Vertex

Synapse Bootcamp - Module 17

Network Infrastructure Analysis - Exercises

Objectives

In these exercises you will learn how to:

- Use Power-Ups to research and characterize network infrastructure

> **Note:** We are constantly updating Synapse and its Power-Ups! We do our best to make sure our course documents (slides, exercises, and answer keys) are up-to-date. However, you may notice small differences (such as between a screen capture in the documents and the appearance of your current instance of Synapse).
>
> If something is unclear or if you identify an error, please reach out to us so we can assist!

Exercises

- All exercises use the **Research Tool** with the **Storm Mode Selector** set to **Storm mode.**
- Some example queries may wrap due to length.

The **Storm Jump Start** (included with the supplemental materials provided for this course) includes sample Storm queries / pivots for some common analysis tasks and may be useful for this module.

Analyzing and Identifying Network Infrastructure

Exercise 1

Objective:

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

A Microsoft blog from December 2021[1] described activity related to a China-based threat actor Microsoft calls NICKEL. Microsoft noted that they had recently seized a number of FQDNs used by the NICKEL threat group.

You want to examine infrastructure associated with one of these seized domains.

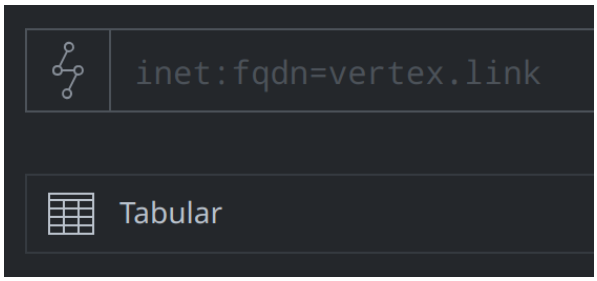
(**Note:** In April 2023, Microsoft renamed its threat groups. Microsoft now tracks NICKEL as Nylon Typhoon.[2] [3])

[1] 2021/12/06, "NICKEL targeting government organizations across Latin America and Europe", https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe/ , accessed 2023/11/02.
[2] 2023/04/18, "Microsoft shifts to a new threat actor naming taxonomy", https://www.microsoft.com/en-us/security/blog/2023/04/18/microsoft-shifts-to-a-new-threat-actor-naming-taxonomy/, accessed 2023/11/02.
[3] 2023/07/12, "How Microsoft names threat actors", https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide, accessed 2023/11/02.

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

You want to retrieve the current whois information for one of the NICKEL domains that Microsoft sinkholed.

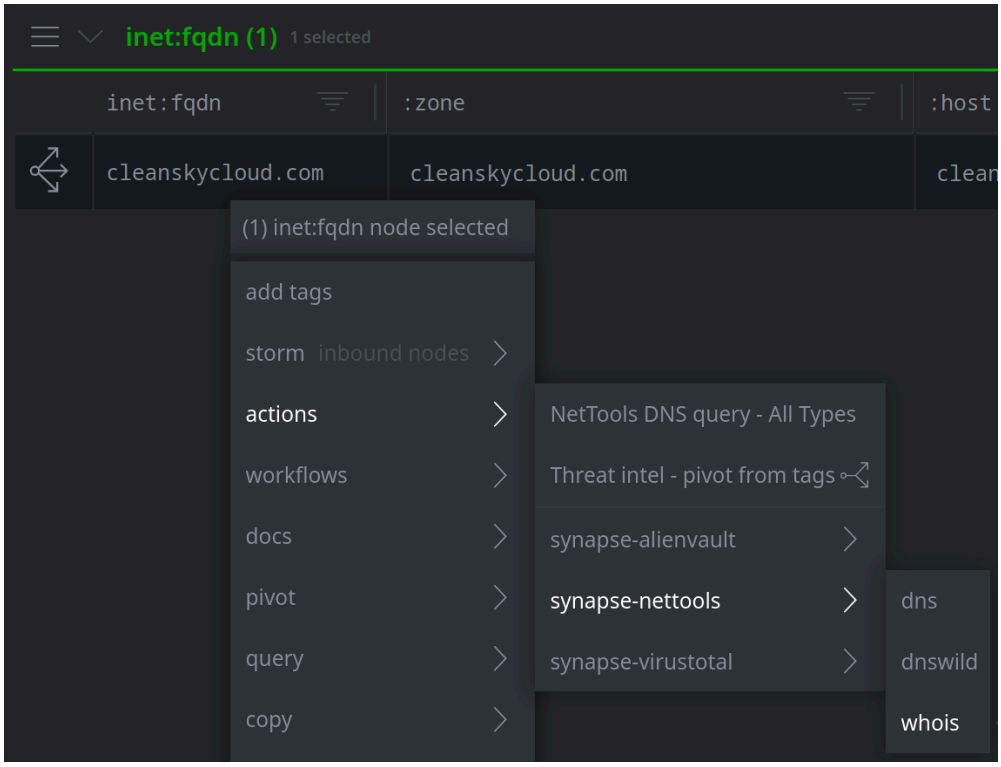
- In the **Research Tool,** ensure your **Storm Query Bar** is in **Storm mode** and your display mode is set to **Tabular:**



- In the **Research Tool,** enter the following in the **Storm Query Bar** and press **Enter** to create a node for one of the NICKEL FQDNs:

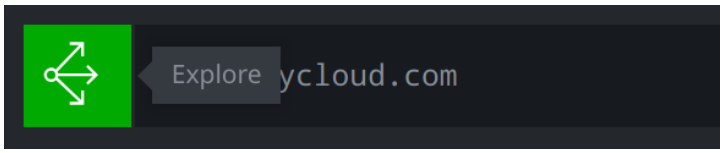
```
[ inet:fqdn=cleanskycloud.com ]
```

- **Right-click** the FQDN and select **actions > synapse-nettools > whois:**

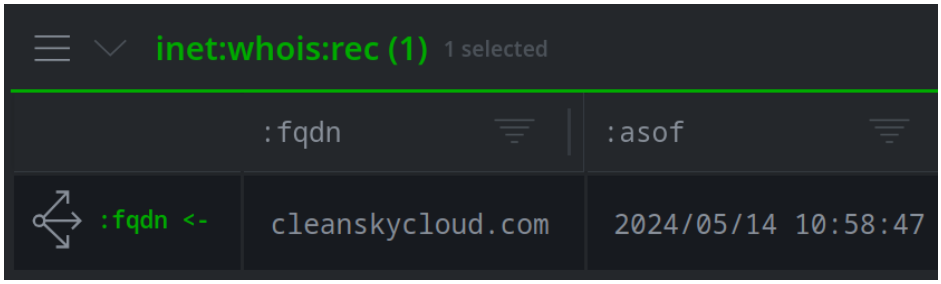


This Node Action performs a **live whois lookup** for the FQDN.

- Click the **Explore** button next to the FQDN to navigate to adjacent nodes:



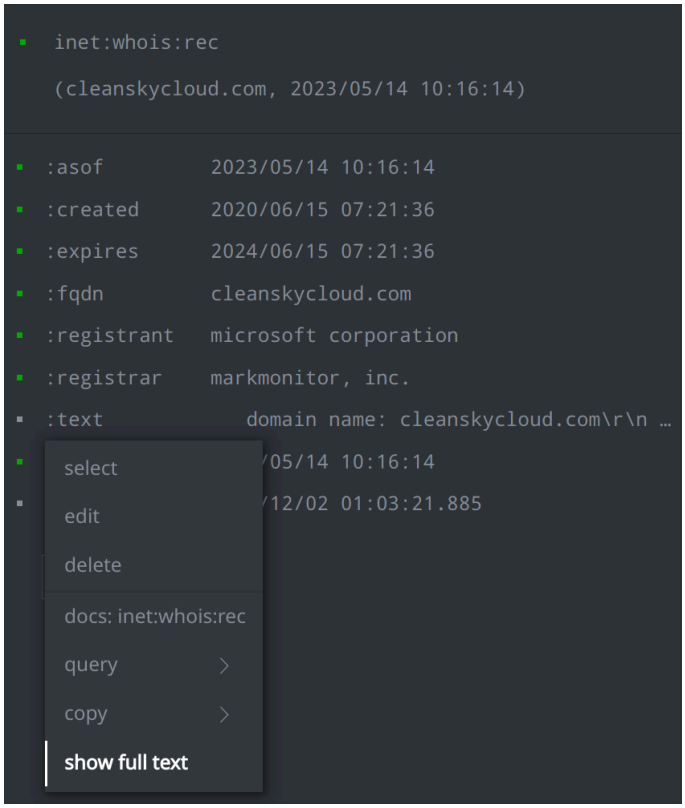
- **Select** the `inet:whois:rec` node (use **Scroll to Form** if needed):



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

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

- In the **Details Panel,** click the **:text** property and select **show full text** to view the full whois record:



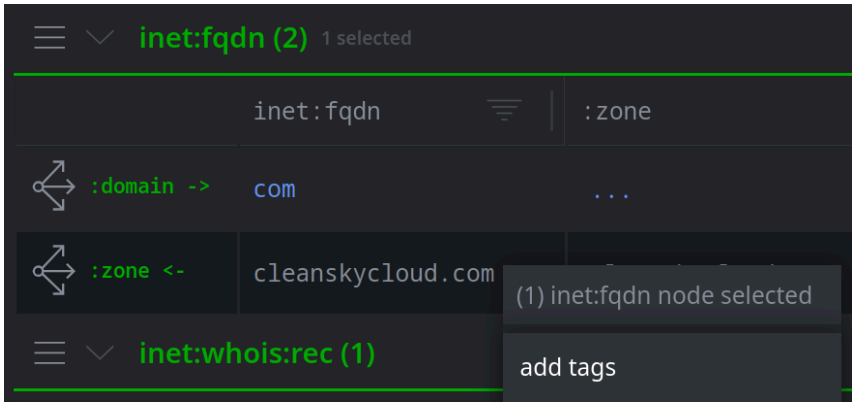
Question 3: Looking at the 'registrant' details in the raw text record, what department within Microsoft registered the FQDN?

Note: you may need to scroll the popup window to view the full record.

