

Synapse Bootcamp - Module 16

Dynamic Malware Analysis - Exercises

Dynamic Malware Analysis - Exercises	1
Objectives	1
Exercises	2
Dynamic Malware Analysis	2
Exercise 1	2
Exercise 2	14
Exercise 3	20

Objectives

In these exercises you will learn:

- How to use Synapse Power-Ups to retrieve dynamic analysis data for selected files
- How to model file behavior information using Synapse' data model
- Common queries and pivots to use when analyzing a file's behavior

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.

Dynamic Malware Analysis

Exercise 1

Objective:

- Use dynamic execution data to identify network activity and look for potential malware command and control (C2) communications.

You are researching a known malware sample. You have already:

- Downloaded and parsed the file.
- Reviewed the static analysis data / VirusTotal file report.
- Determined the file is malicious and tagged it **cno.mal**.

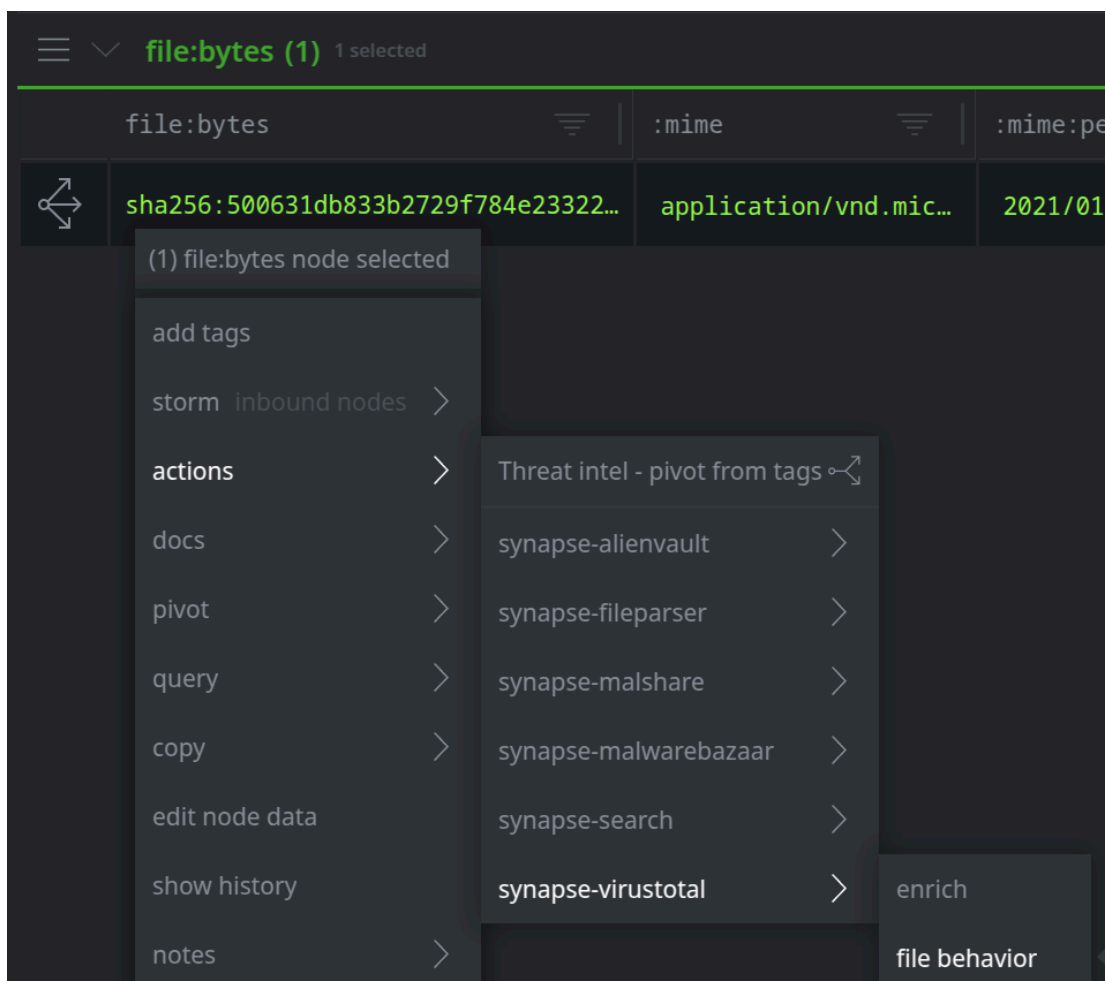
Now you want to download and examine execution data.

- In the **Research Tool**, enter the following into the **Storm Query Bar** and press **Enter** to view the file (**file:bytes**) associated with the hash:

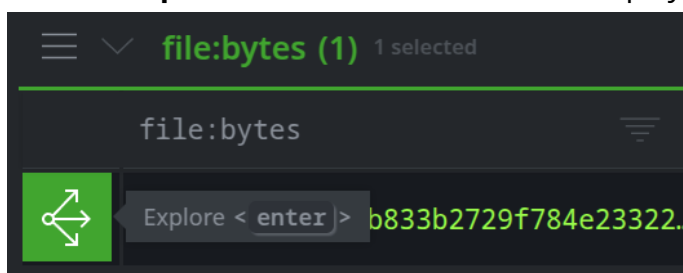
```
file:bytes=sha256:500631db833b2729f784e233225621ddff411d7da49bd82cfd51a49b9600438f
```

Note: The exercise PDFs may insert line breaks or spaces where values (such as the SHA256, above) are forced to wrap. If you copy the above into your Storm query bar and the query fails to run, you may need to manually remove the space / break.

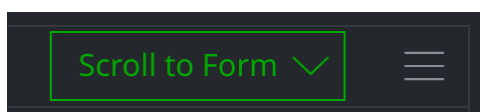
- **Right-click** the file and select **actions > synapse-virustotal > file behavior** to download execution data for the file:



- Click the **Explore** button next to the file to display adjacent nodes:

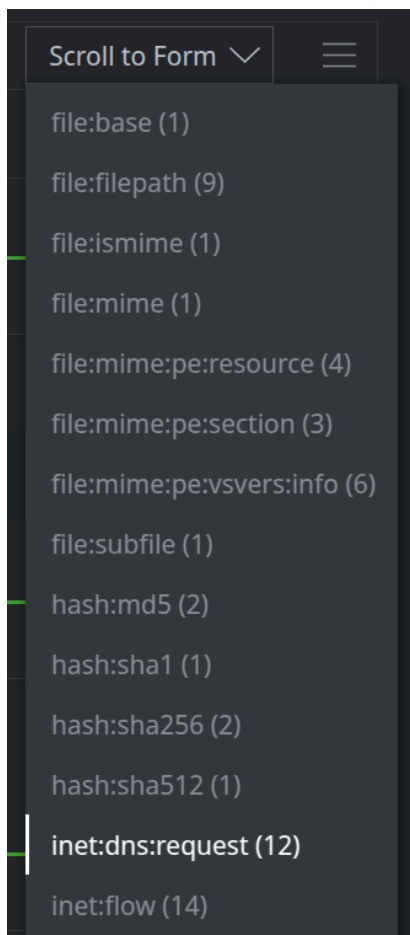


- Click the **Scroll to Form** button to browse the results:



Question 1: Are there any forms that might provide us with information about **network-based** communications or command and control (C2)?

- Use **Scroll to Form** to navigate to the **inet:dns:request** nodes:

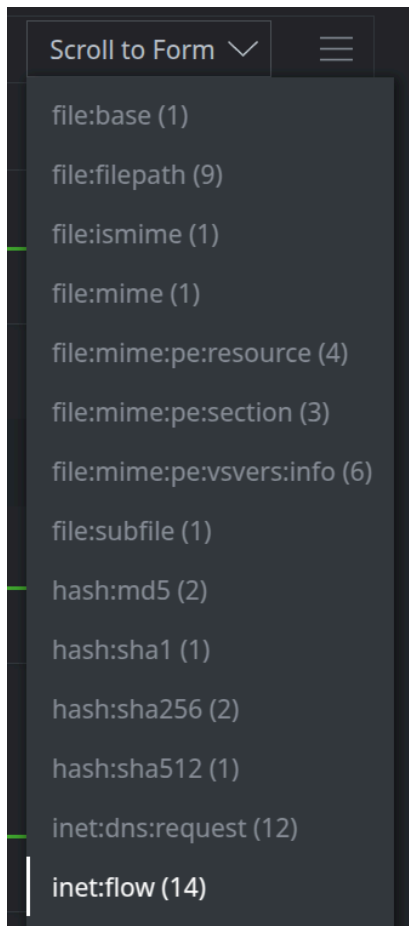


Question 2: When were the DNS queries made?

