Vertex

Synapse Bootcamp - Module 17

Network Infrastructure Analysis - Answer Key

Answer Key

Analyzing and Identifying Network Infrastructure

Exercise 1 Answer

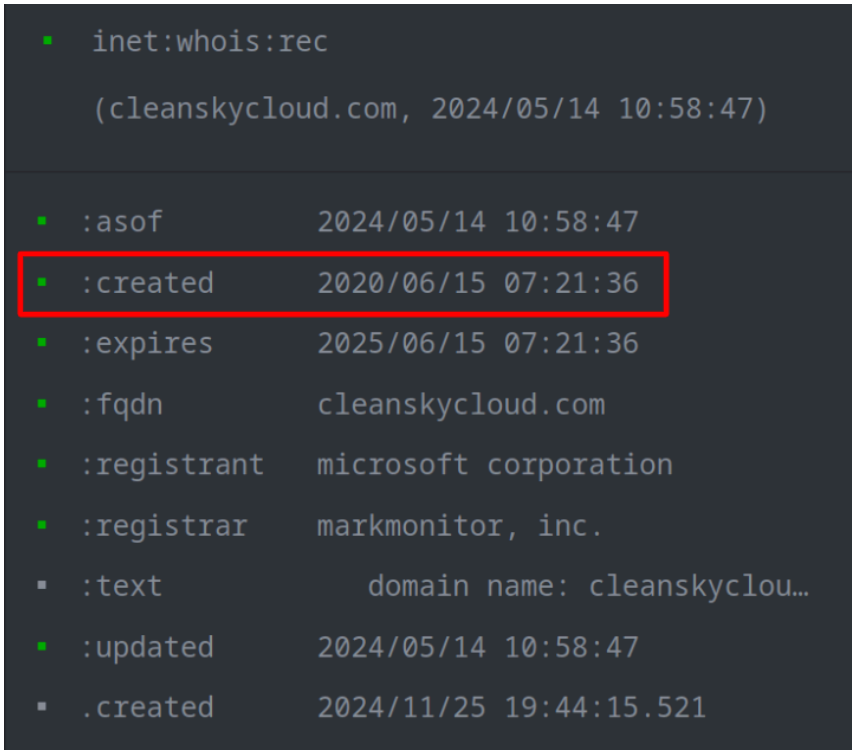
Objective:

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

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

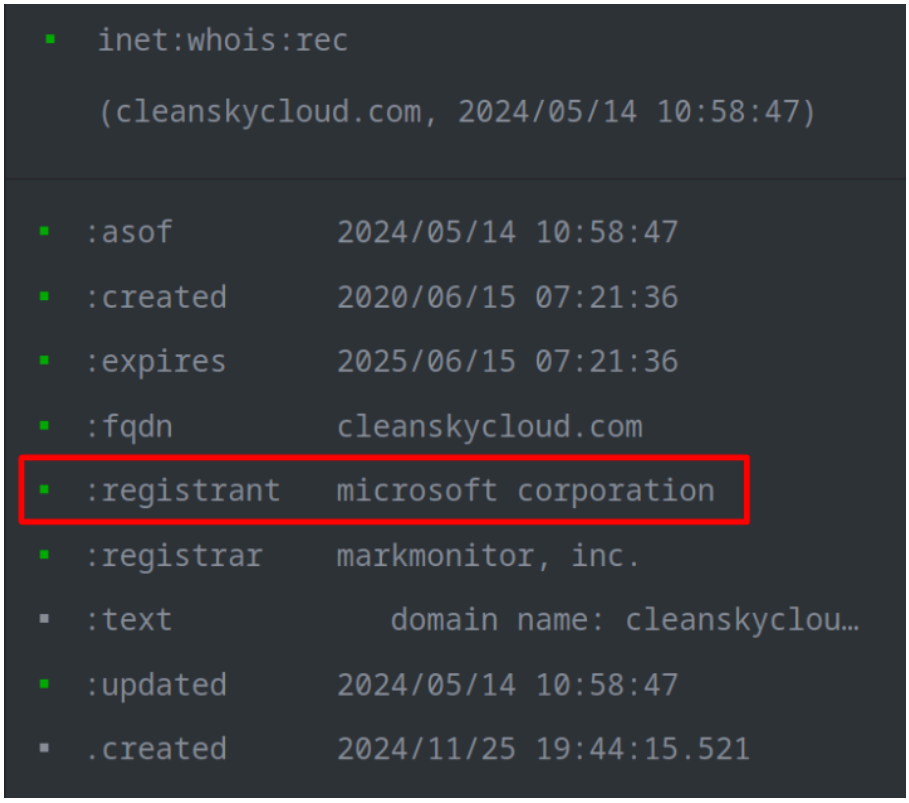
Question 1: Based on this current whois record, when was the FQDN registered?

