SOC ANALYST TRANING REPORT

ON

MALWARE ANALYSIS USING WIRESHARK

ANALYSED AND REPORTED

BY

ALI CHINASA JULIET

INSTRUCTOR: MR OLA OLAITAN

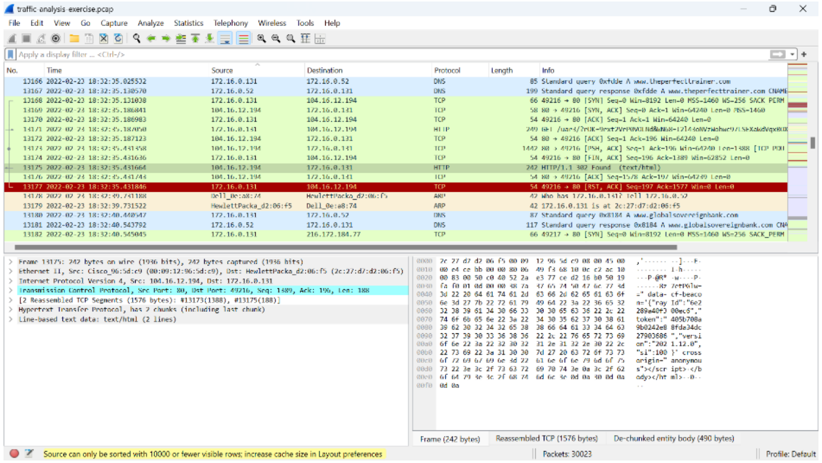
DATE: AUGUST 2024

Executive Summary

This report presents the findings from a network traffic analysis using Wireshark. The investigation focused on identifying anomalies, suspicious activities, and potential security threats within the captured network traffic. The analysis uncovered several points of concern, including communication with potentially malicious IP addresses, anomalies in DHCP and Kerberos authentication, and interactions between specific devices. Immediate and long-term recommendations are provided to address the identified risks and enhance the network's security posture.

Overview

The analysis was conducted by examining captured network traffic in Wireshark. Several protocols, including IPv4, IPv6, UDP, and TCP,HTTP were analyzed to identify unusual activities. The investigation also involved filtering for specific traffic types, such as DHCP and Kerberos, and resolving device names and MAC addresses to understand the communication patterns within the network. The use of external tools like VirusTotal, AbuseIPDB, IPInfo, and Pulsedive allowed for the evaluation of the reputation of certain IP addresses, contributing to a comprehensive understanding of the network's security status.


