Synapse Bootcamp - Module 6

Putting it All Together - Answer Key

Answer Key

Summary Exercise: Modules 1 - 5

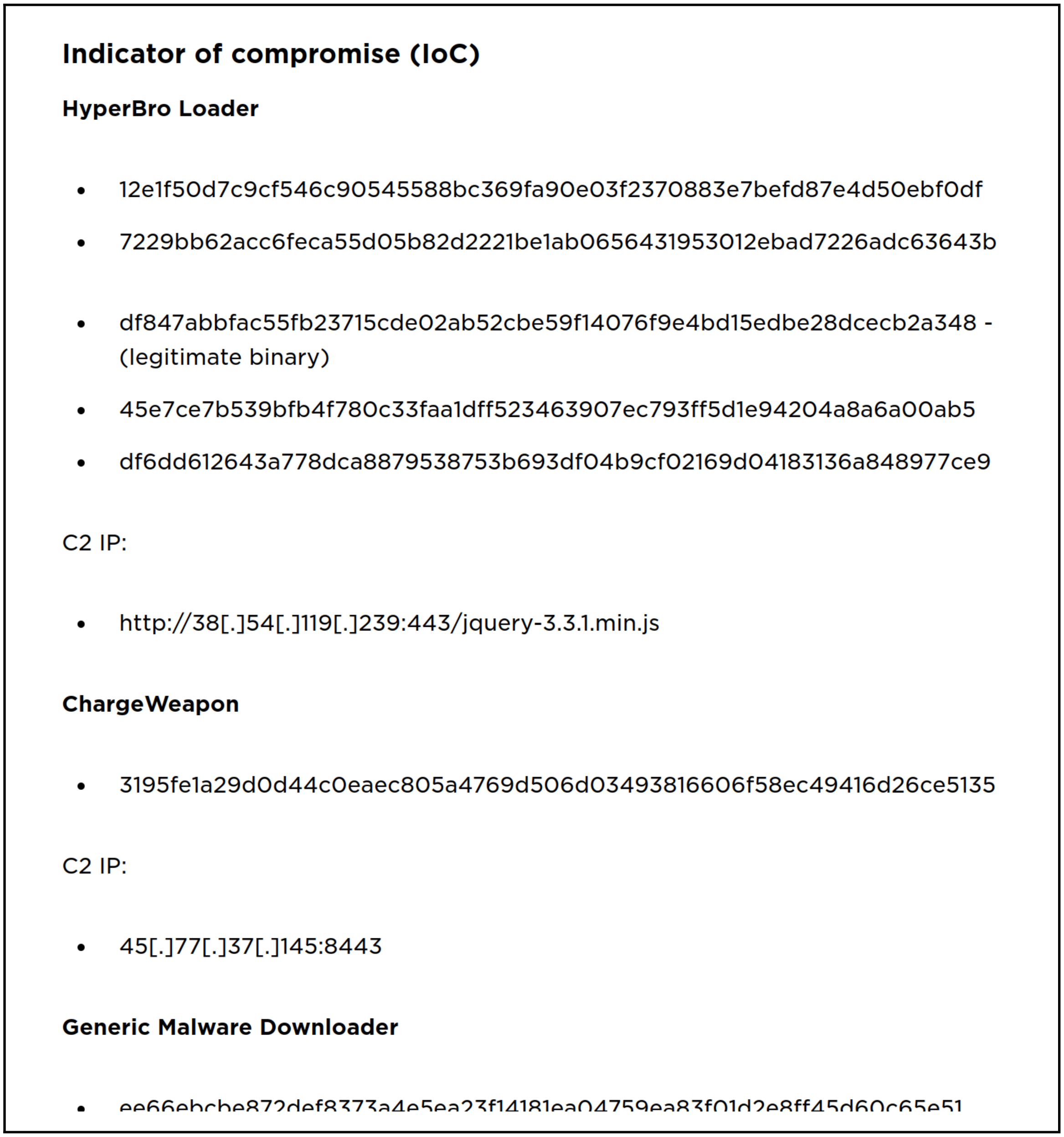
Objectives:

- **Apply what you've learned in Modules 1 - 5 using real world data.**
- **Continue to explore the features available in the Synapse UI.**

There is no "right" answer to this exercise! In the sections below we've listed a few of the possible tasks / investigative paths (in no particular order) that you could take based on this data.

Adding Indicators to Synapse

- The EclecticIQ blog lists **18 indicators of compromise (IOCs)** at the end of the blog:



Indicator of compromise (IoC)

HyperBro Loader

- 12e1f50d7c9cf546c90545588bc369fa90e03f2370883e7befd87e4d50ebf0df
- 7229bb62acc6feca55d05b82d2221be1ab0656431953012ebad7226adc63643b
- df847abbfac55fb23715cde02ab52cbe59f14076f9e4bd15edbe28dcecb2a348 - (legitimate binary)
- 45e7ce7b539bfb4f780c33faa1dff523463907ec793ff5d1e94204a8a6a00ab5
- df6dd612643a778dca8879538753b693df04b9cf02169d04183136a848977ce9

C2 IP:

- http://38[.]54[.]119[.]239:443/jquery-3.3.1.min.js

ChargeWeapon

- 3195fe1a29d0d44c0eaec805a4769d506d03493816606f58ec49416d26ce5135

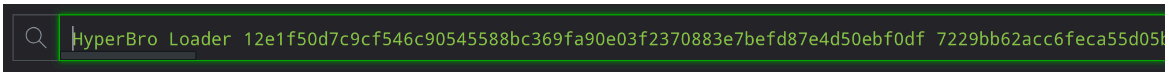
C2 IP:

- 45[.]77[.]37[.]145:8443

Generic Malware Downloader

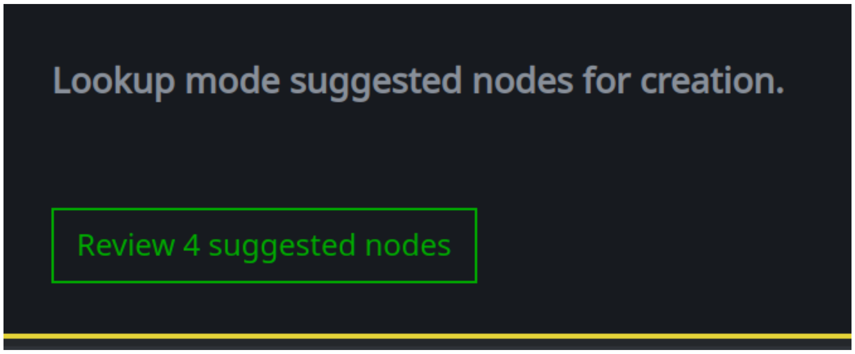
- ee66ebcbe872def8373a4e5ea23f14181ea04759ea83f01d2e8ff45d60c65e51

- You can **paste** these into the **Storm Query Bar** in **Lookup** mode and press **Enter** to **review** (or **lift**) the nodes:

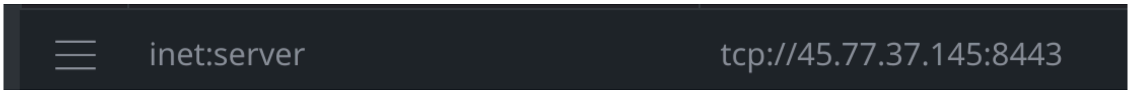


```
HyperBro Loader 12e1f50d7c9cf546c90545588bc369fa90e03f2370883e7befd87e4d50ebf0df 7229bb62acc6feca55d05b
```

- **Review** and **add** any nodes that do not exist:



Lookup mode suggested nodes for creation.