Question 3: How many unique FQDNs were queried?

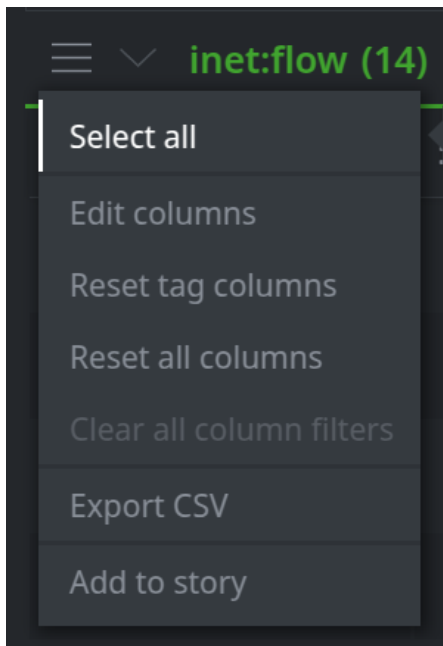
Question 4: Which FQDNs (if any) would you investigate?

- Use **Scroll to Form** to navigate to the **inet:flow** nodes:

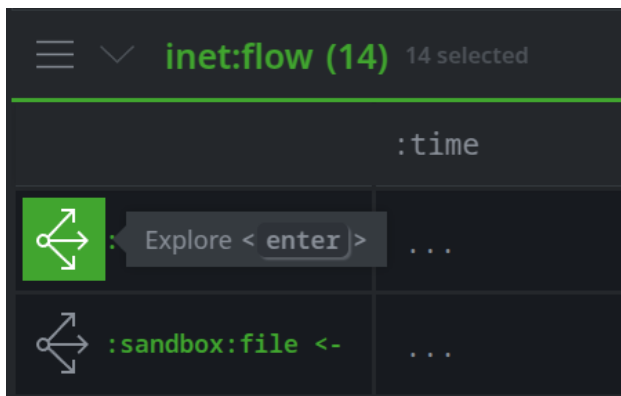


(If you navigated away from the previous results, use your **breadcrumbs** to return.)

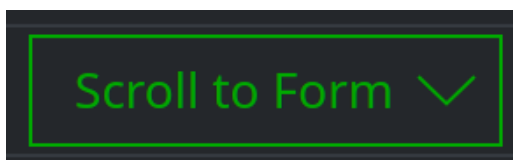
- Click the **hamburger menu** next to the **inet:flow** header and choose **Select all**:



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



- Locate the **inet:ipv4** nodes (use **Scroll to Form** if necessary):



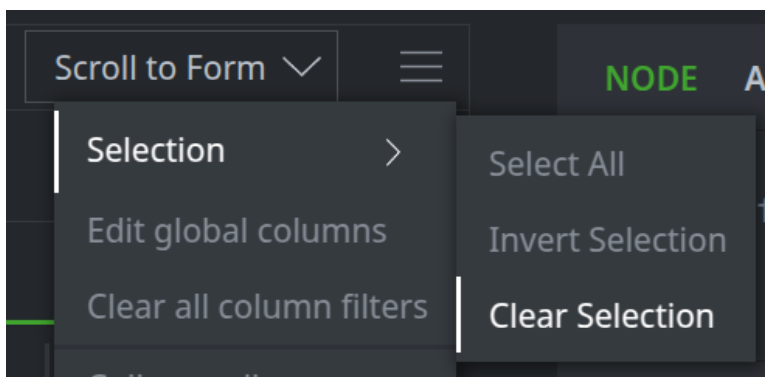
Question 5: How many unique IPv4s were contacted?

You want to see if any IPv4 addresses are the result of a DNS query.

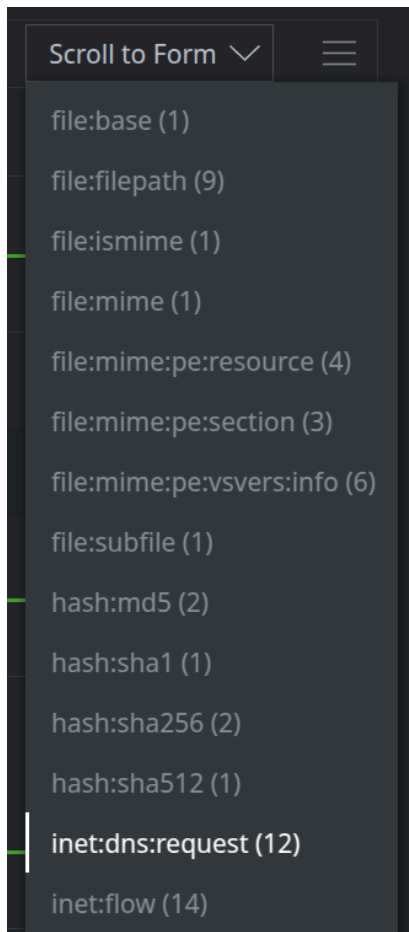
- Use your **breadcrumbs** to return to the prior query:



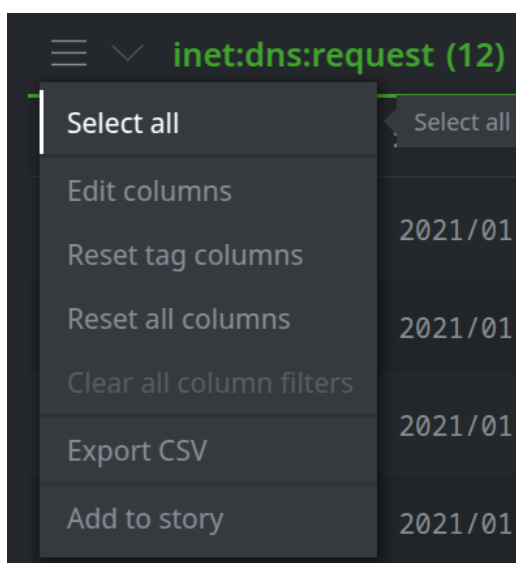
- Click the **main hamburger menu** and choose **Selection > Clear Selection** to de-select the **inet:flow** nodes:



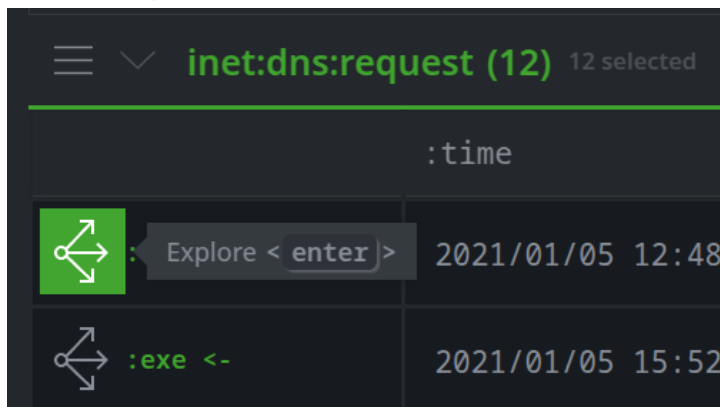
- Use **Scroll to Form** to return to the **inet:dns:request** nodes:



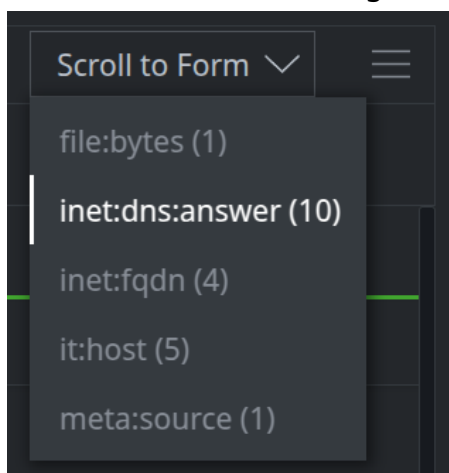
- Click the **hamburger menu** next to the **inet:dns:request** header and choose **Select all**:



- Use the **Explore** button next to any selected node to display adjacent nodes:



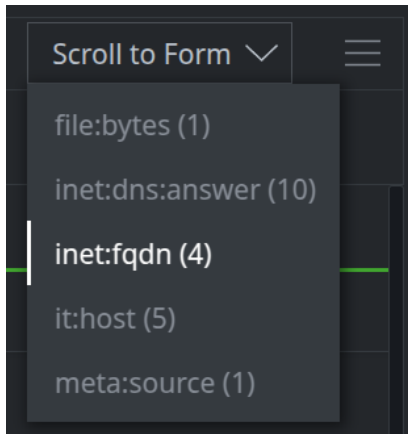
- Use **Scroll to Form** to navigate to the **inet:dns:answer** nodes:



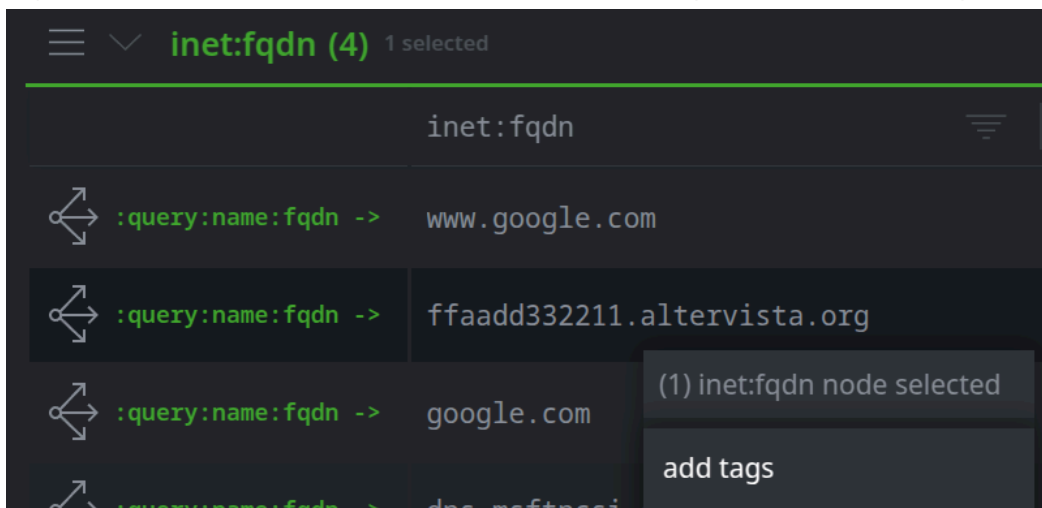
Question 6: Which IPv4 address (if any) is associated with FQDN ffaadd332211.altervista.org?

This FQDN may be malware C2, but you want to do more research. You can tag it for review so you do not forget to come back to it.

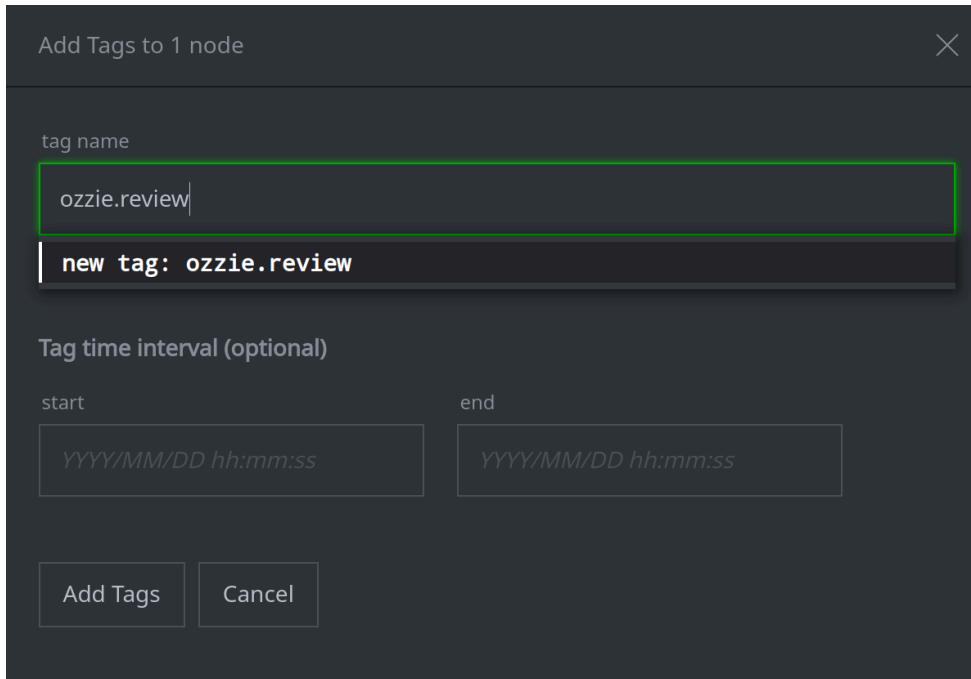
- Use **Scroll to Form** to navigate to the **inet:fqdn** nodes:



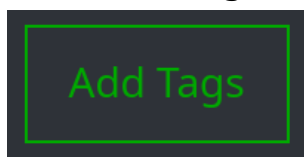
- **Right-click** the FQDN **ffaadd332211.altervista.org** and select **add tags**:



- Add the tag **<yourname>.review** to the FQDN to flag it for further analysis:

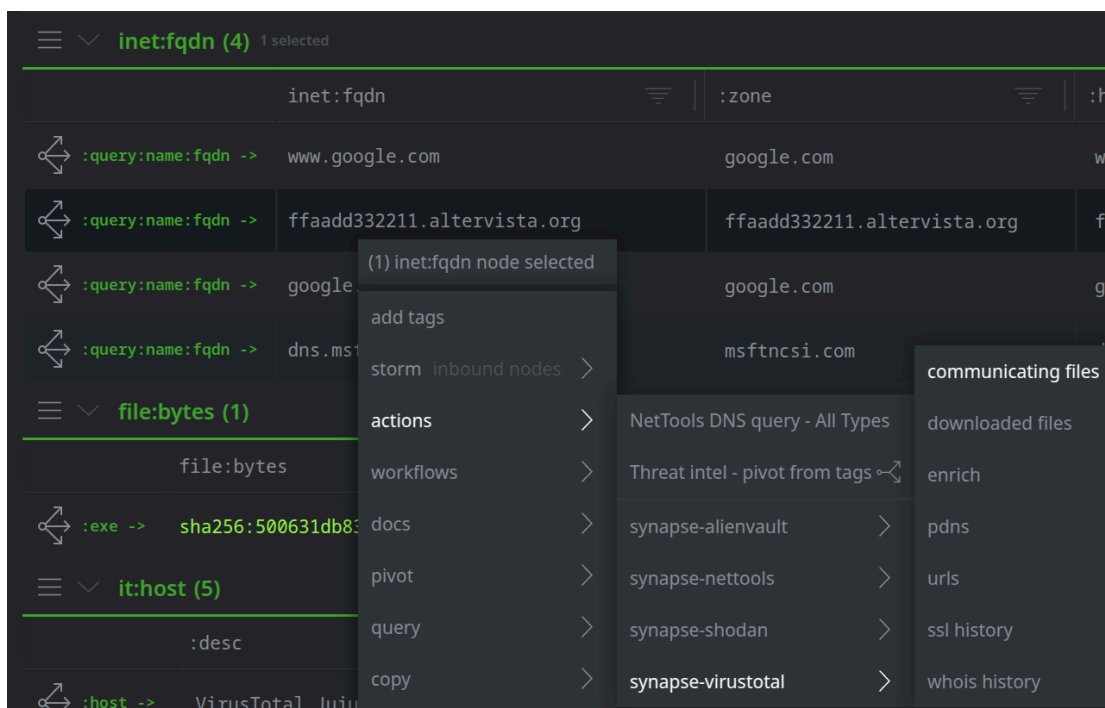


- Click the **Add Tags** button to apply the tag:

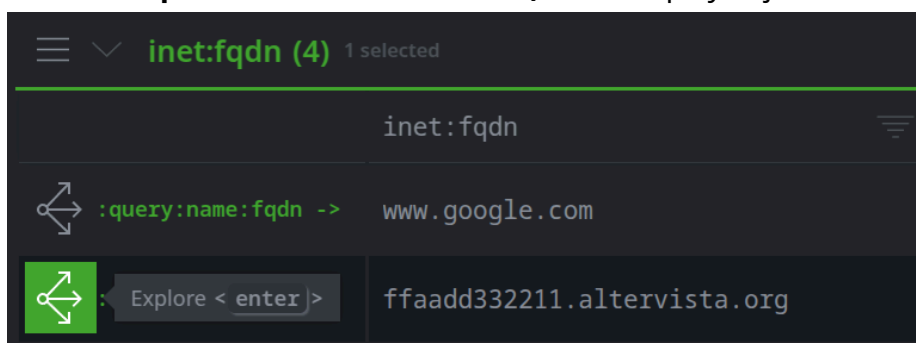


You want to see if you can identify any other files that communicate with FQDN **ffaadd332211.altervista.org**.