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

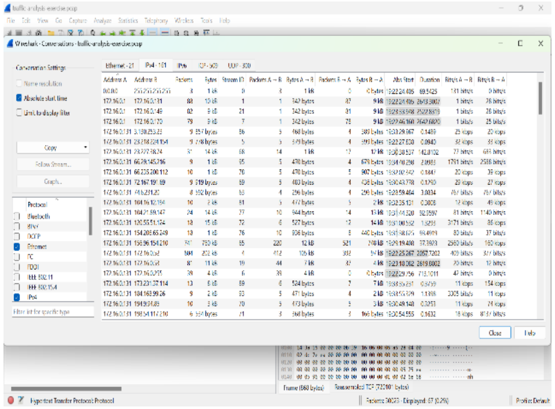
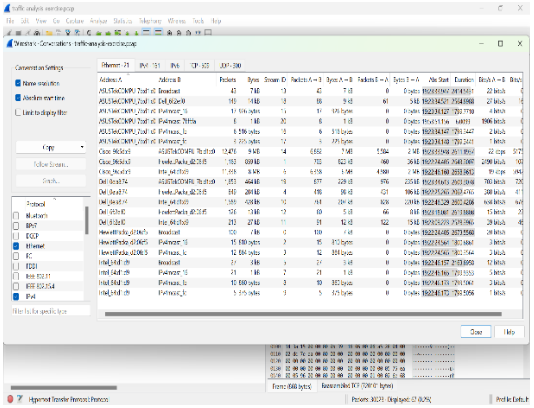
```
No.    Time                        Source                 Destination            Protocol  Length  Info
13166  2022-02-23 18:32:35.025532  172.16.0.131           172.16.0.52            DNS           85  Standard query 0xfdde A www.theperfecttrainer.com
13167  2022-02-23 18:32:35.130570  172.16.0.52            172.16.0.131           DNS          199  Standard query response 0xfdde A www.theperfecttrainer.com CNAME
13168  2022-02-23 18:32:35.131038  172.16.0.131           104.16.12.194          TCP           66  49216 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
13169  2022-02-23 18:32:35.186841  104.16.12.194          172.16.0.131           TCP           58  80 → 49216 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
13170  2022-02-23 18:32:35.186983  172.16.0.131           104.16.12.194          TCP           54  49216 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
13171  2022-02-23 18:32:35.187050  172.16.0.131           104.16.12.194          HTTP         249  GET /uar3/?rUK-9rxt2VrP0VOLNd&wN68-1214oNVzWohwc97LSEXaWdVqxBOX
13172  2022-02-23 18:32:35.187123  104.16.12.194          172.16.0.131           TCP           54  80 → 49216 [ACK] Seq=1 Ack=196 Win=64240 Len=0
13173  2022-02-23 18:32:35.431358  104.16.12.194          172.16.0.131           TCP         1442  80 → 49216 [PSH, ACK] Seq=1 Ack=196 Win=64240 Len=1388 [TCP PDU
13174  2022-02-23 18:32:35.431636  172.16.0.131           104.16.12.194          TCP           54  49216 → 80 [FIN, ACK] Seq=196 Ack=1389 Win=62852 Len=0
13175  2022-02-23 18:32:35.431664  104.16.12.194          172.16.0.131           HTTP         242  HTTP/1.1 302 Found  (text/html)
13176  2022-02-23 18:32:35.431743  104.16.12.194          172.16.0.131           TCP           54  80 → 49216 [ACK] Seq=1578 Ack=197 Win=64239 Len=0
13177  2022-02-23 18:32:35.431846  172.16.0.131           104.16.12.194          TCP           54  49216 → 80 [RST, ACK] Seq=197 Ack=1577 Win=0 Len=0
13178  2022-02-23 18:32:39.731188  Dell_0e:a8:74          HewlettPacka_d2:06:f5  ARP           42  Who has 172.16.0.131? Tell 172.16.0.52
13179  2022-02-23 18:32:39.731522  HewlettPacka_d2:06:f5  Dell_0e:a8:74          ARP           42  172.16.0.131 is at 2c:27:d7:d2:06:f5
13180  2022-02-23 18:32:40.440547  172.16.0.131           172.16.0.52            DNS           87  Standard query 0x8184 A www.globalsovereignbank.com
13181  2022-02-23 18:32:40.543792  172.16.0.52            172.16.0.131           DNS          117  Standard query response 0x8184 A www.globalsovereignbank.com CNA
13182  2022-02-23 18:32:40.545045  172.16.0.131           216.172.184.77         TCP           66  49217 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM

> Frame 13175: 242 bytes on wire (1936 bits), 242 bytes captured (1936 bits)
> Ethernet II, Src: Cisco_96:5d:c9 (00:09:12:96:5d:c9), Dst: HewlettPacka_d2:06:f5 (2c:27:d7:d2:06:f5)
> Internet Protocol Version 4, Src: 104.16.12.194, Dst: 172.16.0.131
> Transmission Control Protocol, Src Port: 80, Dst Port: 49216, Seq: 1389, Ack: 196, Len: 188
> [2 Reassembled TCP Segments (1576 bytes): #13173(1388), #13175(188)]
> Hypertext Transfer Protocol, has 2 chunks (including last chunk)
> Line-based text data: text/html (2 lines)

0000  2c 27 d7 d2 06 f5 00 09  12 96 5d c9 08 00 45 00   ,'······ ··]···E·
0010  00 e4 ce bb 00 00 80 06  49 f3 68 10 0c c2 ac 10   ········ I·h·····
0020  00 83 00 50 c0 40 52 2a  e3 77 ce d2 16 b0 50 19   ···P·@R* ·w····P·
0030  fa f0 01 0d 00 00 38 7a  37 65 74 50 47 6c 77 3d   ······8z 7etPGlw=
0040  3d 22 20 64 61 74 61 2d  63 66 2d 62 65 61 63 6f   =" data- cf-beaco
0050  6e 3d 27 7b 22 72 61 79  49 64 22 3a 22 36 65 32   n='{"ray Id":"6e2
0060  32 38 39 61 34 30 66 33  30 30 65 63 36 22 2c 22   289a40f3 00ec6","
0070  74 6f 6b 65 6e 22 3a 22  34 30 35 62 37 30 38 61   token":" 405b708a
0080  39 62 30 32 34 32 65 38  38 66 64 61 33 34 64 63   9b0242e8 8fda34dc
0090  32 37 39 30 33 36 38 36  22 2c 22 76 65 72 73 69   27903686 ","versi
00a0  6f 6e 22 3a 22 32 30 32  31 2e 31 32 2e 30 22 2c   on":"202 1.12.0",
00b0  22 73 69 22 3a 31 30 30  7d 27 20 63 72 6f 73 73   "si":100 }' cross
00c0  6f 72 69 67 69 6e 3d 22  61 6e 6f 6e 79 6d 6f 75   origin=" anonymou
00d0  73 22 3e 3c 2f 73 63 72  69 70 74 3e 0a 3c 2f 62   s"></scr ipt>·</b
00e0  6f 64 79 3e 3c 2f 68 74  6d 6c 3e 0d 0a 30 0d 0a   ody></ht ml>··0··
00f0  0d 0a                                              ··
```

