LAB 06 – GRAYLOG HUNTING

INSTRUCTIONS

The lab employs Graylog server and provided data to investigate the effectiveness of leveraging several sensors deployed in a small geographic area. The objective is to detect various attacks and conduct real-time analysis, complemented by historical data for context and insight.

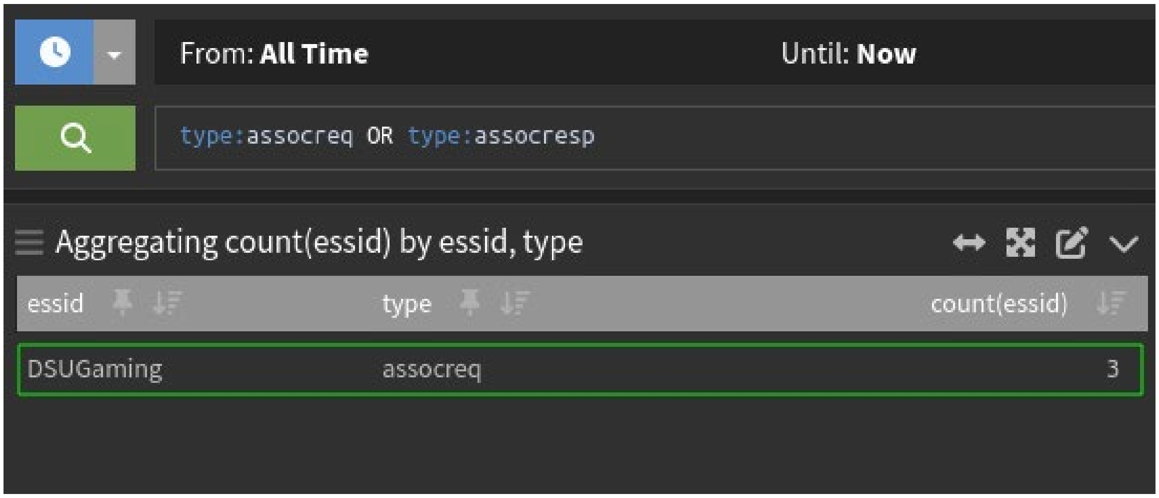
Given the utilization of real-world 802.11 traffic, the detection of irrelevant signals (aka: The Neighbors) is anticipated. In an effort to leave the neighbors alone, the only SSIDs we will use for this lab will be GoTrojans, CubeFarm, CHP, Vlads_Place, Putin_Home, gencyber, DSUnix, DSUmobile, DSUGaming, eduroam, GoCrony!, FreeCandy, IA_IOT and Guest. You can safely ignore all other SSID's.

Note: it is recommended to verify certain findings using an OUI reference tool.

QUESTIONS

[1] WHAT NETWORK HAS THE MOST ASSOCIATION FRAMES?

DSUGaming



From: **All Time** Until: **Now**

```
type:assocreq OR type:assocresp
```

Aggregating count(essid) by essid, type

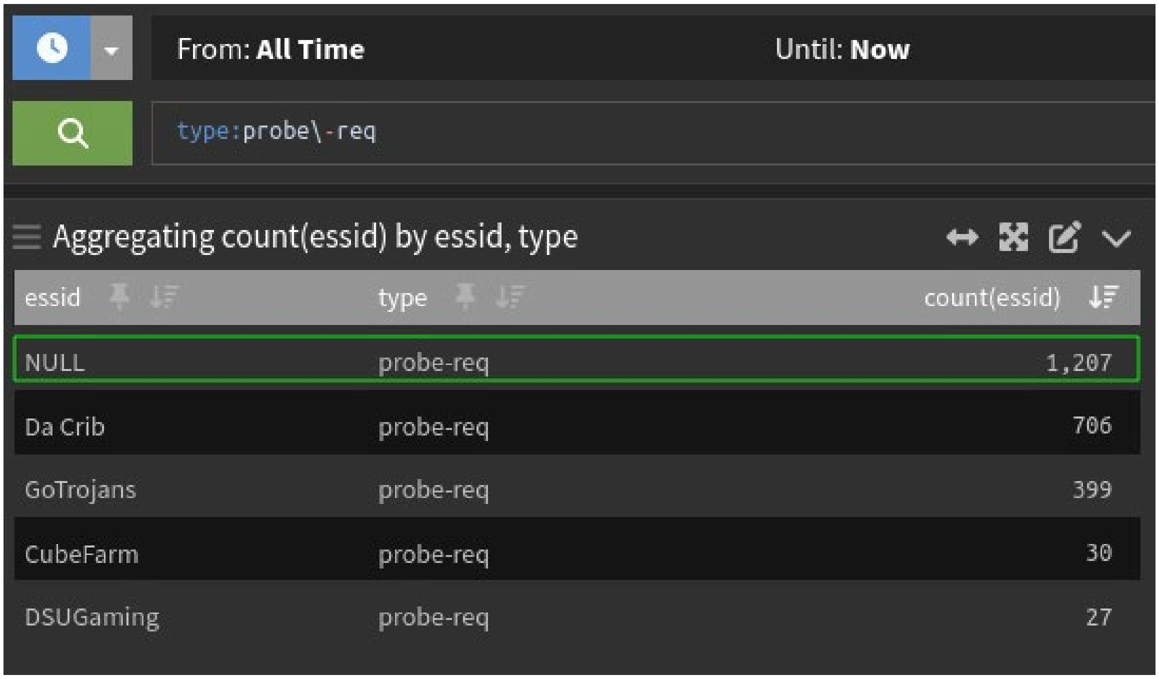
essid	type	count(essid)
DSUGaming	assocreq	3

1.1 - *Association frame count by network, filtering for assocreq and assocresp types*

[2] WHICH NETWORK HAS THE MOST PROBE REQUESTS? WHY ARE MOST PROBES WILDCARDS (OR NULL)?