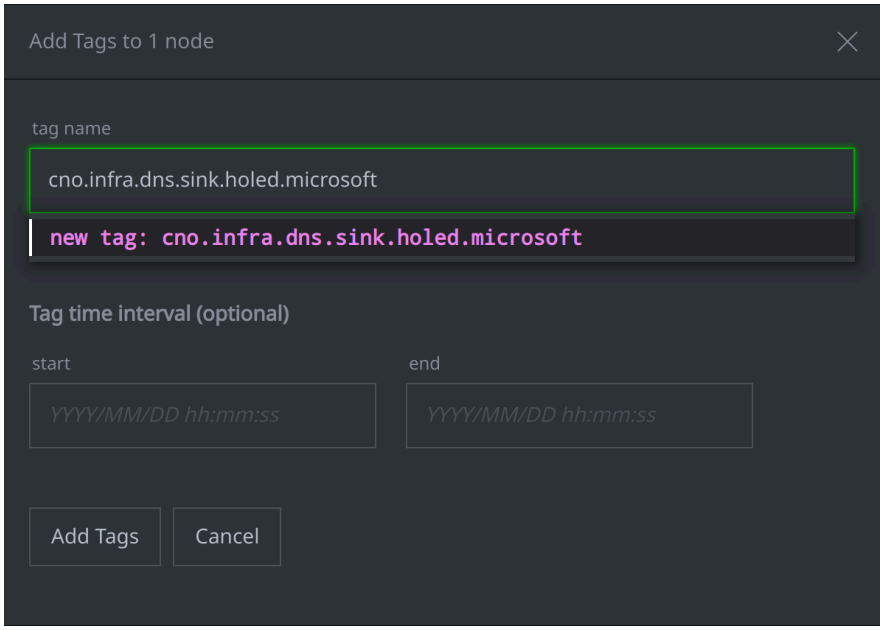
Question 4: Based on the whois data, what DNS **name servers** are used by the FQDN?

It looks like the FQDN **cleanskycloud.com** has been sinkholed by Microsoft. We will apply a tag to the FQDN to indicate that.

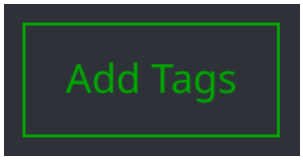
- In the **Results Panel,** locate the **`inet:fqdn`** nodes. **Right-click** the FQDN **cleanskycloud.com** and select **add tags:**



- In the **Add Tags** dialog, enter the tag **cno.infra.dns.sink.holed.microsoft:**



- Click the **Add Tags** button to apply the tag:

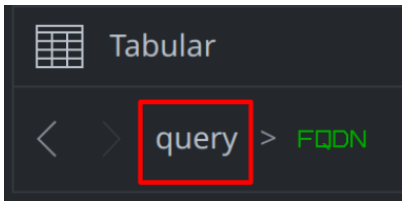


Question 5: What does the FQDN **cleanskycloud.com** look like now?

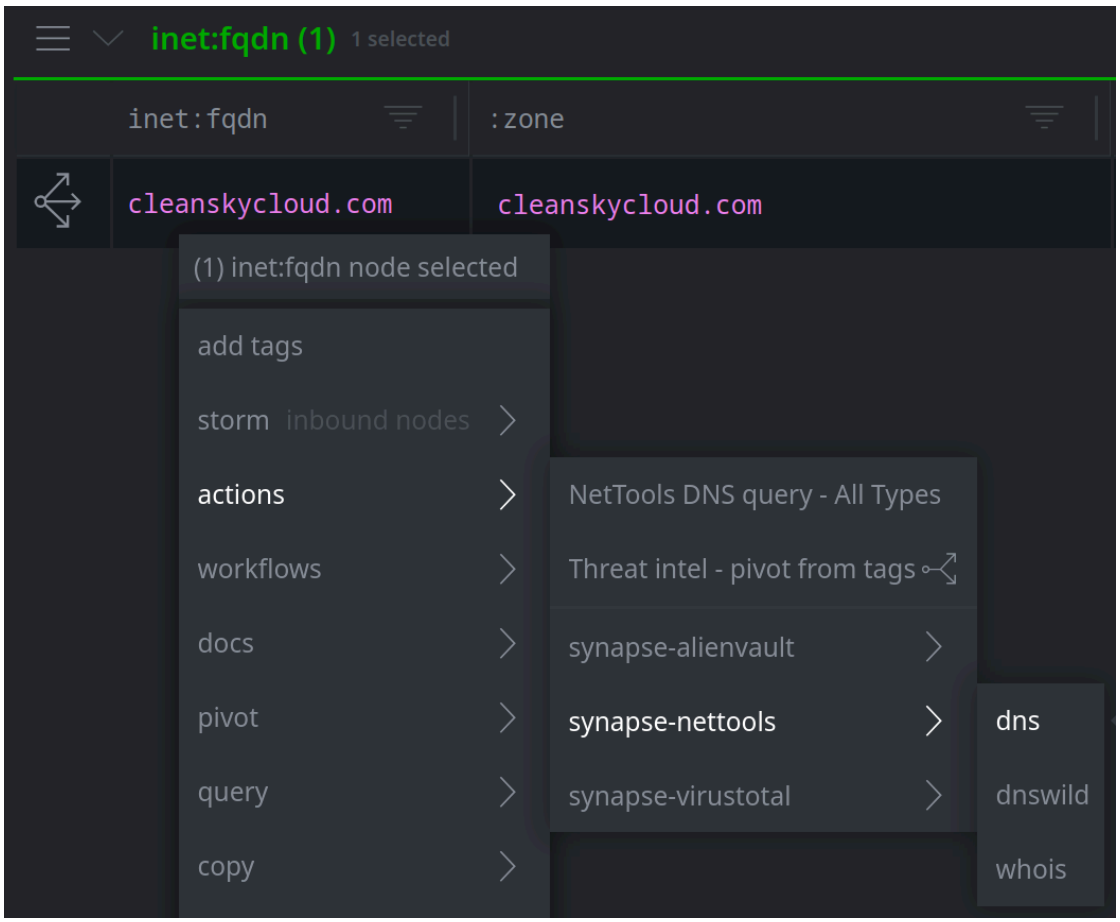
Part 2 - Enriching Data with the NetTools Power-Up - DNS Data

Now that we know **cleanskycloud.com** has been sinkholed by Microsoft, we want to try and identify the IPv4 address of Microsoft's sinkhole server.

- In the **Research Tool,** in your **Breadcrumbs,** click **query** to return to your original query:

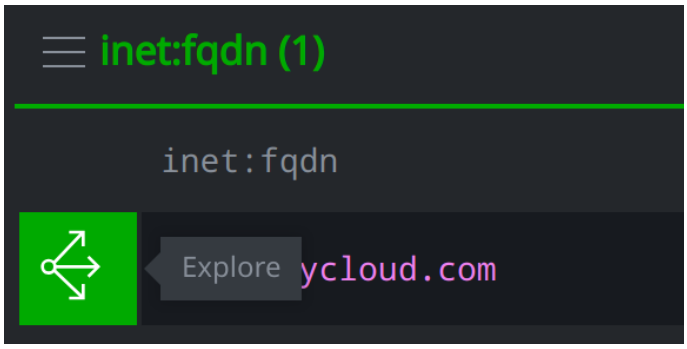


- In the **Results Panel, right-click** the FQDN, and select **actions > synapse-nettools > dns**:



This Node Action performs a **live DNS lookup** for the FQDN using the **default** settings for the NetTools command.

- Click the **Explore** button next to the FQDN to navigate to adjacent nodes:

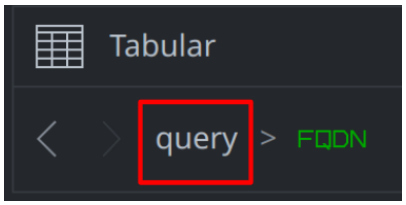


Question 6: What type(s) of DNS records were created (e.g., A, AAAA, MX, etc.?)

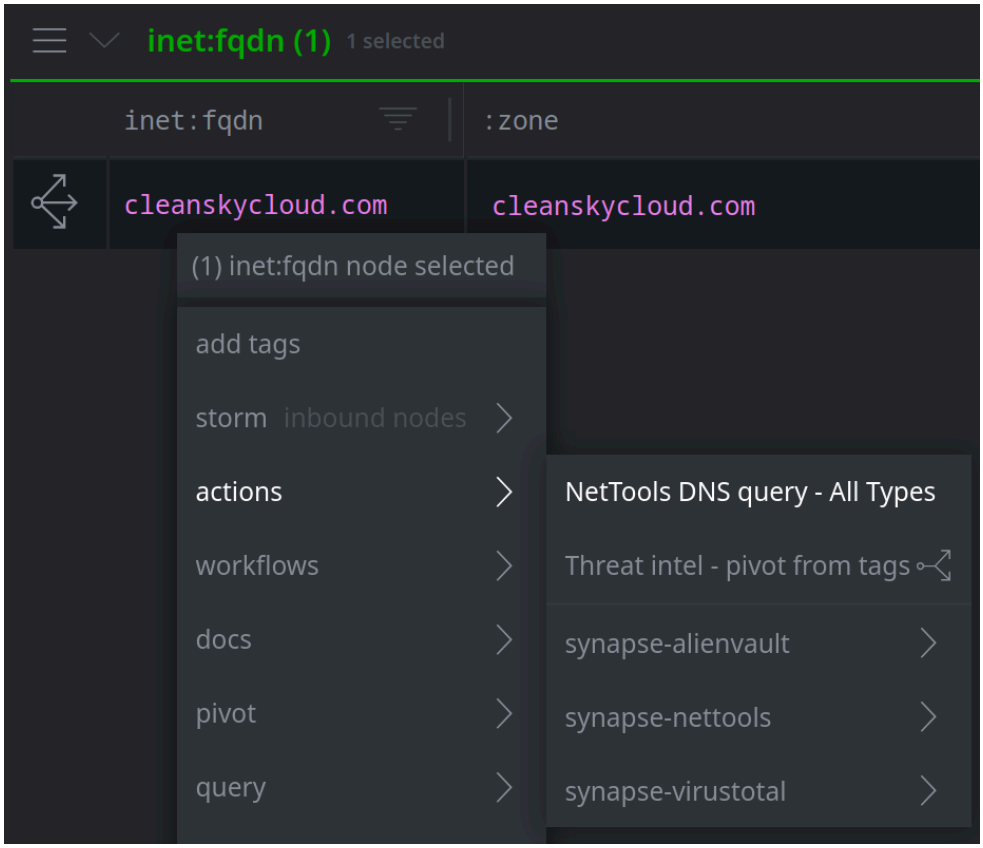
Question 7: What IPv4 address does the FQDN resolve to?

