Synapse Bootcamp - Module 17

Network Infrastructure Analysis - Answer Key

Answer Key

Analyzing and Identifying Network Infrastructure

Exercise 1 Answer

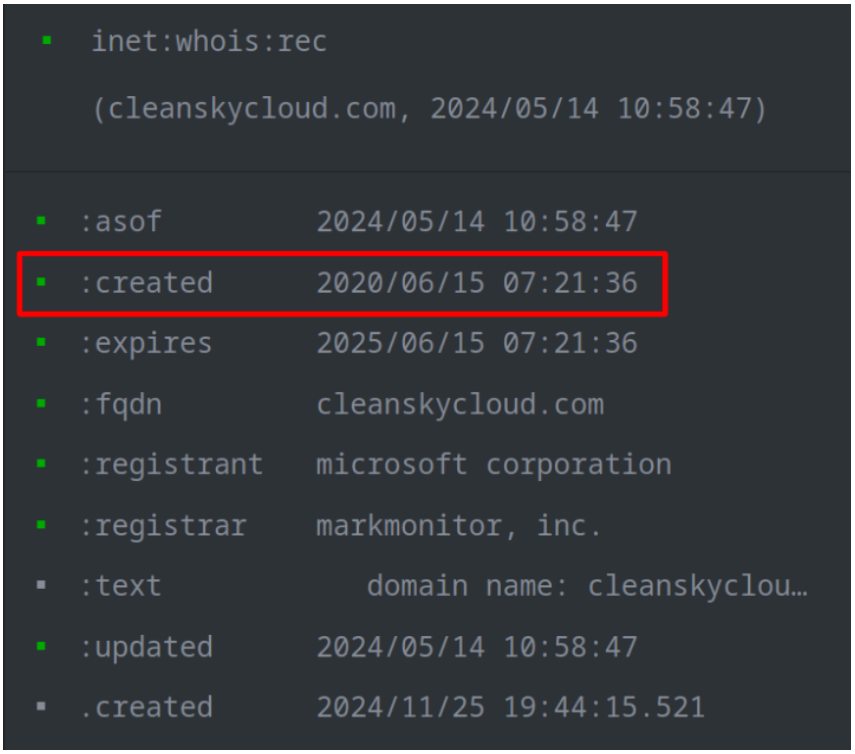
Objective:

- **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?

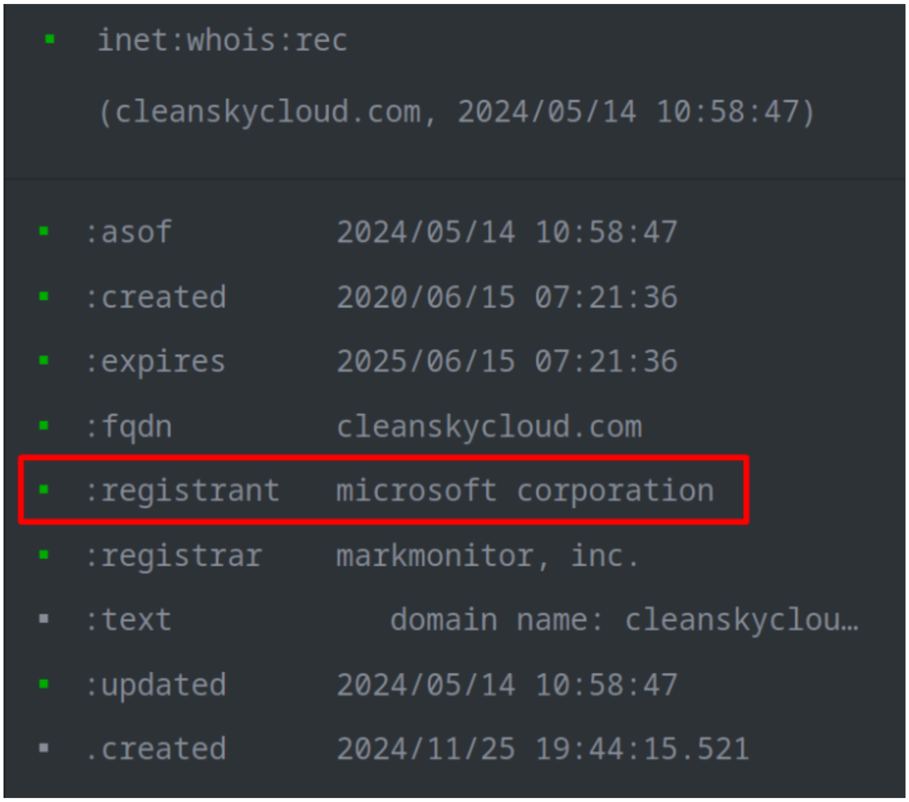
- The FQDN was registered on **June 15, 2020** (2020/06/15):



```
▪  inet:whois:rec
   (cleanskycloud.com, 2024/05/14 10:58:47)

▪  :asof          2024/05/14 10:58:47
▪  :created       2020/06/15 07:21:36
▪  :expires       2025/06/15 07:21:36
▪  :fqdn          cleanskycloud.com
▪  :registrant    microsoft corporation
▪  :registrar     markmonitor, inc.
▪  :text             domain name: cleanskyclou…
▪  :updated       2024/05/14 10:58:47
▪  .created       2024/11/25 19:44:15.521
```