"NULL" has the most probe requests.

Most probe requests are NULL or Wildcards because they function as "searching" probes. Unlike "directed" probes, which specifically request connection from certain access points, these broadcast probe requests are sent by client devices to all nearby access points. By using wildcards or null values, the client can broadcast their request and discover available networks within range without specifying a particular Service Set Identifier (SSID) or other parameters.



From: **All Time** Until: **Now**

type:probe\-req

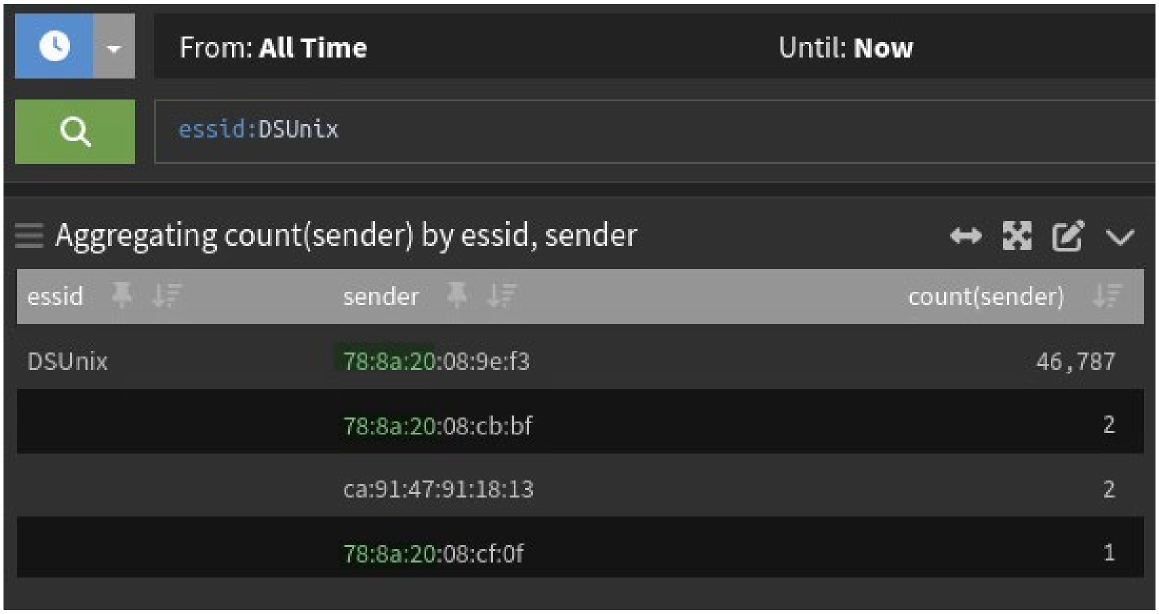
Aggregating count(essid) by essid, type

essid	type	count(essid)
NULL	probe-req	1,207
Da Crib	probe-req	706
GoTrojans	probe-req	399
CubeFarm	probe-req	30
DSUGaming	probe-req	27

2.1 - *Aggregated probe request count by ESSID and type, filtered for 'type:probe-req'*

[3] Who is the manufacturer of the network DSUnix?

Ubiquiti Inc



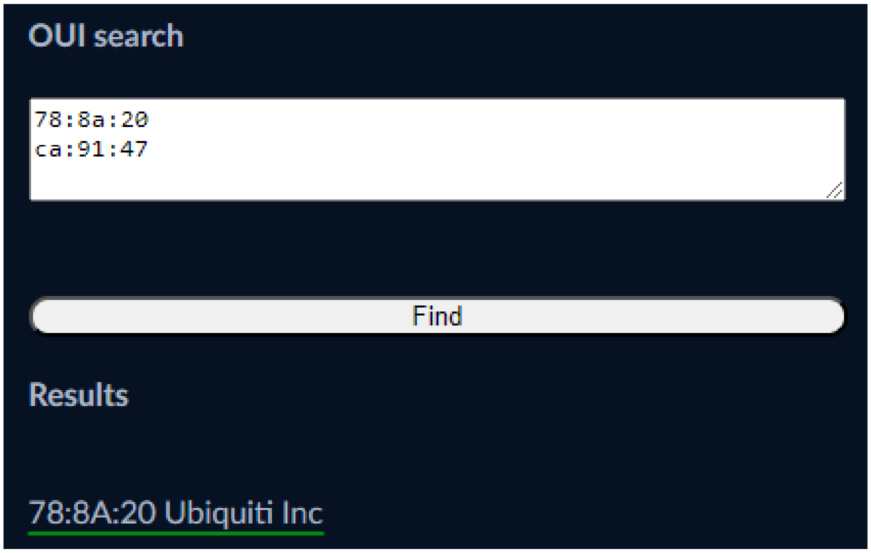
From: **All Time** Until: **Now**

essid:DSUnix

Aggregating count(sender) by essid, sender

essid	sender	count(sender)
DSUnix	78:8a:20:08:9e:f3	46,787
	78:8a:20:08:cb:bf	2
	ca:91:47:91:18:13	2
	78:8a:20:08:cf:0f	1

3.1 - *BSSID for the network 'DSUnix' based on the aggregated count of sender MAC addresses, filtered for 'essid:DSUnix'*



