Synapse Bootcamp - Module 17

Network Infrastructure Analysis - Answer Key

Answer Key

Analyzing and Identifying Network Infrastructure

Exercise 1 Answer

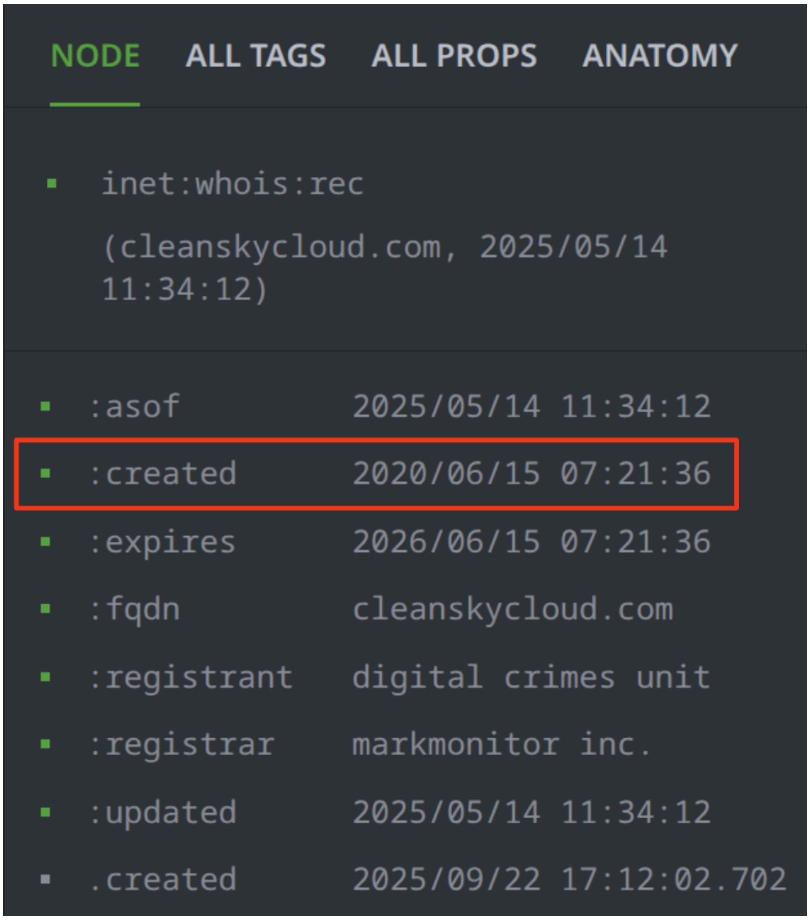
Objective:

- **Use Power-Ups to obtain network-based data and characterize network infrastructure.**

Part 1 - Enriching Data with the NetTools Power-Up - Whois data

Question 1: Based on this current whois record, when was the FQDN registered?

- The FQDN was registered on **June 15, 2020** (2020/06/15):

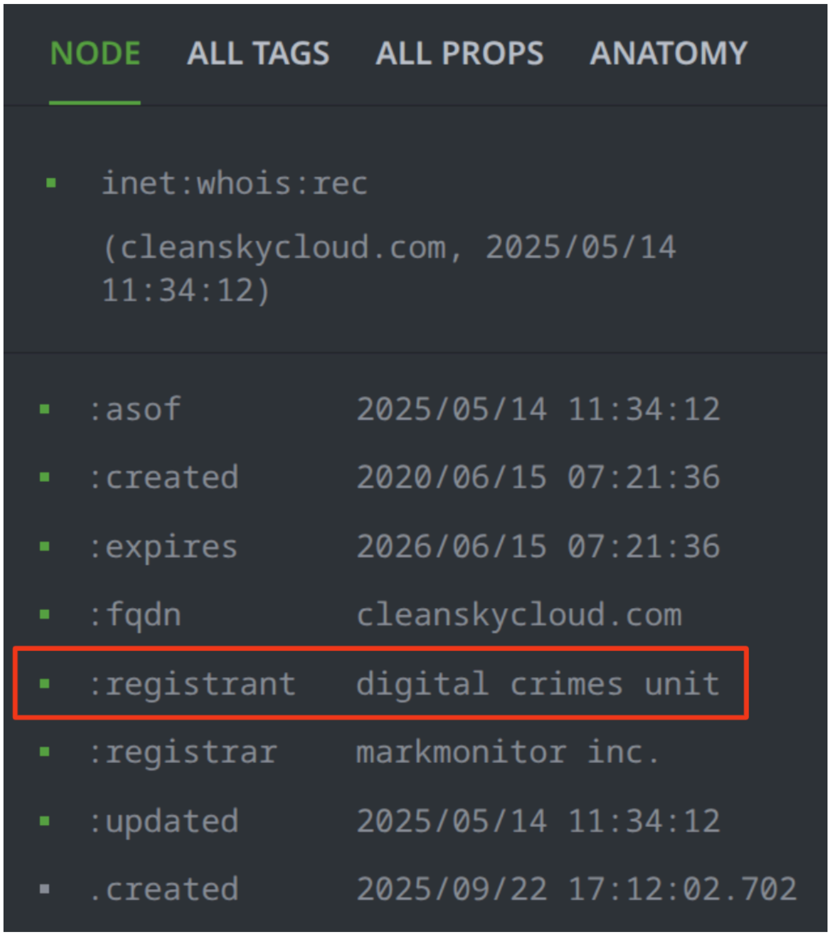


```
inet:whois:rec
(cleanskycloud.com, 2025/05/14
11:34:12)

:asof         2025/05/14 11:34:12
:created      2020/06/15 07:21:36
:expires      2026/06/15 07:21:36
:fqdn         cleanskycloud.com
:registrant   digital crimes unit
:registrar    markmonitor inc.
:updated      2025/05/14 11:34:12
.created      2025/09/22 17:12:02.702
```

Question 2: Who is the **registrant** for the FQDN?