We want to look for additional DNS records for this domain.

- In your **Breadcrumbs,** click **query** to return to your original query:

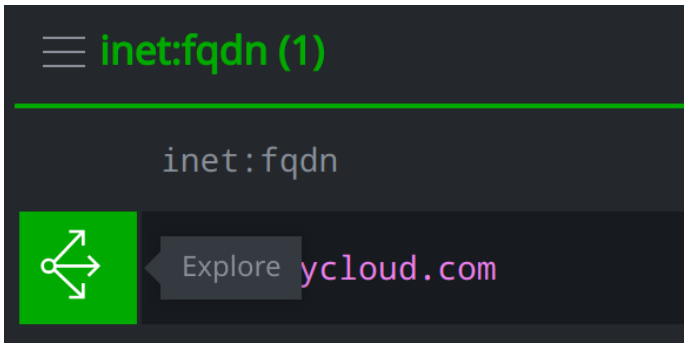


- In the **Results Panel, right-click** the FQDN and select **actions > NetTools DNS query - All Types:**



This is a **custom** Node Action configured in your Workspace. The Node Action runs **live** queries for **all** supported DNS types.

- Click the **Explore** button next to the FQDN to navigate to adjacent nodes:

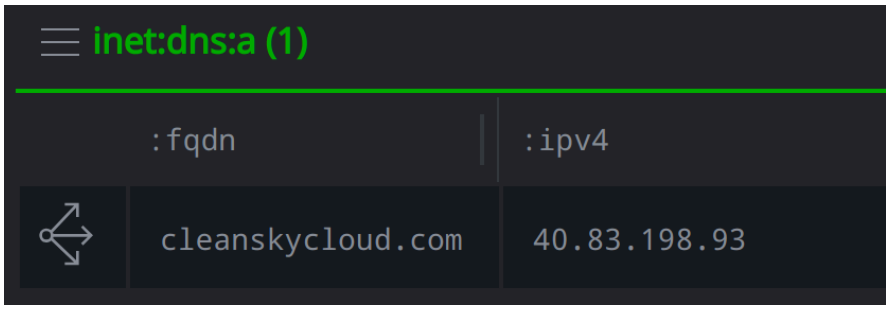


Question 8: What type(s) of DNS records were created (e.g., A, AAAA, MX, etc.?)

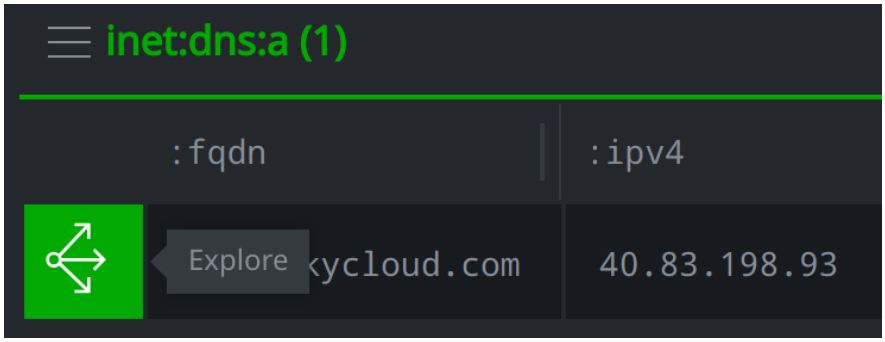
Part 3 - Enriching Data with the NetTools Power-Up - Network Whois Data

We want to investigate the IPv4 address of our suspected sinkhole to see if we can tie it more closely to Microsoft. We can check the network whois information for the IP to see who the network is registered to.

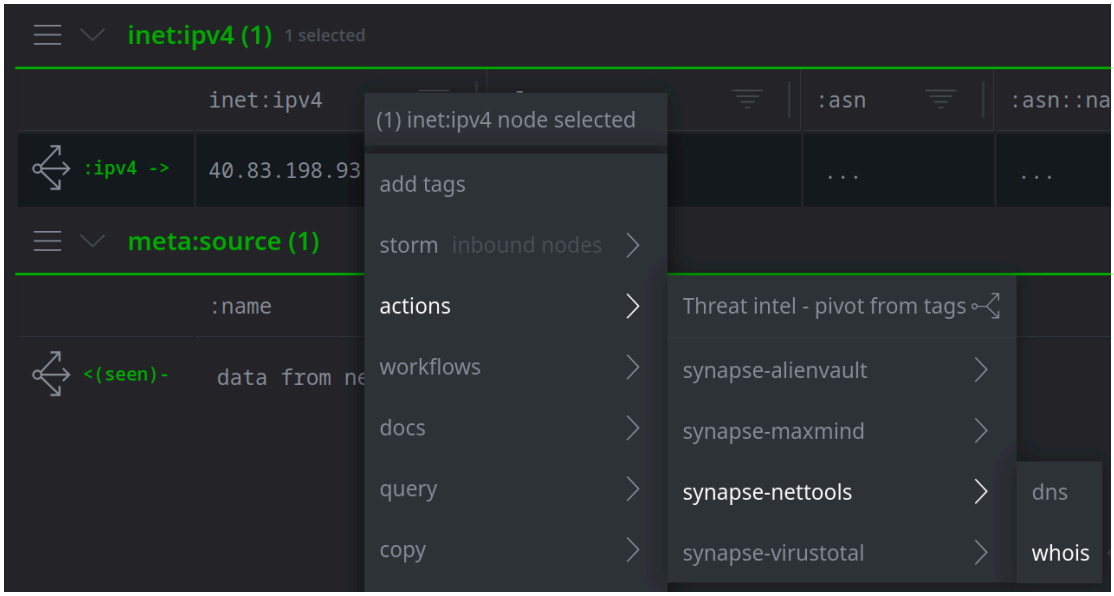
- In your **Results Panel, select** the **`inet:dns:a`** node:



- Click the **Explore** button next to navigate to adjacent nodes:

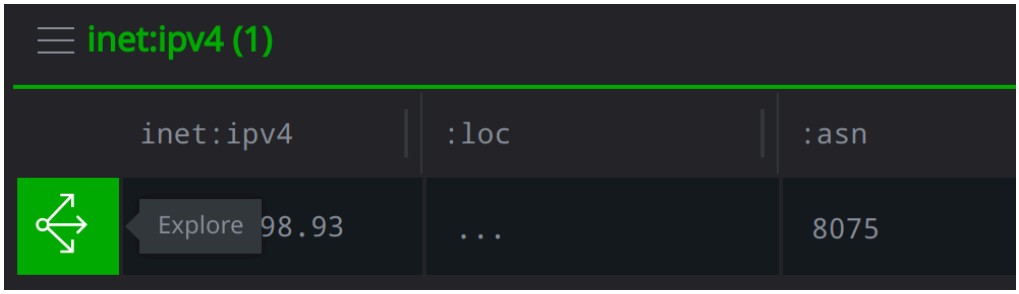


- **Right-click** the **`inet:ipv4`** node and **actions > synapse-nettools > whois**:

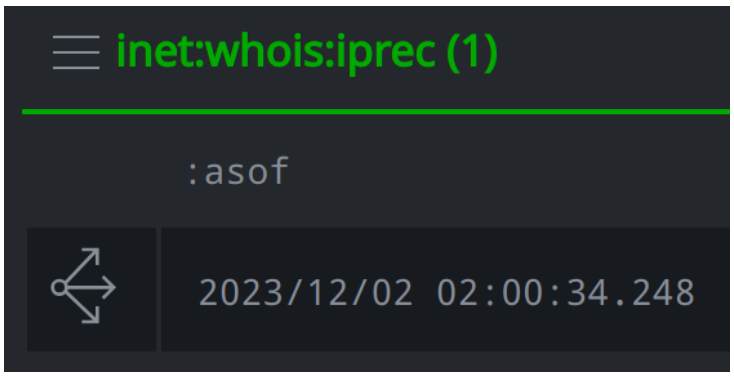


> This Node Action performs a **live network whois lookup** for the IPv4 address to return its network registration data.

- Click the **Explore** button next to the IPv4 to navigate to adjacent nodes:



- In the **Results Panel, select** the **`inet:whois:iprec`** node:



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

Question 10: What are the starting and ending IPv4 addresses associated with this netblock?

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

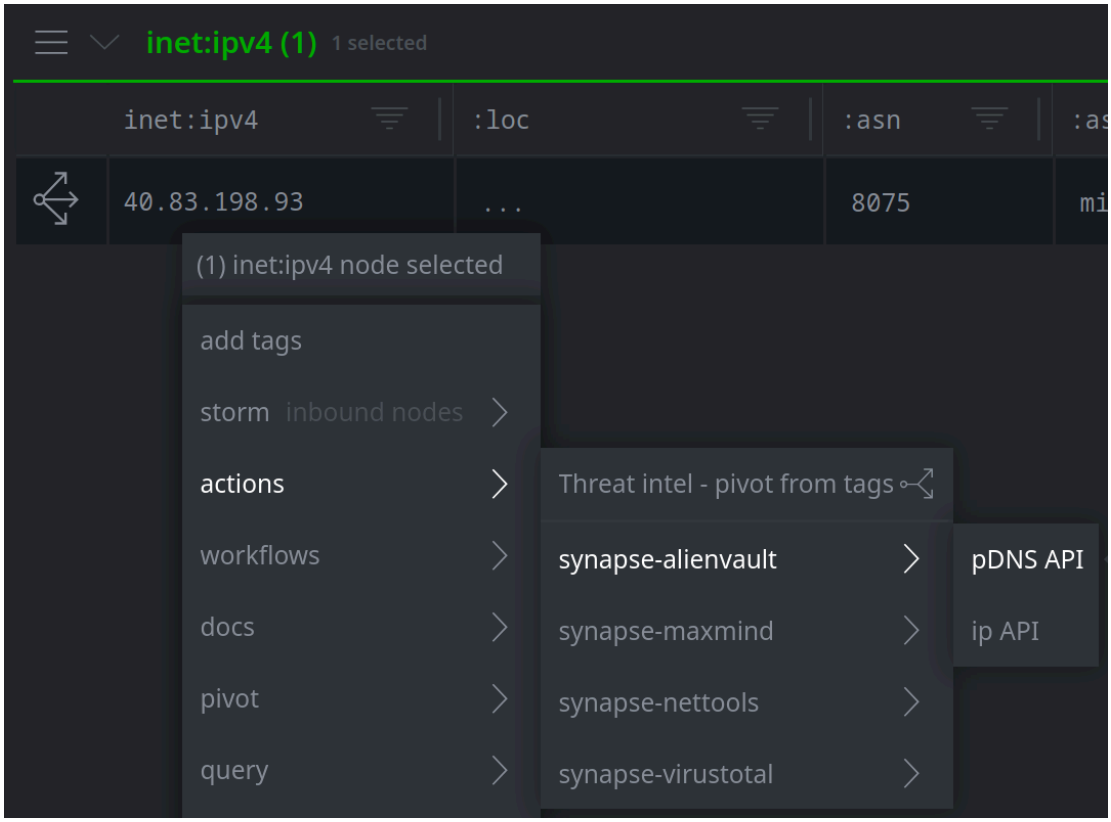
The IPv4 seems to be a Microsoft IPv4 address. It is probably Microsoft's sinkhole server, but we want to collect more data to be certain.