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



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

- The registrant is **microsoft corporation**:

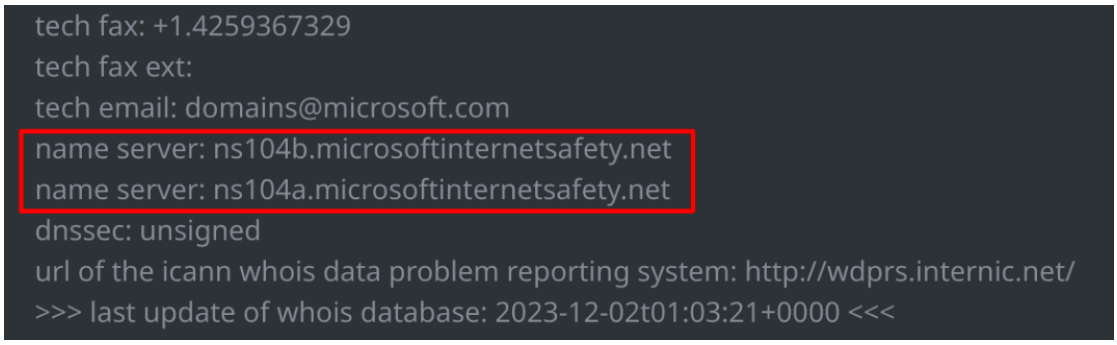


Question 3: Looking at the 'registrant' details, what department within Microsoft registered the FQDN?

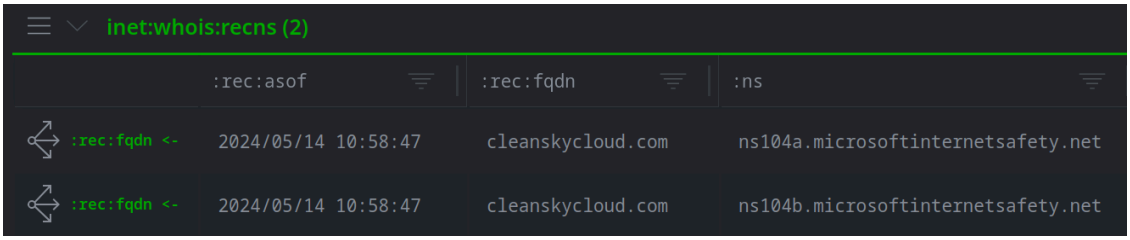
- The domain was registered by Microsoft's **Digital Crimes Unit.**

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`**:

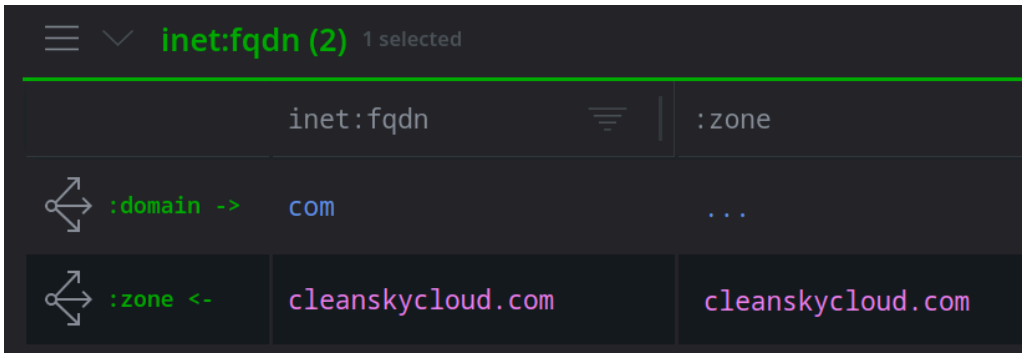


Tip: If a domain whois record lists the DNS name servers for the FQDN, this information is modeled using **`inet:whois:recns`** nodes. You can see these nodes in your **Results Panel**:

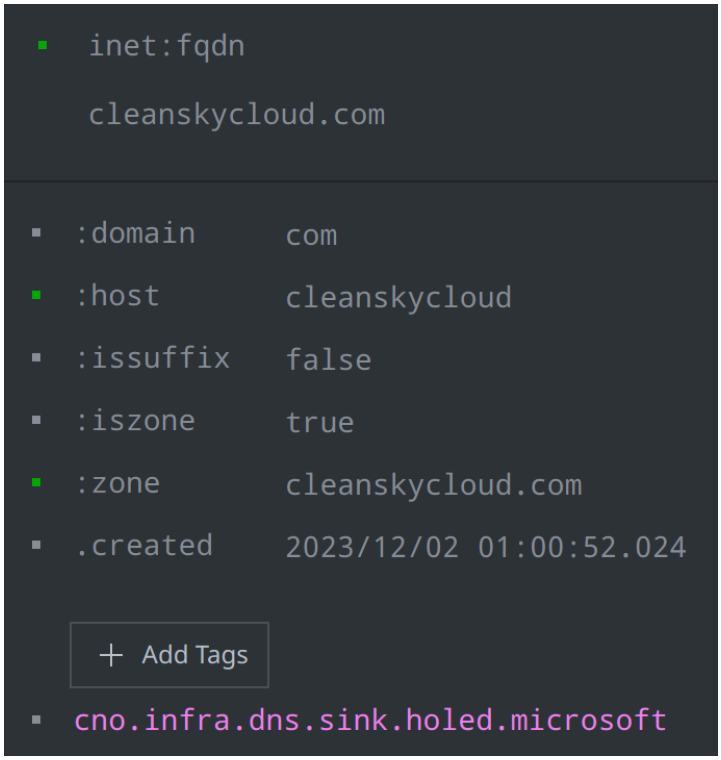


Question 5: What does the FQDN **cleanskycloud.com** look like now?

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

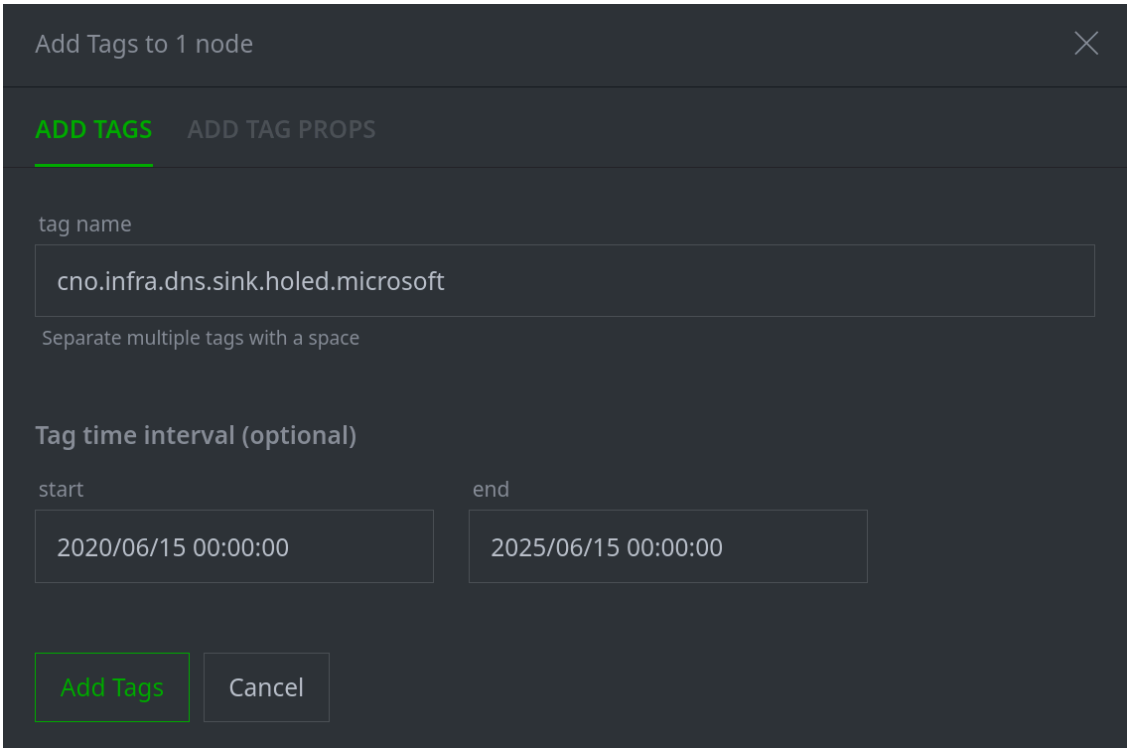


The new tag is also visible in the **Details Panel:**



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

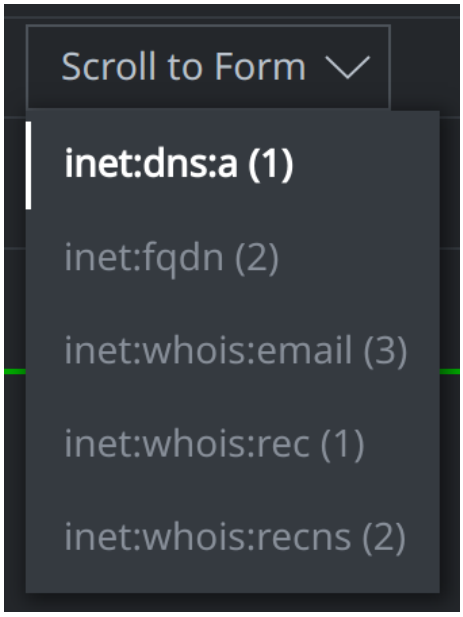
We could **optionally** use this information to add **timestamps** to show "when" Microsoft sinkholed the domain:



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.?)