- The registrant is **digital crimes unit**:

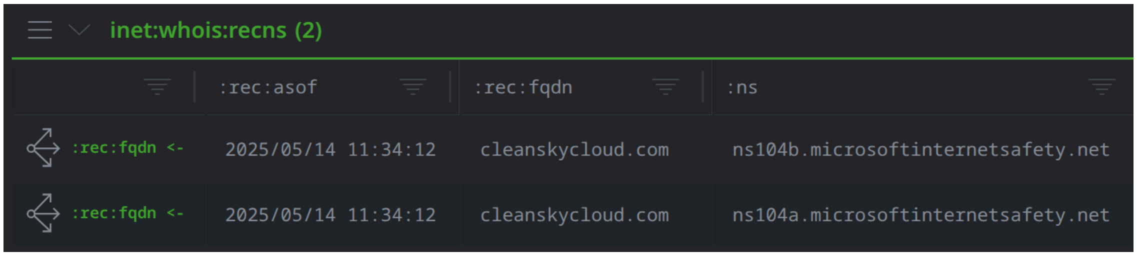


```
▪ inet:whois:rec
  (cleanskycloud.com, 2025/05/14
  11:34:12)

▪ :asof         2025/05/14 11:34:12
▪ :created      2020/06/15 07:21:36
▪ :expires      2026/06/15 07:21:36
▪ :fqdn         cleanskycloud.com
▪ :registrant   digital crimes unit
▪ :registrar    markmonitor inc.
▪ :updated      2025/05/14 11:34:12
▪ .created      2025/09/22 17:12:02.702
```

Question 3: Based on the whois data, what DNS **name servers** are used by the FQDN?

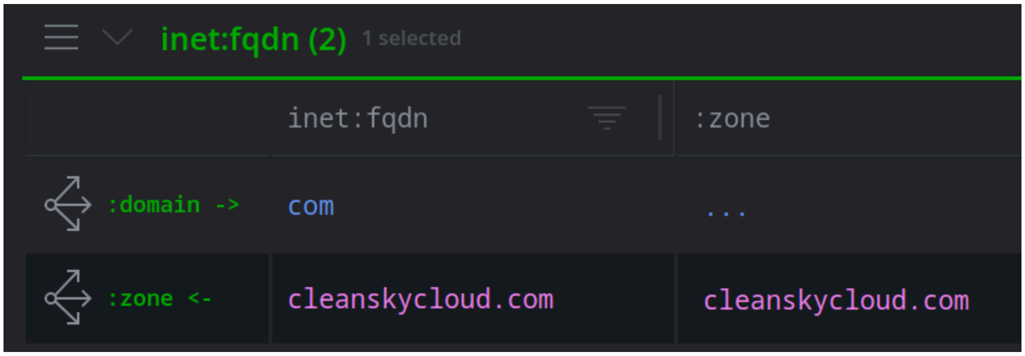
- The FQDN uses the DNS name servers **`ns104a.microsoftinternetsafety.net`** and **`ns104b.microsoftinternetsafety.net`**:



	:rec:asof	:rec:fqdn	:ns
:rec:fqdn <-	2025/05/14 11:34:12	cleanskycloud.com	ns104b.microsoftinternetsafety.net
:rec:fqdn <-	2025/05/14 11:34:12	cleanskycloud.com	ns104a.microsoftinternetsafety.net

Question 4: What does the FQDN **cleanskycloud.com** look like now?

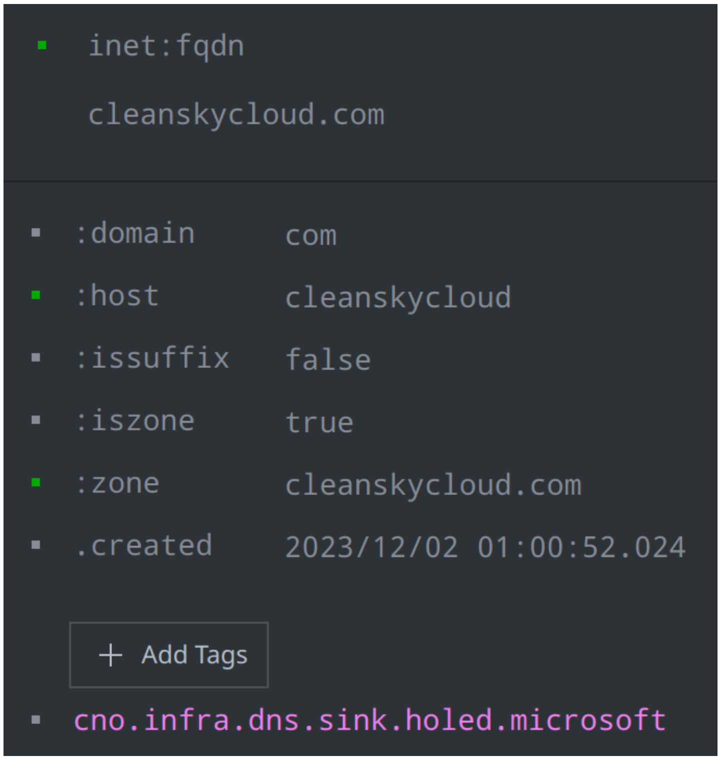
- The color of the node changed in the **Results Panel**, based on our tag color rules:



inet:fqdn (2) 1 selected

	inet:fqdn	:zone
:domain ->	com	...
:zone <-	cleanskycloud.com	cleanskycloud.com

The new tag is also visible in the **Details Panel:**



inet:fqdn

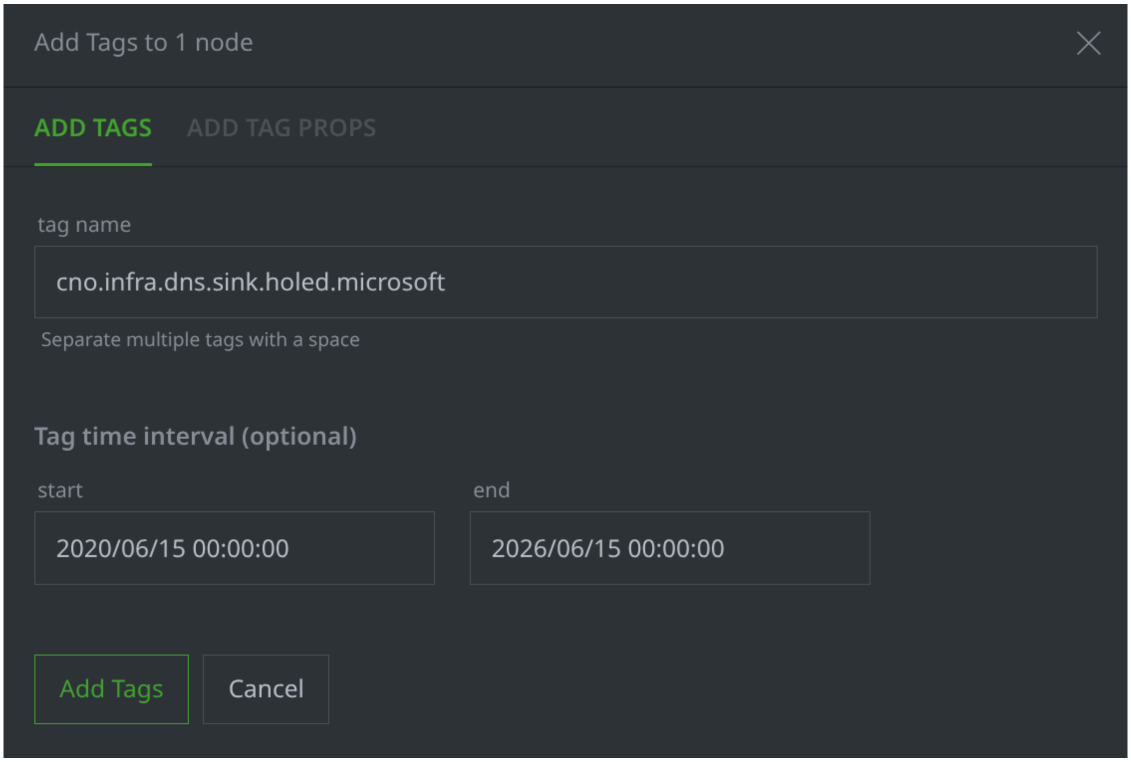
cleanskycloud.com

:domain	com
:host	cleanskycloud
:issuffix	false
:iszone	true
:zone	cleanskycloud.com
.created	2023/12/02 01:00:52.024

cno.infra.dns.sink.holed.microsoft

Tip: the domain whois information shows **when** Microsoft registered the domain (the `:created` property) and when the current registration expires (the `:expires` property).

We could **optionally** use this information to add **timestamps** to show "when" Microsoft sinkholed the domain:

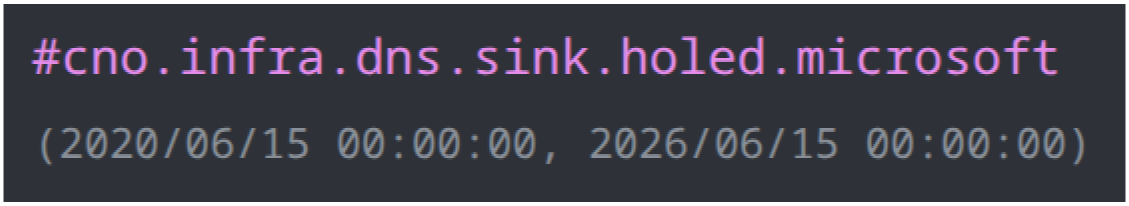


tag name: cno.infra.dns.sink.holed.microsoft

Tag time interval (optional)

start: 2020/06/15 00:00:00

end: 2026/06/15 00:00:00

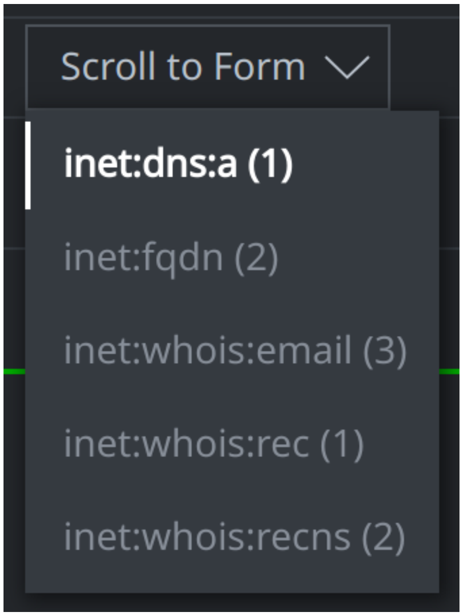


```
#cno.infra.dns.sink.holed.microsoft
(2020/06/15 00:00:00, 2026/06/15 00:00:00)
```

Part 2 - Enriching Data with the NetTools Power-Up - DNS Data

Question 5: What type(s) of DNS records were created (e.g., A, AAAA, MX, etc.?)

- The NetTools Power-Up created an `inet:dns:a` node:



Scroll to Form

inet:dns:a (1)

inet:fqdn (2)

inet:whois:email (3)

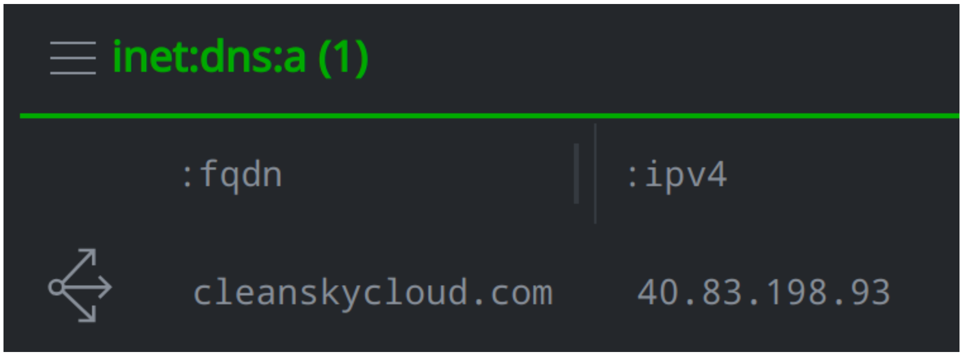
inet:whois:rec (1)

inet:whois:recns (2)

> The **default** behavior for the **nettools.dns** Storm command (and the associated Node Action) is to perform a **DNS A** lookup for FQDNs.

Question 6: What IPv4 address does the FQDN resolve to?

- The FQDN resolves to IPv4 **40.83.198.93** (as of August 2025):

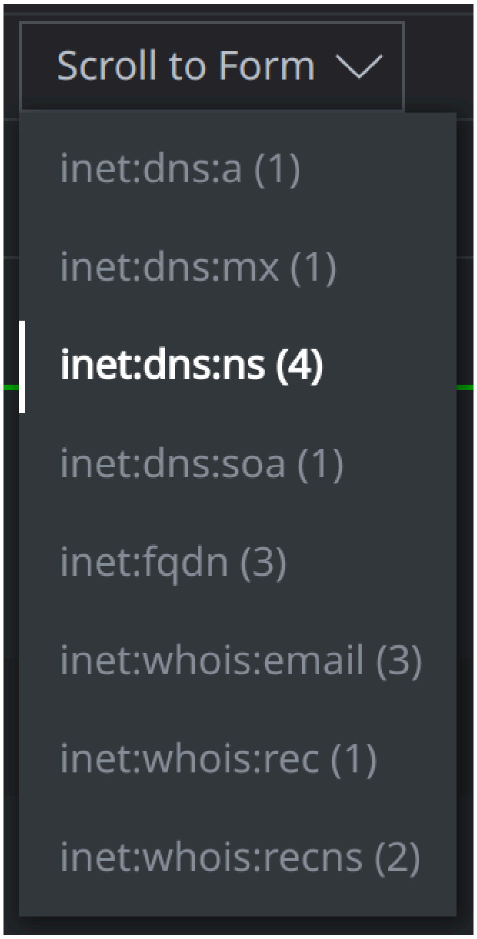


inet:dns:a (1)

:fqdn	:ipv4
cleanskycloud.com	40.83.198.93

Question 7: What **new** type(s) of DNS records were created (e.g., AAAA, MX, etc.?)