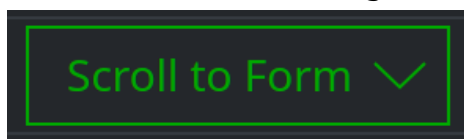
- **Right-click** the FQDN and select **actions > synapse-virustotal > communicating files** to check for other files that communicate with the FQDN:



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

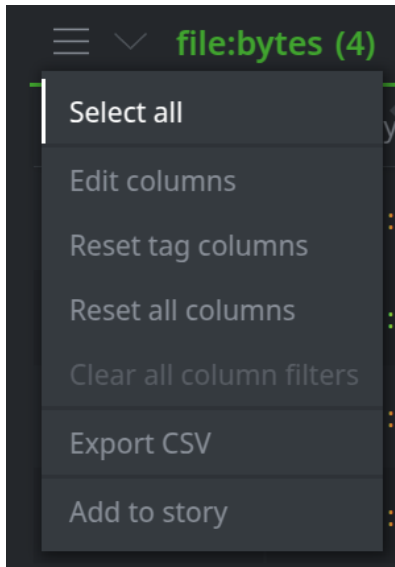


- Use **Scroll to Form** to navigate to the **file:bytes** nodes:

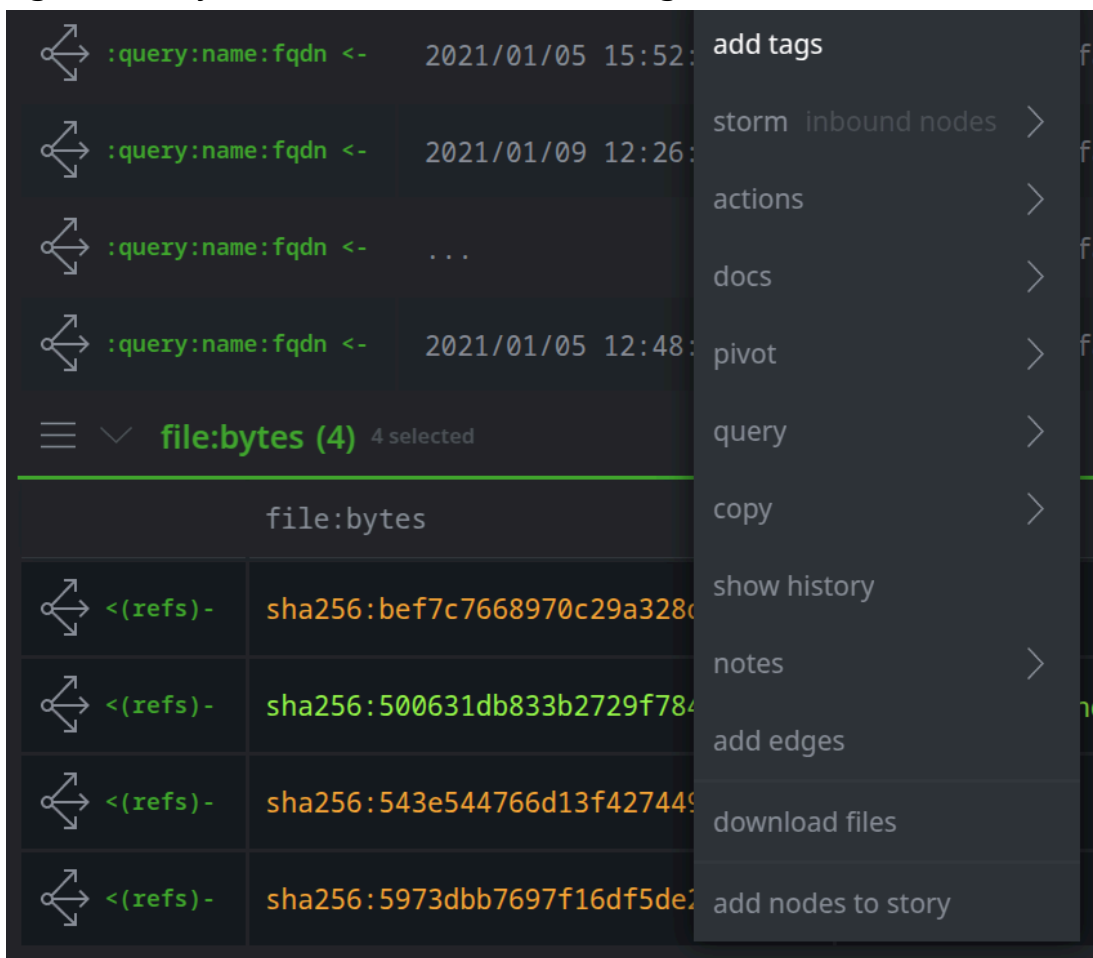


Question 7: How many files "communicate with" the FQDN?

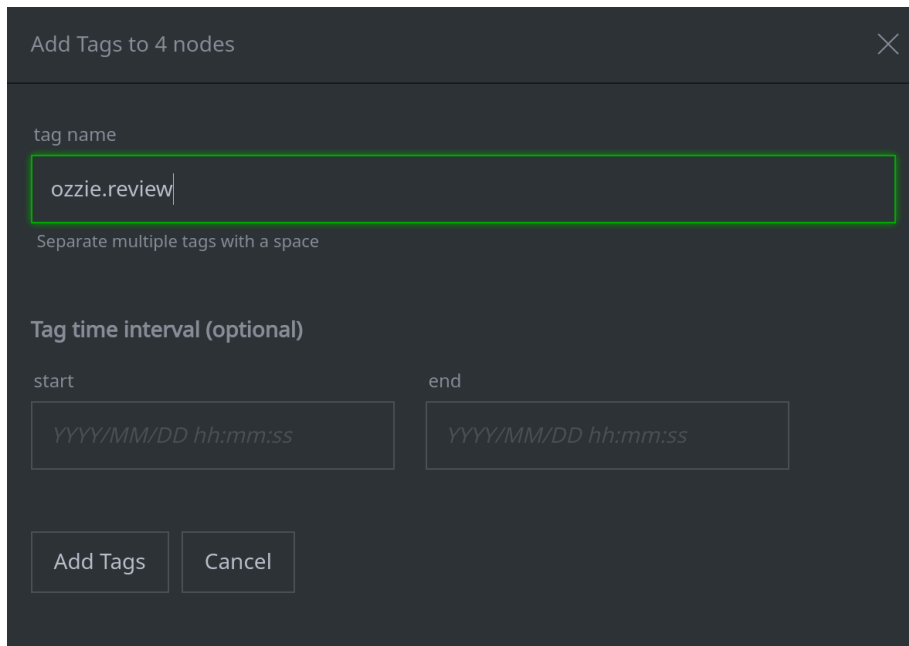
- Click the **hamburger menu** next to the **file:bytes** header and choose **Select all**:



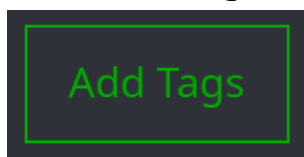
- Right-click** any selected node and select **add tags**:



- Add the tag **<yourname>.review** to the four files:



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

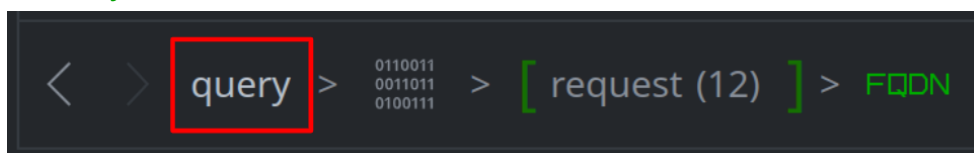


Tagging the files helps you to keep track of them. You can come back to these files and investigate them later.

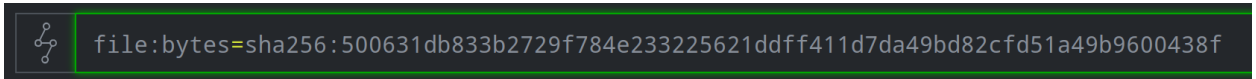
Exercise 2

Objective:

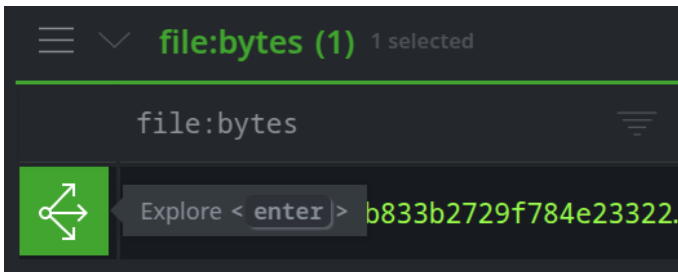
- Use dynamic execution data to identify changes made to the host and look for additional host-based IOCs.
- In your **breadcrumbs**, click **query** to return to your original query for the **file:bytes** node:



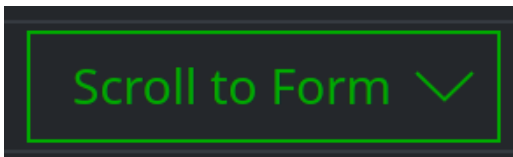
Alternatively, simply **re-run** the existing query in your **Query Bar**:



- Click the **Explore** button next to the file to display adjacent nodes:



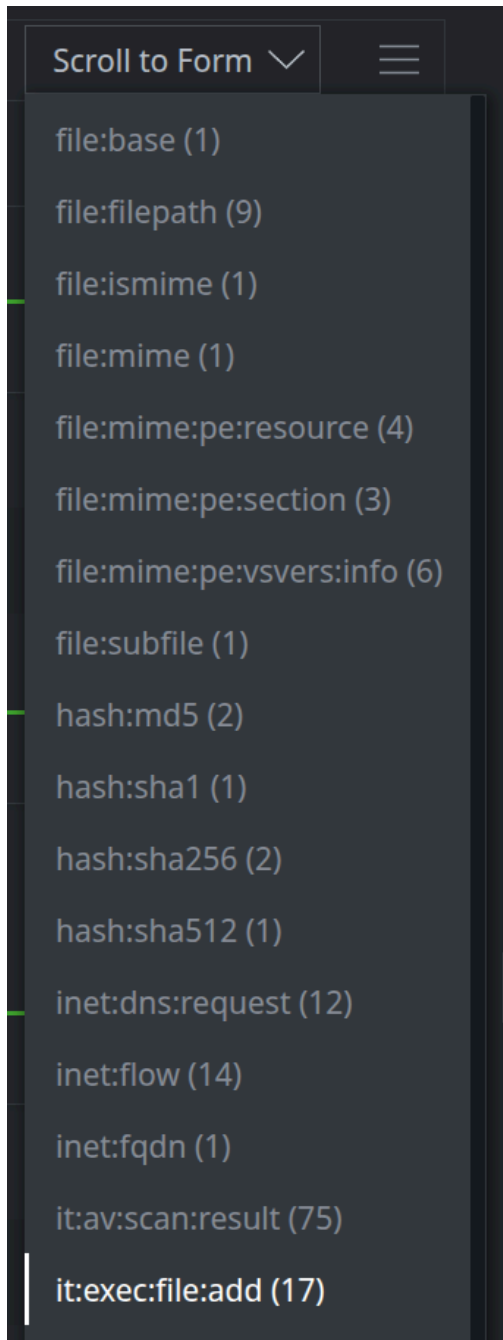
- Click the **Scroll to Form** button to browse the results:



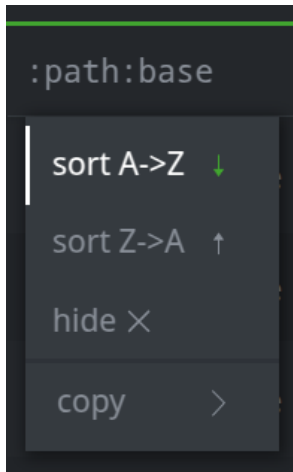
Question 1: Are there any forms that might provide us with information about **host-based** activity for the file?

You want to see if the file adds any files to disk during execution.

- Use **Scroll to Form** to navigate to the **it:exec:file:add** nodes:



- **Sort** the nodes by the **:path:base** property (the file name):



Question 2: Were any executable (**exe**) files added during any sandbox runs?

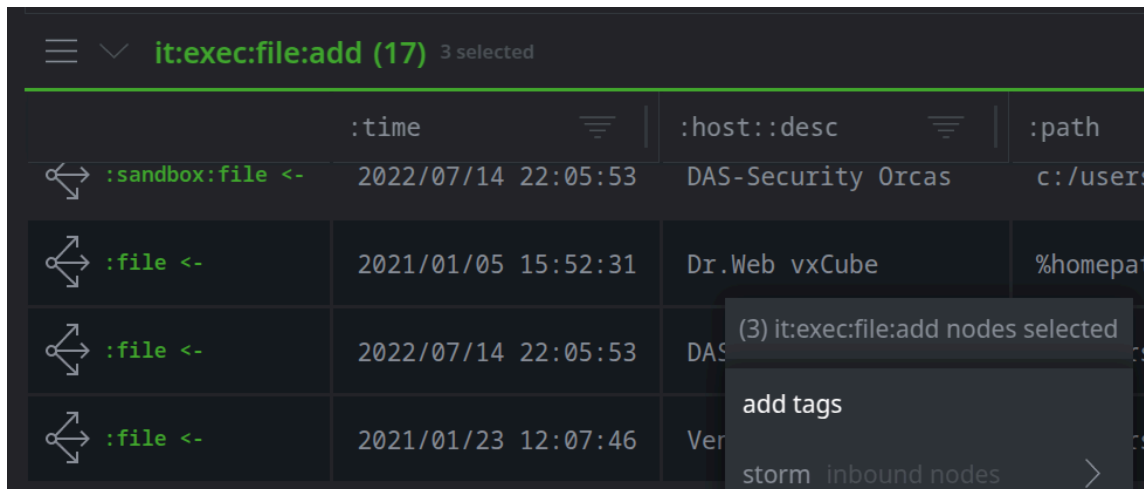
Question 3: How many sandboxes (hosts) observed the file? When was the activity captured?

You decide that the **it:exec:file:add** activity is related to your malicious sample and want to tag it.

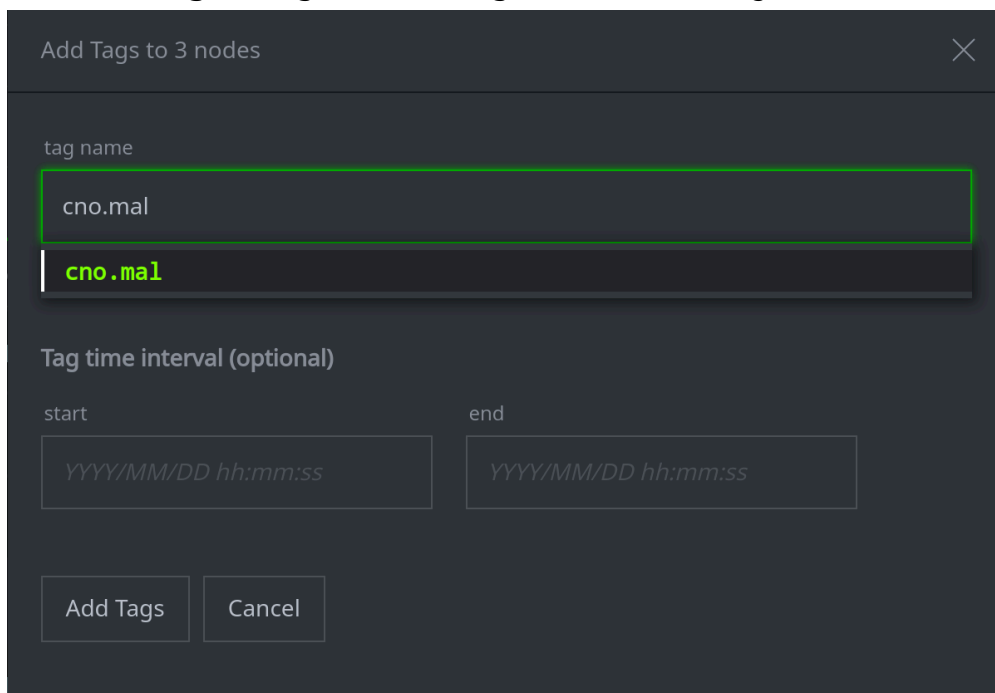
- **Select** the three **it:exec:file:add** nodes that create the **sysc32cmd.exe** file (use **Shift-click** or **Ctrl-click**):

it:exec:file:add (17) 3 selected				
	:time	:host::desc	:path	:path:base ↓
↔ :sandbox:file <-	2022/07/14 22:05:53	DAS-Security Orcas	c:/users/admin/pp	pp
↔ :file <-	2021/01/05 15:52:31	Dr.Web vxCube	%homepath%/sysc32cmd.exe	sysc32cmd.exe
↔ :file <-	2022/07/14 22:05:53	DAS-Security Orcas	c:/users/admin/sysc32cmd.exe	sysc32cmd.exe
↔ :file <-	2021/01/23 12:07:46	VenusEye Sandbox	c:/users/<user>/sysc32cmd.exe	sysc32cmd.exe
↔ :sandbox:file <-	2021/01/23 12:07:46	VenusEye Sandbox	c:/users/<user>/unix1.reg	unix1.reg

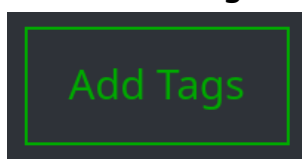
- **Right-click** any of the selected nodes and choose **add tags**:



- In the **Add Tags** dialog, enter the tag **cno.mal** in the *tag name* field:



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



You want to find out more information about the dropped (added) file.