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

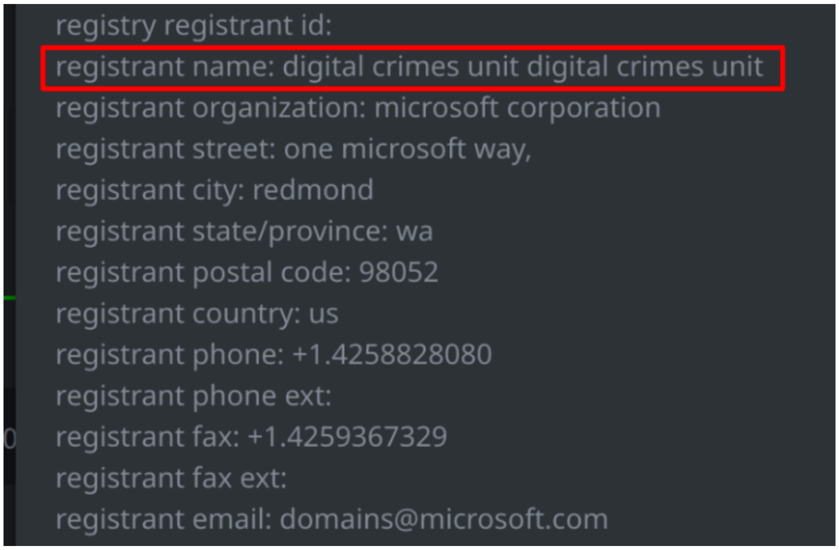
- The registrant is **microsoft corporation**:



```
▪ inet:whois:rec
  (cleanskycloud.com, 2024/05/14 10:58:47)

▪ :asof          2024/05/14 10:58:47
▪ :created       2020/06/15 07:21:36
▪ :expires       2025/06/15 07:21:36
▪ :fqdn          cleanskycloud.com
▪ :registrant    microsoft corporation
▪ :registrar     markmonitor, inc.
▪ :text             domain name: cleanskyclou…
▪ :updated       2024/05/14 10:58:47
▪ .created       2024/11/25 19:44:15.521
```

Question 3: Looking at the 'registrant' details, what department within Microsoft registered the FQDN?

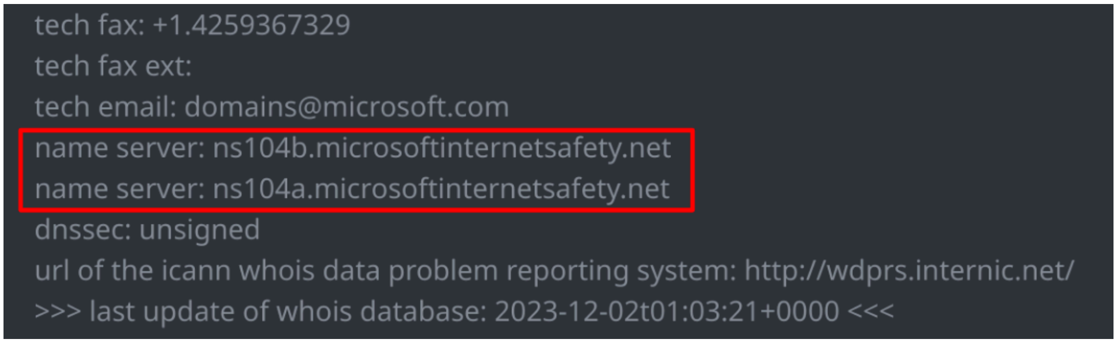
- The domain was registered by Microsoft's **Digital Crimes Unit.**



```
registry registrant id:
registrant name: digital crimes unit digital crimes unit
registrant organization: microsoft corporation
registrant street: one microsoft way,
registrant city: redmond
registrant state/province: wa
registrant postal code: 98052
registrant country: us
registrant phone: +1.4258828080
registrant phone ext:
registrant fax: +1.4259367329
registrant fax ext:
registrant email: domains@microsoft.com
```

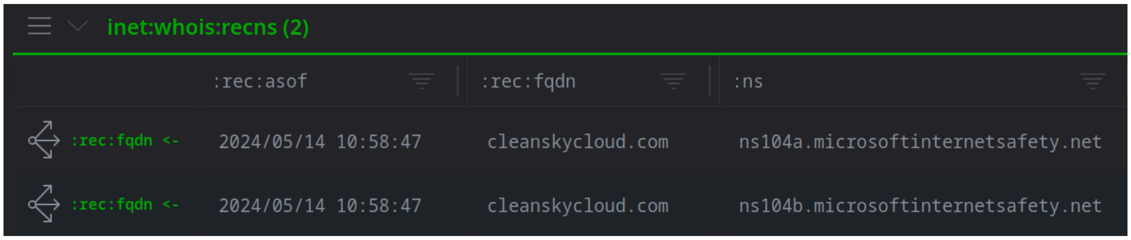
Question 4: Based on the whois data, what DNS **name servers** are used by the FQDN?

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



```
tech fax: +1.4259367329
tech fax ext:
tech email: domains@microsoft.com
name server: ns104b.microsoftinternetsafety.net
name server: ns104a.microsoftinternetsafety.net
dnssec: unsigned
url of the icann whois data problem reporting system: http://wdprs.internic.net/
>>> last update of whois database: 2023-12-02t01:03:21+0000 <<<
```

Tip: If a domain whois record lists the DNS name servers for the FQDN, this information is modeled using **`inet:whois:recns`** nodes. You can see these nodes in your **Results Panel**:

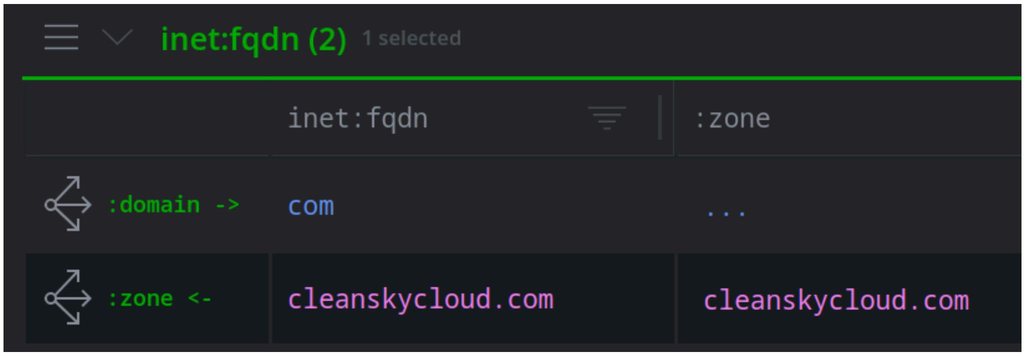


inet:whois:recns (2)

	:rec:asof	:rec:fqdn	:ns
:rec:fqdn <-	2024/05/14 10:58:47	cleanskycloud.com	ns104a.microsoftinternetsafety.net
:rec:fqdn <-	2024/05/14 10:58:47	cleanskycloud.com	ns104b.microsoftinternetsafety.net

Question 5: What does the FQDN **cleanskycloud.com** look like now?

