS Name Service: Protocol | Packets: 26922 · Displayed: 20 (0.1%) | Profile: Default

4. Key Observations

- A DNS query followed by a TLS handshake with a cracked APK domain suggests suspicious software use.
- Unencrypted POST requests to an external IP hint at data exfiltration or command-and-control.

- Several requests attempted to determine the system's geo-location, which is often behavior seen in RATs.
- The IOC matches aligned with public threat intel sources like THREATfox and VirusTotal.

5. IOC Table

Type	Value	Source / Notes
IP	194.180.191.64	Malicious IP associated with C2 server
Domain	modandcrackedapk.com	Flagged on VirusTotal (10/94 score)
URL	hxxp://194[.]180[.]191[.]64/fakeurl.htm	Observed in HTTP POST

7. What I Learned

This project helped reinforce key Blue Team analysis skills. Notably, I improved in:

- Crafting effective Wireshark filters to isolate relevant traffic.
- Cross-referencing IOCs with threat intelligence platforms.
- Understanding attacker communication patterns (C2, beaconing, etc.).
- Documenting findings clearly and professionally for further response.