We will use passive DNS (PDNS) data to see if other domains that resolve to this IPv4 are also sinkholed.

- Enter the following in the **Storm Query Bar** and press **Enter** to start a new query for the Microsoft IPv4 associated with the DNS A record:

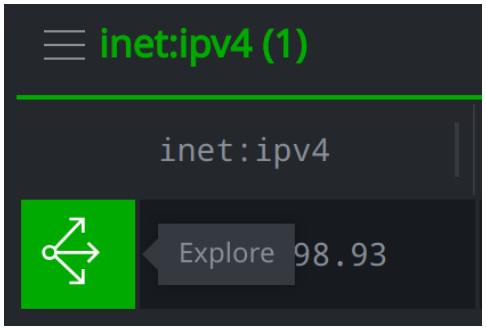
```
inet:ipv4=40.83.198.93
```

- **Right-click** the IPv4 and select **actions > synapse-alienvault > pDNS API:**

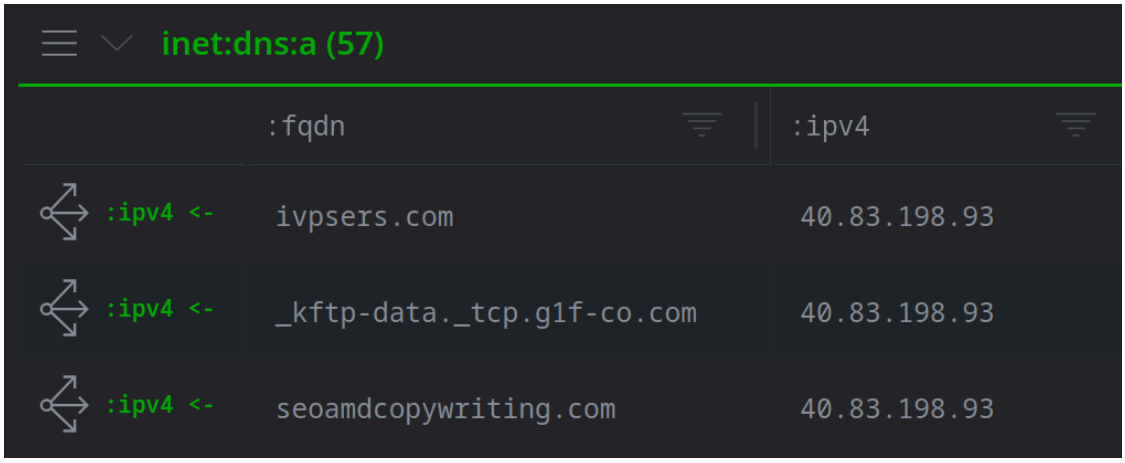


This Node Action retrieves passive DNS data from AlienVault.

- Click the **Explore** button next to the **`inet:ipv4`** to navigate to adjacent nodes:



- Locate the **`inet:dns:a`** nodes:



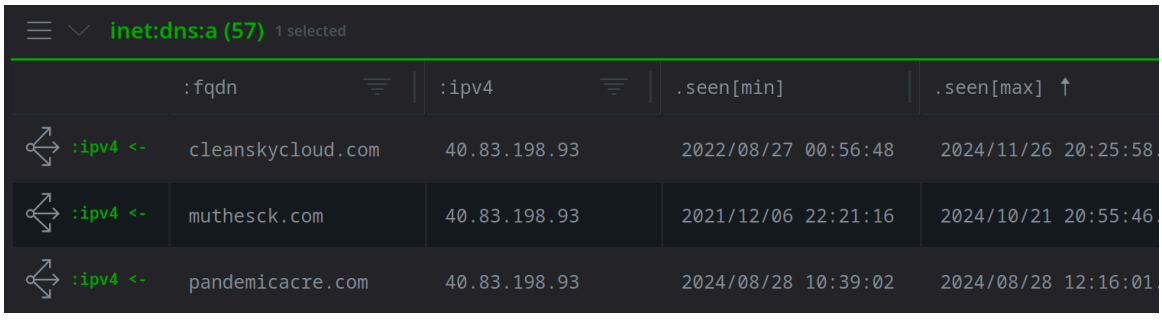
Question 11: What is the **earliest** (**`.seen[min]`**) date that an FQDN resolved to the IPv4?

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

Part 5 - Comparing Domain Whois and DNS Data

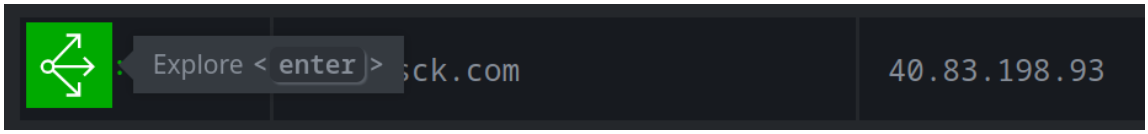
Based on the DNS A records, the FQDN **muthesck.com** is one of the domains that recently resolved to our suspected sinkhole IPv4. We want to check the domain whois information to see if this domain is also registered to Microsoft's Digital Crime Unit.

- In your **Results Panel,** locate the **`inet:dns:a`** record for the FQDN **muthesck.com:**

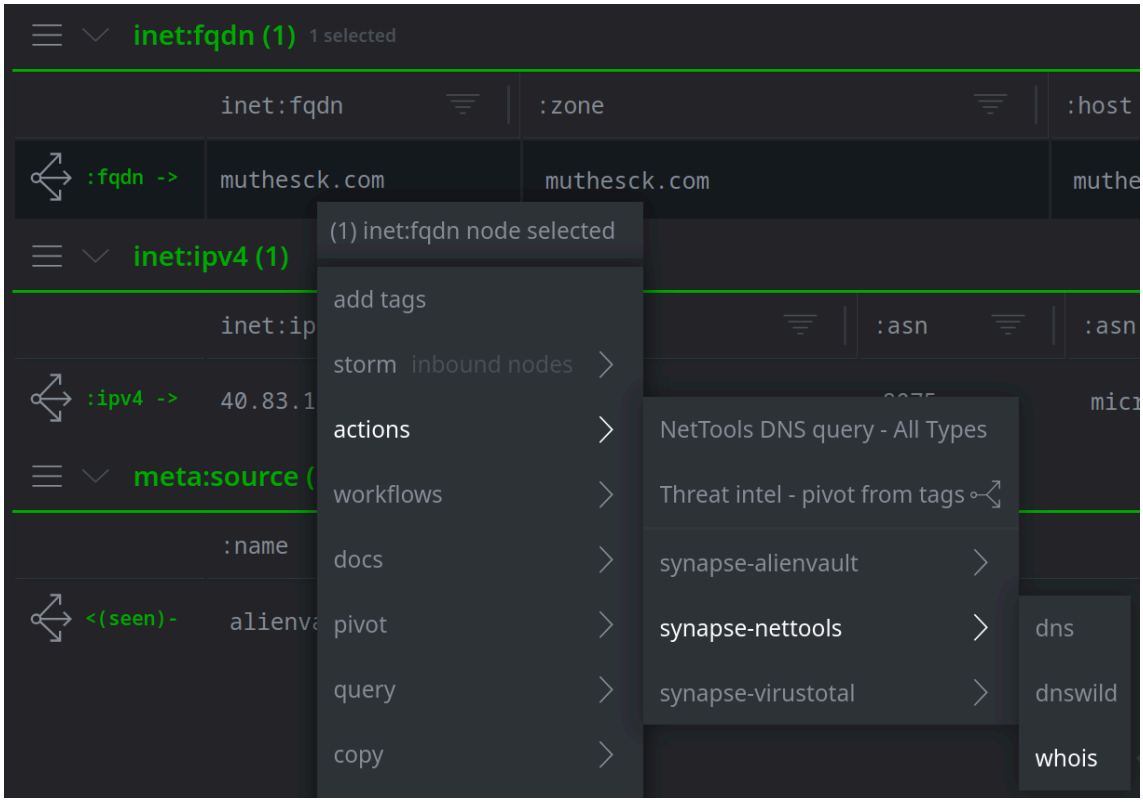


If for some reason AlienVault did not return this FQDN, choose another FQDN zone.