- The NetTools custom Node Action created additional MX, NS, and SOA records:



Scroll to Form

inet:dns:a (1)

inet:dns:mx (1)

inet:dns:ns (4)

inet:dns:soa (1)

inet:fqdn (3)

inet:whois:email (3)

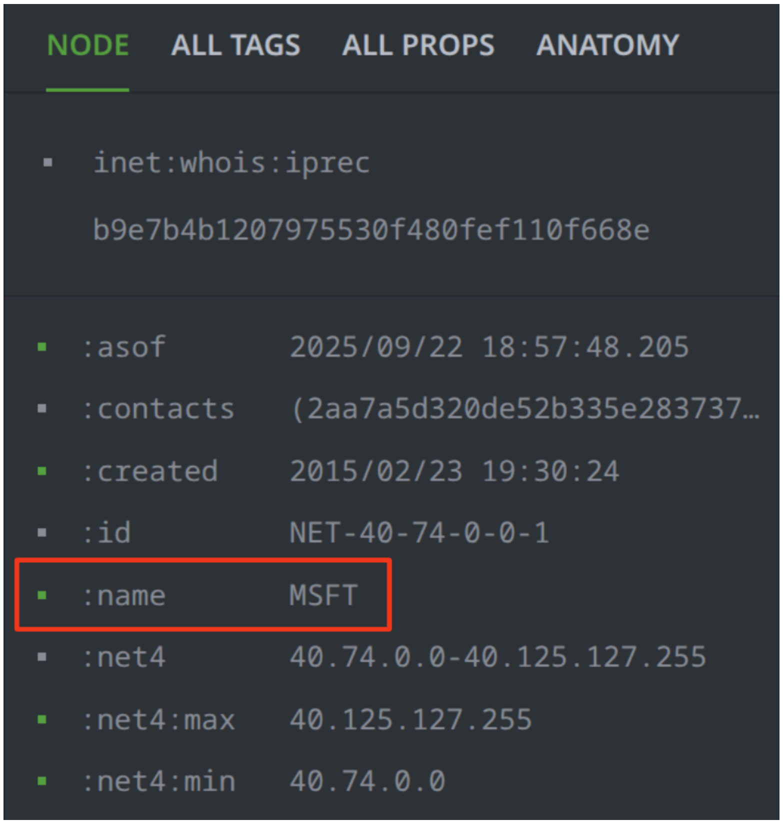
inet:whois:rec (1)

inet:whois:recns (2)

Part 3 - Enriching Data with the NetTools Power-Up - Network Whois Data

Question 8: What is the network name (**`:name`** property) associated with this netblock?

- The netblock name is **MSFT**:

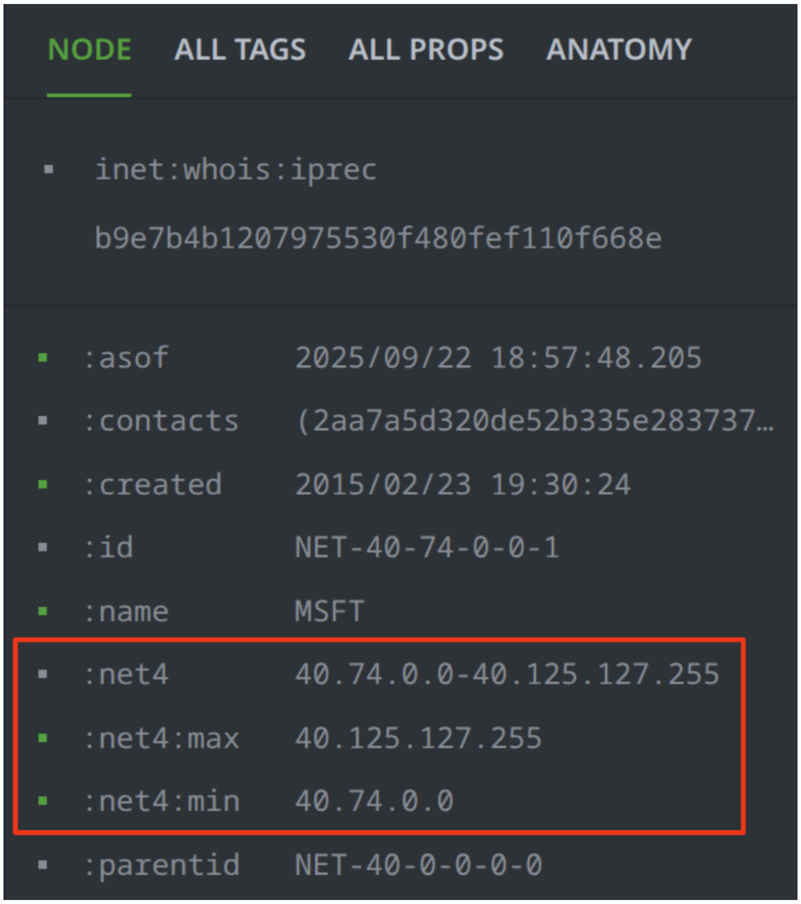


```
▪  inet:whois:iprec
   b9e7b4b1207975530f480fef110f668e

▪ :asof        2025/09/22 18:57:48.205
▪ :contacts    (2aa7a5d320de52b335e283737…
▪ :created     2015/02/23 19:30:24
▪ :id          NET-40-74-0-0-1
▪ :name        MSFT
▪ :net4        40.74.0.0-40.125.127.255
▪ :net4:max    40.125.127.255
▪ :net4:min    40.74.0.0
```

Question 9: What are the starting and ending IPv4 addresses associated with this netblock?