Frame (242 bytes)
Reassembled TCP (1576 bytes)
De-chunked entity body (490 bytes)
Source can only be sorted with 10000 or fewer visible rows; increase cache size in Layout preferences
Packets: 30023
Profile: Default

Analysis and Investigation

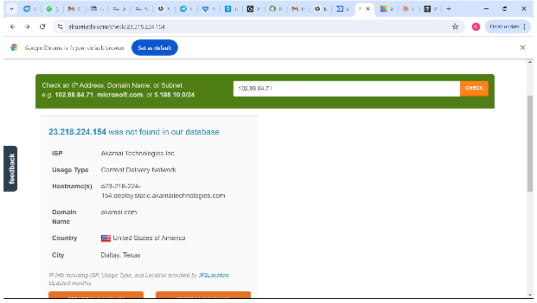
1. Traffic Examination:

- **Conversation Analysis**: Name resolution was applied to the network traffic, revealing several devices and their MAC addresses. For example:
- **Device**: **HewlettPacka_d2:06:f5 (2c:27:d7:d2:06:f5)**

- **Communication**: This device was involved in multiple conversations with IP addresses such as **23.218.224.154** which is the destination address and others over the IPv4 protocol.
- **Traffic Details**: The conversations involved data exchanges with varying durations, the longest lasting **2619.8802 seconds**. The analysis showed communication between devices with MAC addresses like **Cisco_96:5d:c9 and Intel_64:d1:d9**, highlighting the interactions between different network entities.

- **Geolocation and IP Reputation**: The **IP 23.218.224.154**, identified in one of the conversations, was checked using VirusTotal and AbuseIPDB, IPinfo etc revealing that no security vendor flagged to be associated with malicious activities. Geolocation analysis indicated the IP's origin, helping to contextualize its involvement in the network traffic.


abuseipdb.com/check/23.218.224.154

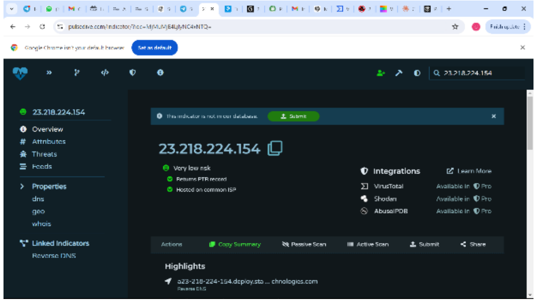
Check an IP Address, Domain Name, or Subnet
e.g. **102.88.84.71**, **microsoft.com**, or **5.188.10.0/24**

102.88.84.71

23.218.224.154 was not found in our database

ISP	Akamai Technologies Inc.
Usage Type	Content Delivery Network
Hostname(s)	a23-218-224-154.deploy.static.akamaitechnologies.com
Domain Name	akamai.com
Country	United States of America
City	Dallas, Texas

IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.


pulsedive.com/indicator/?ioc=MjMuMjE4LjIyNC4xNTQ=

This indicator is not in our database.

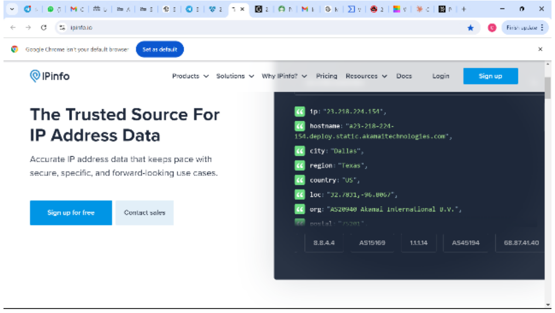
23.218.224.154

Very low risk
Returns PTR record
Hosted on common ISP

Integrations

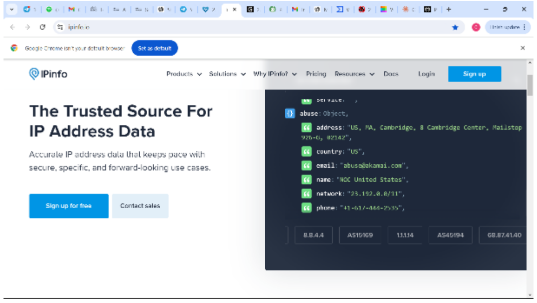
VirusTotal	Available in Pro
Shodan	Available in Pro
AbuseIPDB	Available in Pro