- Click the **Explore** button to navigate to adjacent nodes:

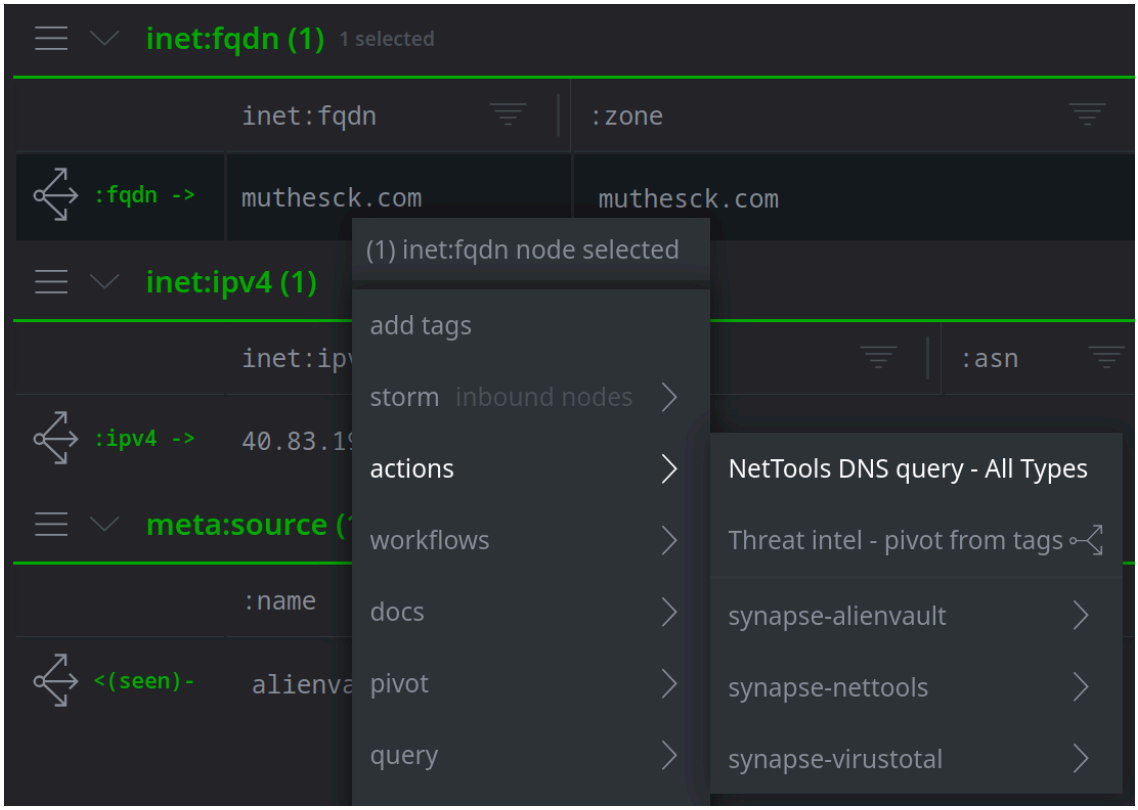


- In the **Results Panel, right-click** the `inet:fqdn` node and select **actions > synapse-nettools > whois**:



This Node Action performs a **live whois lookup** for the FQDN.

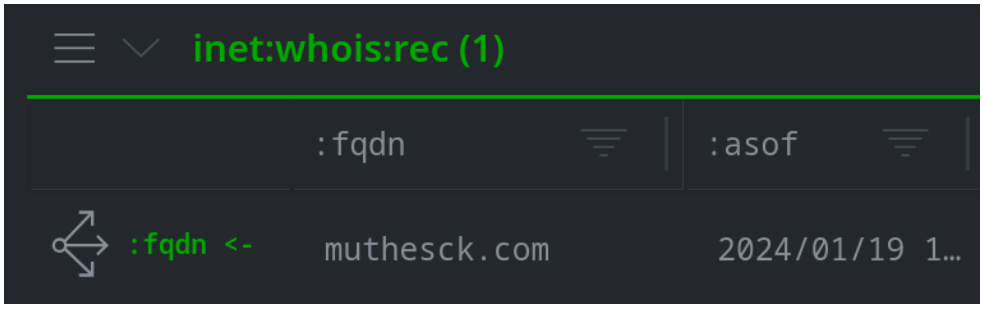
- In the **Results Panel, right-click** the **inet:fqdn** node and select **actions > NetTools DNS - Query all types** to retrieve live DNS data:



This Node Action performs **live DNS queries** for all supported DNS types (e.g., A, AAAA, MX, etc.).

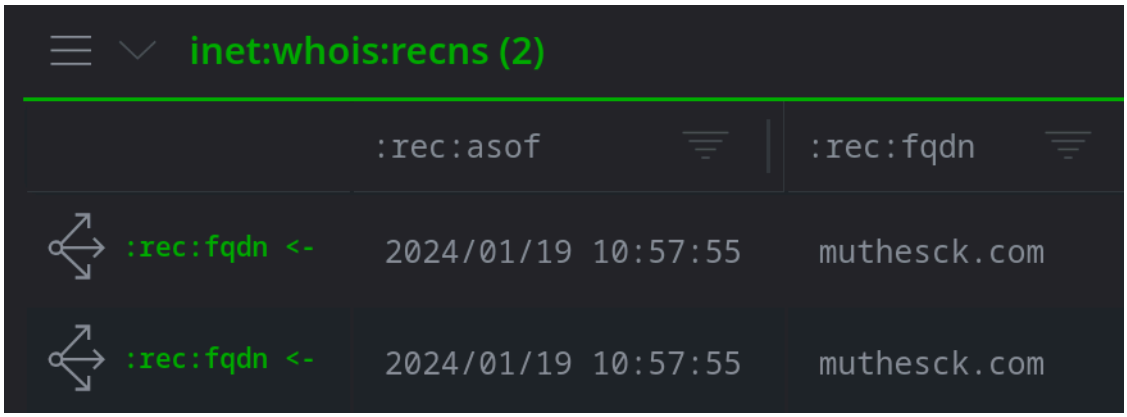
- Click the **Explore** button next to the FQDN to navigate to adjacent nodes:

- Locate the domain whois record (**`inet:whois:rec`** node - use **Scroll to Form** if needed):



Question 13: Who is the registrant for the FQDN?

- Locate the whois name server records (**`inet:whois:recns`** nodes - use **Scroll to Form** if needed):



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

- Locate the DNS NS records (**`inet:dns:ns`** nodes - use **Scroll to Form** if needed):

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

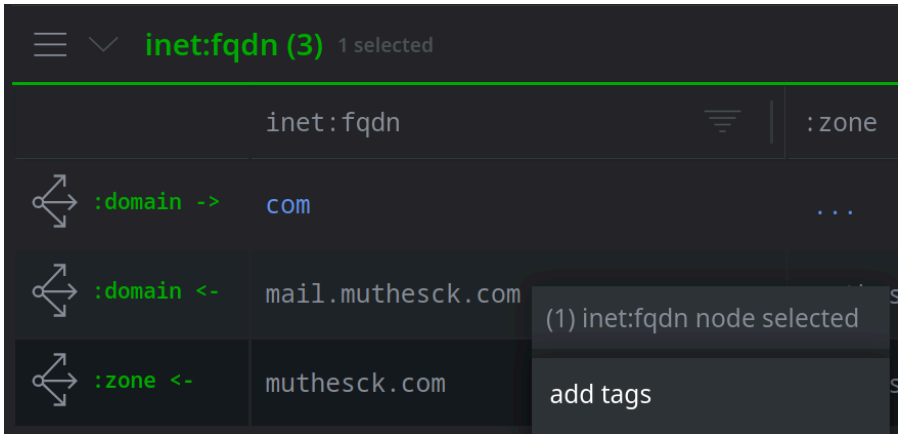
So far we have discovered:

- Both **muthesck.com** and **cleanskycloud.com** have been sinkholed by Microsoft.
- Both domains resolve to IPv4 **40.83.198.93**.
- IPv4 **40.83.198.93** resides on a Microsoft network.
- This IPv4 is very likely a Microsoft sinkhole server.

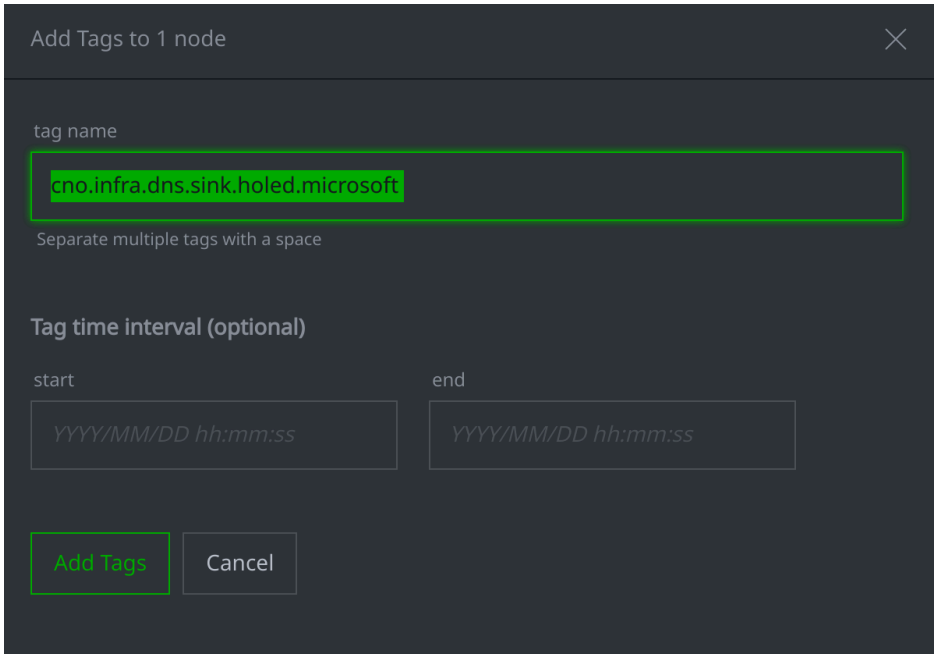
We want to **tag** these nodes to record our findings.