- The **:sandbox:file** property is the file that ran in the sandbox - your original file.
- The **:file** property is the **sysc32cmd.exe** file that was **added** during execution.

- For your three **it:exec:file:add** nodes, **compare** the **:sandbox:file** and **:file** properties

Question 4: Are the property values the same or different? What does this tell you?

You want to see if there are other files in Synapse that create a file named **sysc32cmd.exe**.

- **Select** the three **it:exec:file:add** nodes that create the **sysc32cmd.exe** file (use **Shift-click** or **Ctrl-click** - they may still be selected from the previous step):

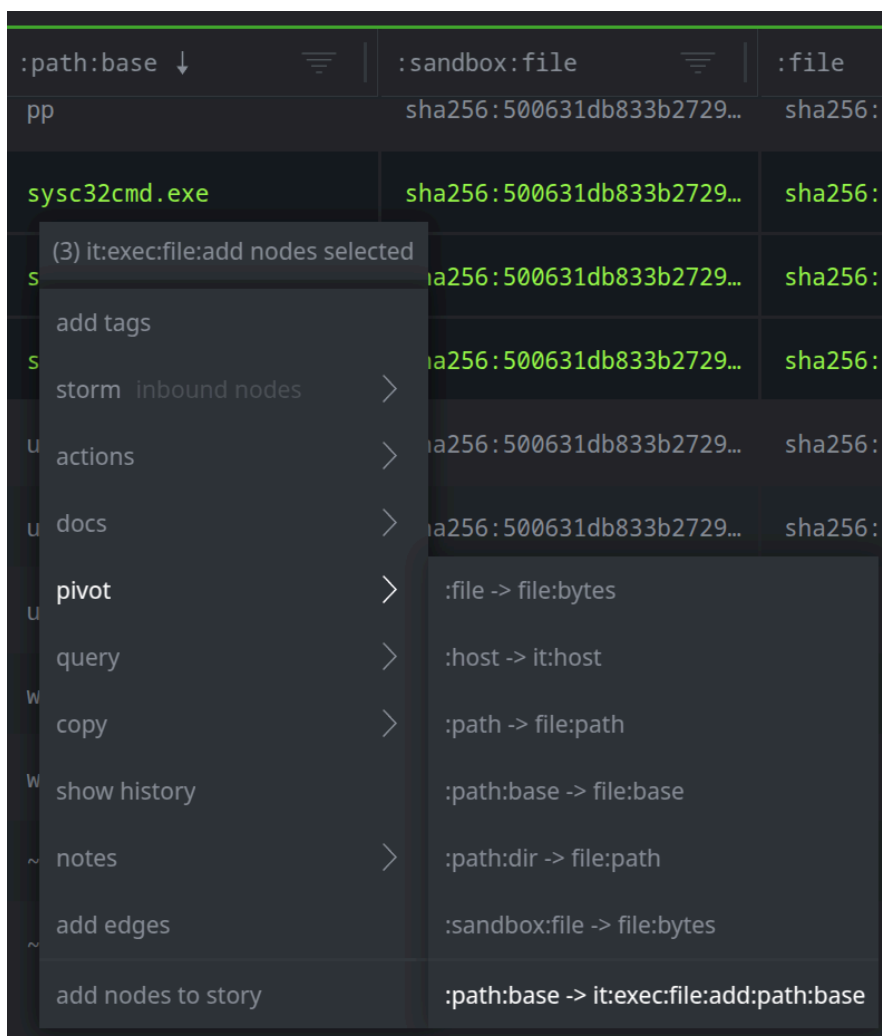
it:exec:file:add (17) 3 selected				
	:time	:host::desc	:path	:path:base ↓
↔ :sandbox:file <-	2022/07/14 22:05:53	DAS-Security Orcas	c:/users/admin/pp	pp
↔ :file <-	2021/01/05 15:52:31	Dr.Web vxCube	%homepath%/sysc32cmd...	sysc32cmd.exe
↔ :file <-	2022/07/14 22:05:53	DAS-Security Orcas	c:/users/admin/sysc32...	sysc32cmd.exe
↔ :file <-	2021/01/23 12:07:46	VenusEye Sandbox	c:/users/<user>/sysc3...	sysc32cmd.exe
↔ :sandbox:file <-	2021/01/23 12:07:46	VenusEye Sandbox	c:/users/<user>/unix1...	unix1.reg

- Locate the **:path:base** column:

```
:path:base
sysc32cmd.exe
sysc32cmd.exe
sysc32cmd.exe
```

- **Right-click** one of the **sysc32cmd.exe** file names in this column.

Use the **pivot > :path:base -> it:exec:file:add:path:base** option to search for any **it:exec:file:add** nodes that create a file with this name:



Question 5: How many **it:exec:file:add** nodes are in your results?

Question 6: Did your query identify any **new** files that write to the same path?

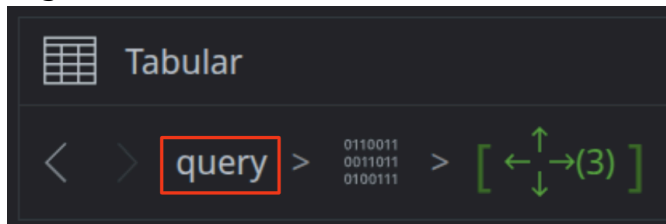
Exercise 3

Objective:

- View host-specific (sandbox-specific) execution data associated with a file.

You want to look at the data captured by different sandboxes (hosts / **it:host** nodes) for this sample. We'll look at some of the sandboxes that captured DNS request data.

- In the **Research Tool**, click the **query** option in your **breadcrumbs** to return to the original file:

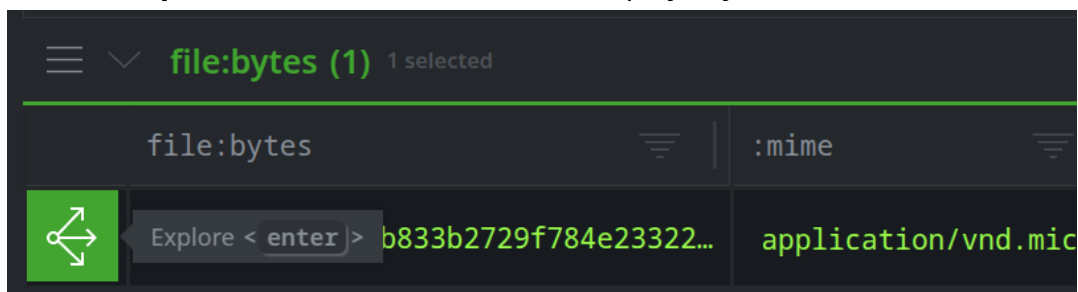


(Or, you can just re-run the original query in your **Storm Query Bar**):

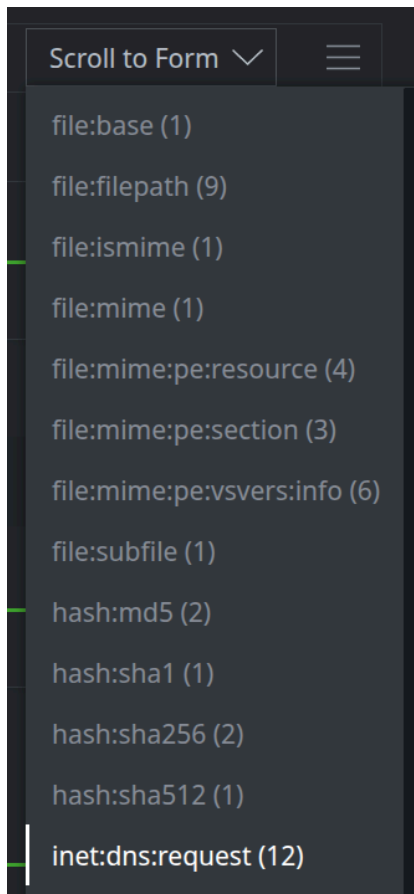
```
file:bytes=sha256:500631db833b2729f784e233225621ddff411d7da49bd82cfd51a49b9600438f
```

Note: The exercise PDFs may insert line breaks or spaces where values (such as the SHA256, above) are forced to wrap. If you copy the above into your Storm query bar and the query fails to run, you may need to manually remove the space / break.