> **Note** that one of the indicators (`45[.]77[.]37[.]145:8443`) does not have a protocol.
>
> Synapse recognizes the IOC as an `inet:server` node and suggests creating the following:
>
> 
>
> inet:server tcp://45.77.37.145:8443

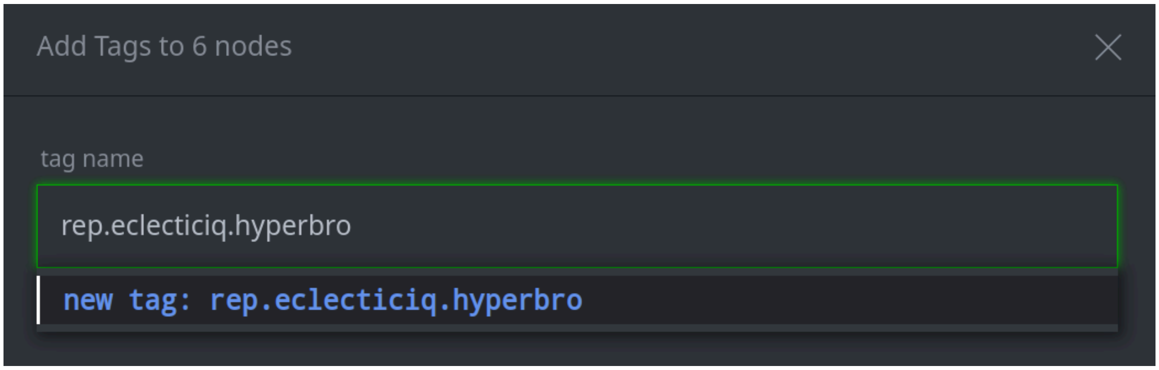
Tagging Indicators

EclecticIQ Tags

> EclecticIQ associates some of the IOCs with specific tools (HyperBro and ChargeWeapon).
>
> For other IOCs, EclecticIQ says they are malicious but does not associate them with any specific tool ("Generic Malware Downloader", "IP address of second stage malware").
>
> We can record all of these assessments using tags.

Note: Some of the IOCs were already present in Synapse and have existing tags from AlienVault (e.g., **rep.alienvault.cobalt**).

- For IOCs that belong to a specific tool / malware family, you might tag them with `rep.eclecticiq.hyperbro`:



Add Tags to 6 nodes

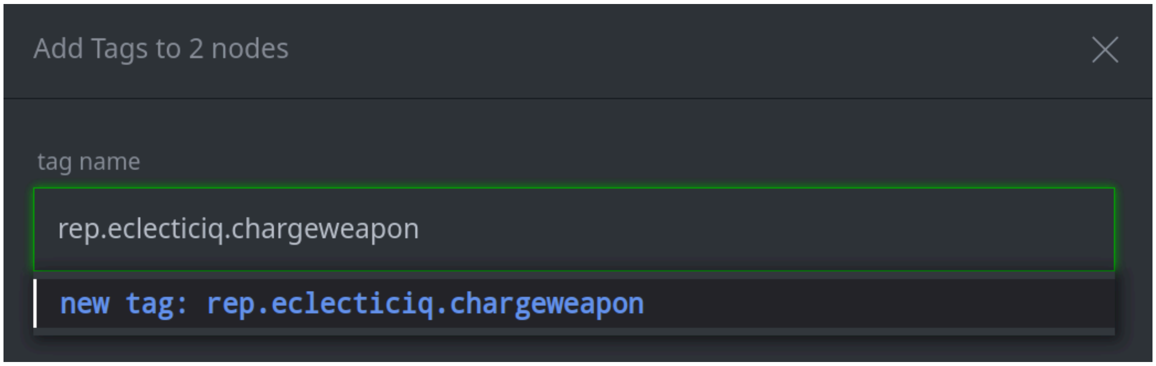
tag name

rep.eclecticiq.hyperbro

`new tag: rep.eclecticiq.hyperbro`

> **Tip:** Instead of selecting individual IOCs from your full list of new nodes, you can paste **only** the IOCs that you want to tag (e.g., the HyberBro hashes and associated C2 URL) into the Query Bar.

- Similarly, you might tag the ChargeWeapon hash and server with `rep.eclecticiq.chargeweapon`:



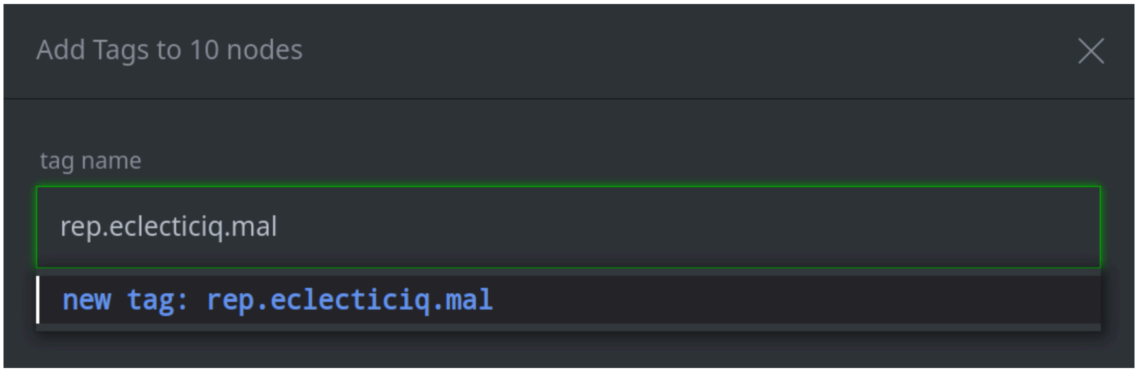
Add Tags to 2 nodes

tag name

rep.eclecticiq.chargeweapon

`new tag: rep.eclecticiq.chargeweapon`

- For the rest of the IOCs, you can simply indicate that EclecticIQ says they are **malicious:**



Add Tags to 10 nodes

tag name

rep.eclecticiq.mal

`new tag: rep.eclecticiq.mal`

Tip: Once you have tagged all of the IOCs, you can lift **all** of them using the tag **rep.eclecticiq** (currently, these are the only IOCs from EclecticIQ in your demo instance):

```
| #rep.eclecticiq
```

Your Tags

- If you come to your own conclusions about the indicators ("yes, I agree these are malicious" or "yes, I agree this is ChargeWeapon malware") **and** you want to track your assessments separately from "what EclecticIQ says", you can apply additional tags such as:
  - `cno.mal` or
  - `cno.mal.chargeweapon`

- You can also use "personal" tags for anything you like! For example:
  - Things you want to revisit (**<myname>.review**)
  - Things think are suspicious (**<myname>.suspicious**)
  - Things that **aren't** suspicious / may be legitimate (**<myname>.ignore**)
  - Preliminary conclusions (**<myname>.hyperbro.maybe**)

  Since these are "personal" or "scratch" tags, the exact tag name doesn't matter - whatever works for you.

Guiding Questions

Question 1

What are some of the possible group and malware names that appear in AlienVault tags on the `file:bytes` nodes?