OUI search

```
78:8a:20
ca:91:47
```

Results

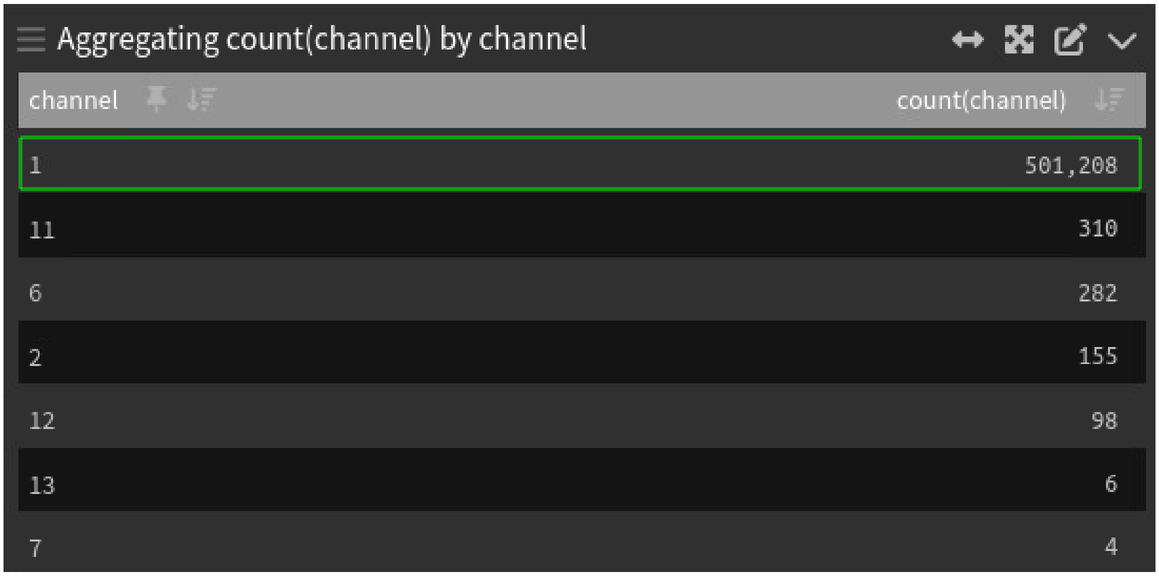
78:8A:20 Ubiquiti Inc

3.2 - *OUI search results for the MAC addresses associated with the network 'DSUnix'*

---

[4] What is the most popular channel in use?

Channel 1



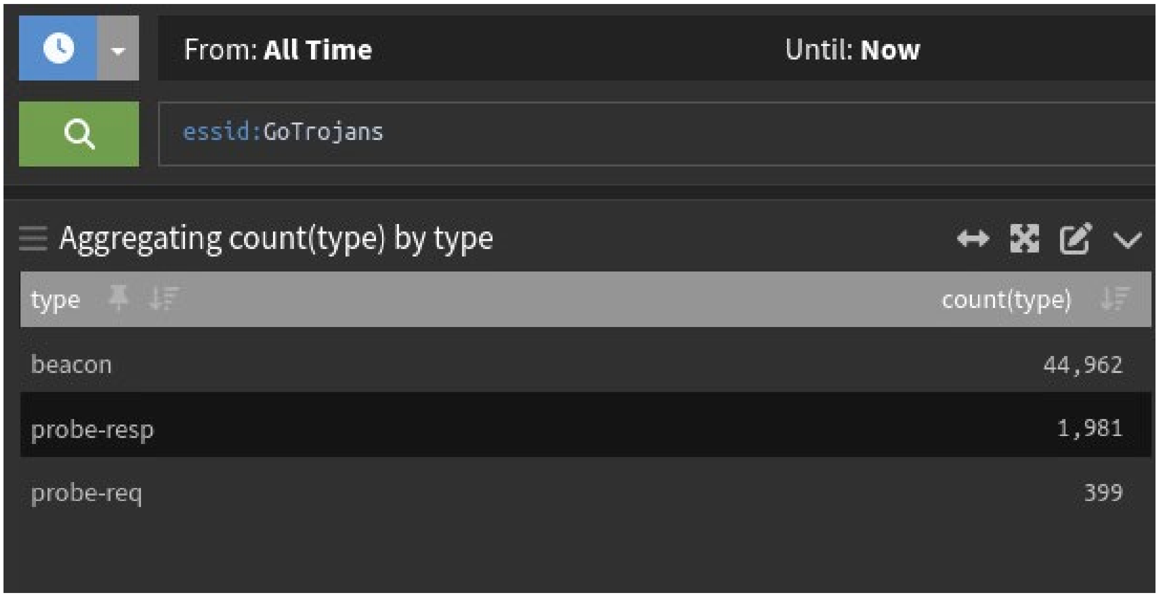
Aggregating count(channel) by channel

channel	count(channel)
1	501,208
11	310
6	282
2	155
12	98
13	6
7	4

4.1 - *Aggregating count of channels to determine the most popular channel in use*

[5] How many association requests exist for GoTrojans?

