Synapse Bootcamp - Module 3

Exploring and Filtering Data - Answer Key

Answer Key

Navigating Data in Synapse

Exercise 1 Answer

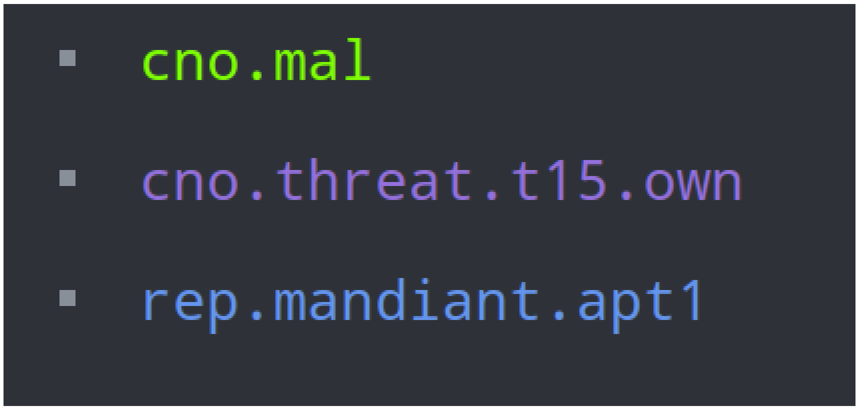
Objective:

- **Use the Synapse Explore button to navigate and view data in Tabular display mode.**

Part 1

Question 1: What do the tags tell us about this FQDN?

- The node has three tags:

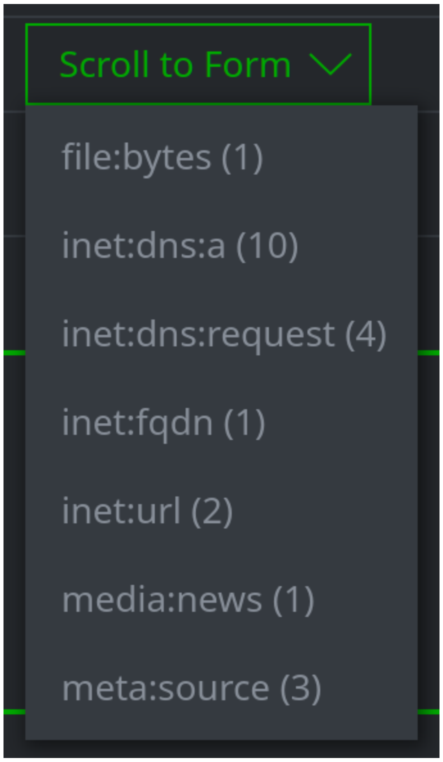


- cno.mal
- cno.threat.t15.own
- rep.mandiant.apt1

  - Vertex says the FQDN is malicious (**cno.mal**).
  - Vertex says the FQDN is associated with a threat they call T15 (**cno.threat.t15.own**).
  - Mandiant says the FQDN is associated with a threat they call APT1 (**rep.mandiant.apt1**).

Question 2: What kinds of nodes are "connected" to the FQDN?

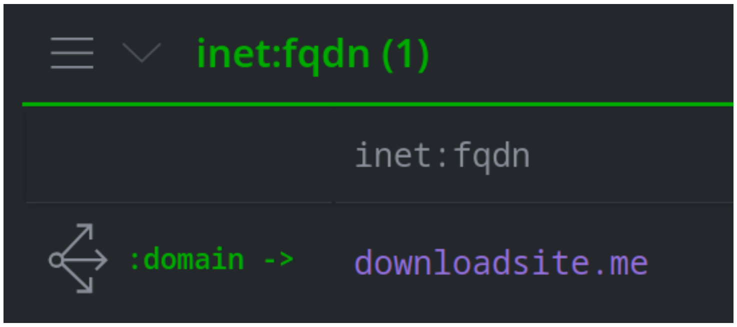
- The FQDN is connected to several other objects (forms):



These include:
  - Files (**`file:bytes`**)
  - DNS A records (**`inet:dns:a`**)
  - DNS requests (**`inet:dns:request`**)
  - Additional FQDNs (**`inet:fqdn`**)
  - URLs (**`inet:url`**)
  - Articles or publications (**`media:news`**)
  - Data sources (**`meta:source`**)

Question 3: How is the FQDN **`downloadsite.me`** connected to your original FQDN (`documents.downloadsite.me`)?