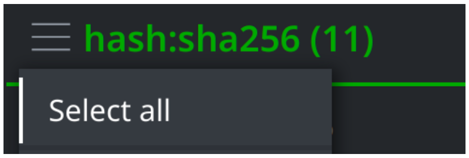
- Lift the hashes provided in the IOC list by copying and pasting them into the **Query Bar** (in Lookup mode)

  OR

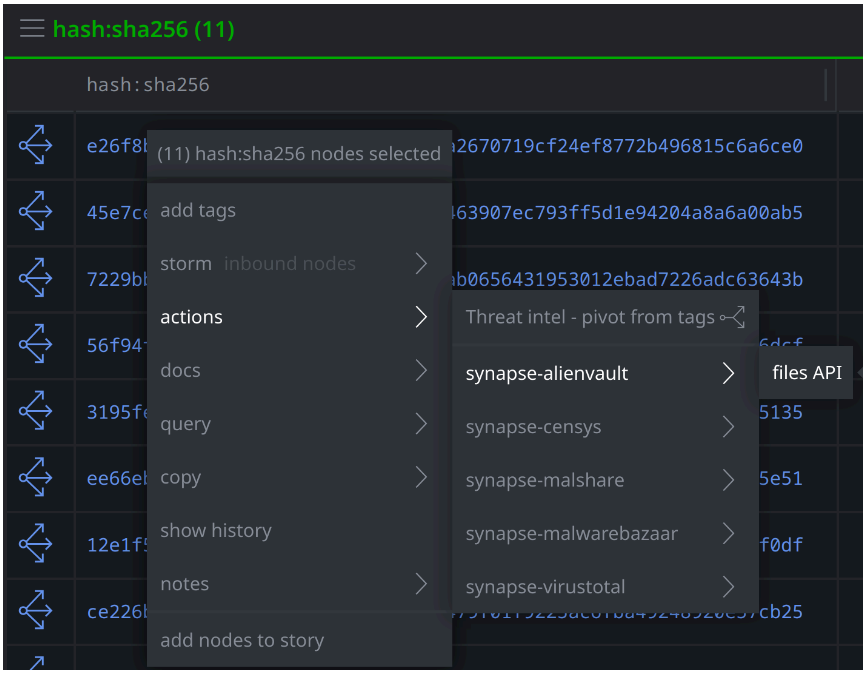
  Lift all of the EclecticIQ indicators using the `#rep.eclecticiq` tag:

  ```
  | #rep.eclecticiq
  ```

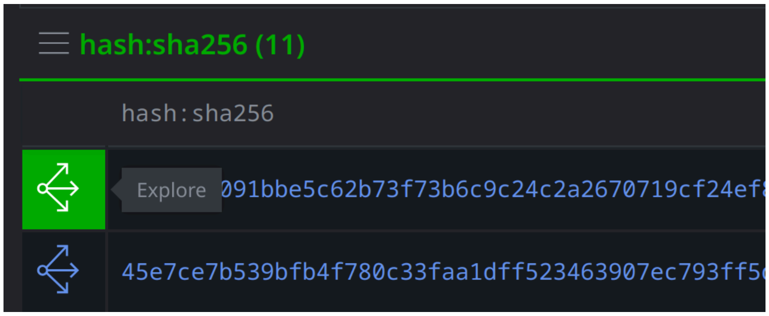
- **Select All** **`hash:sha256`** nodes:



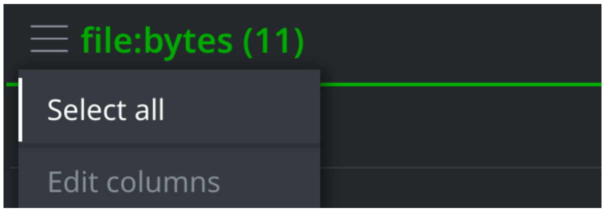
- Right-click on the **`hash:sha256`** nodes and select **actions > synapse-alienvault > files API** from the Context menu to enrich the hashes:



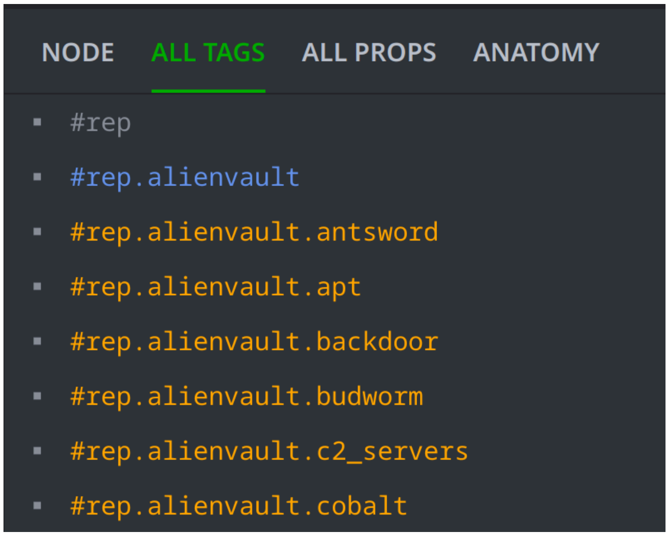
- Click the **Explore** button to navigate to the associated **`file:bytes`** nodes:


hash:sha256 (11)
hash:sha256
Explore
091bbe5c62b73f73b6c9c24c2a2670719cf24ef
45e7ce7b539bfb4f780c33faa1dff523463907ec793ff5

- Click on the hamburger menu and **Select All** **`file:bytes`** nodes:



- Select the **All Tags** tab in the **Details pane** to view all the tags on the `file:bytes` nodes:



- #rep
- #rep.alienvault
- #rep.alienvault.antsword
- #rep.alienvault.apt
- #rep.alienvault.backdoor
- #rep.alienvault.budworm
- #rep.alienvault.c2_servers
- #rep.alienvault.cobalt

- There are a variety of AlienVault tags shown, some of which are likely references to malware or threat group names. These include: antsword, budworm, doraemon, earth lusca, funnyswitch, shadowpad, and winnti, among others.

Note: The ALL TAGS tab shows all tags that are present on **any** nodes in your results; it does not mean that all of these tags appear on every node.

The ALL TAGS tab is good for getting an **overview** of your results. Select **individual** nodes to view the specific tag(s) present on that node (using the NODE tab).

Question 2

Which of the URLs does AlienVault associate with Cobalt Strike? How can you tell?

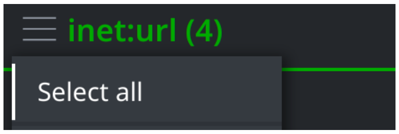
- Copy and paste the URLs from the IOC list into the **Query Bar** (in Lookup mode) to lift the associated `inet:url` nodes

  OR

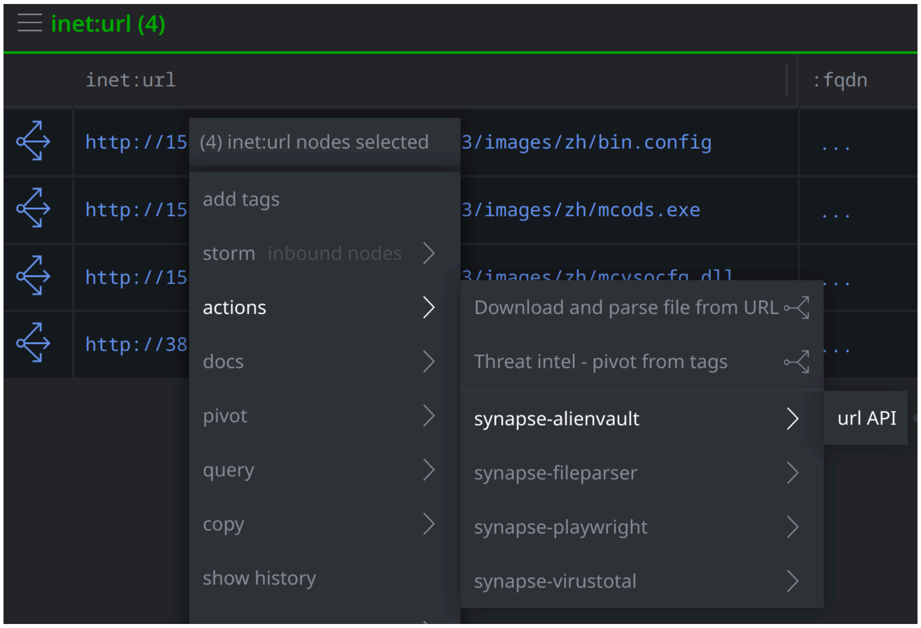
  Lift all of the EclecticIQ indicators using the `#rep.eclecticiq` tag:

  ```
  | #rep.eclecticiq
  ```