There are 0 association requests for GoTrojans



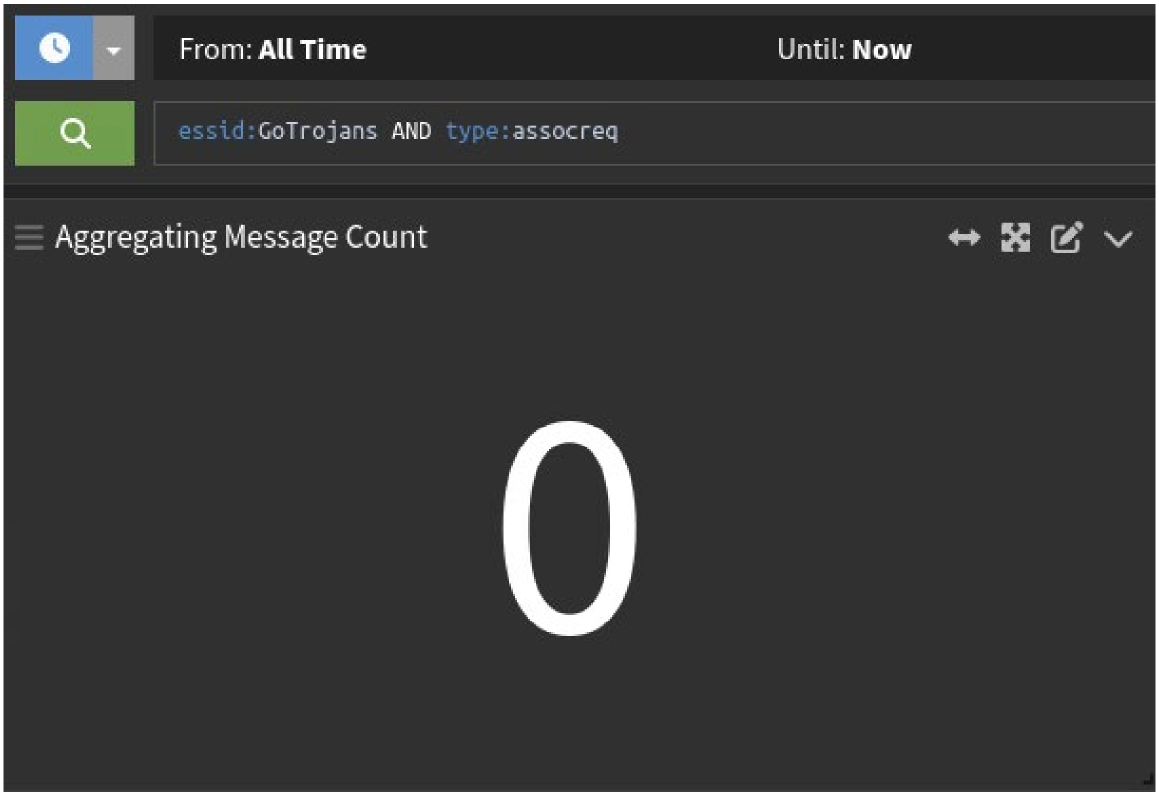
From: **All Time** Until: **Now**

```
essid:GoTrojans
```

Aggregating count(type) by type

type	count(type)
beacon	44,962
probe-resp	1,981
probe-req	399

5.1 - *Aggregating count of association requests for the network 'GoTrojans'.*



From: **All Time** Until: **Now**

```
essid:GoTrojans AND type:assocreq
```

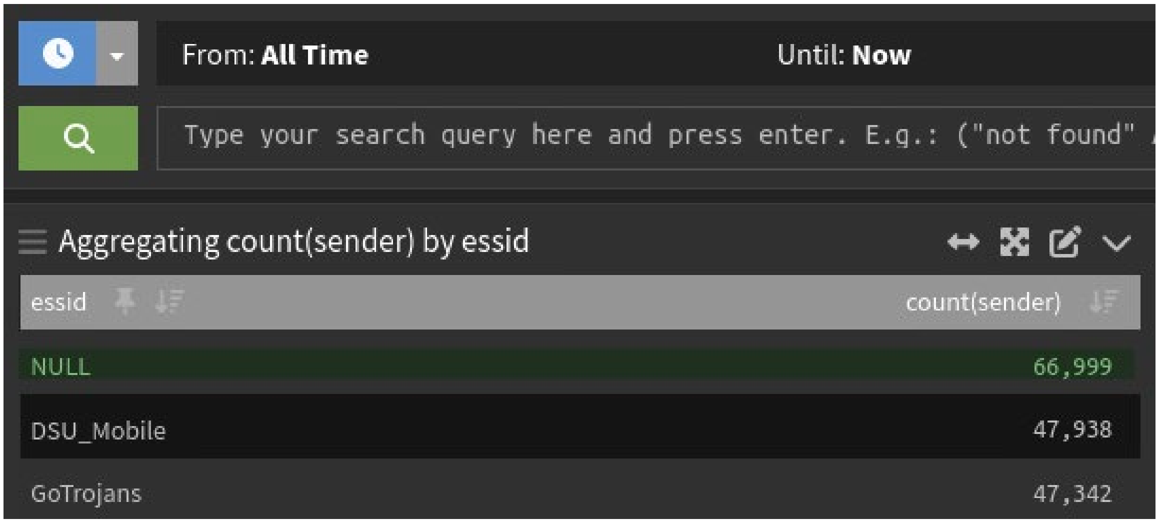
Aggregating Message Count

0

5.2 - *Verification figure: Aggregating count of association requests for the network 'GoTrojans' with the filter 'type:assocreq'.*