- The link column reads:
  :domain ->



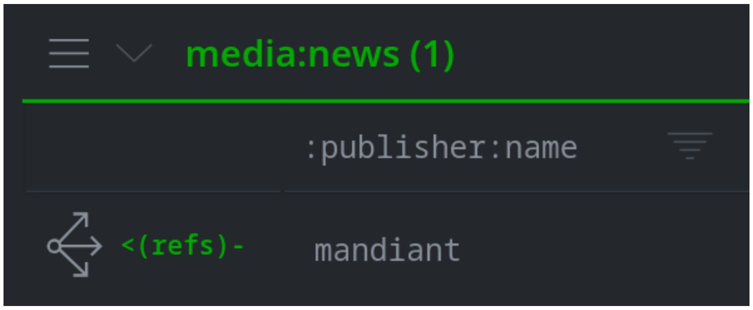
inet:fqdn (1)

	inet:fqdn
:domain ->	downloadsite.me

This indicates that when you used the **Explore** button, Synapse navigated from the **`:domain`** property of your original FQDN to that property's value - the FQDN **`downloadsite.me`**.

Question 4: How is the **`media:news`** node connected to your original FQDN (`documents.downloadsite.me`)?

- The link column reads:
  <(refs)-



media:news (1)

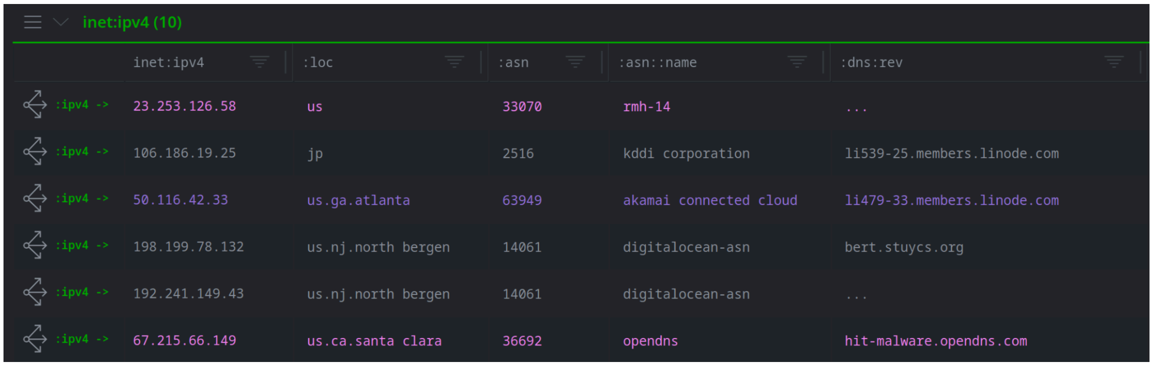
	:publisher:name
<(refs)-	mandiant

This indicates that the **`media:news`** node **references** the original FQDN.

Part 2

Question 5: What information is available for the IP addresses, based on their properties and tags?

- There are several **properties** displayed for the Pv4 nodes:



inet:ipv4 (10)