Tag the FQDN

- In your **Results Panel,** locate the **inet:fqdn** nodes (use **Scroll to form** if necessary). **Right-click** the FQDN **muthesck.com** and select **add tags**:



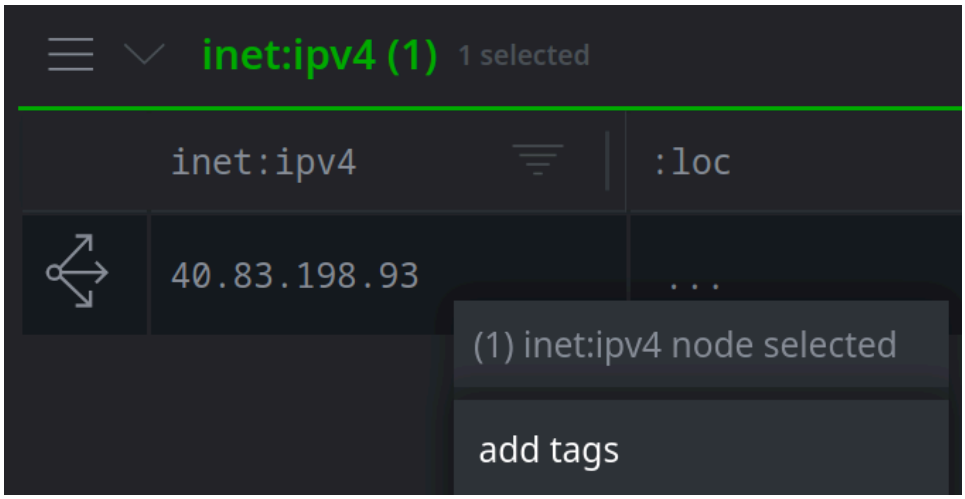
- In the **Add Tags** dialog, enter the tag **cno.infra.dns.sink.holed.microsoft.** Click the **Add Tags** button to apply the tag:



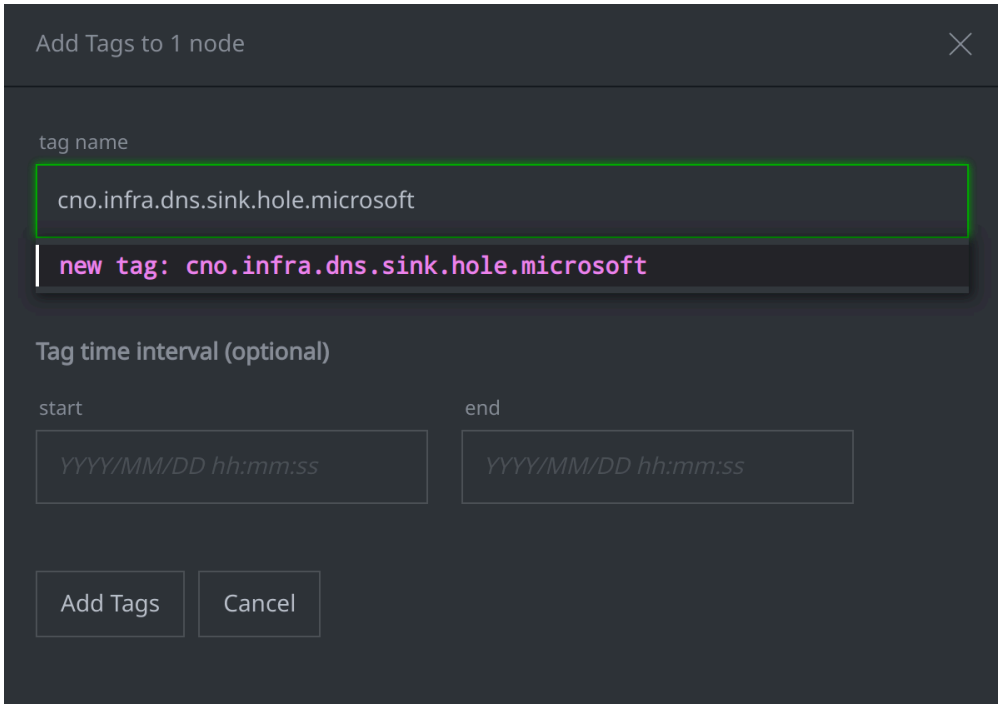
Tag the IPv4

- In your **Breadcrumbs,** click **query** to return to your original query (for the IPv4):

- **Right-click** the IPv4 and select **add tags:**

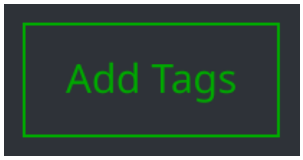


- In the **Add Tags** dialog, in the *tag name* field, enter the tag **cno.infra.dns.sink.hole.microsoft:**



> **Note:** within Vertex, we use two tags to show the difference between a **sinkholed** domain (**sink.holed**) and an IPv4 address that is a **sinkhole** (**sink.hole**).

- Click the **Add Tags** button to apply the tag:

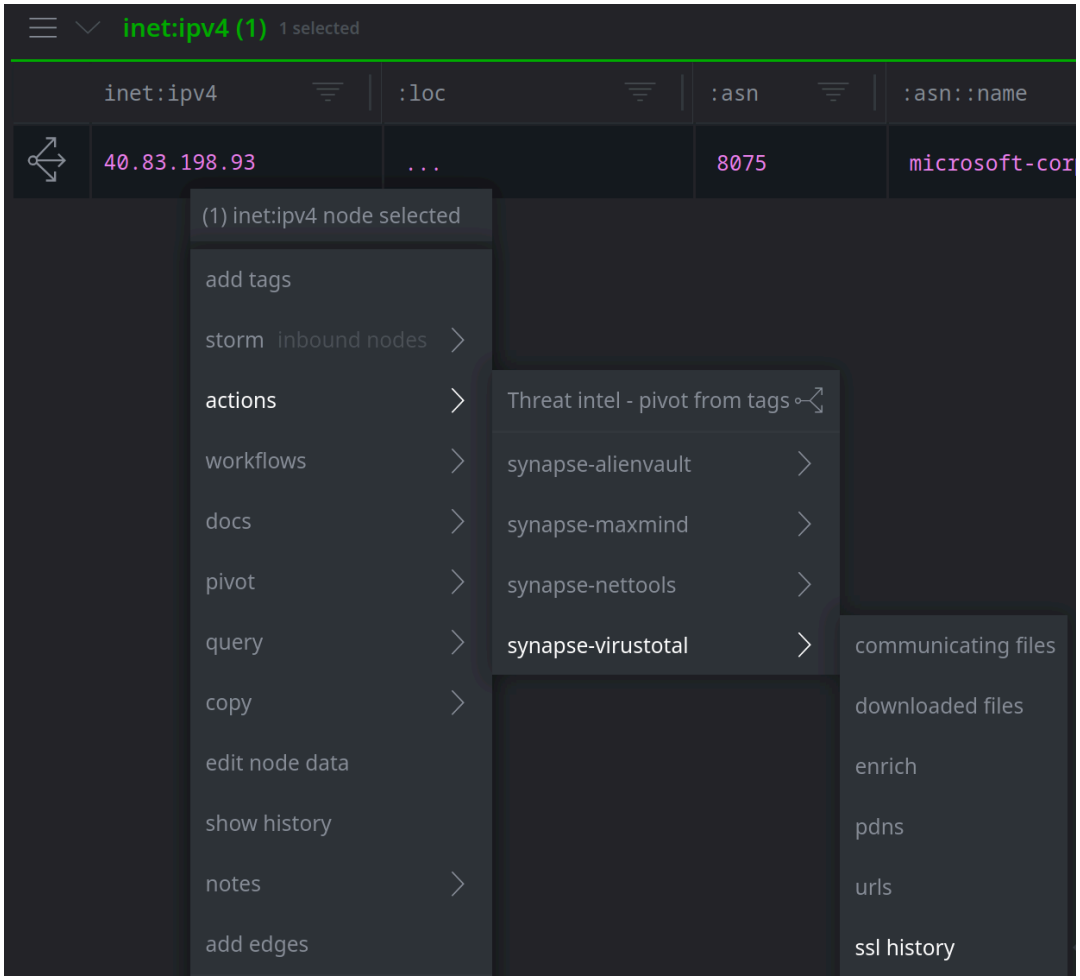


Part 6 - Checking Network Infrastructure

Nice work! You have identified a Microsoft sinkhole, along with some indicators (such as DNS name servers) that can help us identify sinkholed domains.

Now we want to look at the sinkhole IPv4 in more detail. Maybe the host has some features that can help us identify similar sinkholes.

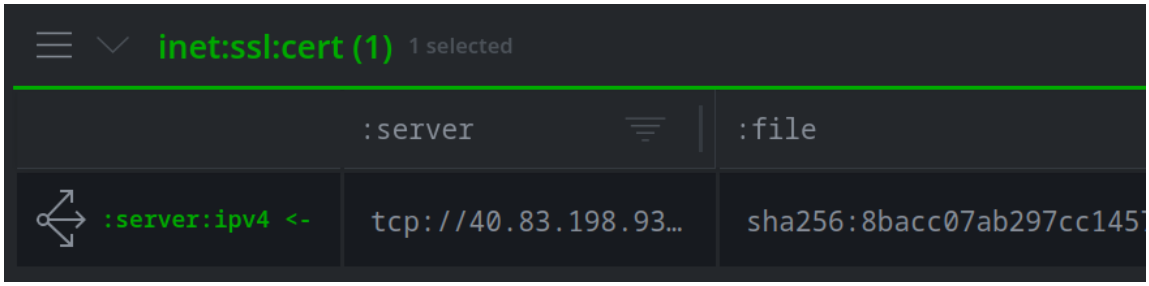
- In the **Results Panel, right-click** the IPv4 and select **actions > synapse-virustotal > ssl history:**



This Node Action retrieves any SSL/TLS certificate information for the IPv4 from VirusTotal.

- Click the **Explore** button next to the IPv4 to navigate to adjacent nodes:

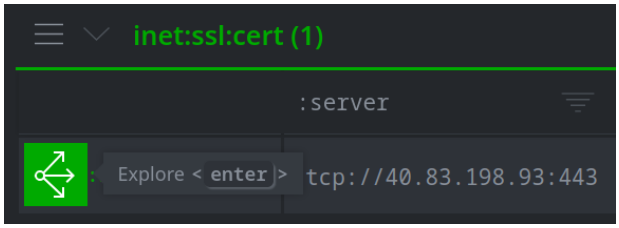
- Locate the **`inet:ssl:cert`** node (use **Scroll to Form** if necessary):



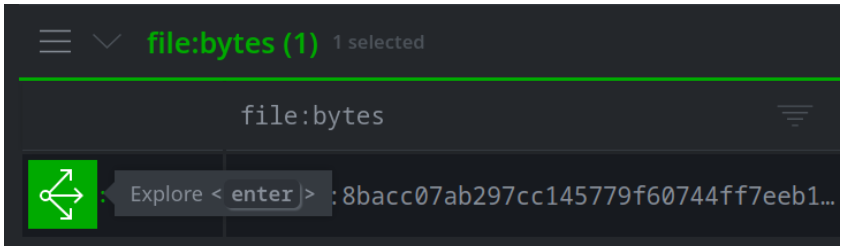
Question 16: What port was serving the certificate?