Highlights
a23-218-224-154.deploy.sta ... chnologies.com
Reverse DNS



```
ip: "23.218.224.154",
hostname: "a23-218-224-154.deploy.static.akamaitechnologies.com",
city: "Dallas",
region: "Texas",
country: "US",
loc: "32.7831,-96.8067",
org: "AS20940 Akamai International B.V.",
postal: "75201",
```

ipinfo.io
Google Chrome isn't your default browser
Set as default
IPinfo
Products
Solutions
Why IPinfo?
Pricing
Resources
Docs
Login
Sign up
The Trusted Source For IP Address Data
Accurate IP address data that keeps pace with secure, specific, and forward-looking use cases.
Sign up for free
Contact sales
8.8.4.4
AS15169
1.1.1.14
AS45194
68.87.41.40

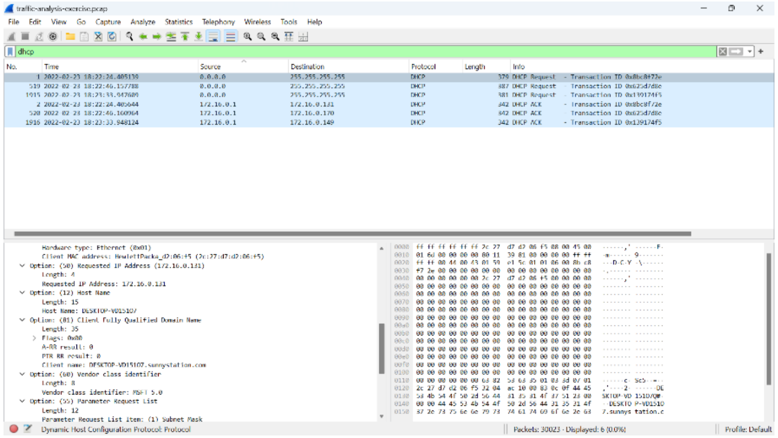


```
service: "",
abuse: Object,
  address: "US, MA, Cambridge, 8 Cambridge Center, Mailstop 926-G, 02142",
  country: "US",
  email: "abuse@akamai.com",
  name: "NOC United States",
  network: "23.192.0.0/11",
  phone: "+1-617-444-2535",
```

ipinfo.io
Google Chrome isn't your default browser
Set as default
IPinfo
Products
Solutions
Why IPinfo?
Pricing
Resources
Docs
Login
Sign up
The Trusted Source For IP Address Data
Accurate IP address data that keeps pace with secure, specific, and forward-looking use cases.
Sign up for free
Contact sales
8.8.4.4
AS15169
1.1.1.14
AS45194
68.87.41.40

2. **DHCP and Kerberos Filtering:**

- **DHCP Analysis**: Filtering for DHCP traffic revealed key information such as:
    - **Host Name**: DESKTOP-VD15107
    - **Client Name**: DESKTOP-VD15107.sunnystation.com
    - **Requested IP Address**: 172.16.0.131
    - **Client MAC Address**: HewlettPacka_d2:06:f5 This analysis suggests that the device with the MAC address 2c:27:d7:d2:06:f5 requested an IP address from the DHCP server, indicating its presence and activity within the network.