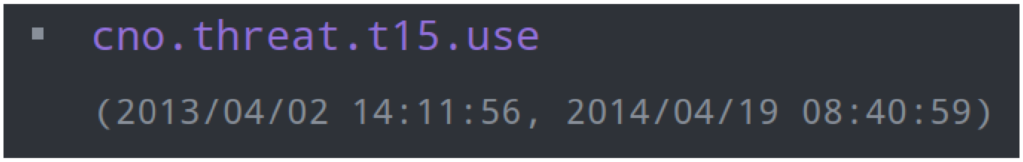
	inet:ipv4	:loc	:asn	:asn::name	:dns:rev
:ipv4 ->	23.253.126.58	us	33070	rmh-14	...
:ipv4 ->	106.186.19.25	jp	2516	kddi corporation	li539-25.members.linode.com
:ipv4 ->	50.116.42.33	us.ga.atlanta	63949	akamai connected cloud	li479-33.members.linode.com
:ipv4 ->	198.199.78.132	us.nj.north bergen	14061	digitalocean-asn	bert.stuycs.org
:ipv4 ->	192.241.149.43	us.nj.north bergen	14061	digitalocean-asn	...
:ipv4 ->	67.215.66.149	us.ca.santa clara	36692	opendns	hit-malware.opendns.com

These include:

  - where the IPs are located (`:loc` property)
  - the Autonomous System (AS) number and name (`:asn` property and `:asn::name` column)
  - any DNS PTR record (FQDN) for the IP (`:dns:rev` property).

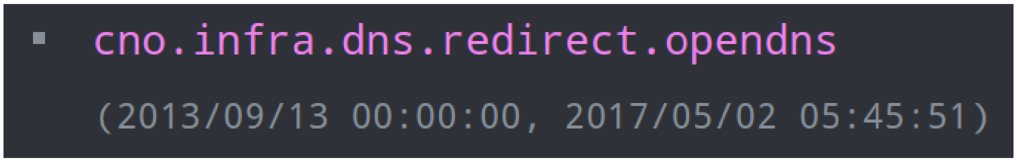
- Based on the **colors** in our display, several IPv4 nodes also have **tags** (you can see these in the **Details Panel** for each node):

  - IPv4 `50.116.42.33` was **used by threat group T15** between April 2, 2013 and April 19, 2014:



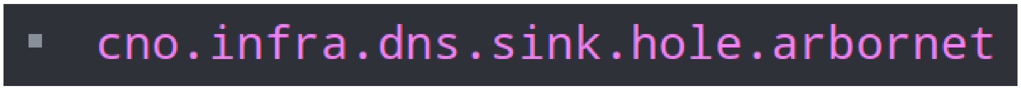
```
▪ cno.threat.t15.use
  (2013/04/02 14:11:56, 2014/04/19 08:40:59)
```

  - IPv4 `67.215.66.149` is a **DNS redirect** used by OpenDNS:



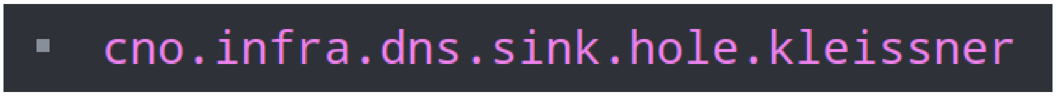
```
▪ cno.infra.dns.redirect.opendns
  (2013/09/13 00:00:00, 2017/05/02 05:45:51)
```

  - IPv4 addresses `104.239.157.210` and `23.253.126.58` are **sinkholes** associated with Arbornet:



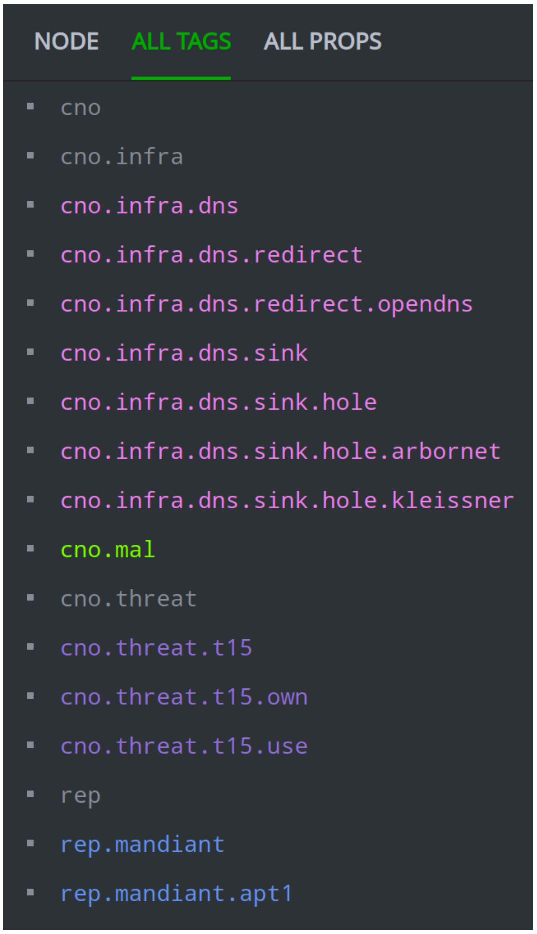
```
▪ cno.infra.dns.sink.hole.arbornet
```