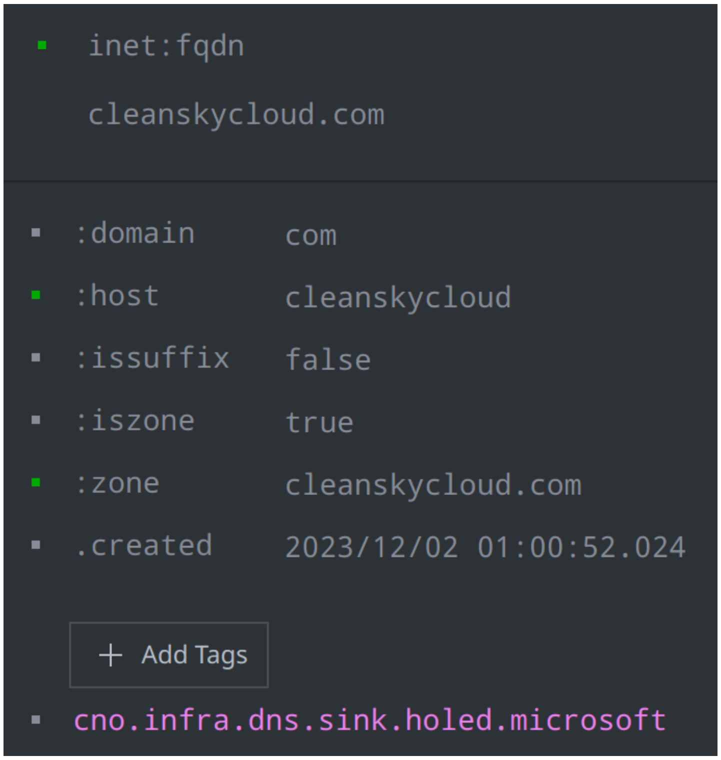
- The color of the node changed in the **Results Panel**, based on our tag color rules:



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:**

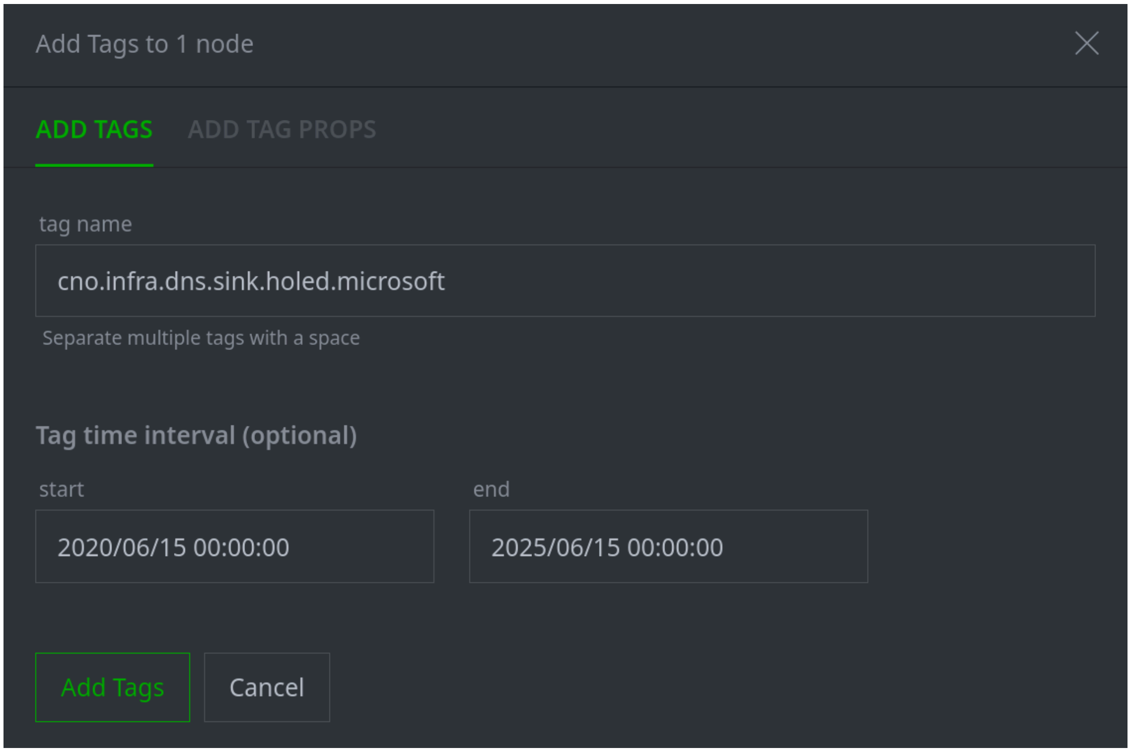


```
inet:fqdn

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

Separate multiple tags with a space

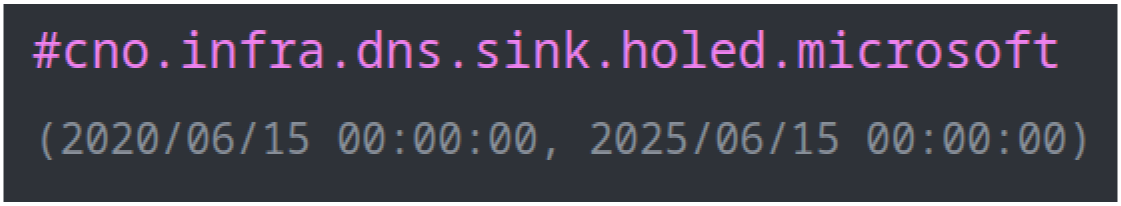
Tag time interval (optional)

start

2020/06/15 00:00:00

end

2025/06/15 00:00:00

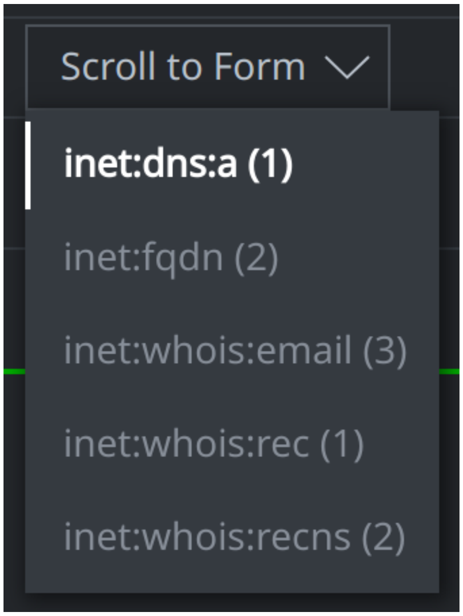