- The starting IPv4 is **40.74.0.0.** The ending IPv4 **40.125.127.255** (as of August 2025):



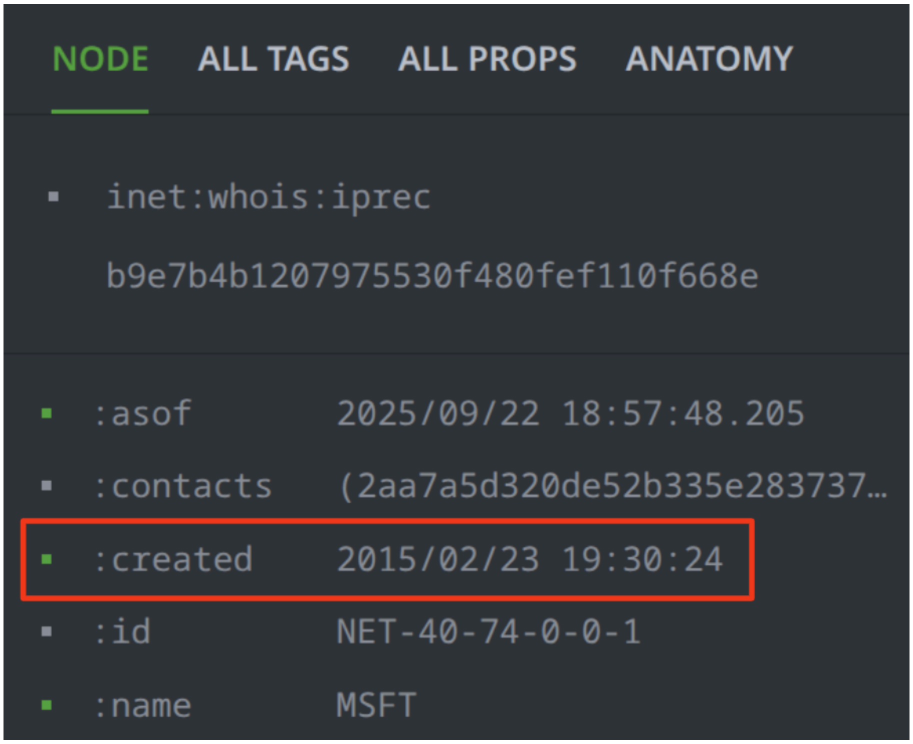
```
▪ inet:whois:iprec
  b9e7b4b1207975530f480fef110f668e

▪ :asof       2025/09/22 18:57:48.205
▪ :contacts   (2aa7a5d320de52b335e283737…
▪ :created    2015/02/23 19:30:24
▪ :id         NET-40-74-0-0-1
▪ :name       MSFT
▪ :net4       40.74.0.0-40.125.127.255
▪ :net4:max   40.125.127.255
▪ :net4:min   40.74.0.0
▪ :parentid   NET-40-0-0-0-0
```

The **range** of IPv4 addresses for this network is shown in the `:net4` property. The first IPv4 (`:net4:min`) and last IPv4 (`:net4:max`) are also stored separately so you can pivot from them.

Question 10: When (on what date) was this network range registered to Microsoft?

- The **`:created`** date for the network whois record shows that the network range was registered to Microsoft on **February 23, 2015** (2015/02/23):



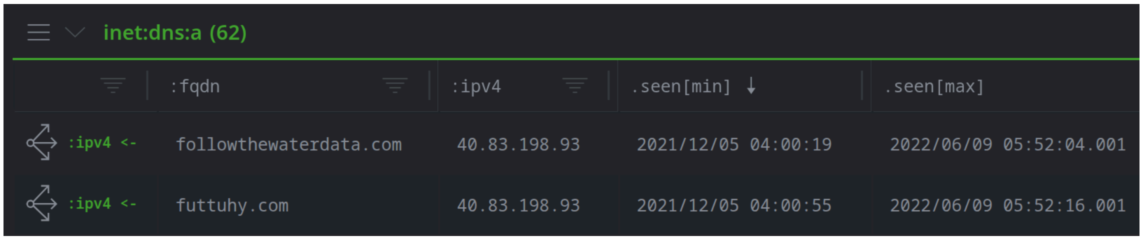
```
inet:whois:iprec
b9e7b4b1207975530f480fef110f668e

:asof        2025/09/22 18:57:48.205
:contacts    (2aa7a5d320de52b335e283737…
:created     2015/02/23 19:30:24
:id          NET-40-74-0-0-1
:name        MSFT
```

Part 4 - Enriching Data with the AlienVault Power-Up - Passive DNS

Question 11: What is the **earliest** (**`.seen[min]`**) date that an FQDN resolved to the IPv4?

- If we sort by the **.seen[min]** column, the **earliest** resolution was **December 5, 2021** (2021/12/05 04:00:19):

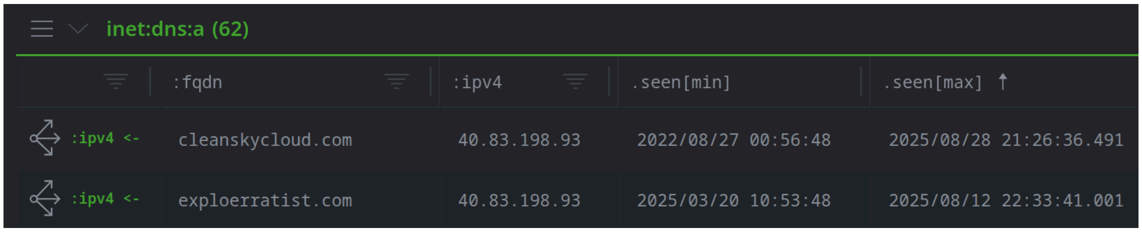


	:fqdn	:ipv4	.seen[min] ↓	.seen[max]
:ipv4 <-	followthewaterdata.com	40.83.198.93	2021/12/05 04:00:19	2022/06/09 05:52:04.001
:ipv4 <-	futtuhy.com	40.83.198.93	2021/12/05 04:00:55	2022/06/09 05:52:16.001

> **Note:** your answer may vary based on current data returned by the AlienVault Power-Up.

Question 12: What is the **most recent** (**`.seen[max]`**) date that an FQDN resolved to the IPv4?