  - IPv4 addresses **69.195.129.70** and **69.195.129.72** are **sinkholes** associated with Kleissner & Associates:



    - cno.infra.dns.sink.hole.kleissner

- You can use the **ALL TAGS** tab to view a summary of **all** tags that appear on **any** node in **any** of your results:

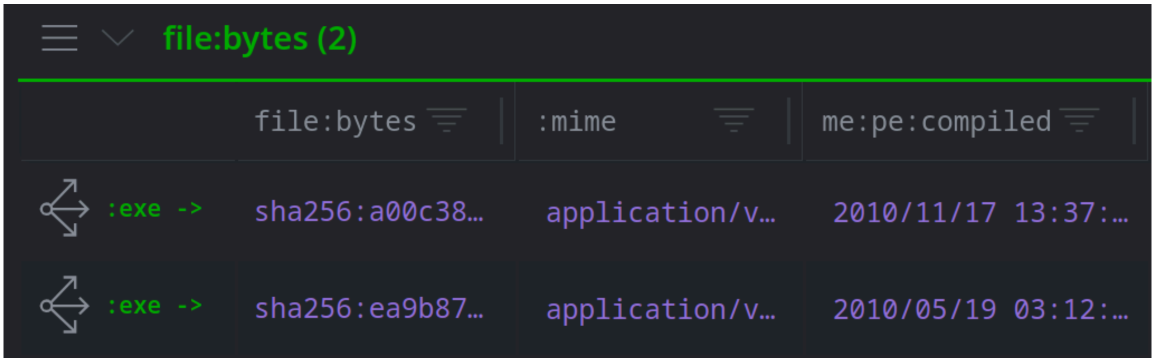


- cno
- cno.infra
- cno.infra.dns
- cno.infra.dns.redirect
- cno.infra.dns.redirect.opendns
- cno.infra.dns.sink
- cno.infra.dns.sink.hole
- cno.infra.dns.sink.hole.arbornet
- cno.infra.dns.sink.hole.kleissner
- cno.mal
- cno.threat
- cno.threat.t15
- cno.threat.t15.own
- cno.threat.t15.use
- rep
- rep.mandiant
- rep.mandiant.apt1

Part 3

Question 6: How many files query the FQDN **documents.downloadsite.me**?

- **Two** files query the FQDN:



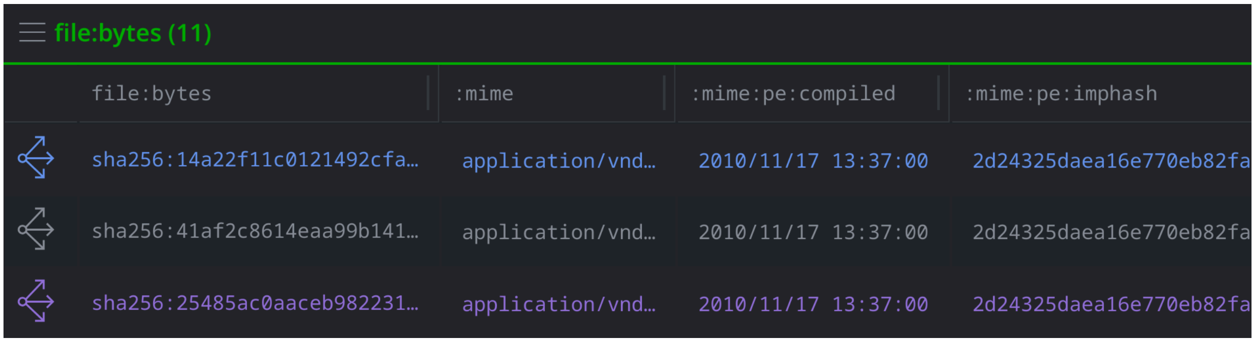
file:bytes (2)