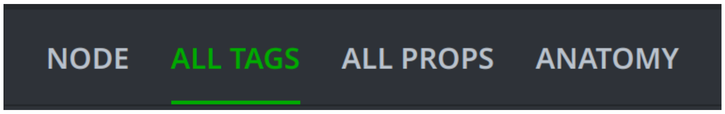
- **Select All** `inet:url` nodes:



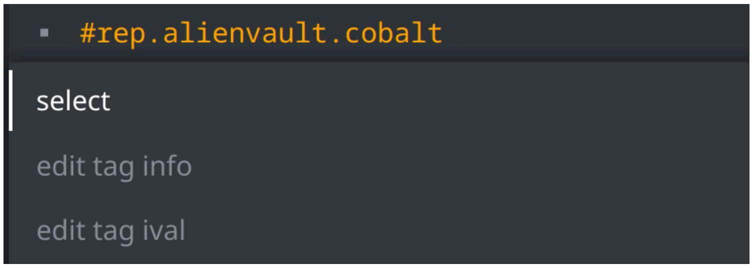
- Right-click on the nodes and select **actions > synapse-alienvault > url API** from the Context menu:



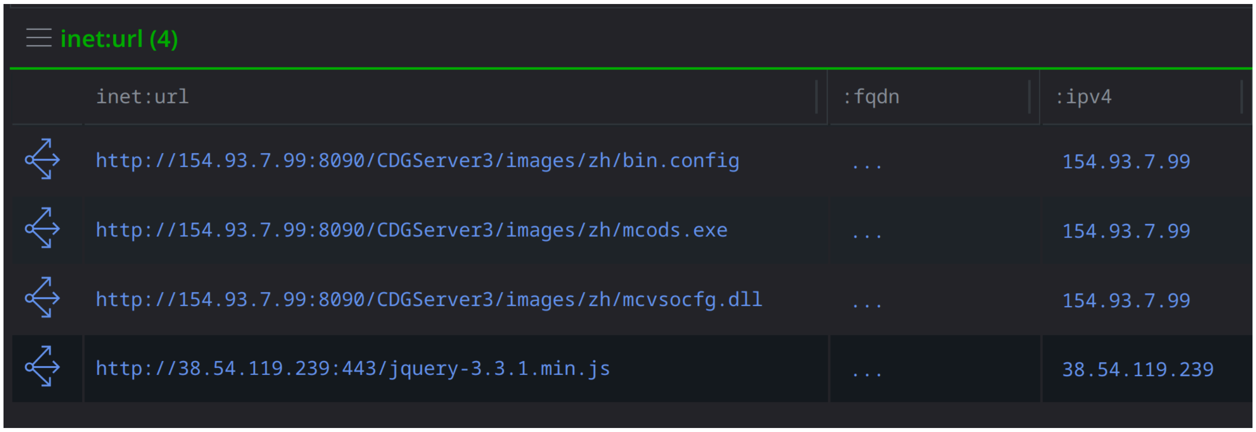
- Select the **All Tags** tab in the **Details pane** to view all the tags that appear on the nodes:



- Click on the tag `#rep.alienvault.cobalt` and choose **Select** from the menu:



- This will highlight any node(s) in the Results panel that are tagged with **#rep.alienvault.cobalt**:



inet:url (4)

inet:url	:fqdn	:ipv4
http://154.93.7.99:8090/CDGServer3/images/zh/bin.config	...	154.93.7.99
http://154.93.7.99:8090/CDGServer3/images/zh/mcods.exe	...	154.93.7.99
http://154.93.7.99:8090/CDGServer3/images/zh/mcvsocfg.dll	...	154.93.7.99
http://38.54.119.239:443/jquery-3.3.1.min.js	...	38.54.119.239

- AlienVault associates **`https://38.54.119[.]239:443/jquery-3.3.1.min.js`** with Cobalt Strike.

Question 3

What steps can you take to identify which file makes this reference in its filename?

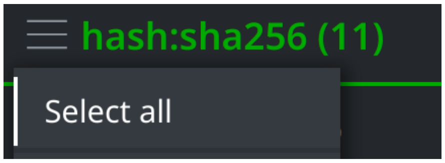
- Lift the **`hash:sha256`** nodes included in the IOC list by copying and pasting them into the Query Bar (Lookup mode)

  OR

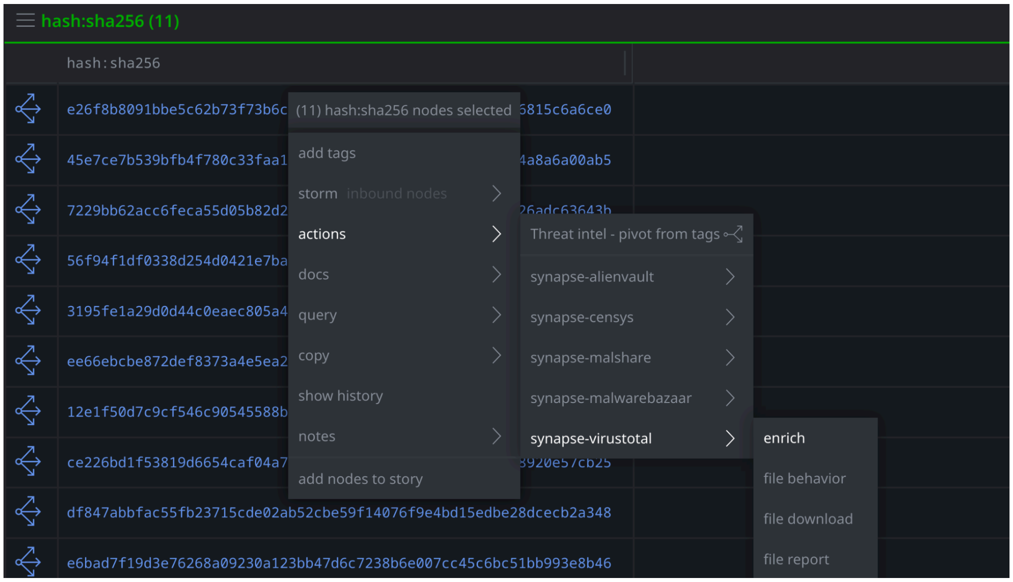
  Lift all of the EclecticIQ indicators using the `#rep.eclecticiq` tag:

```
| #rep.eclecticiq
```

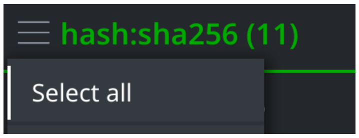
- **Select All** **`hash:sha256`** nodes:



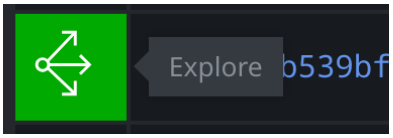
- Right-click on the nodes and select **actions > synapse-virustotal > enrich**:


hash:sha256 (11)
hash:sha256
e26f8b8091bbe5c62b73f73b6c
6815c6a6ce0
45e7ce7b539bfb4f780c33faa1
4a8a6a00ab5
7229bb62acc6feca55d05b82d2
26adc63643b
56f94f1df0338d254d0421e7ba
3195fe1a29d0d44c0eaec805a4
ee66ebcbe872def8373a4e5ea2
12e1f50d7c9cf546c90545588b
ce226bd1f53819d6654caf04a7
3920e57cb25
df847abbfac55fb23715cde02ab52cbe59f14076f9e4bd15edbe28dcecb2a348
e6bad7f19d3e76268a09230a123bb47d6c7238b6e007cc45c6bc51bb993e8b46
(11) hash:sha256 nodes selected
add tags
storm inbound nodes
actions
docs
query
copy
show history
notes
add nodes to story
Threat intel - pivot from tags
synapse-alienvault
synapse-censys
synapse-malshare
synapse-malwarebazaar
synapse-virustotal
enrich
file behavior
file download
file report

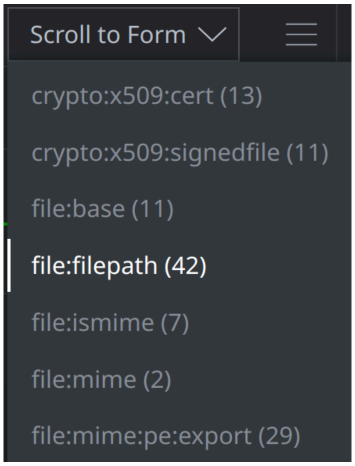
- Select all **hash:sha256** nodes:



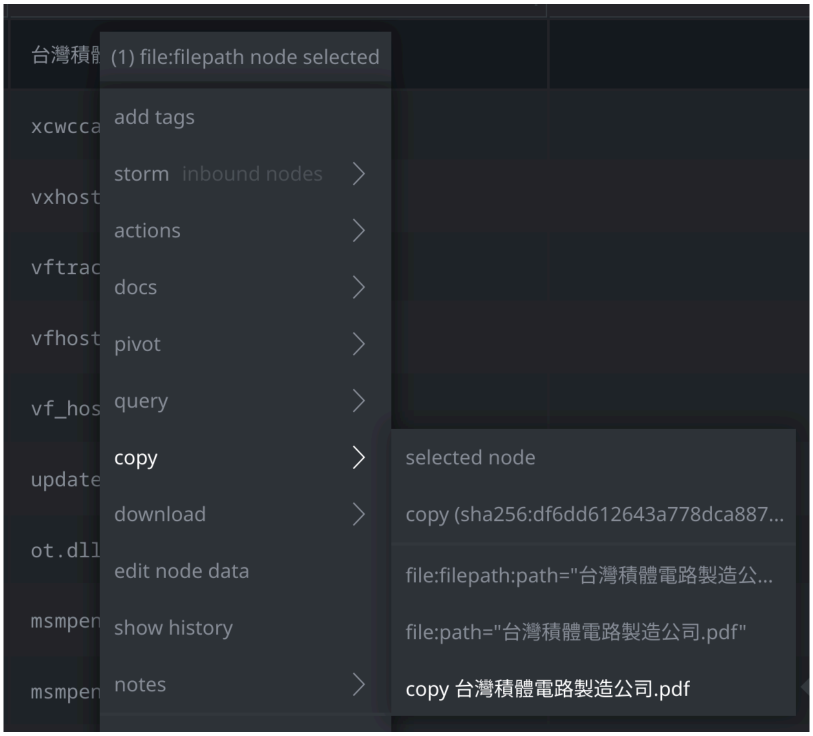
- Click on the **Explore** button to navigate to the associated **file:bytes** nodes:



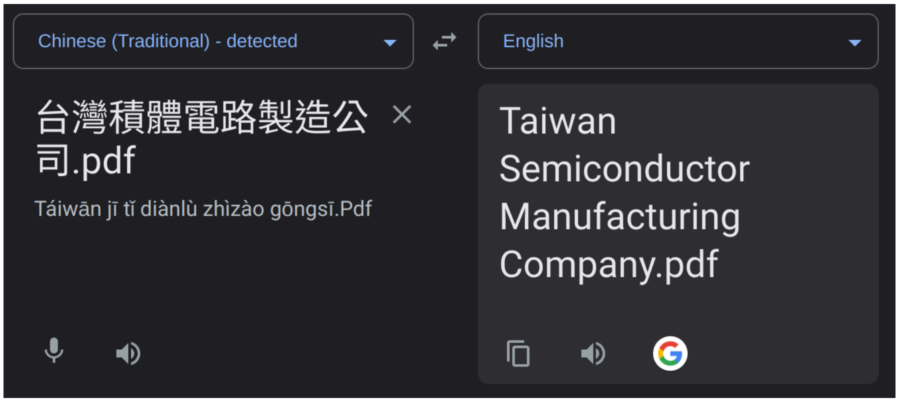
- Select all **file:bytes** nodes and click the **Explore** button again to pivot to related nodes. Use the **Scroll to Form** tool to lift the **file:filepath** nodes:



- Scan the **`file:filepath:path`** property values to find the Mandarin filename. Right-click on it and select **copy > 台灣積體電路製造公司.pdf** from the **Context Menu**:


台灣積體
xcwcca
vxhost
vftrac
vfhost
vf_hos
update
ot.dll
msmpen
msmpen
(1) file:filepath node selected
add tags
storm inbound nodes
actions
docs
pivot
query
copy
download
edit node data
show history
notes
selected node
copy (sha256:df6dd612643a778dca887...
file:filepath:path="台灣積體電路製造公...
file:path="台灣積體電路製造公司.pdf"
copy 台灣積體電路製造公司.pdf

- Paste the characters into Google Translate to check the translation:



台灣積體電路製造公司.pdf

Táiwān jī tǐ diànlù zhìzào gōngsī.Pdf

Taiwan Semiconductor Manufacturing Company.pdf

Question 4

How many files (total) communicate with the two IPv4 addresses?

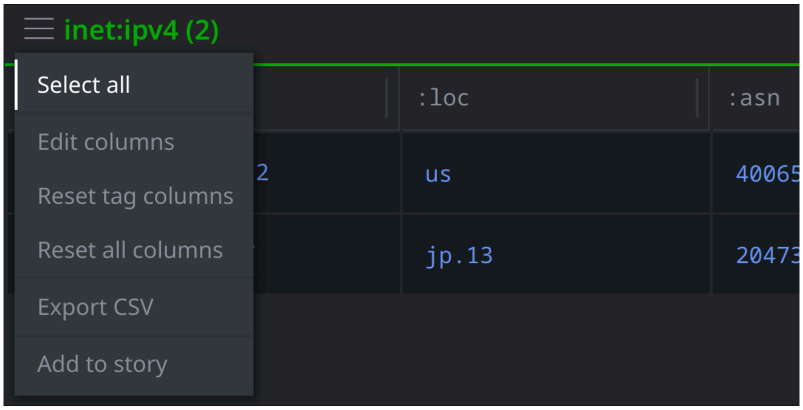
- Lift the IPv4 addresses from the IOC list by copying and pasting them into the **Query Bar** (Lookup mode)