- If we sort by the **.seen[max]** column, the **most recent** was **today:**



inet:dns:a (62)

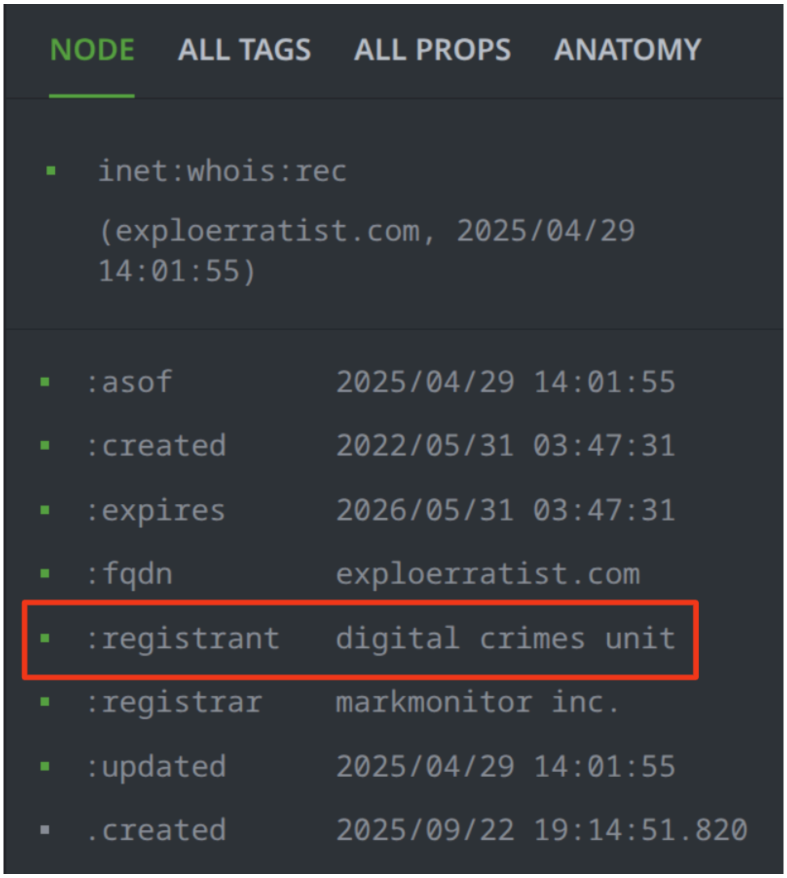
	:fqdn	:ipv4	.seen[min]	.seen[max] ↑
:ipv4 <-	cleanskycloud.com	40.83.198.93	2022/08/27 00:56:48	2025/08/28 21:26:36.491
:ipv4 <-	exploerratist.com	40.83.198.93	2025/03/20 10:53:48	2025/08/12 22:33:41.001

> The **.seen[max]** column should reflect the time of the live DNS A query you ran for **cleanskycloud.com.**

Part 5 - Comparing Domain Whois and DNS Data

Question 13: Who is the registrant for the FQDN?

- The registrant is **digital crimes unit:**

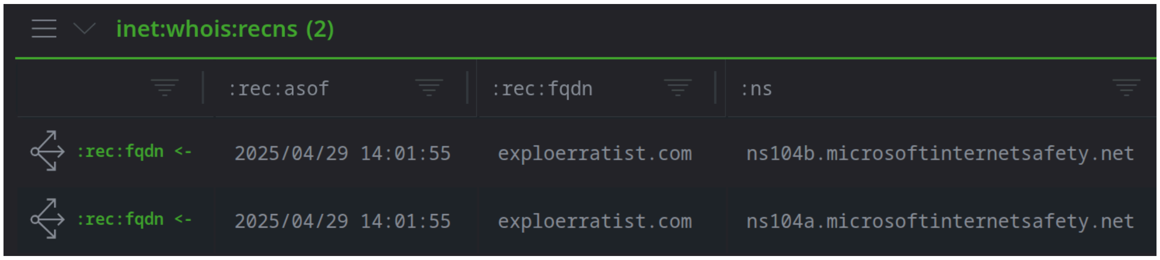


- inet:whois:rec (exploerratist.com, 2025/04/29 14:01:55)

:asof	2025/04/29 14:01:55
:created	2022/05/31 03:47:31
:expires	2026/05/31 03:47:31
:fqdn	exploerratist.com
:registrant	digital crimes unit
:registrar	markmonitor inc.
:updated	2025/04/29 14:01:55
.created	2025/09/22 19:14:51.820

Question 14: What DNS name servers does the FQDN use, according to the whois data?

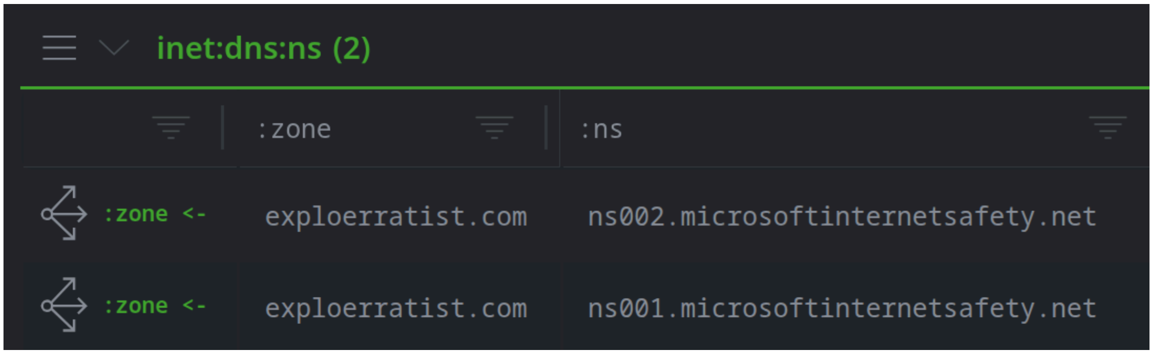
- The FQDN uses the names servers **`ns104a.microsoftinternetsafety.net`** and **`ns104b.microsoftinternetsafety.net`**:


inet:whois:recns (2)

	:rec:asof	:rec:fqdn	:ns
:rec:fqdn <-	2025/04/29 14:01:55	exploerratist.com	ns104b.microsoftinternetsafety.net
:rec:fqdn <-	2025/04/29 14:01:55	exploerratist.com	ns104a.microsoftinternetsafety.net

Question 15: What DNS name servers does the FQDN use, according to the DNS lookup data?