```
#cno.infra.dns.sink.holed.microsoft
(2020/06/15 00:00:00, 2025/06/15 00:00:00)
```

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

Question 6: What type(s) of DNS records were created (e.g., A, AAAA, MX, etc.?)

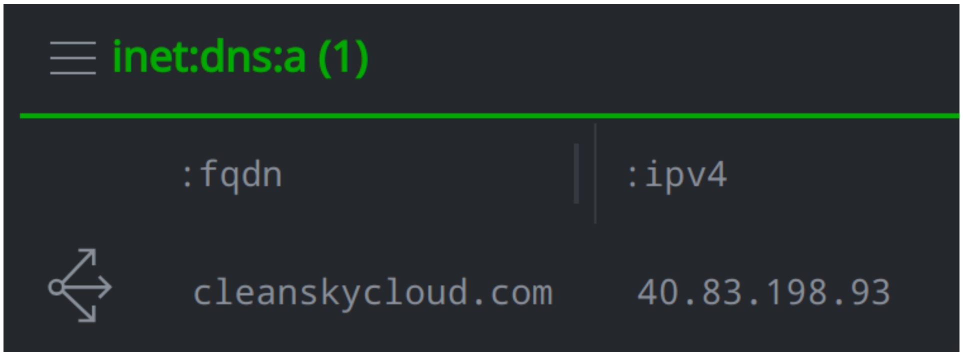
- The NetTools Power-Up created an **`inet:dns:a`** node:



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

Question 7: What IPv4 address does the FQDN resolve to?

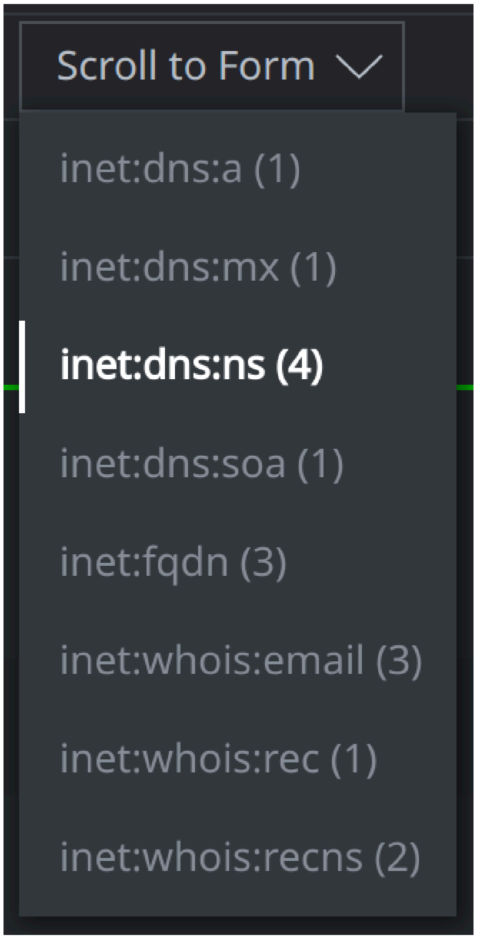
- The FQDN resolves to IPv4 **40.83.198.93** (as of November 2024):



:fqdn	:ipv4
cleanskycloud.com	40.83.198.93

Question 8: What type(s) of DNS records were created (e.g., A, AAAA, MX, etc.?)

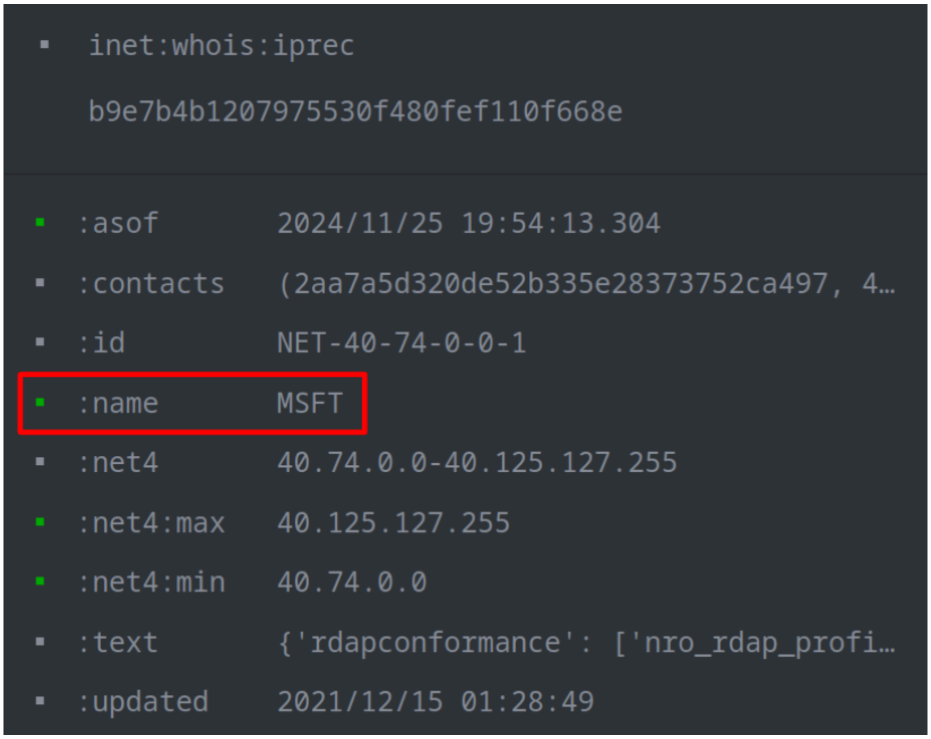
- The NetTools custom Node Action created additional MX, NS, and SOA records:



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

Question 9: What is the network name (**`:name`** property) associated with this netblock?

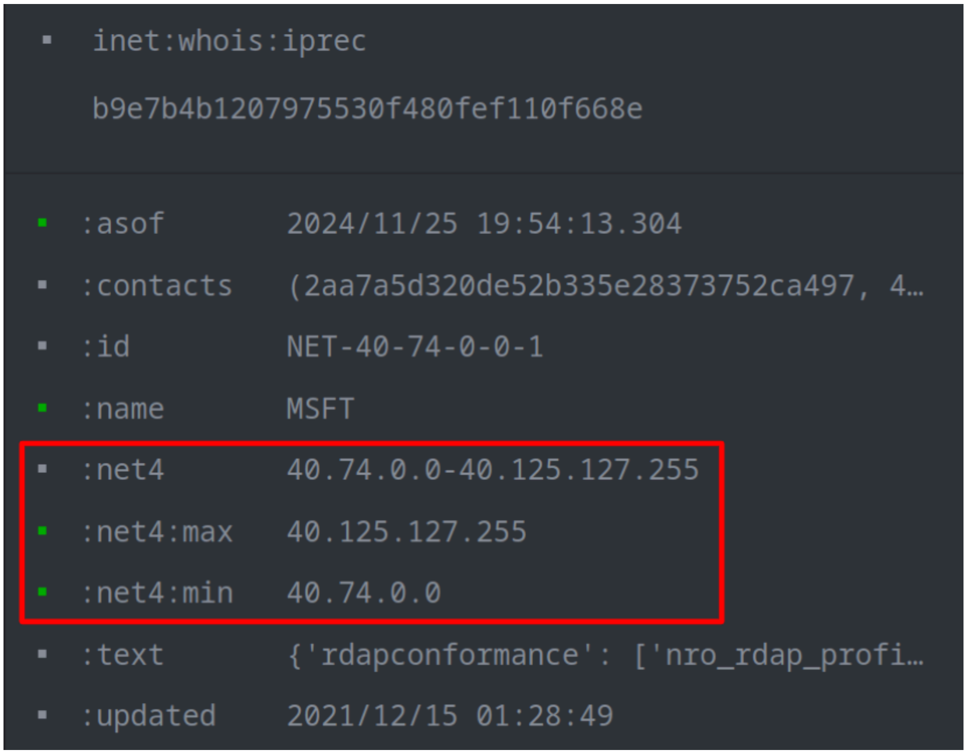
- The netblock name is **MSFT**:



```
▪  inet:whois:iprec
   b9e7b4b1207975530f480fef110f668e

▪  :asof        2024/11/25 19:54:13.304
▪  :contacts    (2aa7a5d320de52b335e28373752ca497, 4…
▪  :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
▪  :text        {'rdapconformance': ['nro_rdap_profi…
▪  :updated     2021/12/15 01:28:49
```

Question 10: 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 November 2024):



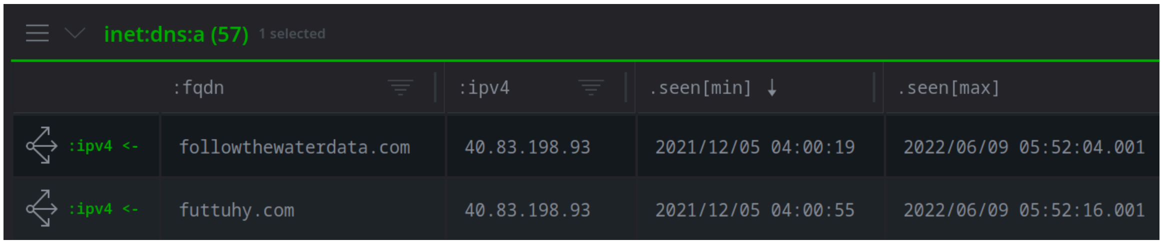
```
▪  inet:whois:iprec
   b9e7b4b1207975530f480fef110f668e