[6] Identify the SSID with the most BSSIDs

Most Overall: (1) NULL, (2) DSU_Mobile

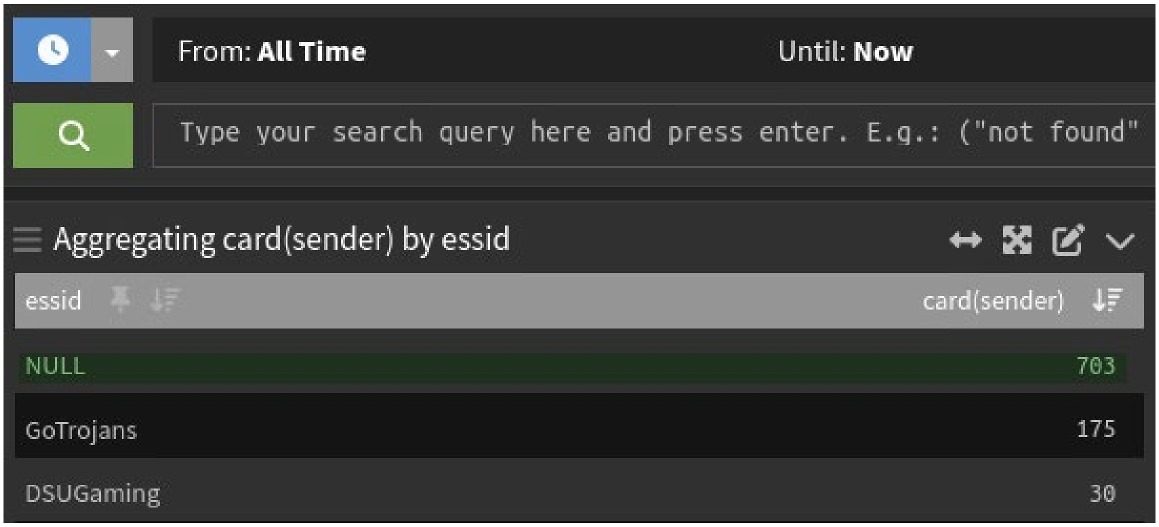

From: All Time
Until: Now
Type your search query here and press enter. E.g.: ("not found"

Aggregating count(sender) by essid

essid	count(sender)
NULL	66,999
DSU_Mobile	47,938
GoTrojans	47,342

6.1 - *Aggregating count of BSSIDs by SSID across all networks.*

Most Unique: (1) NULL, (2) GoTrojans


From: All Time
Until: Now
Type your search query here and press enter. E.g.: ("not found"

Aggregating card(sender) by essid

essid	card(sender)
NULL	703
GoTrojans	175
DSUGaming	30

6.2 - *Aggregating cardinality of BSSIDs by SSID across all networks*

[7] A deauth attack occurred. Those are super annoying. What client was attacked specifically?

There is a mutual deauthentication attack being executed by 00:c0:ca:a7:7f:6d, associated with Alfa, Inc., and 34:fc:b9:7b:94:22, linked to Hewlett Packard Enterprise (HPE). In this exchange, a total of 1,392 deauthentication frames were exchanged. (7.1) (7.2)

Initially, it appeared that Alfa faced a deauthentication attack from HPE, which sent 722 deauthentication frames. In a potential retaliatory or automated response to this attack, it seemed that Alfa responded with 670 deauthentication frames.

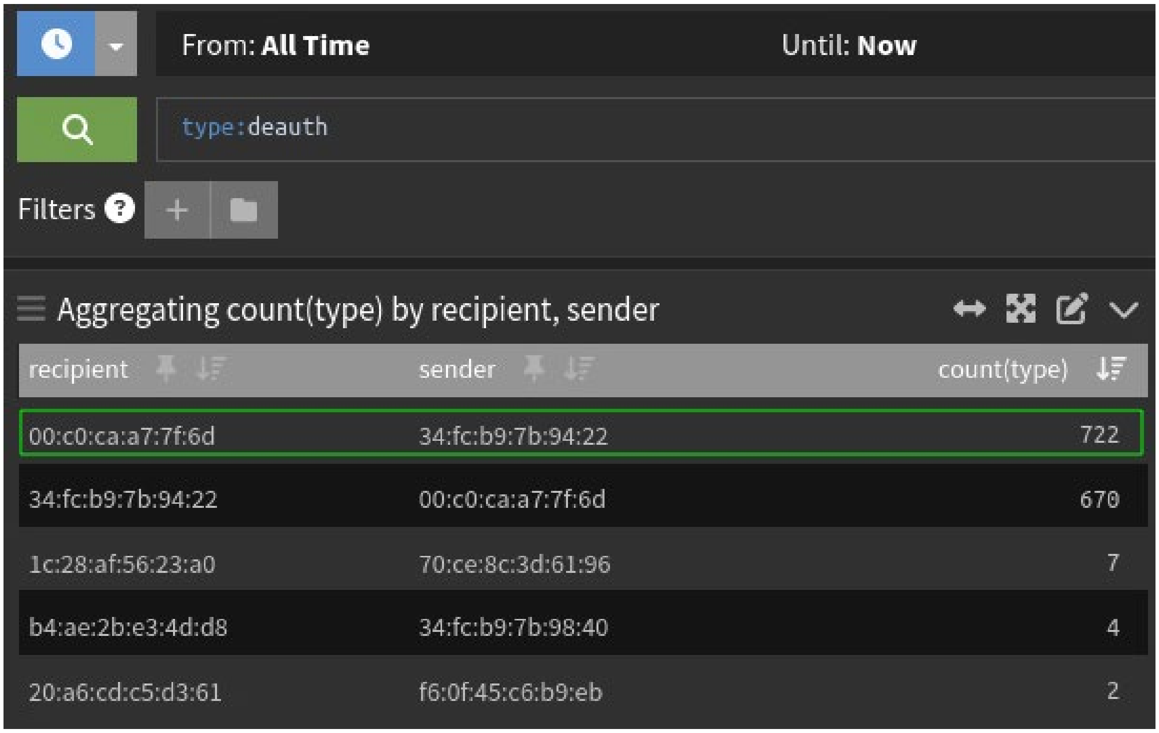
However, a closer look at timestamps (7.3) revealed that the initial deauthentication frames originated from Alfa to HPE, which altered my interpretation of the attack. Given this new information, there are a few potential scenarios:

1) HPE as a Malicious Entity: HPE may have engaged in malicious behavior on the network. Alfa detected suspicious activity or anomalies and initiated a legitimate deauthentication process. In response to being discovered, HPE launched a deauthentication attack, which caused Alfa to respond with its own attack.