- The **live** DNS NS lookup returned **two** NS records (**`inet:dns:ns`**):



inet:dns:ns (2)

	:zone	:ns
:zone <-	exploerratist.com	ns002.microsoftinternetsafety.net
:zone <-	exploerratist.com	ns001.microsoftinternetsafety.net

The DNS records show the servers:

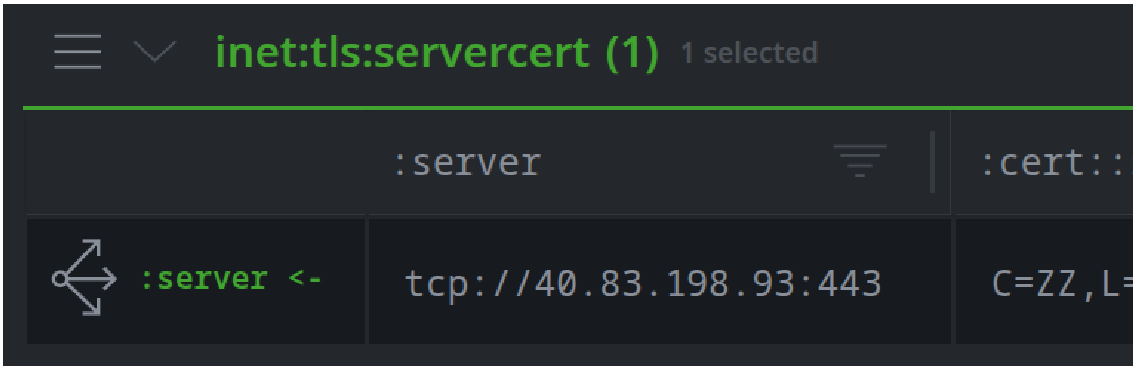
- **`ns001.microsoftinternetsafety.net`**
- **`ns002.microsoftinternetsafety.net`**

Although the hostnames vary between the WHOIS name servers and the NS records, all four name servers use the FQDN **microsoftinternetsafety.net**.

Part 6 - Checking Network Infrastructure

Question 16: What port was serving the certificate?

- The certificate was hosted on port **443:**



inet:tls:servercert (1) 1 selected

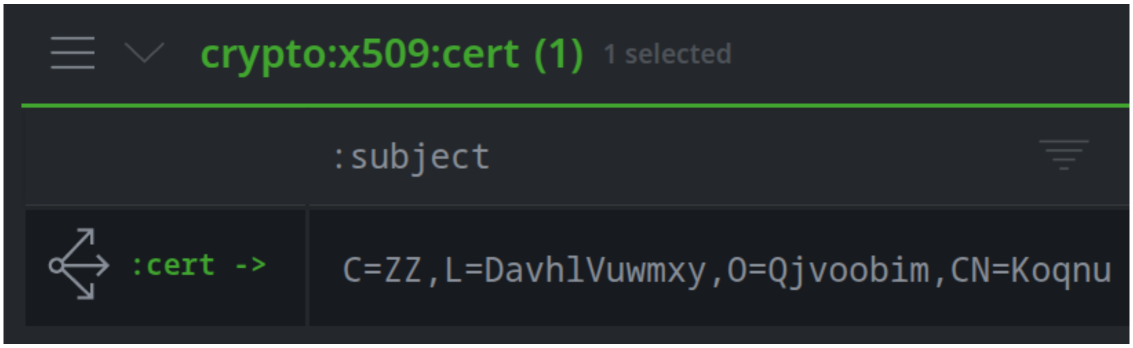
	:server	:cert::
:server <-	tcp://40.83.198.93:443	C=ZZ,L=

Tip: An **`inet:tls:servercert`** node links a server (**`inet:server`**) with the metadata (**`crypto:x509:cert`**) for the certificate that was observed there.

Question 17: Who was the certificate issued to (i.e., what is the **`:subject`** of the certificate)?

- The **:subject** field of the certificate is:

  C=ZZ,L=DavhlVuwmxy,O=Qjvoobim,CN=Koqnu

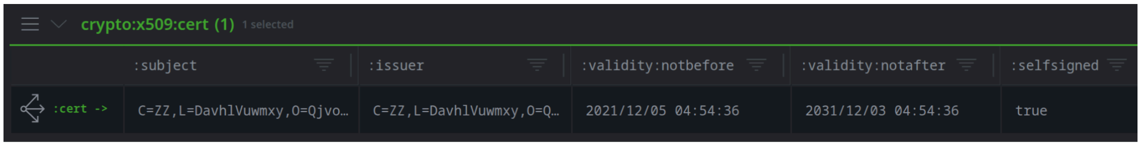


crypto:x509:cert (1) 1 selected

	:subject
:cert ->	C=ZZ,L=DavhlVuwmxy,O=Qjvoobim,CN=Koqnu

Question 18: Is the certificate self-signed (vs. issued and signed by a Certificate Authority)?

- **Yes,** the certificate is self-signed (the **:selfsigned** property is **true**):



crypto:x509:cert (1) 1 selected

	:subject	:issuer	:validity:notbefore	:validity:notafter	:selfsigned
:cert ->	C=ZZ,L=DavhlVuwmxy,O=Qjvo…	C=ZZ,L=DavhlVuwmxy,O=Q…	2021/12/05 04:54:36	2031/12/03 04:54:36	true

---

Look for Similar Certificates

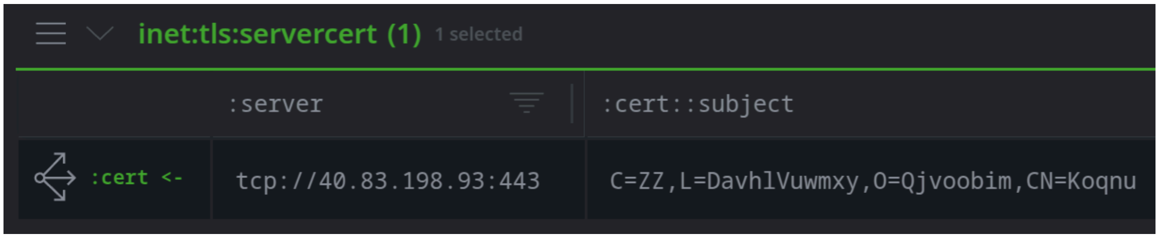
Exercise 2 Answer

Objective:

- **Look for similar certificates and associated servers based on certificate metadata properties.**

Question 1: How many **inet:tls:servercert** nodes are in the results?