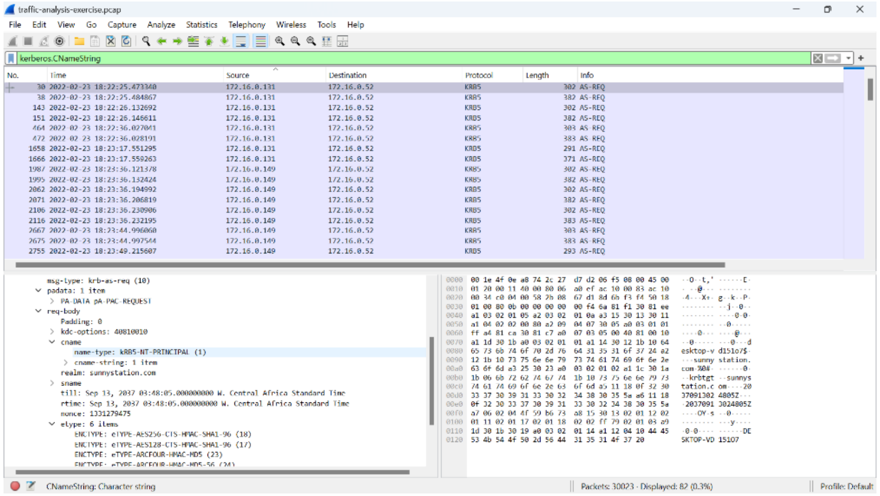


```
No.   Time                        Source      Destination       Protocol  Length  Info
    1 2022-02-23 18:22:24.405139  0.0.0.0     255.255.255.255   DHCP         379  DHCP Request  - Transaction ID 0x8bc8f72e
  519 2022-02-23 18:22:46.157788  0.0.0.0     255.255.255.255   DHCP         387  DHCP Request  - Transaction ID 0x625d7d8e
 1915 2022-02-23 18:23:33.947689  0.0.0.0     255.255.255.255   DHCP         381  DHCP Request  - Transaction ID 0x139174f5
    2 2022-02-23 18:22:24.405644  172.16.0.1  172.16.0.131      DHCP         342  DHCP ACK      - Transaction ID 0x8bc8f72e
  520 2022-02-23 18:22:46.160964  172.16.0.1  172.16.0.170      DHCP         342  DHCP ACK      - Transaction ID 0x625d7d8e
 1916 2022-02-23 18:23:33.948124  172.16.0.1  172.16.0.149      DHCP         342  DHCP ACK      - Transaction ID 0x139174f5
```

```
    Hardware type: Ethernet (0x01)
    Client MAC address: HewlettPacka_d2:06:f5 (2c:27:d7:d2:06:f5)
v Option: (50) Requested IP Address (172.16.0.131)
    Length: 4
    Requested IP Address: 172.16.0.131
v Option: (12) Host Name
    Length: 15
    Host Name: DESKTOP-VD15107
v Option: (81) Client Fully Qualified Domain Name
    Length: 35
  > Flags: 0x00
    A-RR result: 0
    PTR RR result: 0
    Client name: DESKTOP-VD15107.sunnystation.com
v Option: (60) Vendor class identifier
    Length: 8
    Vendor class identifier: MSFT 5.0
v Option: (55) Parameter Request List
    Length: 12
    Parameter Request List Item: (1) Subnet Mask
```

traffic-analysis-exercise.pcap
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
dhcp
Dynamic Host Configuration Protocol: Protocol
Packets: 30023 · Displayed: 6 (0.0%)
Profile: Default