▪  :asof        2024/11/25 19:54:13.304
▪  :contacts    (2aa7a5d320de52b335e28373752ca497, 4…
▪  :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
▪  :text        {'rdapconformance': ['nro_rdap_profi…
▪  :updated     2021/12/15 01:28:49
```

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.

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):



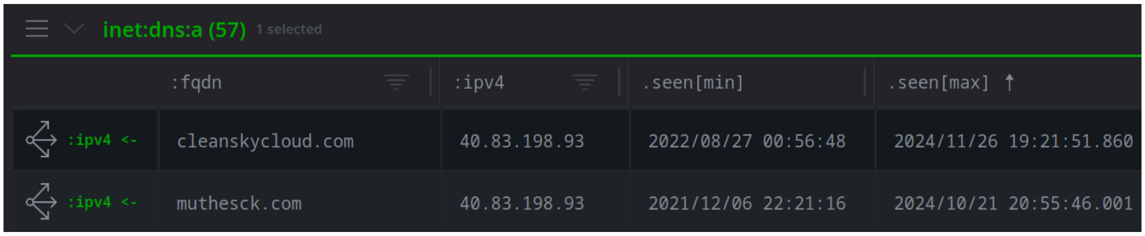
inet:dns:a (57) 1 selected

	: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 (57) 1 selected

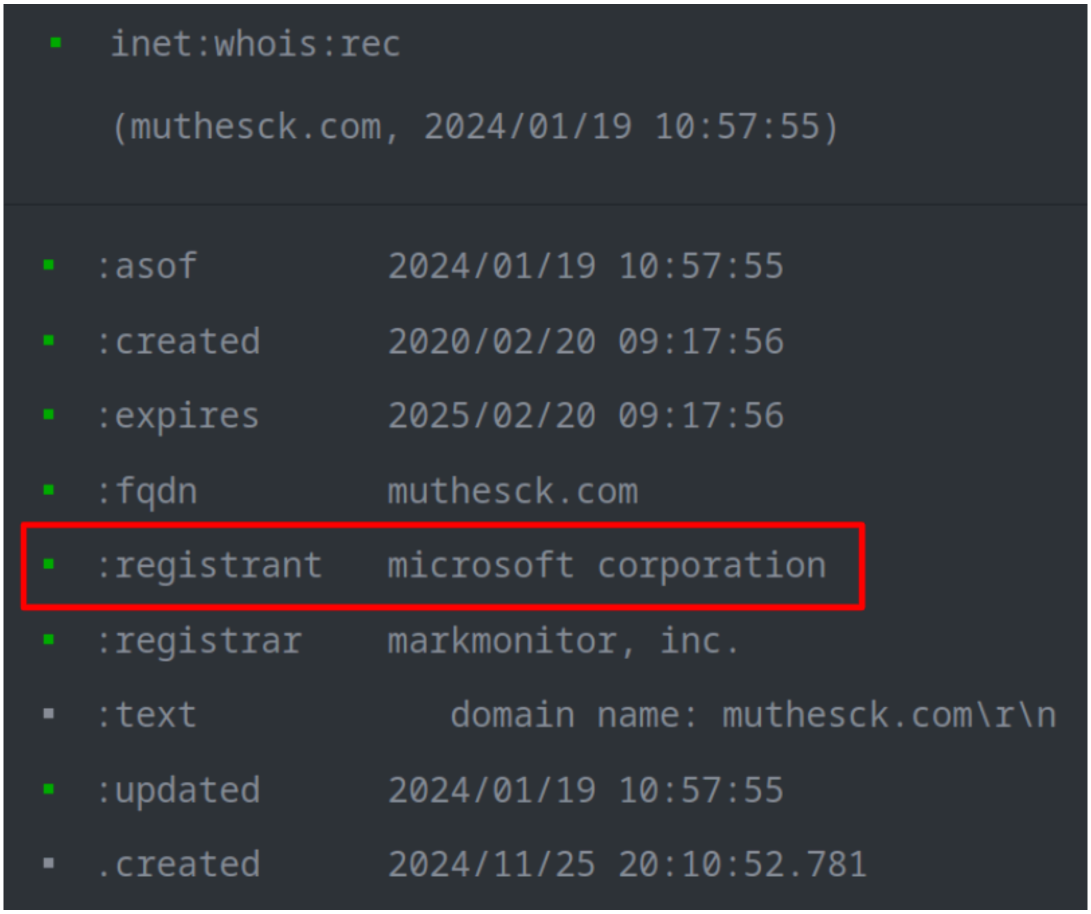
	:fqdn	:ipv4	.seen[min]	.seen[max] ↑
:ipv4 <-	cleanskycloud.com	40.83.198.93	2022/08/27 00:56:48	2024/11/26 19:21:51.860
:ipv4 <-	muthesck.com	40.83.198.93	2021/12/06 22:21:16	2024/10/21 20:55:46.001

The column should reflect 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 **microsoft corporation:**

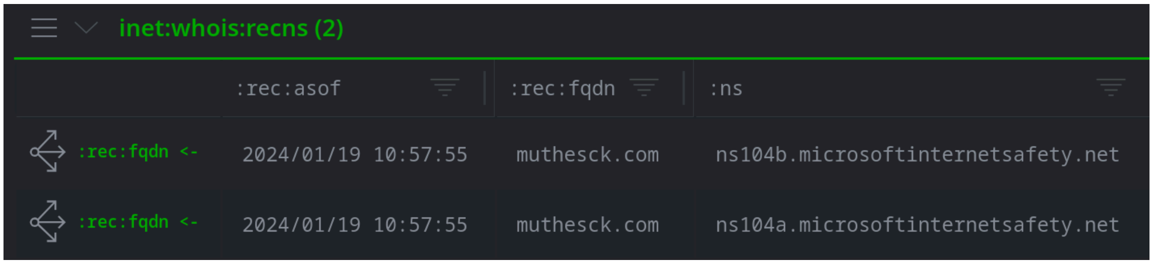


```
▪  inet:whois:rec
   (muthesck.com, 2024/01/19 10:57:55)