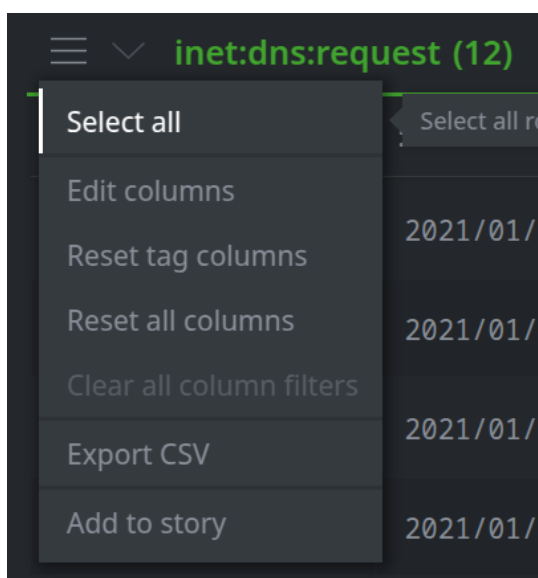
- Click the **Explore** button next to the file to display adjacent nodes:



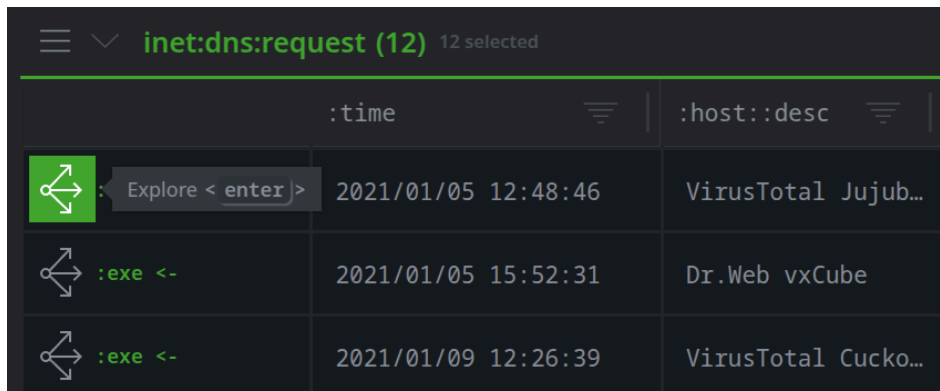
- Use **Scroll to Form** to navigate to the **inet:dns:request** nodes:






- Click the **hamburger menu** next to the **inet:dns:request** header and choose **Select All**:

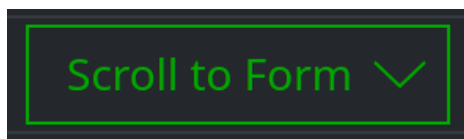


- Click the **Explore** button next to any selected node to display adjacent nodes:



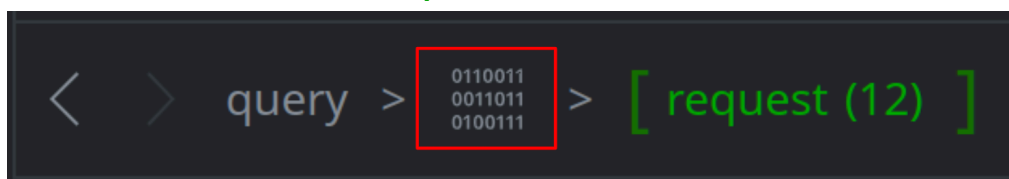
	:time	:host::desc
 Explore < enter >	2021/01/05 12:48:46	VirusTotal Jujub...
 :exe <-	2021/01/05 15:52:31	Dr.Web vxCube
 :exe <-	2021/01/09 12:26:39	VirusTotal Cucko...

- Locate the **it:host** nodes (use **Scroll to Form** if necessary):

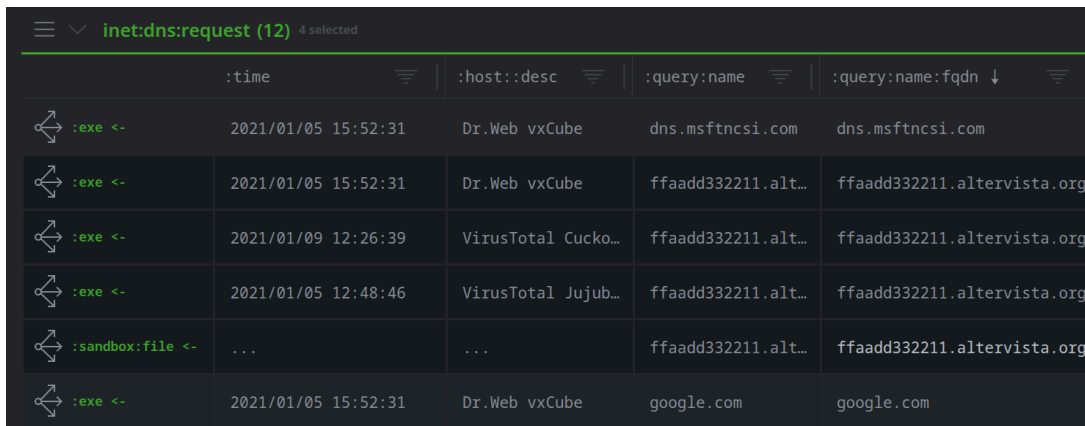








Question 1: How many hosts (sandboxes) recorded DNS queries during file execution?

- In your **breadcrumbs**, click the "ones and zeroes" icon to return to your previous results (i.e., the **inet:dns:request** nodes):

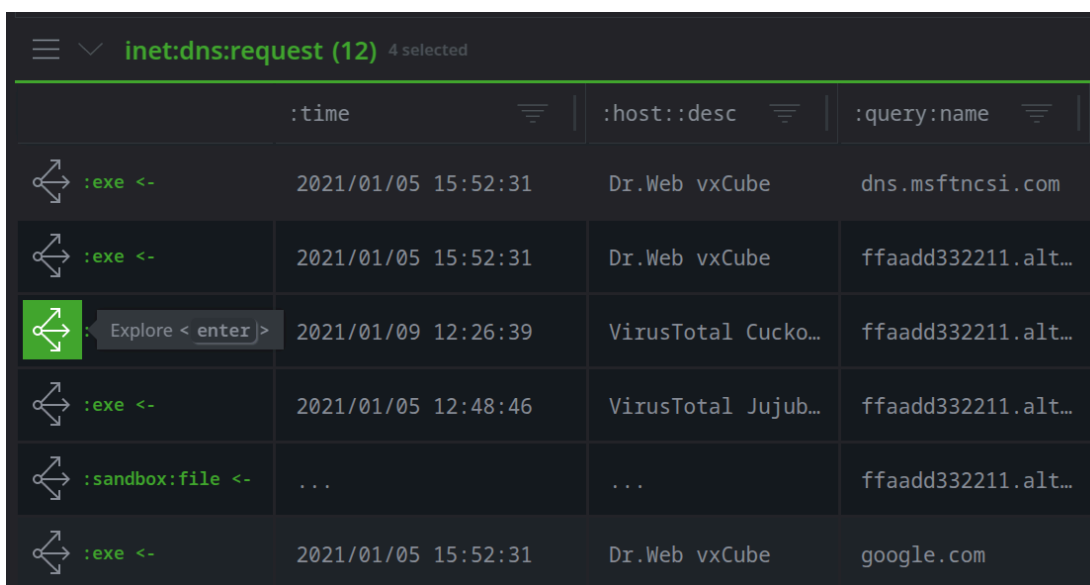








- From the **inet:dns:request** nodes, **select only** the nodes that query the FQDN **ffaadd332211.altervista.org** (use **Shift-click** or **Ctrl-click**):



	:time	:host::desc	:query:name	:query:name:fqdn ↓
 :exe <-	2021/01/05 15:52:31	Dr.Web vxCube	dns.msftncsi.com	dns.msftncsi.com
 :exe <-	2021/01/05 15:52:31	Dr.Web vxCube	ffaadd332211.alt...	ffaadd332211.altervista.org
 :exe <-	2021/01/09 12:26:39	VirusTotal Cucko...	ffaadd332211.alt...	ffaadd332211.altervista.org
 :exe <-	2021/01/05 12:48:46	VirusTotal Jujub...	ffaadd332211.alt...	ffaadd332211.altervista.org
 :sandbox:file <-	ffaadd332211.alt...	ffaadd332211.altervista.org
 :exe <-	2021/01/05 15:52:31	Dr.Web vxCube	google.com	google.com

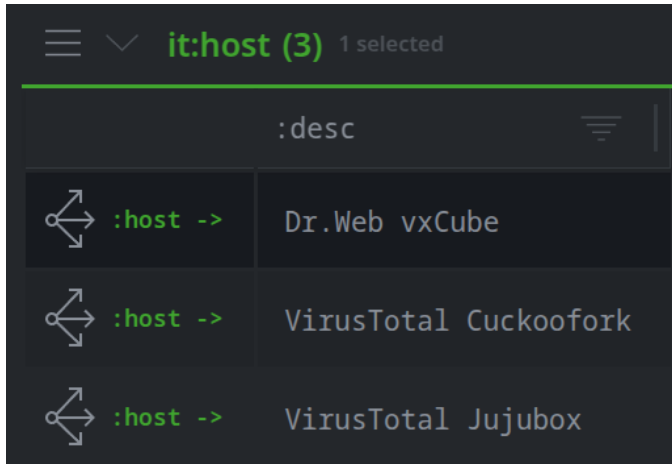
- Click the **Explore** button next to any of the selected nodes to display adjacent nodes:



	:time	:host::desc	:query:name
 :exe <-	2021/01/05 15:52:31	Dr.Web vxCube	dns.msftncsi.com
 :exe <-	2021/01/05 15:52:31	Dr.Web vxCube	ffaadd332211.alt...
 : Explore < enter >	2021/01/09 12:26:39	VirusTotal Cucko...	ffaadd332211.alt...
 :exe <-	2021/01/05 12:48:46	VirusTotal Jujub...	ffaadd332211.alt...
 :sandbox:file <-	ffaadd332211.alt...
 :exe <-	2021/01/05 15:52:31	Dr.Web vxCube	google.com

Question 2: How many hosts (sandboxes) recorded DNS queries for our C2 FQDN?