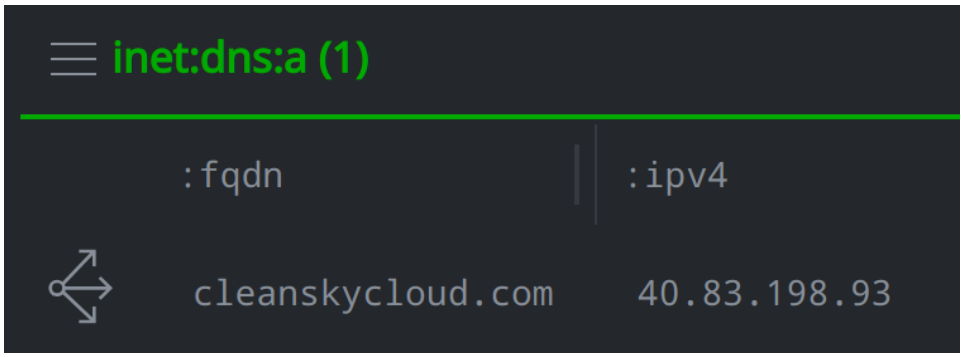
- The NetTools Power-Up created an **`inet:dns:a`** node:



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

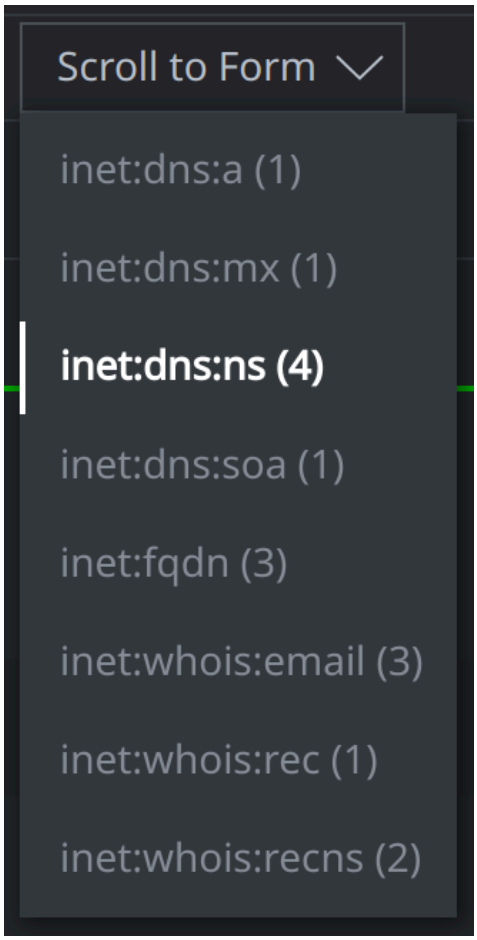
Question 7: What IPv4 address does the FQDN resolve to?

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



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

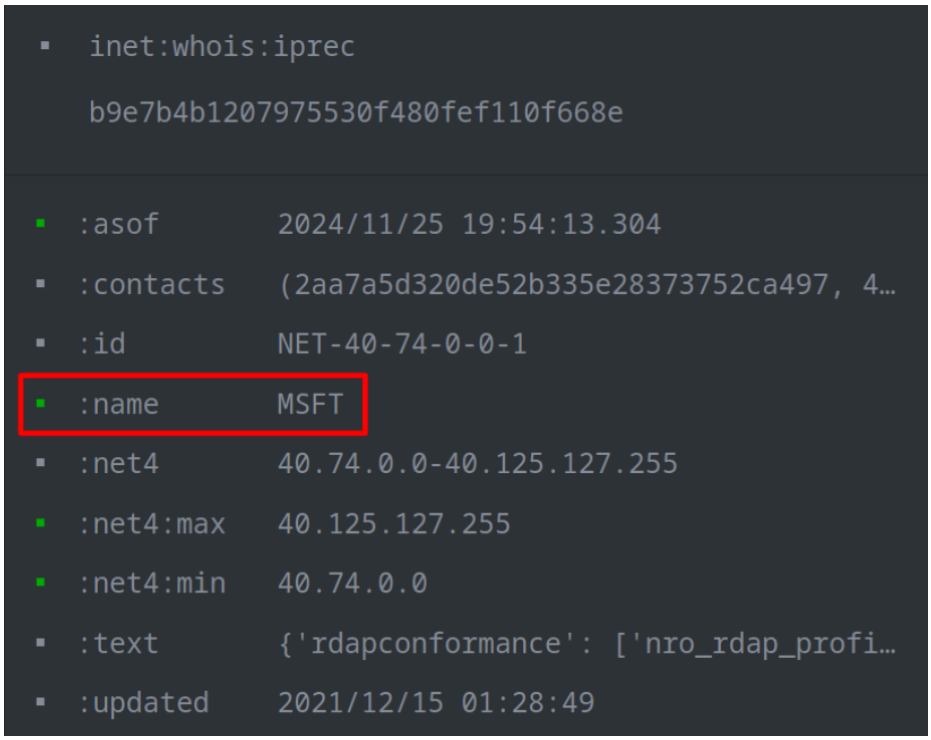
- The NetTools custom Node Action created additional MX, NS, and SOA records:



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

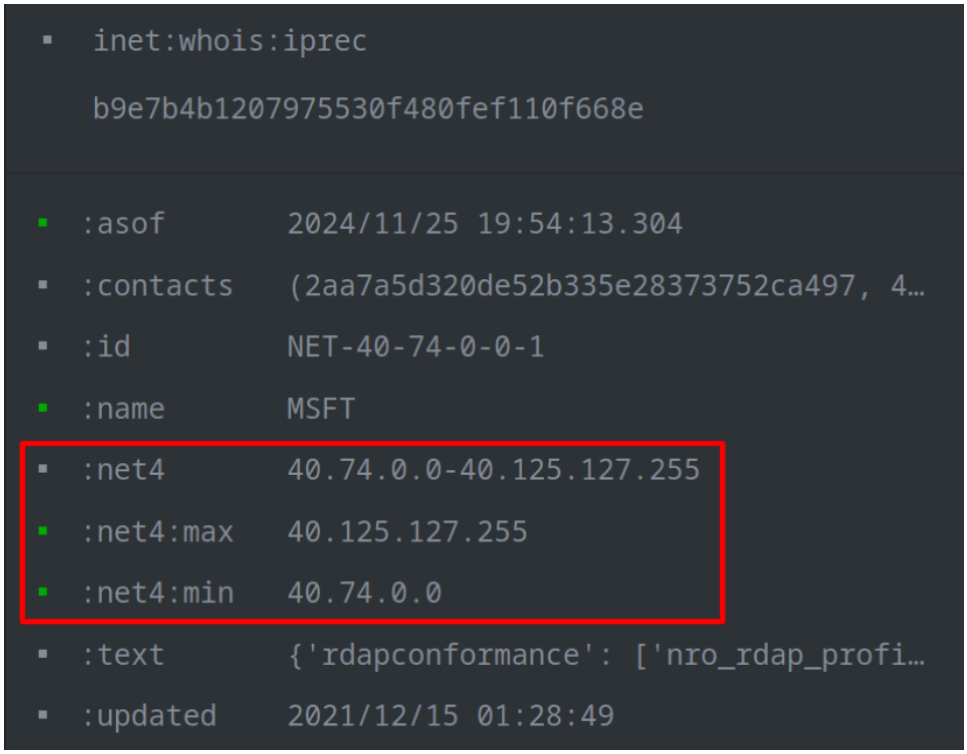
Question 9: What is the network name (**`:name`** property) associated with this netblock?

- The netblock name is **MSFT**:



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 February 2025):

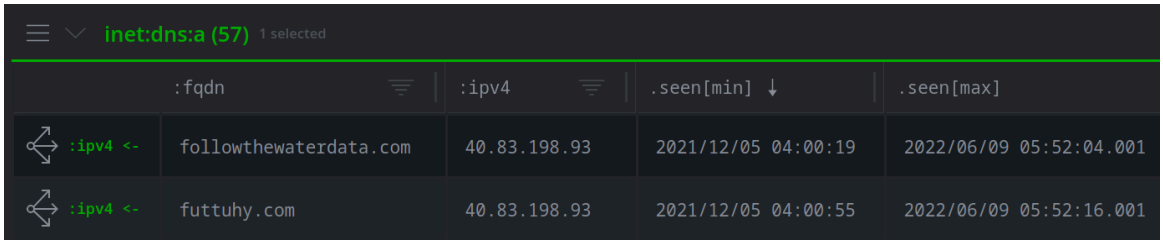


> The **range** of IPv4 addresses for this network is shown in the **`:net4`** property. The first IPv4 (**`:net4:min`**) and last IPv4 (**`:net4:max`**) are also stored separately so you can pivot from them.