2) Alfa as a Malicious Entity: Despite HPE's legitimate presence on the network, Alfa initiated a malicious deauthentication attack against HPE. In this scenario, the attack by HPE was retaliatory in nature.

3) Mutual Misunderstanding: Both Alfa and HPE may have misinterpreted each other's actions or network behavior, which lead to a cycle of defensive responses.

4) Third-Party Interference: In an attempted network-based denial-of-service (DoS) attack, an external device may have instigated the deauthentication attack between Alfa and HPE, causing both of them to responded defensively

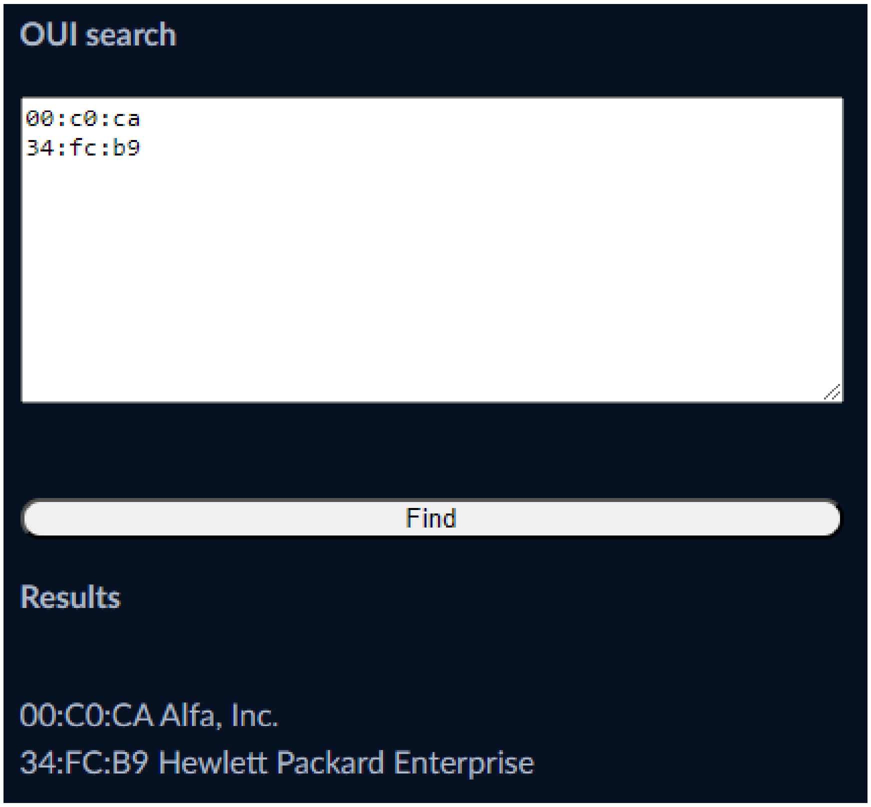


type:deauth

Aggregating count(type) by recipient, sender

recipient	sender	count(type)
00:c0:ca:a7:7f:6d	34:fc:b9:7b:94:22	722
34:fc:b9:7b:94:22	00:c0:ca:a7:7f:6d	670
1c:28:af:56:23:a0	70:ce:8c:3d:61:96	7
b4:ae:2b:e3:4d:d8	34:fc:b9:7b:98:40	4
20:a6:cd:c5:d3:61	f6:0f:45:c6:b9:eb	2

7.1 - *Aggregating count of deauthentication frames by recipient and sender to identify the attacked client.*