Let's examine the certificate in more detail.

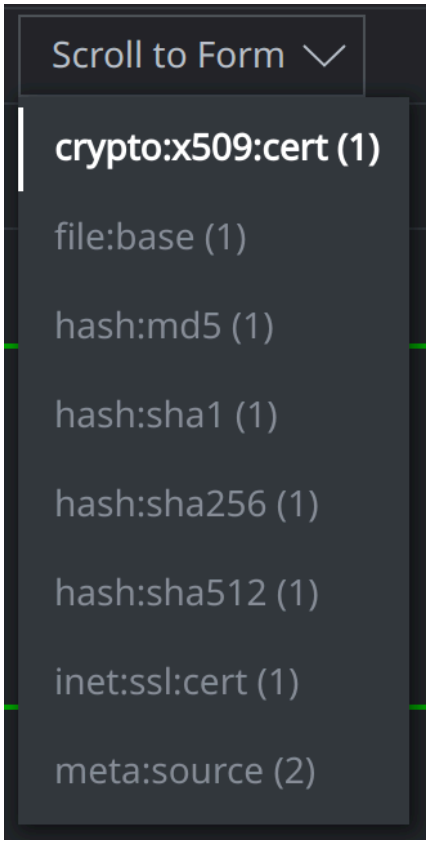
- Click the **Explore** button next to the **`inet:ssl:cert`** node to navigate to adjacent nodes:



- **Select** the **`file:bytes`** node representing the SSL/TLS certificate. Click the **Explore** button to navigate to adjacent nodes:



- Use **Scroll to Form** to locate the `crypto:x509:cert` node:



> The `crypto:x509:cert` node represents the **metadata** (certificate details) returned from any Power-Ups or parsed from the file by Synapse FileParser.

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

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

Look for Similar Certificates

Exercise 2

Objective:

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

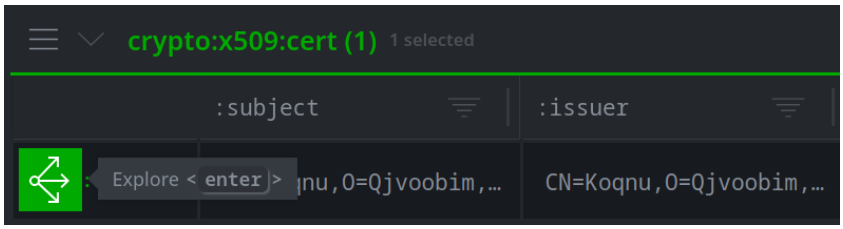
This is unexpected! The certificate is not issued to "Microsoft" and is not signed by a known Certificate Authority. Does Microsoft use strange self-signed certificates for their sinkhole infrastructure? How can we find out?

We can look for additional **hosts** (IPv4 addresses) where:

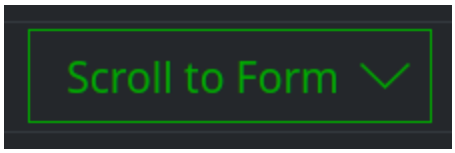
- this **exact** certificate was seen; or
- a similar certificate was seen.

We want to find other hosts where this **exact** certificate was seen. Let's see if any of this information exists in Synapse.

- In the **Results Panel, select** your **`crypto:x509:cert`** node. Click the **Explore** button to navigate to adjacent nodes:



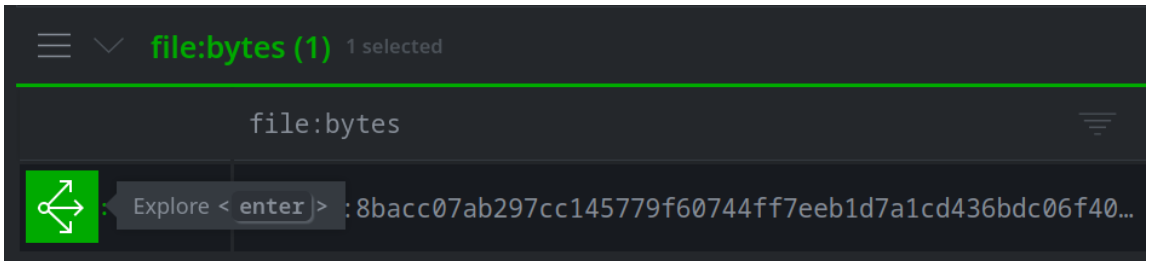
- Use the **Scroll to Form** button to browse the results:



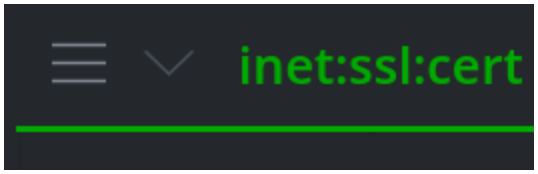
Question 1: Are there any **`inet:tls:servercert`** nodes in the results?

Let's check for any **`inet:ssl:cert`** nodes as well.

- In the **Results Panel, select** the **`file:bytes`** node representing the certificate. Click the **Explore** button to navigate to adjacent nodes:f



- Locate the **inet:ssl:cert** node(s) (use **Scroll to Form** if necessary):



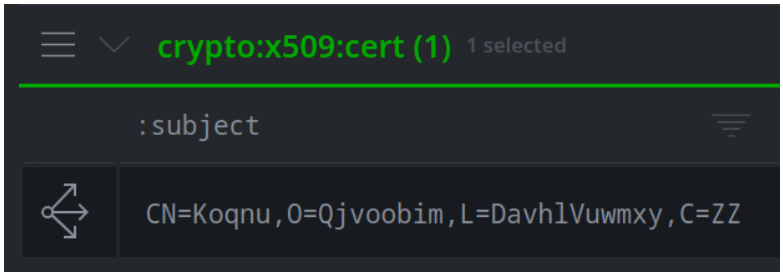
Question 2: How many **inet:ssl:cert** nodes are in the results?

Based on information in Synapse, this **specific** certificate has only been seen on **one** host (our sinkhole IPv4).

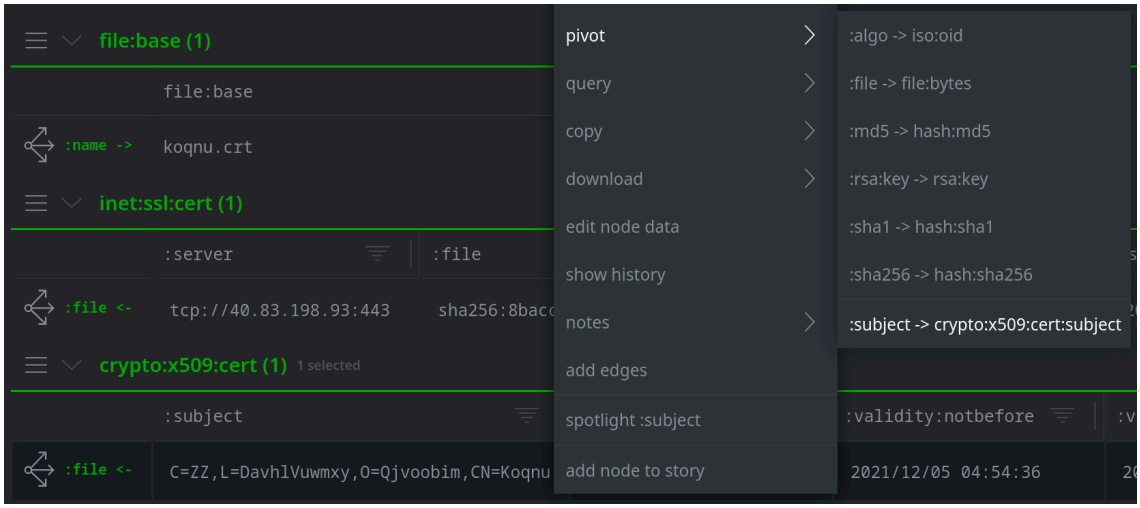
Next we will look for hosts where **similar** certificates were seen.

Our certificate uses some strange naming conventions for the **:subject** and **:issuer**. We will look for any certificates in Synapse that use the exact same **:subject.**

- In your **Results Panel,** locate the **crypto:x509:cert** node:



- **Right-click** the **:subject** field and select **pivot > :subject -> crypto:x509:cert:subject** to pivot to any nodes that share the same **:subject** value:



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

Certificate subjects (and issuers) are string values. Let's perform one more search in case different data sources have provided the same information in a slightly different format.

We'll use **Storm** to perform a regular expression (regex) search on one of our unusual name strings.