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):



> **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 (58)

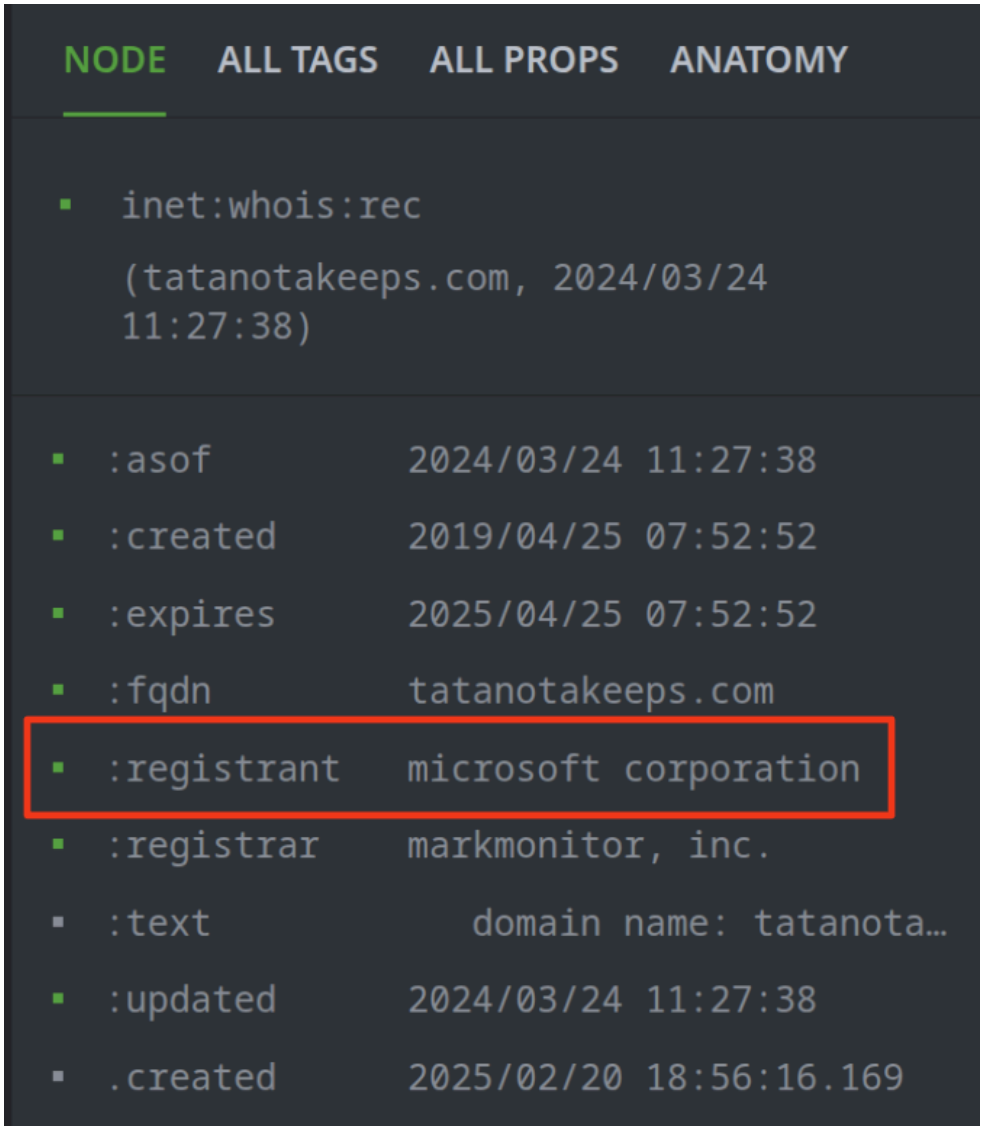
	:fqdn	:ipv4	.seen[min]	.seen[max] ↑
:ipv4 <-	cleanskycloud.com	40.83.198.93	2022/08/27 00:56:48	2025/02/20 18:45:19.532
:ipv4 <-	tatanotakeeps.com	40.83.198.93	2021/12/06 22:21:16	2025/02/06 06:03:44.001

> 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?

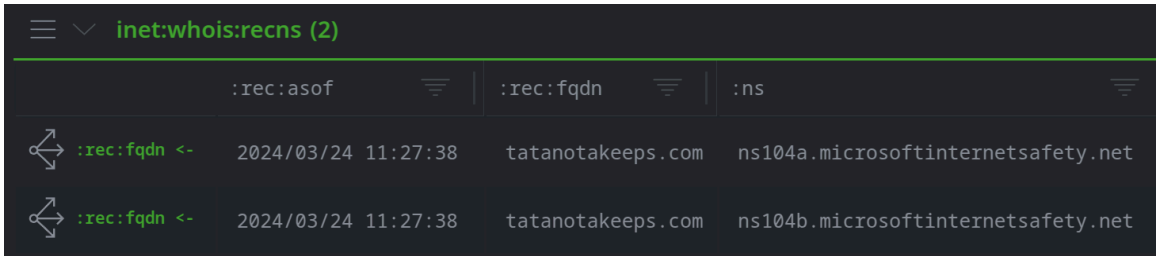
- The registrant is **microsoft corporation:**