- **Kerberos Authentication**: Filtering for Kerberos.CNameString revealed:
    - **CName**: kRB5-NT-PRINCIPAL (1) This indicates an ongoing Kerberos authentication process, with potential anomalies needing further investigation.



```
traffic-analysis-exercise.pcap
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help
kerberos.CNameString

No.   Time                        Source        Destination   Protocol  Length Info
   30 2022-02-23 18:22:25.473340  172.16.0.131  172.16.0.52   KRB5       302 AS-REQ
   38 2022-02-23 18:22:25.484867  172.16.0.131  172.16.0.52   KRB5       382 AS-REQ
  143 2022-02-23 18:22:26.132692  172.16.0.131  172.16.0.52   KRB5       302 AS-REQ
  151 2022-02-23 18:22:26.146611  172.16.0.131  172.16.0.52   KRB5       382 AS-REQ
  464 2022-02-23 18:22:36.027041  172.16.0.131  172.16.0.52   KRB5       303 AS-REQ
  472 2022-02-23 18:22:36.028191  172.16.0.131  172.16.0.52   KRB5       383 AS-REQ
 1658 2022-02-23 18:23:17.551295  172.16.0.131  172.16.0.52   KRB5       291 AS-REQ
 1666 2022-02-23 18:23:17.559263  172.16.0.131  172.16.0.52   KRB5       371 AS-REQ
 1987 2022-02-23 18:23:36.121378  172.16.0.149  172.16.0.52   KRB5       302 AS-REQ
 1995 2022-02-23 18:23:36.132424  172.16.0.149  172.16.0.52   KRB5       382 AS-REQ
 2062 2022-02-23 18:23:36.194992  172.16.0.149  172.16.0.52   KRB5       302 AS-REQ
 2071 2022-02-23 18:23:36.206819  172.16.0.149  172.16.0.52   KRB5       382 AS-REQ
 2106 2022-02-23 18:23:36.230906  172.16.0.149  172.16.0.52   KRB5       302 AS-REQ
 2116 2022-02-23 18:23:36.232195  172.16.0.149  172.16.0.52   KRB5       383 AS-REQ
 2667 2022-02-23 18:23:44.996060  172.16.0.149  172.16.0.52   KRB5       303 AS-REQ
 2675 2022-02-23 18:23:44.997544  172.16.0.149  172.16.0.52   KRB5       383 AS-REQ
 2755 2022-02-23 18:23:49.215607  172.16.0.149  172.16.0.52   KRB5       293 AS-REQ
```

```
    msg-type: krb-as-req (10)
  ∨ padata: 1 item
    > PA-DATA pA-PAC-REQUEST
  ∨ req-body
      Padding: 0
    > kdc-options: 40810010
    ∨ cname
        name-type: kRB5-NT-PRINCIPAL (1)
      > cname-string: 1 item
      realm: sunnystation.com
    > sname
      till: Sep 13, 2037 03:48:05.000000000 W. Central Africa Standard Time
      rtime: Sep 13, 2037 03:48:05.000000000 W. Central Africa Standard Time
      nonce: 1331279475
    ∨ etype: 6 items
        ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
        ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
        ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
        ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5-56 (24)
```

```
0000  00 1e 4f 0e a8 74 2c 27  d7 d2 06 f5 08 00 45 00   ··O··t,' ······E·
0010  01 20 00 11 40 00 80 06  a0 cf ac 10 00 83 ac 10   · ··@··· ········
0020  00 34 c0 04 00 58 2b 08  67 d1 8d 6b f3 f4 50 18   ·4···X+· g··k··P·
0030  01 00 80 0b 00 00 00 00  00 f4 6a 81 f1 30 81 ee   ········ ··j··0··
0040  a1 03 02 01 05 a2 03 02  01 0a a3 15 30 13 30 11   ········ ····0·0·
0050  a1 04 02 02 00 80 a2 09  04 07 30 05 a0 03 01 01   ········ ··0·····
0060  ff a4 81 ca 30 81 c7 a0  07 03 05 00 40 81 00 10   ····0··· ····@···
0070  a1 1d 30 1b a0 03 02 01  01 a1 14 30 12 1b 10 64   ··0····· ···0···d
0080  65 73 6b 74 6f 70 2d 76  64 31 35 31 6f 37 24 a2   esktop-v d151o7$·
0090  12 1b 10 73 75 6e 6e 79  73 74 61 74 69 6f 6e 2e   ···sunny station.
00a0  63 6f 6d a3 25 30 23 a0  03 02 01 02 a1 1c 30 1a   com·%0#· ······0·
00b0  1b 06 6b 72 62 74 67 74  1b 10 73 75 6e 6e 79 73   ··krbtgt ··sunnys
00c0  74 61 74 69 6f 6e 2e 63  6f 6d a5 11 18 0f 32 30   tation.c om····20
00d0  33 37 30 39 31 33 30 32  34 38 30 35 5a a6 11 18   37091302 4805Z···
00e0  0f 32 30 33 37 30 39 31  33 30 32 34 38 30 35 5a   ·2037091 3024805Z
00f0  a7 06 02 04 4f 59 b6 73  a8 15 30 13 02 01 12 02   ····OY·s ··0·····
0100  01 11 02 01 17 02 01 18  02 02 ff 79 02 01 03 a9   ········ ···y····
0110  1d 30 1b 30 19 a0 03 02  01 14 a1 12 04 10 44 45   ·0·0···· ······DE
0120  53 4b 54 4f 50 2d 56 44  31 35 31 4f 37 20         SKTOP-VD 151O7
```

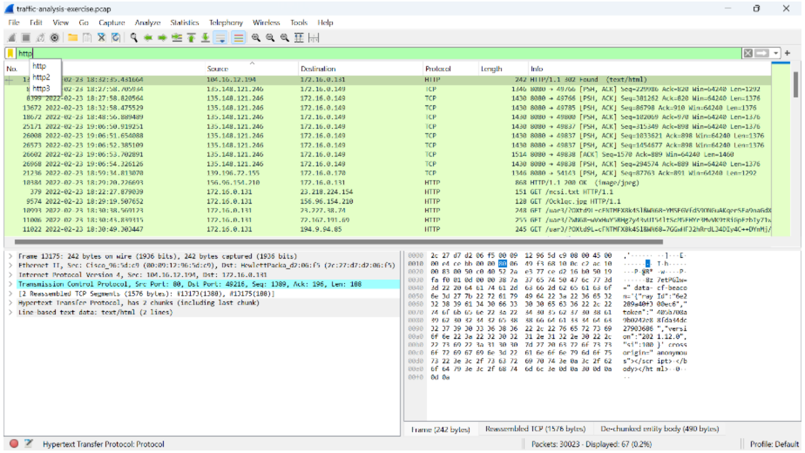
```
CNameString: Character string          Packets: 30023 · Displayed: 82 (0.3%)          Profile: Default
```

Protocol Hierarchy and Expert Information:

- **Protocol Analysis**: The protocol hierarchy showed a significant presence of IPv4 and TCP protocols. The Expert Information feature in Wireshark highlighted potential anomalies, including protocol errors and suspicious traffic patterns, assisting in identifying areas of concern.