	file:bytes	:mime	me:pe:compiled
:exe ->	sha256:a00c38…	application/v…	2010/11/17 13:37:…
:exe ->	sha256:ea9b87…	application/v…	2010/05/19 03:12:…

Part 4

Question 7: How many files share that same compile time?

- There are **eleven** files in Synapse with that compile time:



file:bytes (11)

	file:bytes	:mime	:mime:pe:compiled	:mime:pe:imphash
	sha256:14a22f11c0121492cfa…	application/vnd…	2010/11/17 13:37:00	2d24325daea16e770eb82fa
	sha256:41af2c8614eaa99b141…	application/vnd…	2010/11/17 13:37:00	2d24325daea16e770eb82fa
	sha256:25485ac0aaceb982231…	application/vnd…	2010/11/17 13:37:00	2d24325daea16e770eb82fa

Filtering Results in Synapse

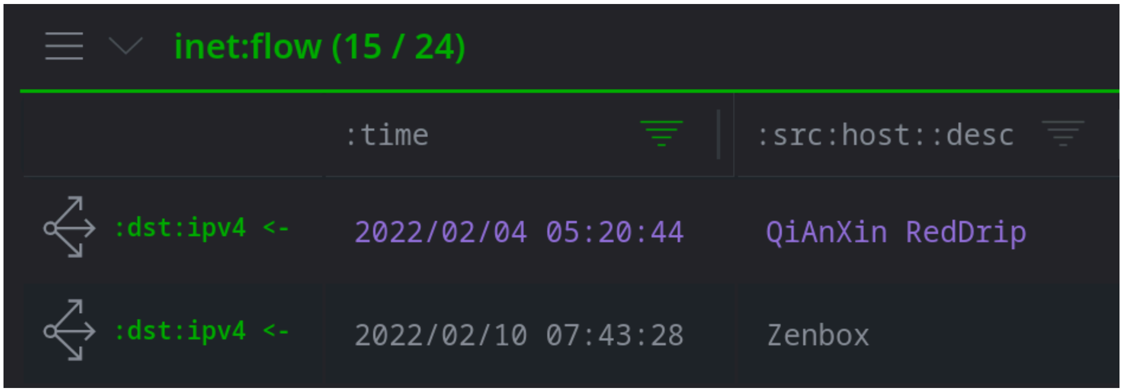
Exercise 2 Answer

Objectives:

- **Use the column filters to display a subset of your results.**

Question 1: How many results are visible after applying the filter?

- There are **15** results displayed (out of 24 total):