▪  :asof         2024/01/19 10:57:55
▪  :created      2020/02/20 09:17:56
▪  :expires      2025/02/20 09:17:56
▪  :fqdn         muthesck.com
▪  :registrant   microsoft corporation
▪  :registrar    markmonitor, inc.
▪  :text             domain name: muthesck.com\r\n
▪  :updated      2024/01/19 10:57:55
▪  .created      2024/11/25 20:10:52.781
```

If you view the full `:text` property, it should also specify the **digital crimes unit.**

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`**:



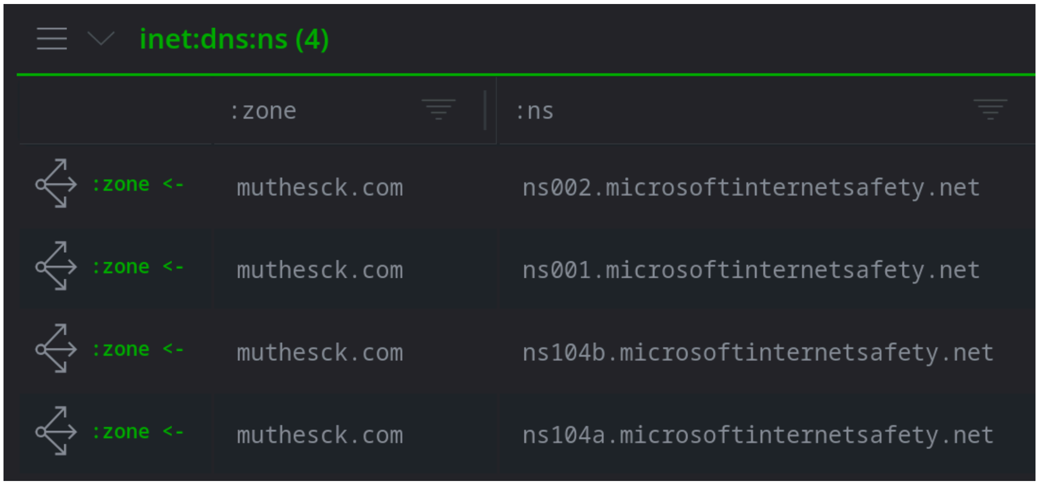
inet:whois:recns (2)

	:rec:asof	:rec:fqdn	:ns
:rec:fqdn <-	2024/01/19 10:57:55	muthesck.com	ns104b.microsoftinternetsafety.net
:rec:fqdn <-	2024/01/19 10:57:55	muthesck.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 **four** NS records (`inet:dns:ns`):



inet:dns:ns (4)

	:zone	:ns
:zone <-	muthesck.com	ns002.microsoftinternetsafety.net
:zone <-	muthesck.com	ns001.microsoftinternetsafety.net
:zone <-	muthesck.com	ns104b.microsoftinternetsafety.net
:zone <-	muthesck.com	ns104a.microsoftinternetsafety.net

The DNS records show the same two servers from the FQDN whois record:

- **`ns104a.microsoftinternetsafety.net`**
- **`ns104b.microsoftinternetsafety.net`**

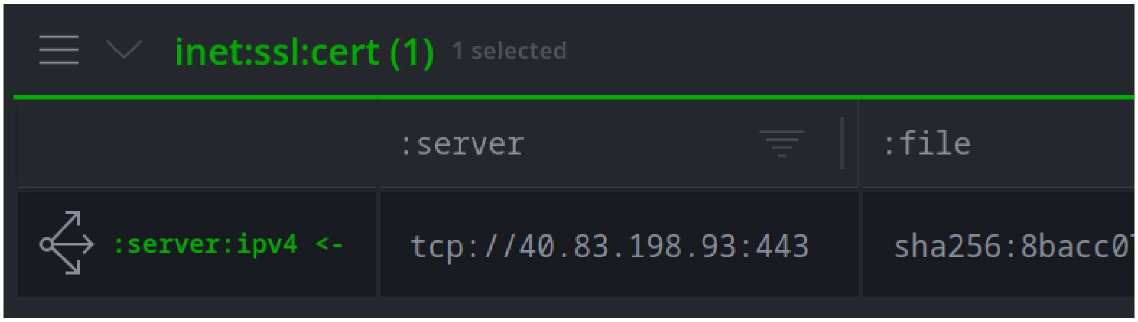
...plus two additional servers:

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

Part 6 - Checking Network Infrastructure

Question 16: What port was serving the certificate?

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



inet:ssl:cert (1) 1 selected

	:server	:file
:server:ipv4 <-	tcp://40.83.198.93:443	sha256:8bacc0

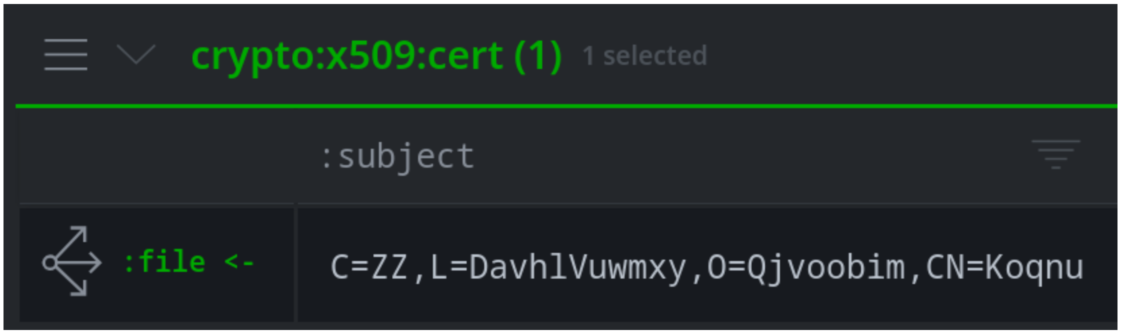
Tip: An **`inet:ssl:cert`** node links an SSL or TLS certificate file (**`file:bytes`**) with a server (**`inet:server`**) where the certificate was observed.

The **`inet:ssl:cert`** form has been replaced by the **`inet:tls:servercert`** form. You may see both forms in Synapse while we update all the Power-Ups to use the newer form.