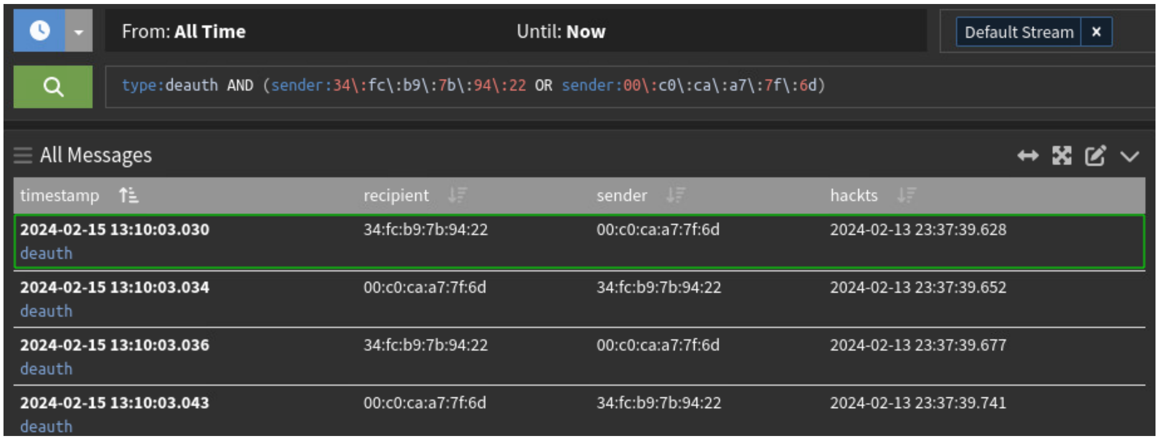
OUI search

```
00:c0:ca
34:fc:b9
```

Results

00:C0:CA Alfa, Inc.
34:FC:B9 Hewlett Packard Enterprise

7.2 - *OUI Lookup Results for Devices Involved in the Deauthentication Attack*



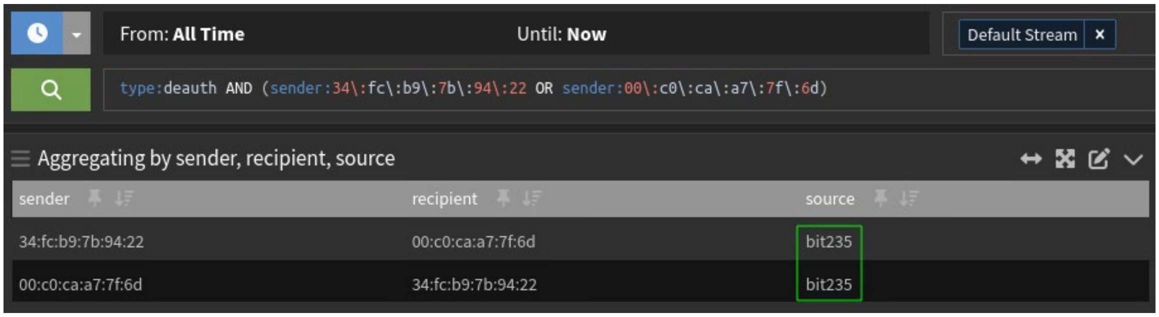
```
type:deauth AND (sender:34\:fc\:b9\:7b\:94\:22 OR sender:00\:c0\:ca\:a7\:7f\:6d)
```

timestamp	recipient	sender	hackts
2024-02-15 13:10:03.030 deauth	34:fc:b9:7b:94:22	00:c0:ca:a7:7f:6d	2024-02-13 23:37:39.628
2024-02-15 13:10:03.034 deauth	00:c0:ca:a7:7f:6d	34:fc:b9:7b:94:22	2024-02-13 23:37:39.652
2024-02-15 13:10:03.036 deauth	34:fc:b9:7b:94:22	00:c0:ca:a7:7f:6d	2024-02-13 23:37:39.677
2024-02-15 13:10:03.043 deauth	00:c0:ca:a7:7f:6d	34:fc:b9:7b:94:22	2024-02-13 23:37:39.741

7.3 - *Timestamp Analysis for the Deauthentication Attack between Devices 34:fc:b9:7b:94:22 and 00:c0:ca:a7:7f:6d*

[8] Around where did the deauth attack take place (hint: think of the sensor names here, as they're room numbers).

BIT235 – Beacom Institute of Technology, Room 235



From: **All Time** Until: **Now**

```
type:deauth AND (sender:34\:fc\:b9\:7b\:94\:22 OR sender:00\:c0\:ca\:a7\:7f\:6d)
```

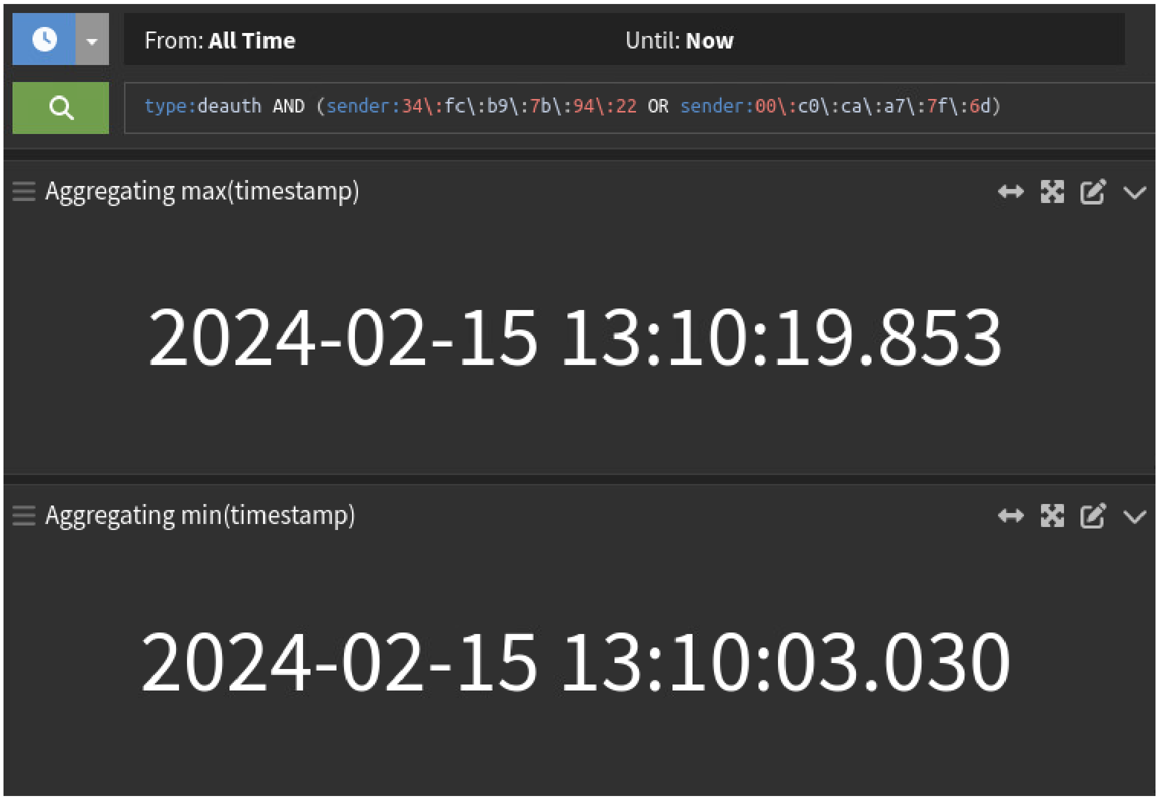
Aggregating by sender, recipient, source