  OR

  Lift all of the EclecticIQ indicators using the `#rep.eclecticiq` tag:

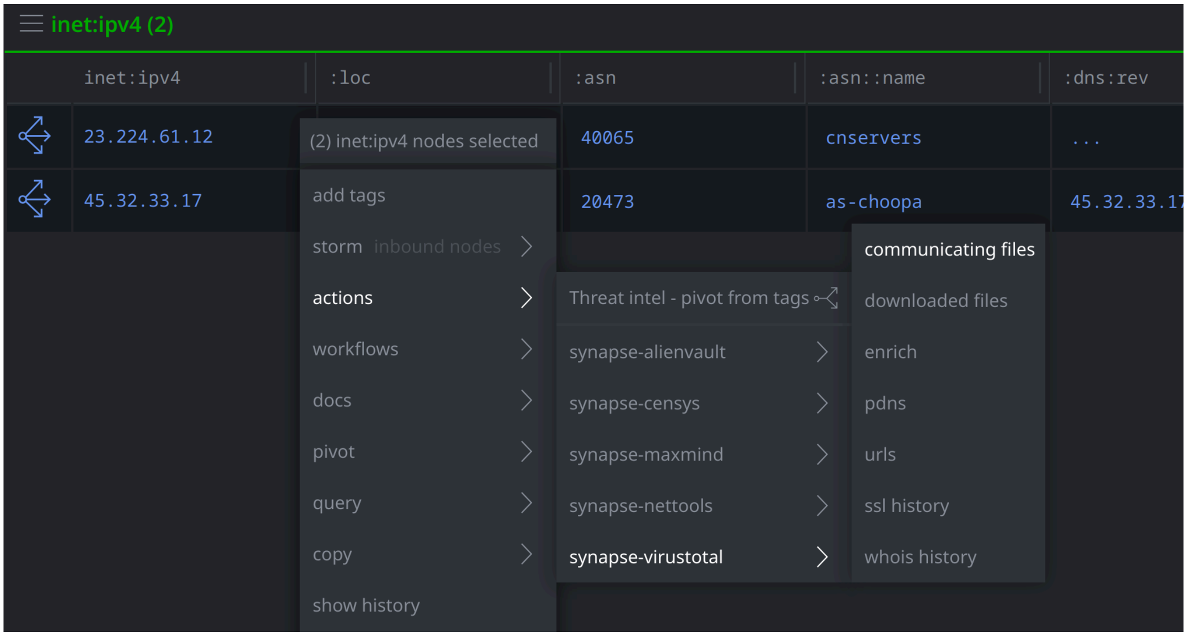
  ```
  | #rep.eclecticiq
  ```

- **Select all** `inet:ipv4` nodes representing the IP addresses included in the IOC list:



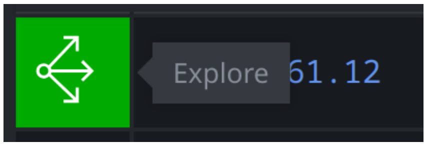
	:loc	:asn
2	us	40065
	jp.13	20473

- Right-click on the `inet:ipv4` nodes and run the **synapse-virustotal > communicating files** Node Action:

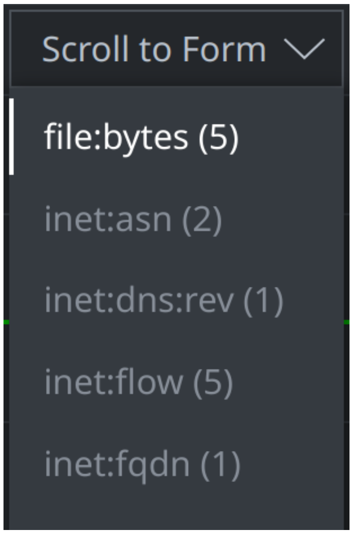


inet:ipv4	:loc	:asn	:asn::name	:dns:rev
23.224.61.12		40065	cnservers	...
45.32.33.17		20473	as-choopa	45.32.33.17

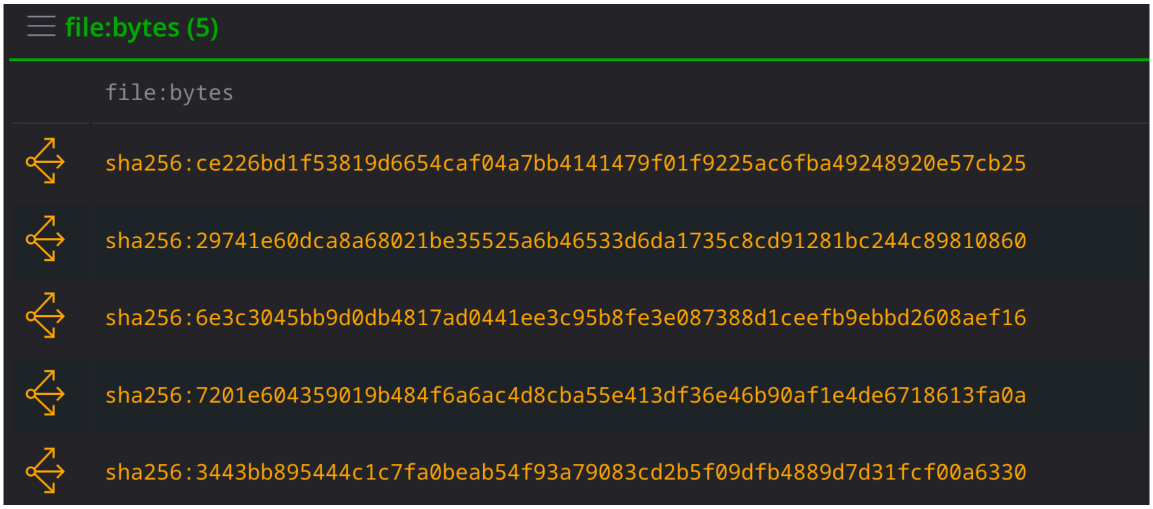
- Click the **Explore** button to explore out from the selected **`inet:ipv4`** nodes:



- Use **Scroll to Form** to lift the **`file:bytes`** nodes:



- According to VirusTotal, there are five files that communicate with the reported IP addresses:



file:bytes (5)

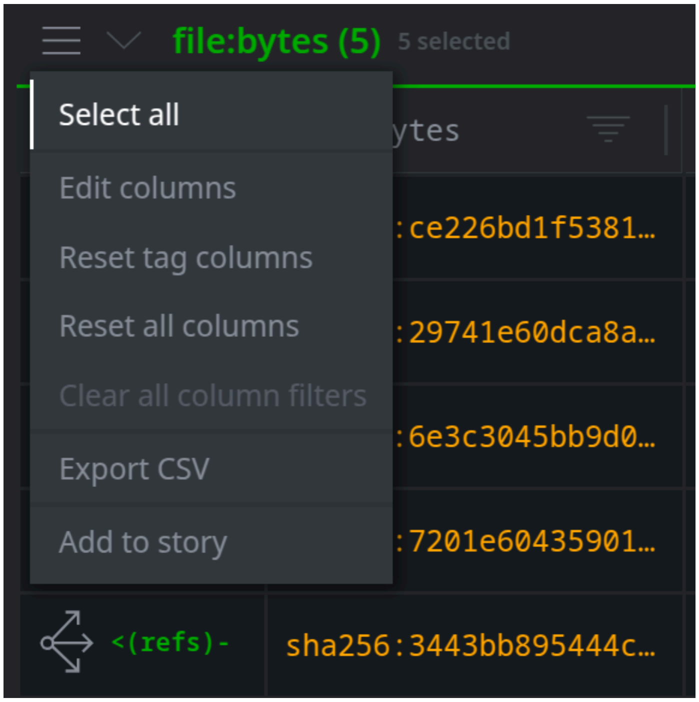
file:bytes
sha256:ce226bd1f53819d6654caf04a7bb4141479f01f9225ac6fba49248920e57cb25
sha256:29741e60dca8a68021be35525a6b46533d6da1735c8cd91281bc244c89810860
sha256:6e3c3045bb9d0db4817ad0441ee3c95b8fe3e087388d1ceefb9ebbd2608aef16
sha256:7201e604359019b484f6a6ac4d8cba55e413df36e46b90af1e4de6718613fa0a
sha256:3443bb895444c1c7fa0beab54f93a79083cd2b5f09dfb4889d7d31fcf00a6330