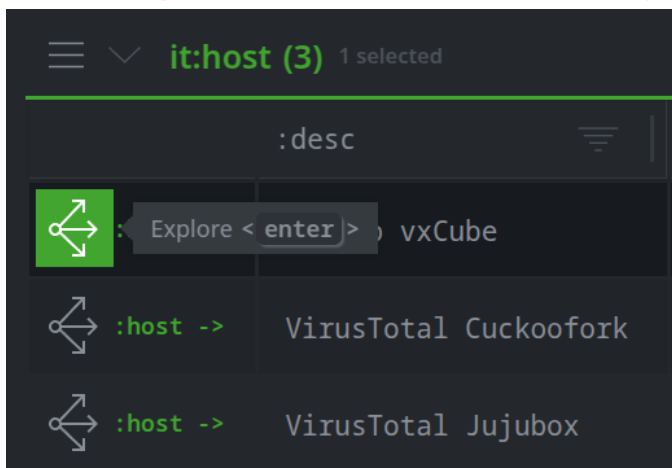
- Select the **it:host** node for **Dr.Web vxCube**:



The screenshot shows a table with a header row containing a menu icon, a dropdown arrow, the text 'it:host (3) 1 selected', and a search bar with ':desc'. Below the header, there are three rows, each starting with a node icon and ':host ->'. The first row is highlighted and contains 'Dr.Web vxCube'. The other two rows contain 'VirusTotal Cuckoofork' and 'VirusTotal Jujubox'.

	:desc
:host ->	Dr.Web vxCube
:host ->	VirusTotal Cuckoofork
:host ->	VirusTotal Jujubox

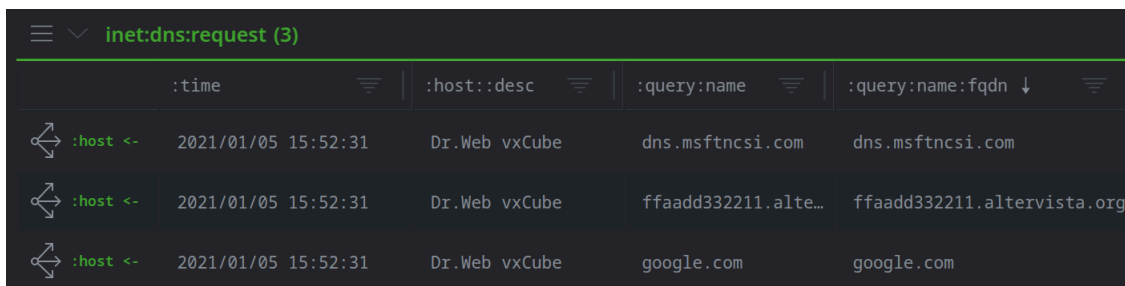
- Click the **Explore** button next to the host to display adjacent nodes:



The screenshot shows the same table as before, but the first row is now highlighted with a green background. A tooltip is visible over the node icon, displaying 'Explore <enter>'.

	:desc
:host ->	Dr.Web vxCube
:host ->	VirusTotal Cuckoofork
:host ->	VirusTotal Jujubox

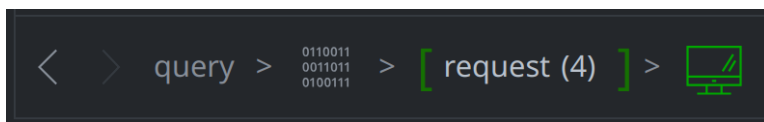
- Review the DNS requests (**inet:dns:request** nodes) recorded by the Dr.Web sandbox:



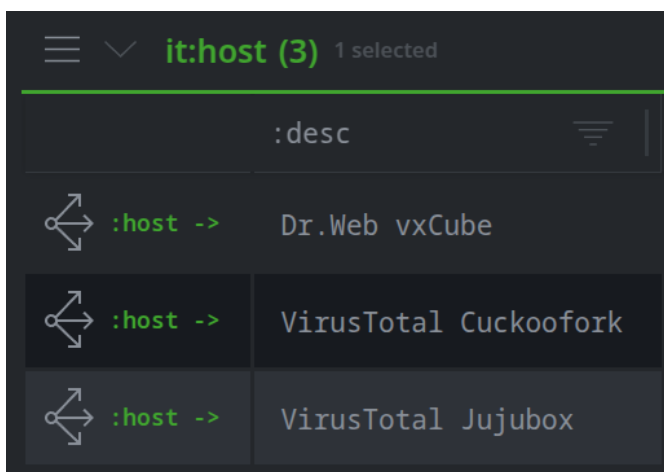
The screenshot shows a table with a header row containing a menu icon, a dropdown arrow, the text 'inet:dns:request (3)', and four columns: ':time', ':host::desc', ':query:name', and ':query:name:fqdn'. Below the header, there are three rows, each starting with a node icon and ':host <-'. The first row contains '2021/01/05 15:52:31', 'Dr.Web vxCube', 'dns.msftncsi.com', and 'dns.msftncsi.com'. The second row contains '2021/01/05 15:52:31', 'Dr.Web vxCube', 'ffaadd332211.alte...', and 'ffaadd332211.altervista.org'. The third row contains '2021/01/05 15:52:31', 'Dr.Web vxCube', 'google.com', and 'google.com'.

	:time	:host::desc	:query:name	:query:name:fqdn
:host <-	2021/01/05 15:52:31	Dr.Web vxCube	dns.msftncsi.com	dns.msftncsi.com
:host <-	2021/01/05 15:52:31	Dr.Web vxCube	ffaadd332211.alte...	ffaadd332211.altervista.org
:host <-	2021/01/05 15:52:31	Dr.Web vxCube	google.com	google.com

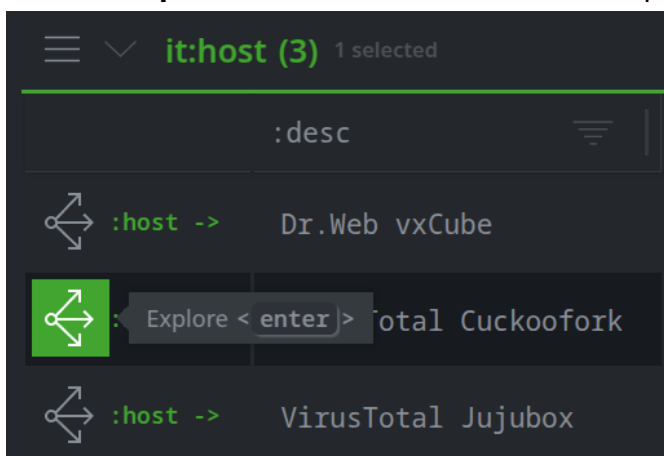
- In your **breadcrumbs**, click the [**request(4)**] icon to return to your previous results (i.e., the **it:host** nodes):



- Select the **it:host** node for **VirusTotal CuckooFork**:



- Click the **Explore** button next to the host to display adjacent nodes:



- **Review** the DNS requests (**inet:dns:request** nodes) recorded by the VirusTotal CuckooFork sandbox:

inet:dns:request (2)				
	:time	ist::desc	query:name	:query:name:fqdn ↓
↔ :host <-	2021/01/09 12:26:39	VirusTotal ...	ffaadd33221...	ffaadd332211.altervista.org
↔ :host <-	2021/01/09 12:26:39	VirusTotal ...	www.google...	www.google.com

Question 3: Was the DNS information captured by the sandboxes identical? If not, how do they differ?