- There is **one** `inet:tls:servercert` node in our results:



inet:tls:servercert (1) 1 selected

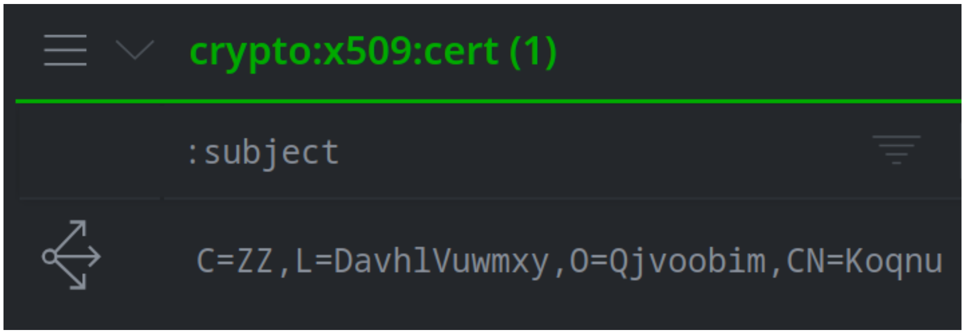
	:server	:cert::subject
:cert <-	tcp://40.83.198.93:443	C=ZZ,L=DavhlVuwmxy,O=Qjvoobim,CN=Koqnu

This is the node for our original Microsoft sinkhole IPv4.

This **exact** certificate has only been seen on one server (IP address / port).

Question 2: How many certificates in Synapse have the same **:subject** value?

- Only **one** certificate in Synapse has this **exact** subject:

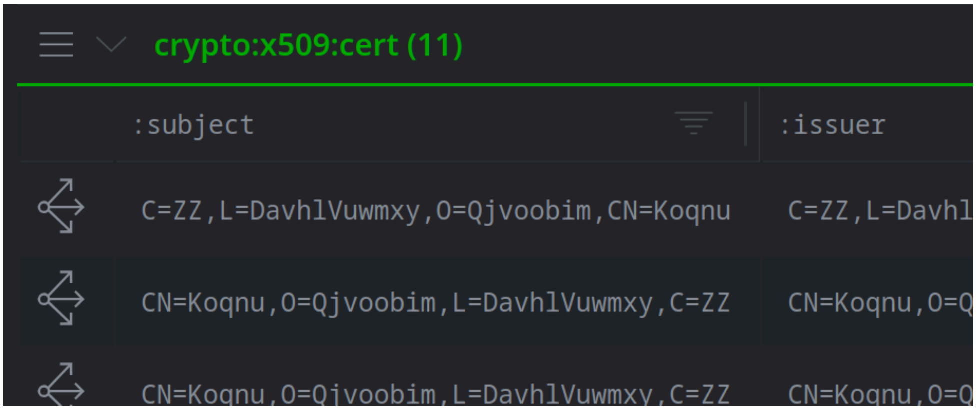


crypto:x509:cert (1)

	:subject
	C=ZZ,L=DavhlVuwmxy,O=Qjvoobim,CN=Koqnu

Question 3: How many certificates in Synapse have a **:subject** that includes this string?

- There are **eleven** certificates with this string in Synapse:



crypto:x509:cert (11)

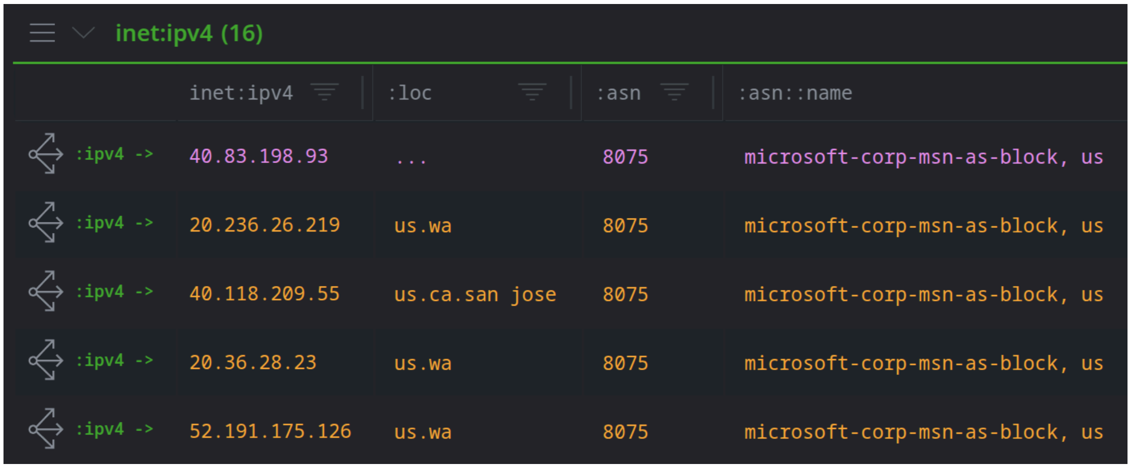
	:subject	:issuer
	C=ZZ,L=DavhlVuwmxy,O=Qjvoobim,CN=Koqnu	C=ZZ,L=Davhl
	CN=Koqnu,O=Qjvoobim,L=DavhlVuwmxy,C=ZZ	CN=Koqnu,O=Q
	CN=Koqnu,O=Qjvoobim,L=DavhlVuwmxy,C=ZZ	CN=Koqnu,O=Q

Tip: This answer is based on data **already** in Synapse. You could use additional Power-Ups (such as Shodan or Censys) to find additional information.

For example, you could query the certificate subject CN to see if a third-party data source had seen any additional certificates with the unusual CN name "Koqnu".

Question 4: What Autonomous System (AS) number(s) and network(s) are the IPv4 addresses associated with?

- The IPv4s are associated with **AS 8075** (microsoft-corp-msn-as-block, us):



inet:ipv4 (16)

	inet:ipv4	:loc	:asn	:asn::name
:ipv4 ->	40.83.198.93	...	8075	microsoft-corp-msn-as-block, us
:ipv4 ->	20.236.26.219	us.wa	8075	microsoft-corp-msn-as-block, us
:ipv4 ->	40.118.209.55	us.ca.san jose	8075	microsoft-corp-msn-as-block, us
:ipv4 ->	20.36.28.23	us.wa	8075	microsoft-corp-msn-as-block, us
:ipv4 ->	52.191.175.126	us.wa	8075	microsoft-corp-msn-as-block, us

Question 5: Does the name **Koqnu** appear to be unique to Microsoft infrastructure?

- **Yes.** Based on the data we have, the name **Koqnu** seems to be unique to Microsoft.

Some additional questions we might ask and try to answer:

- Check any third-party data sources that can provide certificate data to see if there are similar certificates that Synapse does **not** know about. Finding additional certificates may help prove (or disprove!) our theory that these certificates are unique to Microsoft.

- Research the additional IPv4 addresses to see if they are also sinkholes, or simply other Microsoft servers.

- Look for other similarities on the servers (e.g., JARM fingerprints, software or services, etc.).