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

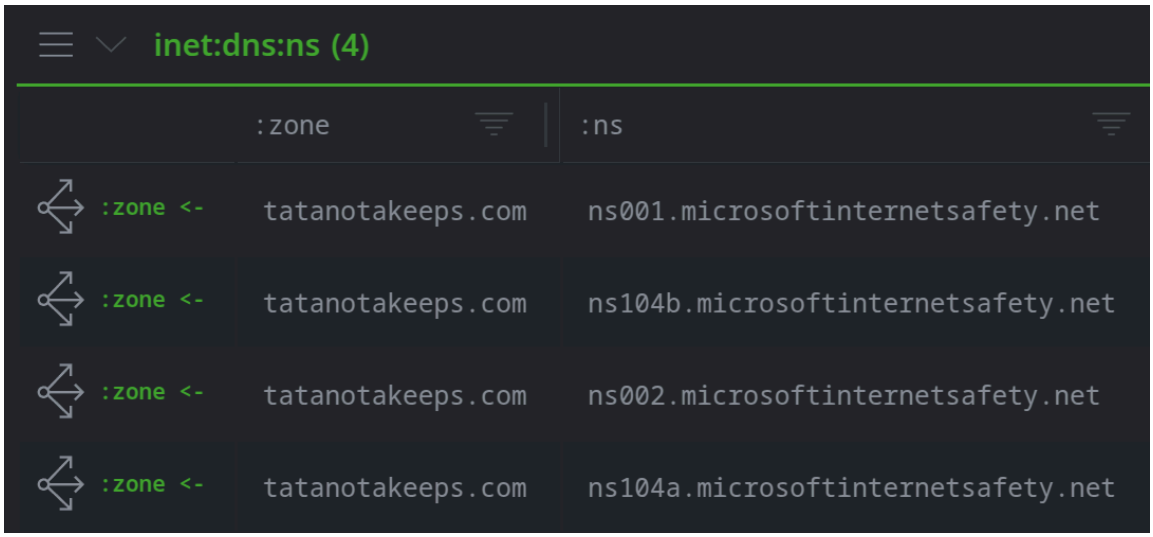
Question 14: What DNS name servers does the FQDN use, according to the whois data?

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



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`**):



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?

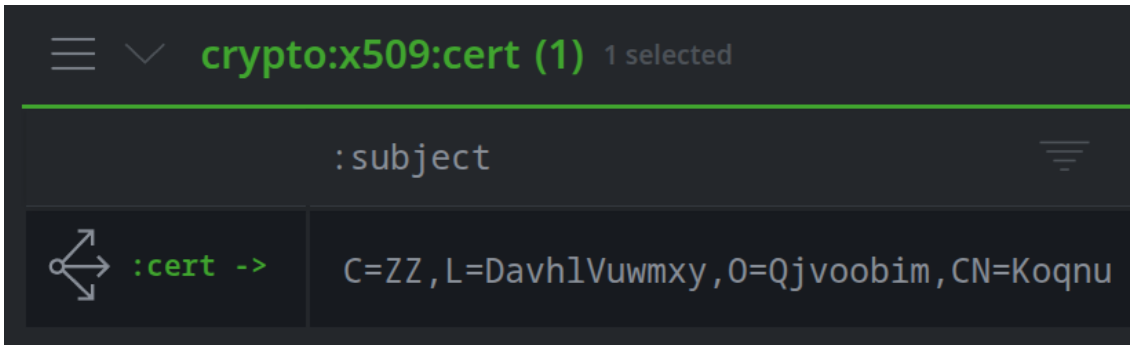
- The certificate was hosted on port **443:**

> **Tip:** An **`inet:tls:servercert`** node links a server (**`inet:server`**) with the metadata (**`crypto:x509:cert`**) for the certificate that was observed there.
>
> The **`inet:tls:servercert`** form replaces the legacy **`inet:ssl:cert`** 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)?

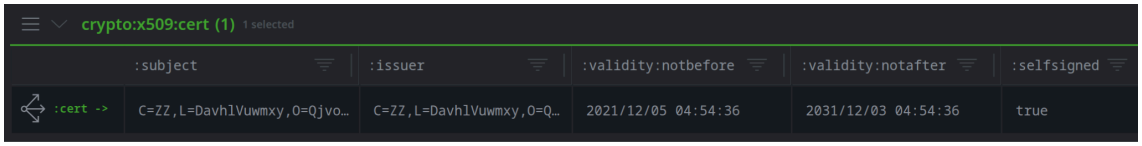
- The **`:subject`** field of the certificate is:

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



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**):