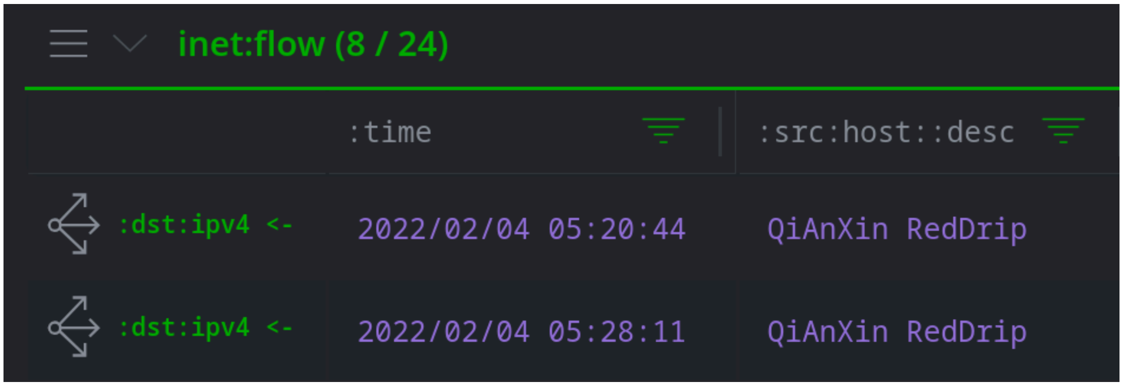


inet:flow (15 / 24)

	:time	:src:host::desc
:dst:ipv4 <-	2022/02/04 05:20:44	QiAnXin RedDrip
:dst:ipv4 <-	2022/02/10 07:43:28	Zenbox

Question 2: How many results are present after applying the filter?

- There are **eight** results displayed (out of 24 total):



inet:flow (8 / 24)

	:time	:src:host::desc
:dst:ipv4 <-	2022/02/04 05:20:44	QiAnXin RedDrip
:dst:ipv4 <-	2022/02/04 05:28:11	QiAnXin RedDrip

Filtering Data in Synapse

Exercise 3 Answer

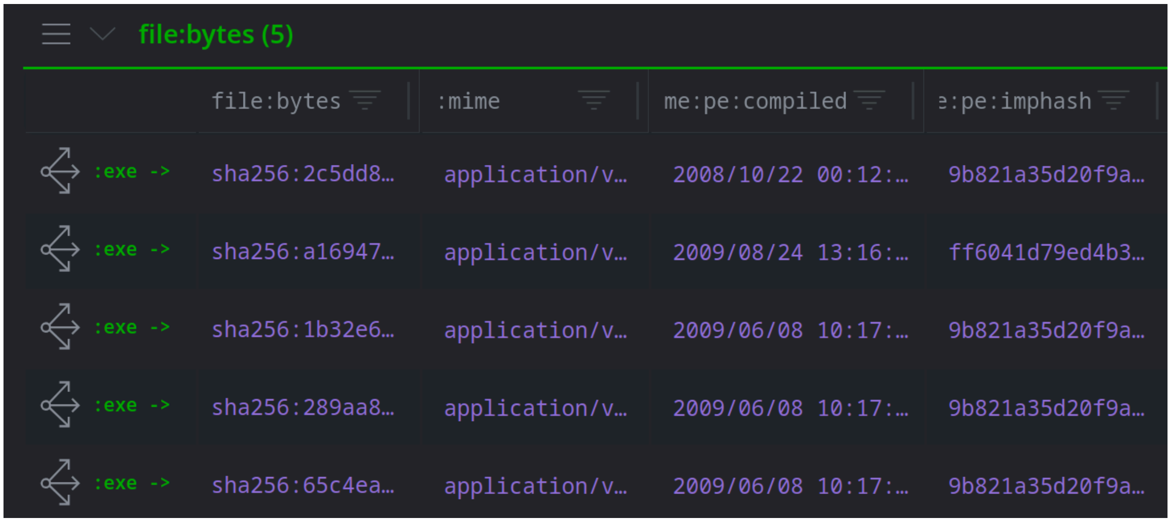
Objectives:

- **Use the 'query' menu to filter your results by running a Storm query.**

Part 1

Question 1: How many files query FQDNs associated with **`earthsolution.org?`**

- **Five** files (`file:bytes` nodes) query various subdomains of `earthsolution.org`:

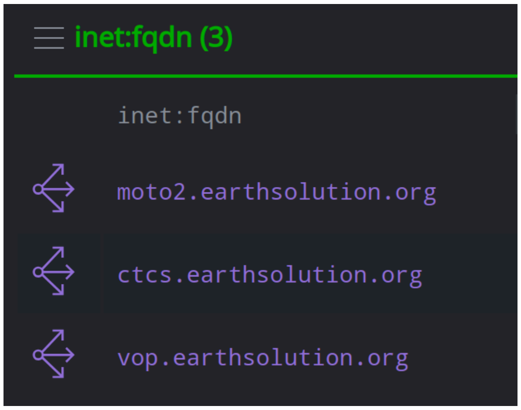


file:bytes (5)

	file:bytes	:mime	me:pe:compiled	e:pe:imphash
:exe ->	sha256:2c5dd8…	application/v…	2008/10/22 00:12:…	9b821a35d20f9a…
:exe ->	sha256:a16947…	application/v…	2009/08/24 13:16:…	ff6041d79ed4b3…
:exe ->	sha256:1b32e6…	application/v…	2009/06/08 10:17:…	9b821a35d20f9a…
:exe ->	sha256:289aa8…	application/v…	2009/06/08 10:17:…	9b821a35d20f9a…
:exe ->	sha256:65c4ea…	application/v…	2009/06/08 10:17:…	9b821a35d20f9a…

Question 2: Which FQDNs do the files query?

- The files query the following FQDNs:
  - `ctcs.earthsolution.org`
  - `moto2.earthsolution.org`
  - `vop.earthsolution.org`



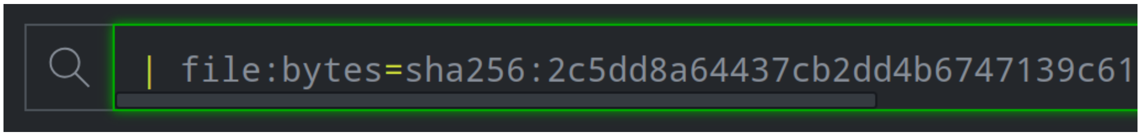
inet:fqdn (3)

inet:fqdn
moto2.earthsolution.org
ctcs.earthsolution.org
vop.earthsolution.org

Part 2

Question 3: What Storm query does Synapse enter into the Storm Query Bar after selecting the **query** option?

- Synapse creates a new Storm query to select (**lift**) the five **`file:bytes`** nodes that you selected:



```
| file:bytes=sha256:2c5dd8a64437cb2dd4b6747139c61
```

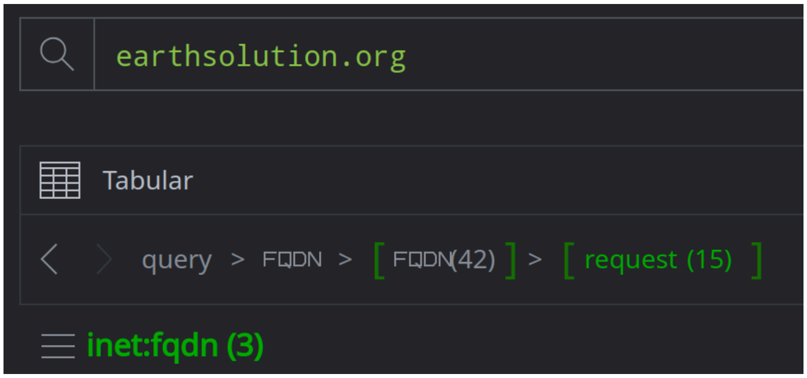
The full query is included below (lines wrap):

```
|
file:bytes=sha256:2c5dd8a64437cb2dd4b6747139c61d2d7f53ab3ddedbf
22df3cb01bae170715b
file:bytes=sha256:a1694725158441219fae3f96aa6b345f610195995568c
9409cf5c9aac029c51a
file:bytes=sha256:1b32e6800b3a80e74f135b75925f3c1e081662adfac53
262ec9a8a830398ff64
file:bytes=sha256:289aa8624ae2ca8485b9a8b73b920c6a53a796426f0da
8befd19bc085c7055fc
file:bytes=sha256:65c4ea8e926bb975d3f905157b33b24b30d6bd5cd2227
8b89222169c0216b606
```

Question 4: What happened to your breadcrumbs after selecting this option?