Tip: To determine "how" these files communicate with the IPv4 addresses, we could perform additional enrichment. For example, running the **synapse-virustotal > file behavior** Node Action to enrich these **`file:bytes`** nodes will retrieve sandbox execution data from VirusTotal. We can then **Explore** from the files to review connected nodes, which may include network communication data. (We'll cover malware data - including VirusTotal data - in more detail later in the course!)

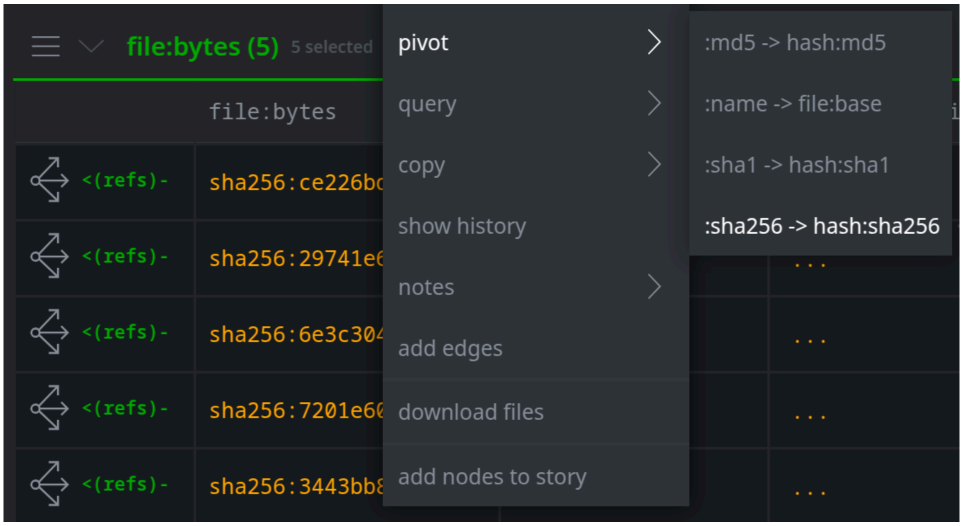
How many files (SHA256 hashes) were **not** included in the EclecticIQ report?

Four of the five files (SHA256 hashes) were not reported by EclecticIQ.

- **Select All** of the **`file:bytes`** nodes:

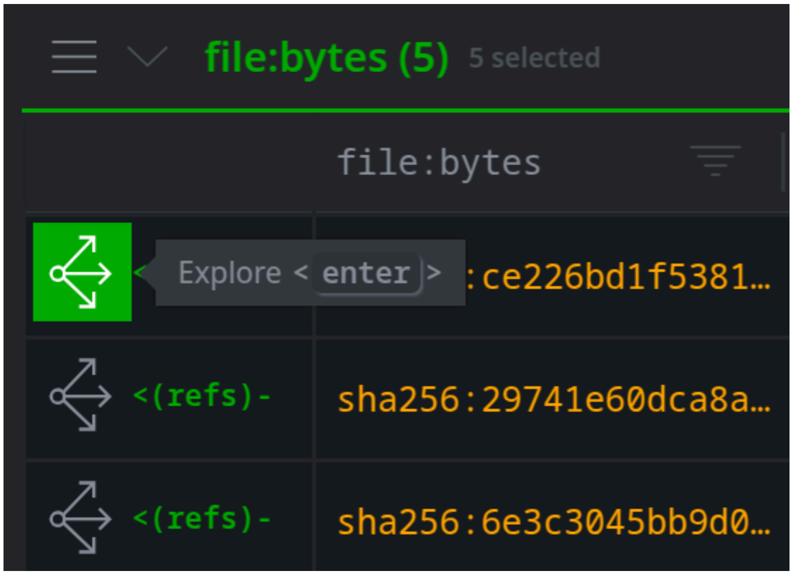


- **Right-click** any of the selected nodes and select **pivot > :sha256 -> hash:sha256** to pivot to the associated hashes:



OR

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

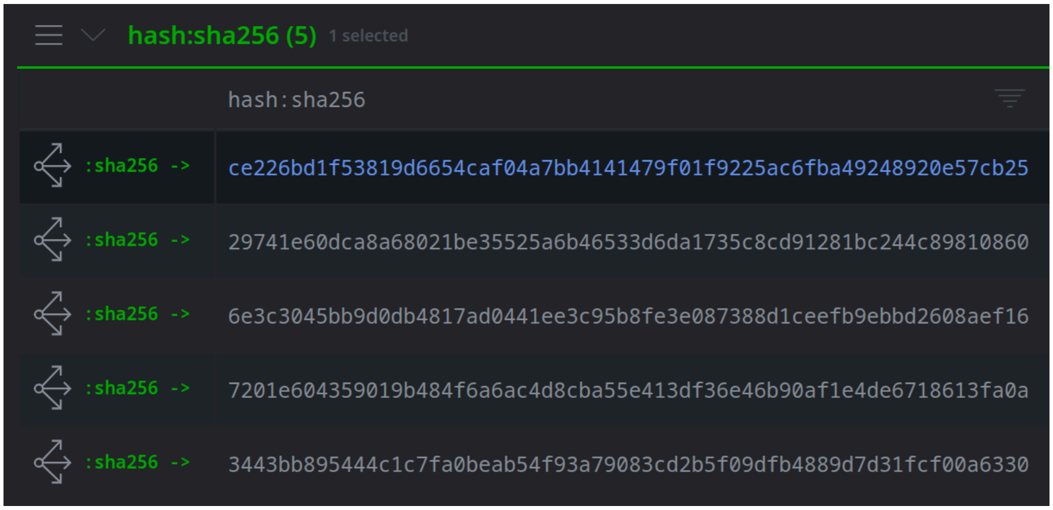


```
file:bytes (5)  5 selected

file:bytes
        Explore < enter >  :ce226bd1f5381…
<(refs)-    sha256:29741e60dca8a…
<(refs)-    sha256:6e3c3045bb9d0…
```

...and locate the **hash:sha256** nodes in your results.

- Only **one** hash has a #rep.eclecticiq tag (assuming you tagged the nodes):



```
hash:sha256 (5)  1 selected

             hash:sha256
:sha256 ->   ce226bd1f53819d6654caf04a7bb4141479f01f9225ac6fba49248920e57cb25
:sha256 ->   29741e60dca8a68021be35525a6b46533d6da1735c8cd91281bc244c89810860
:sha256 ->   6e3c3045bb9d0db4817ad0441ee3c95b8fe3e087388d1ceefb9ebbd2608aef16
:sha256 ->   7201e604359019b484f6a6ac4d8cba55e413df36e46b90af1e4de6718613fa0a
:sha256 ->   3443bb895444c1c7fa0beab54f93a79083cd2b5f09dfb4889d7d31fcf00a6330
```

Question 5

Which of these hashes is associated with the file that attempts to download **bin.config** from **hxxp://154.93.7[.]99:8090/CDGServer3/images/zh/bin.config**?