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`

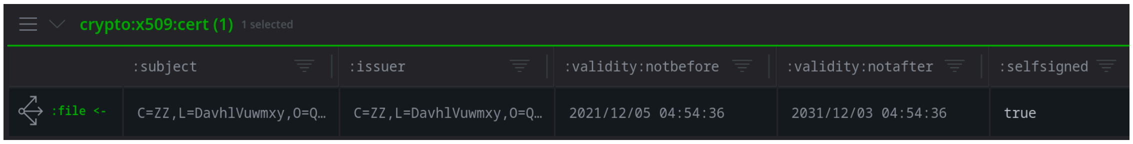


crypto:x509:cert (1) 1 selected

	:subject
:file <-	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
:file <-	C=ZZ,L=DavhlVuwmxy,O=Q…	C=ZZ,L=DavhlVuwmxy,O=Q…	2021/12/05 04:54:36	2031/12/03 04:54:36	true

Look for Similar Certificates

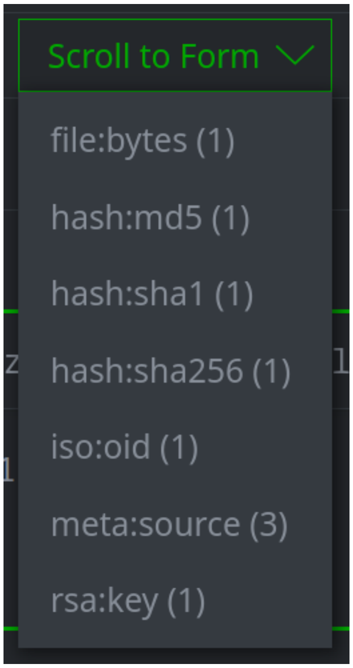
Exercise 2 Answer

Objective:

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

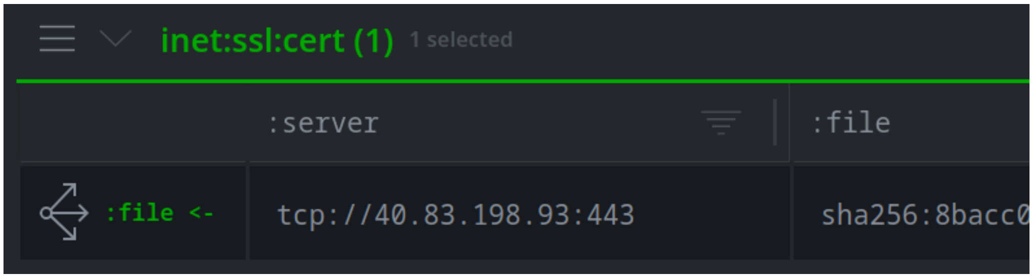
Question 1: Are there any **`inet:tls:servercert`** nodes in the results?

- **No,** there are no **`inet:tls:servercert`** nodes associated with this certificate:



Question 2: How many **`inet:ssl:cert`** nodes are in the results?

- There is only **one** **`inet:ssl:cert`** node, from our original sinkhole IPv4:



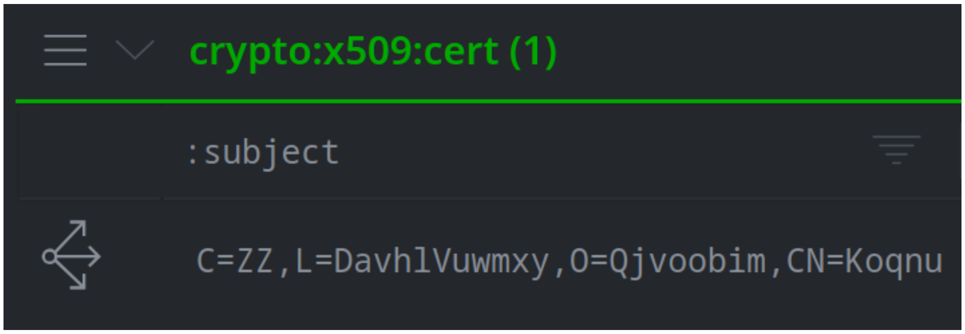
	:server	:file
:file <-	tcp://40.83.198.93:443	sha256:8bacc0

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

For example, you could query the certificate fingerprint (SHA1 hash) to see if a third-party data source had seen this certificate on any other host.

Question 3: How many certificates in Synapse have the same **:subject** value?

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

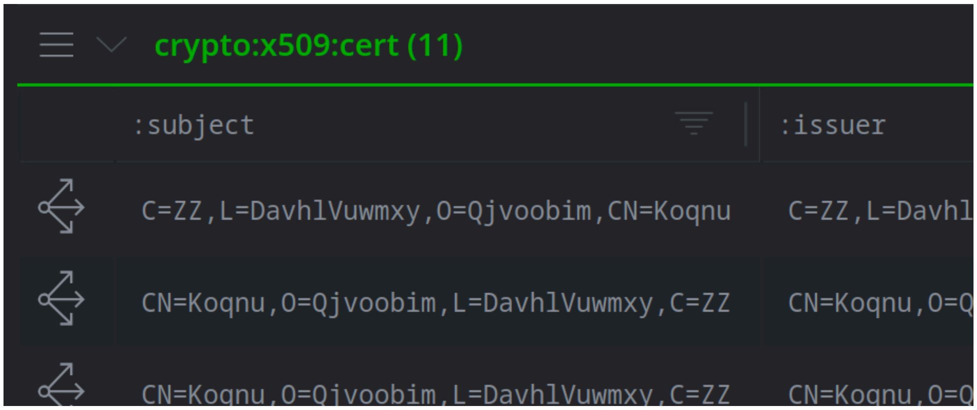


crypto:x509:cert (1)

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

Question 4: How many certificates in Synapse have a **:subject** that includes this string?

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



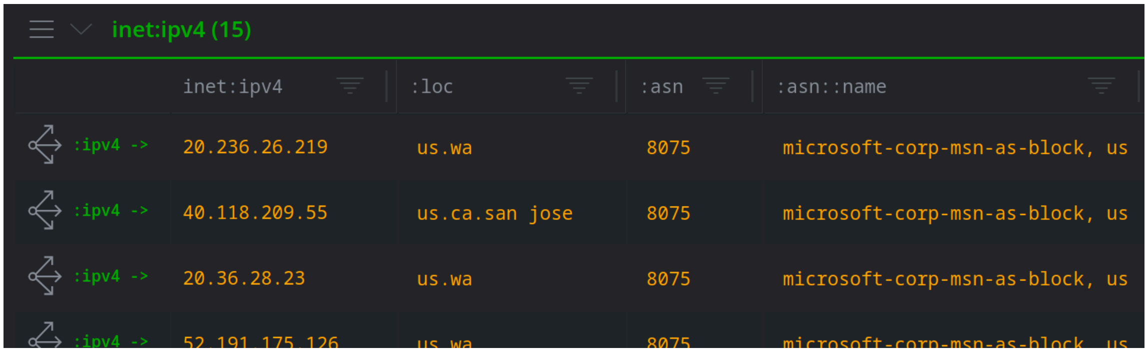
crypto:x509:cert (11)

: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) 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 5: 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 (15)

	inet:ipv4	:loc	:asn	:asn::name
: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 6: 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.).