Endpoint and Geolocation Analysis:

- **Endpoint Analysis**: The analysis of endpoints revealed communication between devices using various MAC addresses and IPs. For instance, the device HewlettPacka_d2:06:f5 communicated with several IP addresses, with geolocation data indicating their physical origins. This information was crucial in identifying potential external threats and internal vulnerabilities.



```
traffic-analysis-exercise.pcap
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help
http
    http
    http2
    http3

No.   Time                         Source           Destination     Protocol Length Info
 1           02-23 18:32:35.431664  104.16.12.194    172.16.0.131    HTTP      242 HTTP/1.1 302 Found  (text/html)
             02-23 18:27:58.705934  135.148.121.246  172.16.0.149    TCP      1346 8080 → 49766 [PSH, ACK] Seq=229986 Ack=820 Win=64240 Len=1292
  8399 2022-02-23 18:27:58.820564  135.148.121.246  172.16.0.149    TCP      1430 8080 → 49766 [PSH, ACK] Seq=381262 Ack=820 Win=64240 Len=1376
 13672 2022-02-23 18:32:58.475529  135.148.121.246  172.16.0.149    TCP      1430 8080 → 49785 [PSH, ACK] Seq=86798 Ack=910 Win=64240 Len=1376
 18672 2022-02-23 18:48:56.889489  135.148.121.246  172.16.0.149    TCP      1430 8080 → 49800 [PSH, ACK] Seq=102069 Ack=970 Win=64240 Len=1376
 25171 2022-02-23 19:06:50.919251  135.148.121.246  172.16.0.149    TCP      1430 8080 → 49837 [PSH, ACK] Seq=315349 Ack=898 Win=64240 Len=1376
 26008 2022-02-23 19:06:51.654088  135.148.121.246  172.16.0.149    TCP      1430 8080 → 49837 [PSH, ACK] Seq=1033621 Ack=898 Win=64240 Len=1376
 26573 2022-02-23 19:06:52.385109  135.148.121.246  172.16.0.149    TCP      1430 8080 → 49837 [PSH, ACK] Seq=1454677 Ack=898 Win=64240 Len=1376
 26602 2022-02-23 19:06:53.702891  135.148.121.246  172.16.0.149    TCP      1514 8080 → 49838 [ACK] Seq=1570 Ack=889 Win=64240 Len=1460
 26968 2022-02-23 19:06:54.326126  135.148.121.246  172.16.0.149    TCP      1430 8080 → 49838 [PSH, ACK] Seq=294574 Ack=889 Win=64240 Len=1376
 21236 2022-02-23 18:59:34.813070  139.196.72.155   172.16.0.170    TCP      1346 8080 → 54143 [PSH, ACK] Seq=87763 Ack=891 Win=64240 Len=1292
 10384 2022-02-23 18:29:20.226693  156.96.154.210   172.16.0.131    HTTP      868 HTTP/1.1 200 OK  (image/jpeg)
   379 2022-02-23 18:22:27.879039  172.16.0.131     23.218.224.154  HTTP      151 GET /ncsi.txt HTTP/1.1
  9574 2022-02-23 18:29:19.507652  172.16.0.131     156.96.154.210  HTTP      128 GET /Ocklqc.jpg HTTP/1.1
 10993 2022-02-23 18:30:38.560123  172.16.0.131     23.227.38.74    HTTP      248 GET /uar3/?0Xtd9L-cFNTMFX8k4Sl8WN68-YM5FGVfd59ONGuAKqerSFa9naGdX
 11006 2022-02-23 18:30:43.839315  172.16.0.131     72.167.191.69   HTTP      255 GET /uar3/?WN68-wVxHuY5RHg7y43vUT54ltScM5FHYr3MvVK9tRiGpFzbIy71w
 11022 2022-02-23 18:30:49.303447  172.16.0.131     194.9.94.85     HTTP      245 GET /uar3/?0Xtd9L-cFNTMFX8k4S18WN68-7GGwHF32hRrdL34DIy4C++DYnMj/
```

```
> Frame 13175: 242 bytes on wire (1936 bits), 242 bytes captured (1936 bits)
> Ethernet II, Src: Cisco_96:5d:c9 (00:09:12:96:5d:c9), Dst: HewlettPacka_d2:06:f5 (2c:27:d7:d2:06:f5)
> Internet Protocol Version 4, Src: 104.16.12.194, Dst: 172.16.0.131
> Transmission Control Protocol, Src Port: 80, Dst Port: 49216, Seq: 1389, Ack: 196, Len: 108
> [2 Reassembled TCP Segments (1576 bytes): #13173(1380), #13175(108)]
> Hypertext Transfer Protocol, has 2 chunks (including last chunk)
> Line-based text data: text/html (2 lines)
```

```
0000  2c 27 d7 d2 06 f5 00 09  12 96 5d c9 08 00 45 00   ,'······ ··]···E·
0010  00 e4 ce bb 00 00 80 06  49 f3 68 10 0c c2 ac 10   ········ I·h·····
0020  00 83 00 50 c0 40 52 2a  e3 77 ce d2 16 b0 50 19   ···P·@R* ·w····P·
0030  fa f0 01 0d 00 00 38 7a  37 65 74 50 47 6c 77 3d   ······8z 7etPGlw=
0040  3d 22 20 64 61 74 61 2d  63 66 2d 62 65 61 63 6f   =" data- cf-beaco
0050  6e 3d 27 7b 22 72 61 79  49 64 22 3a 22 36 65 32   n='{"ray Id":"6e2
0060  32 38 39 61 34 30 66 33  30 30 65 63 36 22 2c 22   289a40f3 00ec6","
0070  74 6f 6b 65 6e 22 3a 22  34 30 35 62 37 30 38 61   token":" 405b708a
0080  39 62 30 32 34 32 65 38  38 66 64 61 33 34 64 63   9b0242e8 8fda34dc
0090  32 37 39 30 33 36 38 36  22 2c 22 76 65 72 73 69   27903686 ","versi
00a0  6f 6e 22 3a 22 32 30 32  31 2e 31 32 2e 30 22 2c   on":"202 1.12.0",
00b0  22 73 69 22 3a 31 30 30  7d 27 20 63 72 6f 73 73   "si":100 }' cross
00c0  6f 72 69 67 69 6e 3d 22  61 6e 6f 6e 79 6d 6f 75   origin=" anonymou
00d0  73 22 3e 3c 2f 73 63 72  69 70 74 3e 0a 3c 2f 62   s"></scr ipt>·</b
00e0  6f 64 79 3e 3c 2f 68 74  6d 6c 3e 0d 0a 30 0d 0a   ody></ht ml>··0··
00f0  0d 0a                                              ··
```

```
Frame (242 bytes)   Reassembled TCP (1576 bytes)   De-chunked entity body (490 bytes)
Hypertext Transfer Protocol: Protocol          Packets: 30023 · Displayed: 67 (0.2%)          Profile: Default
```