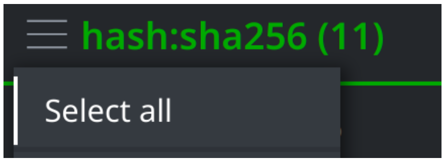
- Lift the **hash:sha256** nodes included in the IOC list by copying and pasting them into the Query Bar (Lookup mode)

OR

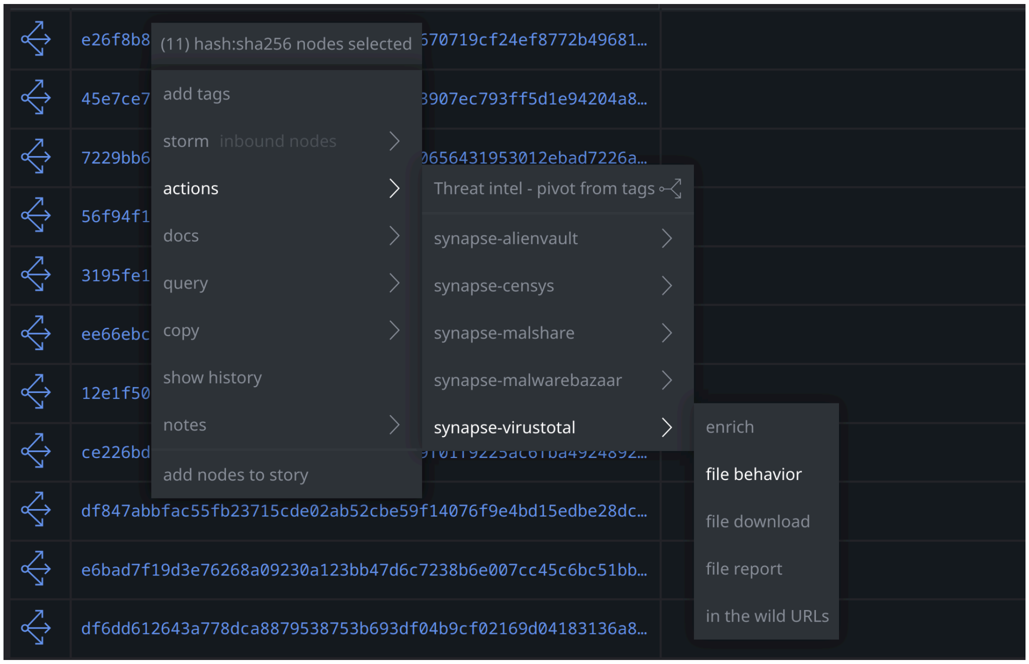
Lift all of the EclecticIQ indicators using the `#rep.eclecticiq` tag:

```
| #rep.eclecticiq
```

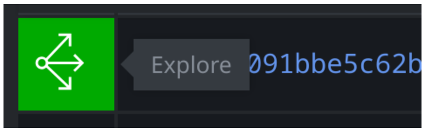
- **Select All** `hash:sha256` nodes:



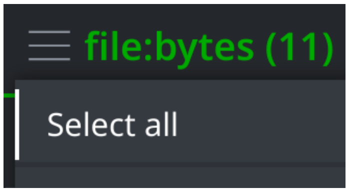
- **Right-click** on the selected hashes and select **actions > synapse-virustotal > file behavior** to run the Node Action:



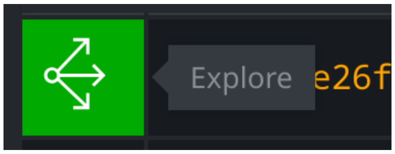
- Click the **Explore** button to navigate to the associated `file:bytes` nodes:



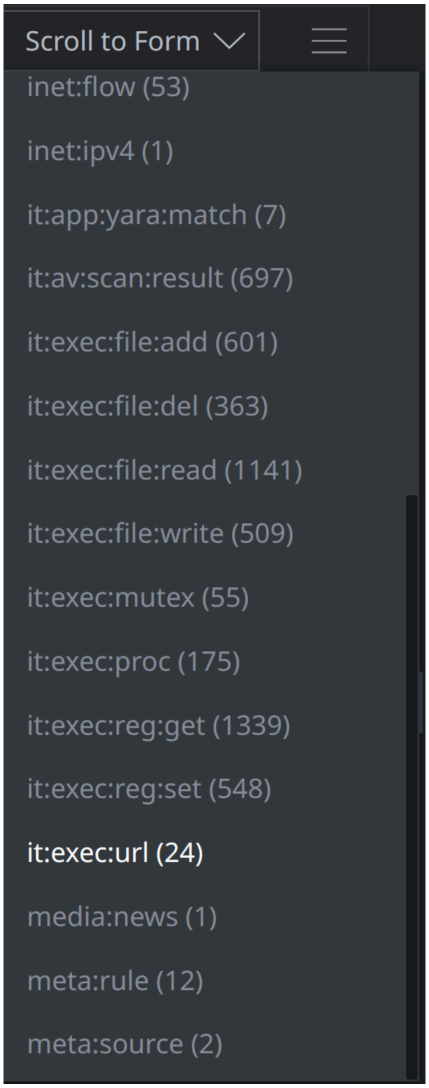
- **Select all** `file:bytes` nodes:



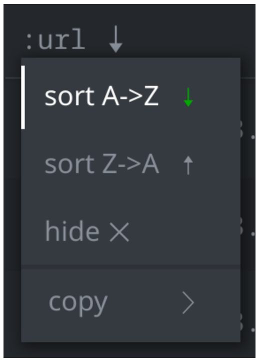
- Click the **Explore** button to navigate to connected nodes:



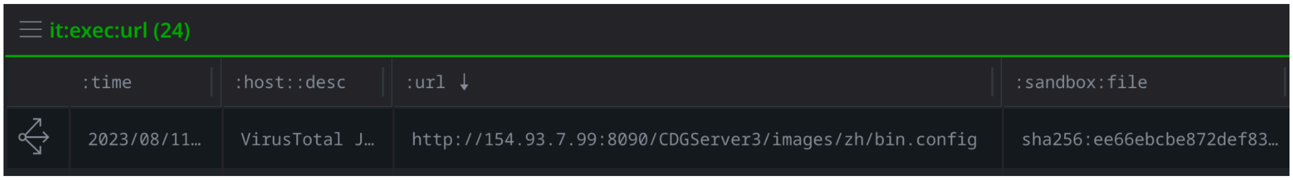
- Use **Scroll to Form** to lift the **`it:exec:url`** nodes:



- Click on the **`:url`** column header to sort the property values in descending order:



- Only one of the files attempts to download a file named **`bin.config`** from the identified URL:



it:exec:url (24)

	:time	:host::desc	:url ↓	:sandbox:file
	2023/08/11…	VirusTotal J…	http://154.93.7.99:8090/CDGServer3/images/zh/bin.config	sha256:ee66ebcbe872def83…

The file's SHA256 hash value, visible in the **`:sandbox:file`** property, is **`ee66ebcbe872def8373a4e5ea23f14181ea04759ea83f01d2e8ff45d60c65e51`**