sender	recipient	source
34:fc:b9:7b:94:22	00:c0:ca:a7:7f:6d	bit235
00:c0:ca:a7:7f:6d	34:fc:b9:7b:94:22	bit235

8.1 - *Source Analysis for the Deauthentication Attack Between Devices 34:fc:b9:7b:94:22 and 00:c0:ca:a7:7f:6d.*

[9] What time did the deauth attack take place?

The deauthentication attack took place from *2024-02-15 13:10:03.030* to *2024-02-15 13:10:19.853*



From: **All Time** Until: **Now**

```
type:deauth AND (sender:34\:fc\:b9\:7b\:94\:22 OR sender:00\:c0\:ca\:a7\:7f\:6d)
```

Aggregating max(timestamp)

2024-02-15 13:10:19.853

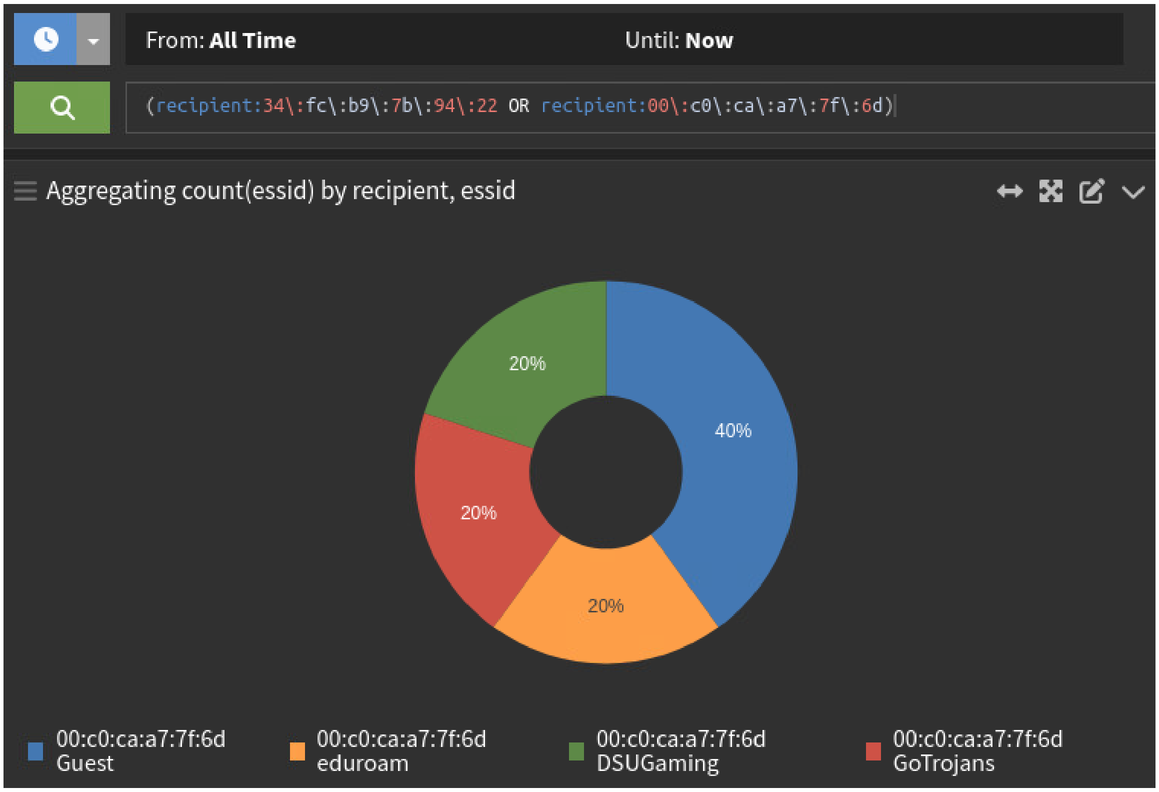
Aggregating min(timestamp)

2024-02-15 13:10:03.030

9.1 - *Timestamp Range for the Deauthentication Attack Between Devices 34:fc:b9:7b:94:22 and 00:c0:ca:a7:7f:6d.*

[10] Identify the SSID or network that the client was DoS'd from in the deauth attack

The primary network the client was DoS'd from in the deauth attack was Guest



From: **All Time** Until: **Now**

```
(recipient:34\:fc\:b9\:7b\:94\:22 OR recipient:00\:c0\:ca\:a7\:7f\:6d)
```

Aggregating count(essid) by recipient, essid

20%
40%
20%
20%
🟦 00:c0:ca:a7:7f:6d Guest
🟧 00:c0:ca:a7:7f:6d eduroam
🟩 00:c0:ca:a7:7f:6d DSUGaming
🟥 00:c0:ca:a7:7f:6d GoTrojans

10.1 - *SSID Distribution for the Deauthentication Attack on Client (00:c0:ca:a7:7f:6d OR 34:fc:b9:7b:94:22)*