In summary

No malicious activity was found when the network traffic connected to IP address 23.218.224.154 was analyzed. Nonetheless, keeping a safe network environment requires close observation and exhaustive research. The organization's capacity to identify and respond to any threats in the future will be greatly enhanced by putting both short- and long-term recommendations into practice, such as strengthening real-time monitoring, updating security protocols, and offering continual employee training. Even if there were no direct threats found, the network needs to be protected from ever-changing cyber threats, so keeping an eye out and taking preventative measures is crucial.

Recommendations

Short-Term Recommendations:

1. **Quarantine Suspicious IPs:** Although the IP address 23.218.224.154 was not flagged for malicious activity, it is still recommended to monitor any unusual traffic associated with this IP and quarantine any suspicious activity.
2. **Monitor Network Traffic:** Implement real-time monitoring and filtering for potentially harmful traffic, particularly from external sources, to promptly identify and respond to threats.
3. **Conduct a Thorough Investigation:** Further analyze the network traffic and involved IPs to ensure no other indicators of compromise are present.

Long-Term Recommendations:

1. **Enhance Network Security Posture:** Strengthen network security by implementing advanced threat detection and response solutions to protect against potential future threats.
2. **Update Security Protocols:** Regularly review and update security protocols to adapt to new and emerging threats, ensuring the network remains resilient against sophisticated attacks.
3. **Employee Security Awareness Training:** Conduct continuous training sessions for employees on cybersecurity best practices, focusing on recognizing and avoiding potential threats.

Lesson learned

This analysis highlights the importance of continuous monitoring and timely response to potential threats. By maintaining up-to-date security measures, including network segmentation and regular audits, organizations can better protect their networks from evolving threats.