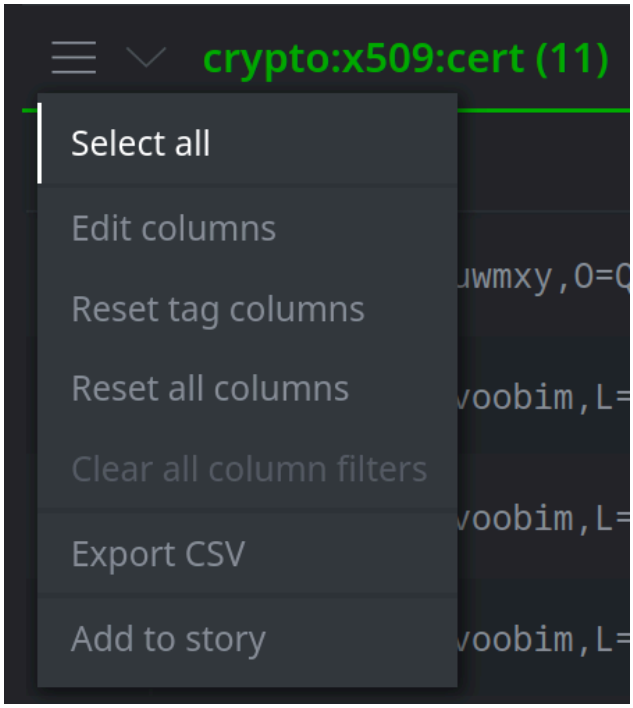
- Enter the following in the **Storm Query Bar** and press **Enter** to search for any `crypto:x509:cert` nodes whose `:subject` contains the string 'Koqnu':

```
crypto:x509:cert:subject~=Koqnu
```

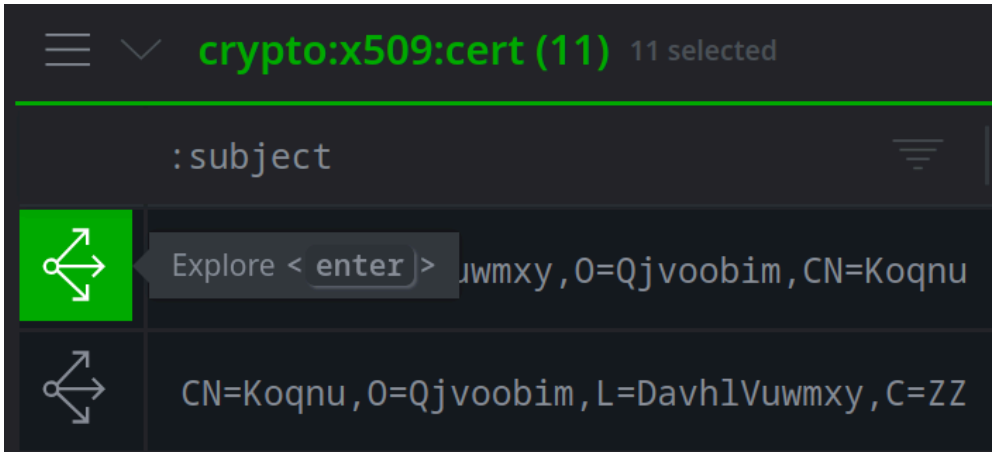
Question 4: How many certificates in Synapse have a **:subject** that includes this string?

Let's see what we know about any IPv4 addresses where these certificates have been seen.

- Click the **hamburger menu** to the left of the **crypto:x509:cert** header and choose **Select all:**



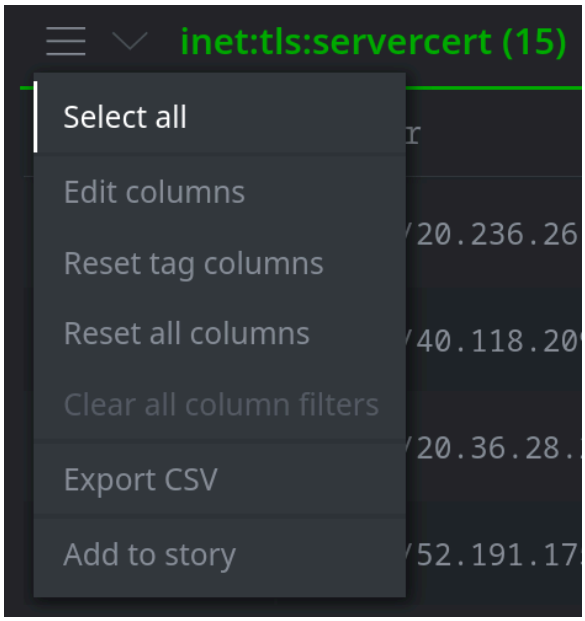
- Click the **Explore** button next to any selected node to navigate to adjacent nodes:



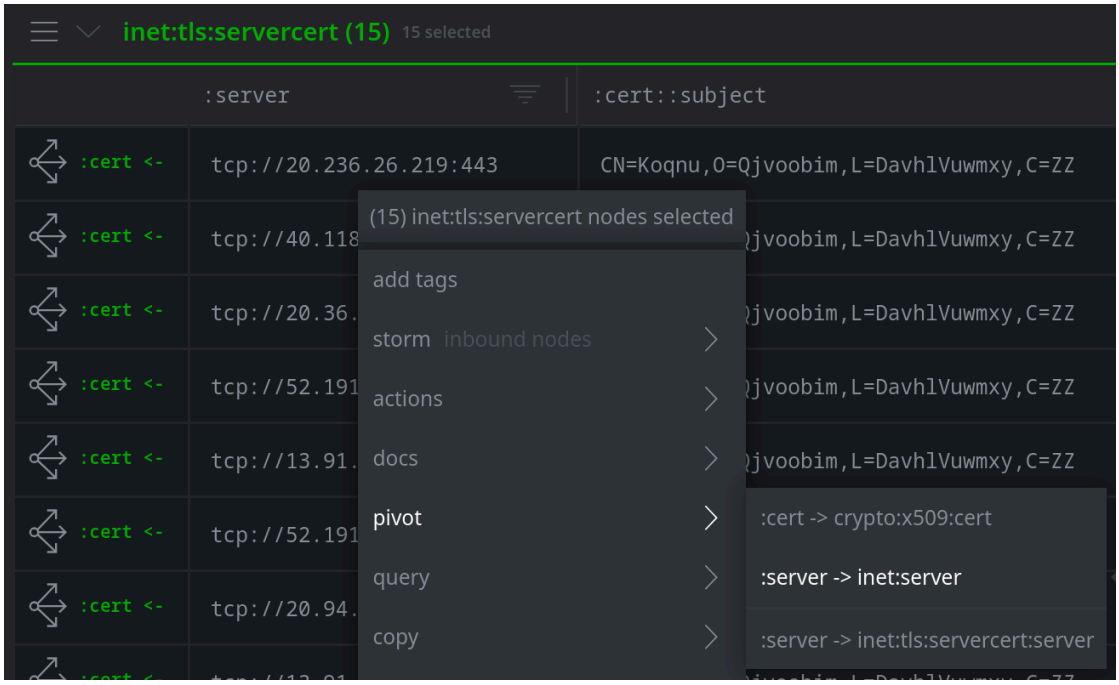
- Locate the **`inet:tls:servercert`** nodes (use **Scroll to Form** if necessary):

These nodes represent the IP and port where the TLS or SSL certificates were seen.

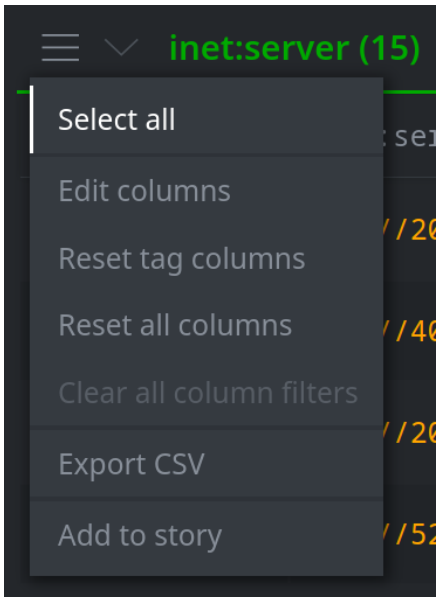
- Click the **hamburger menu** to the left of the **inet:tls:servercert** header and choose **Select all:**



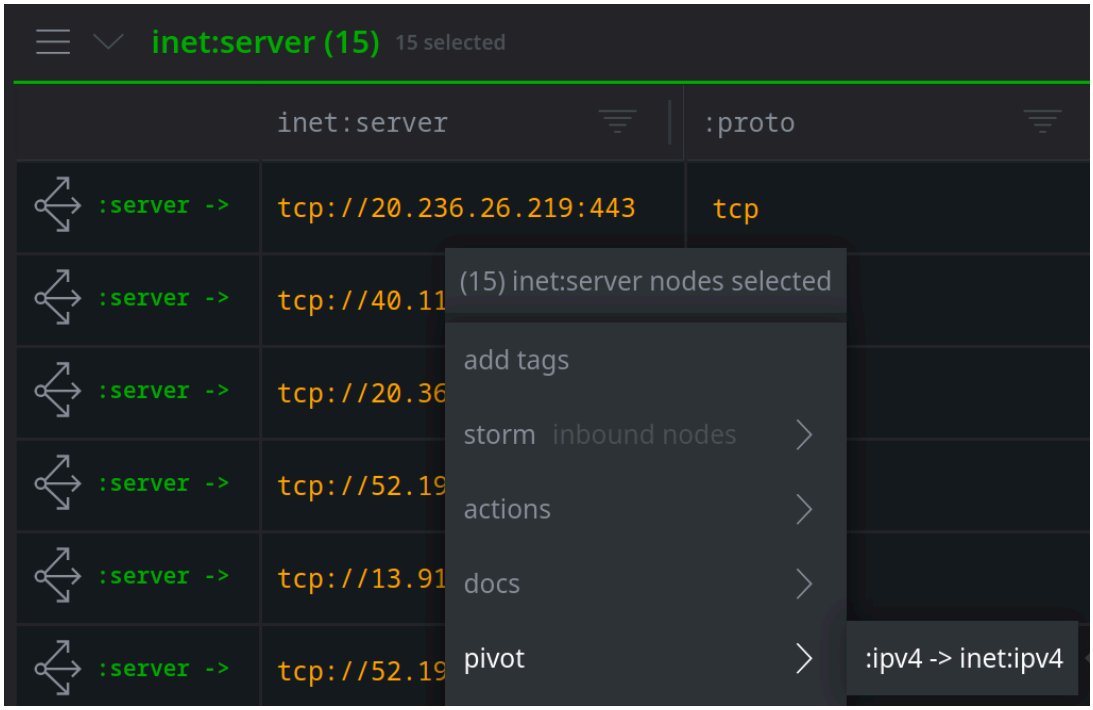
- **Right-click** any selected node and choose **pivot > :server -> inet:server** to navigate to the associated servers:



- Click the **hamburger menu** to the left of the **inet:server** header and choose **Select all:**



- **Right-click** any selected node and choose **pivot > :ipv4 -> inet:ipv4** to navigate to the associated IPv4 nodes:



Question 5: What Autonomous System (AS) number(s) and network(s) are the IPv4 addresses associated with?

Question 6: Does the name **Koqnu** appear to be unique to Microsoft infrastructure?