Look for Similar Certificates

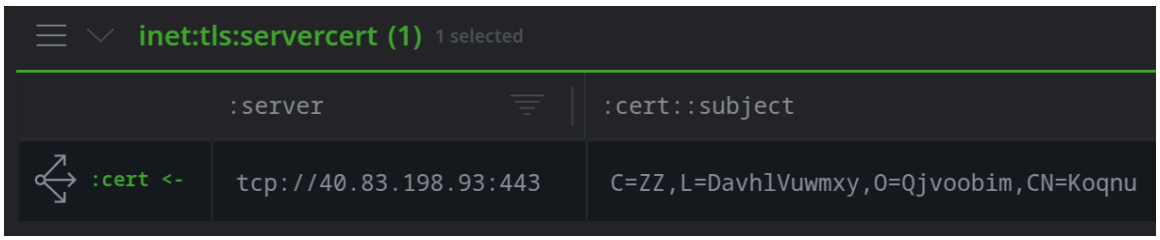
Exercise 2 Answer

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?

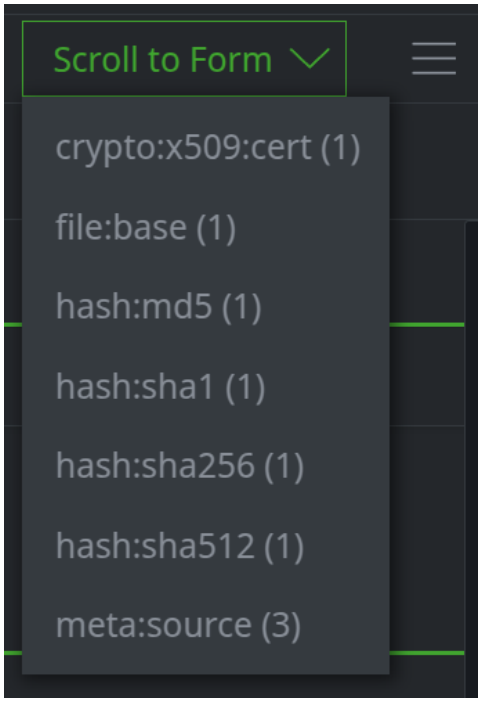
- There is **one** **`inet:tls:servercert`** node in our results:



  This is the node for our original Microsoft sinkhole IPv4.

Question 2: Are there any **`inet:ssl:cert`** nodes in the results?

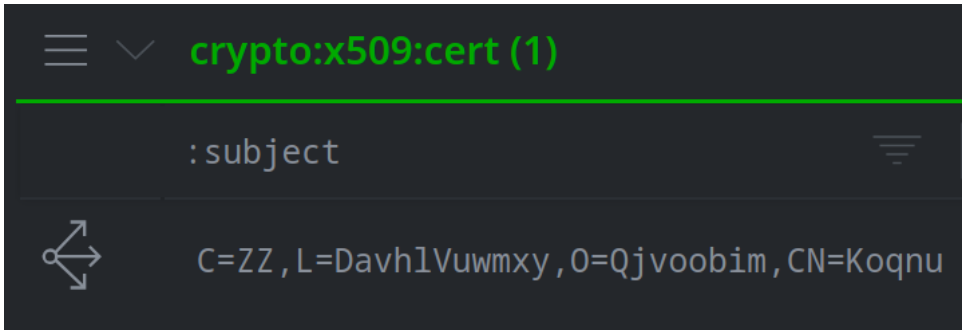
- There are **no** `inet:ssl:cert` nodes:



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

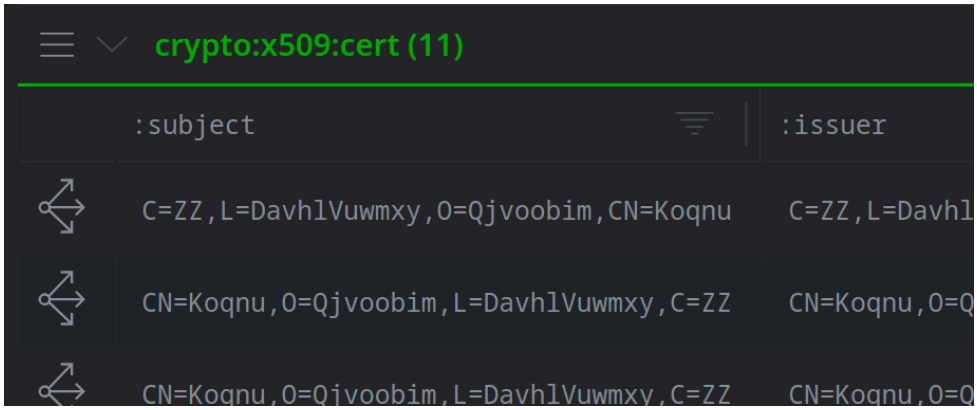
Question 3: How many certificates in Synapse have the same **:subject** value?

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



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

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



> **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):

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.).