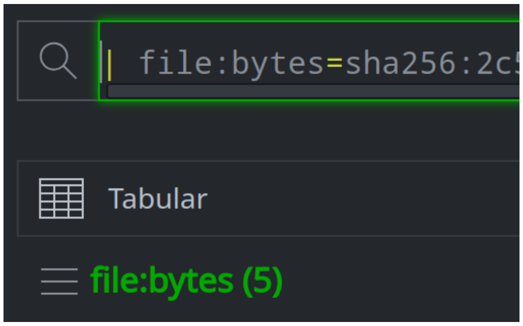
- Because **query** ran a new Storm query, the breadcrumbs from your previous query are removed:

Before:



```
earthsolution.org
```

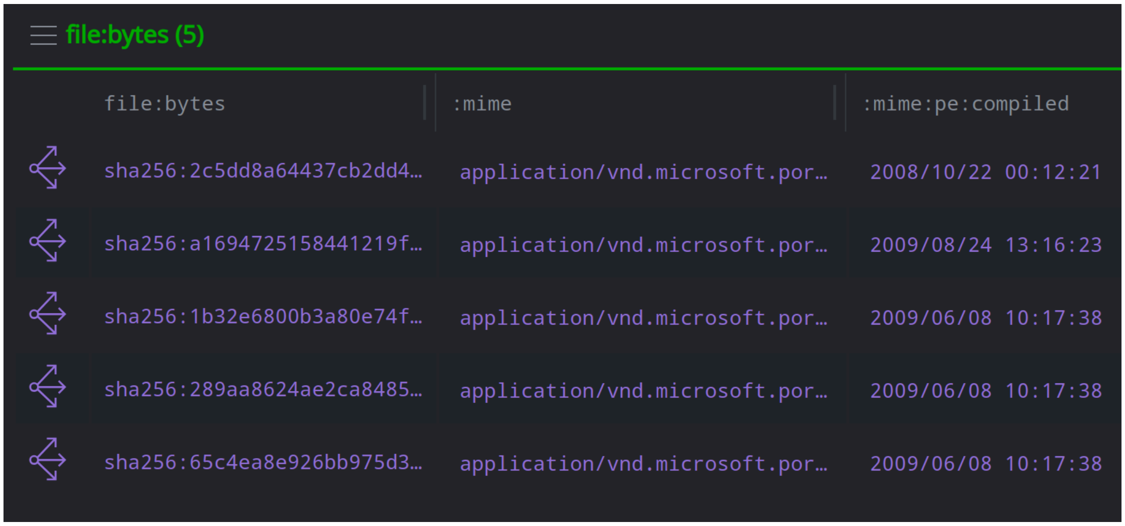
After:



```
| file:bytes=sha256:2c5
```

Question 5: What nodes are visible in your Results Panel after selecting this option?

- Your results include **only** the five files (**`file:bytes`** nodes) selected by the new query:



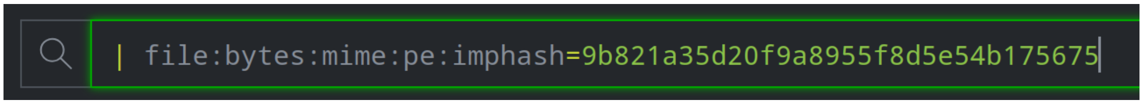
file:bytes (5)

	file:bytes	:mime	:mime:pe:compiled
	sha256:2c5dd8a64437cb2dd4…	application/vnd.microsoft.por…	2008/10/22 00:12:21
	sha256:a1694725158441219f…	application/vnd.microsoft.por…	2009/08/24 13:16:23
	sha256:1b32e6800b3a80e74f…	application/vnd.microsoft.por…	2009/06/08 10:17:38
	sha256:289aa8624ae2ca8485…	application/vnd.microsoft.por…	2009/06/08 10:17:38
	sha256:65c4ea8e926bb975d3…	application/vnd.microsoft.por…	2009/06/08 10:17:38

Part 3

Question 6: What does Synapse enter into your Storm Query Bar after selecting the **query** option?

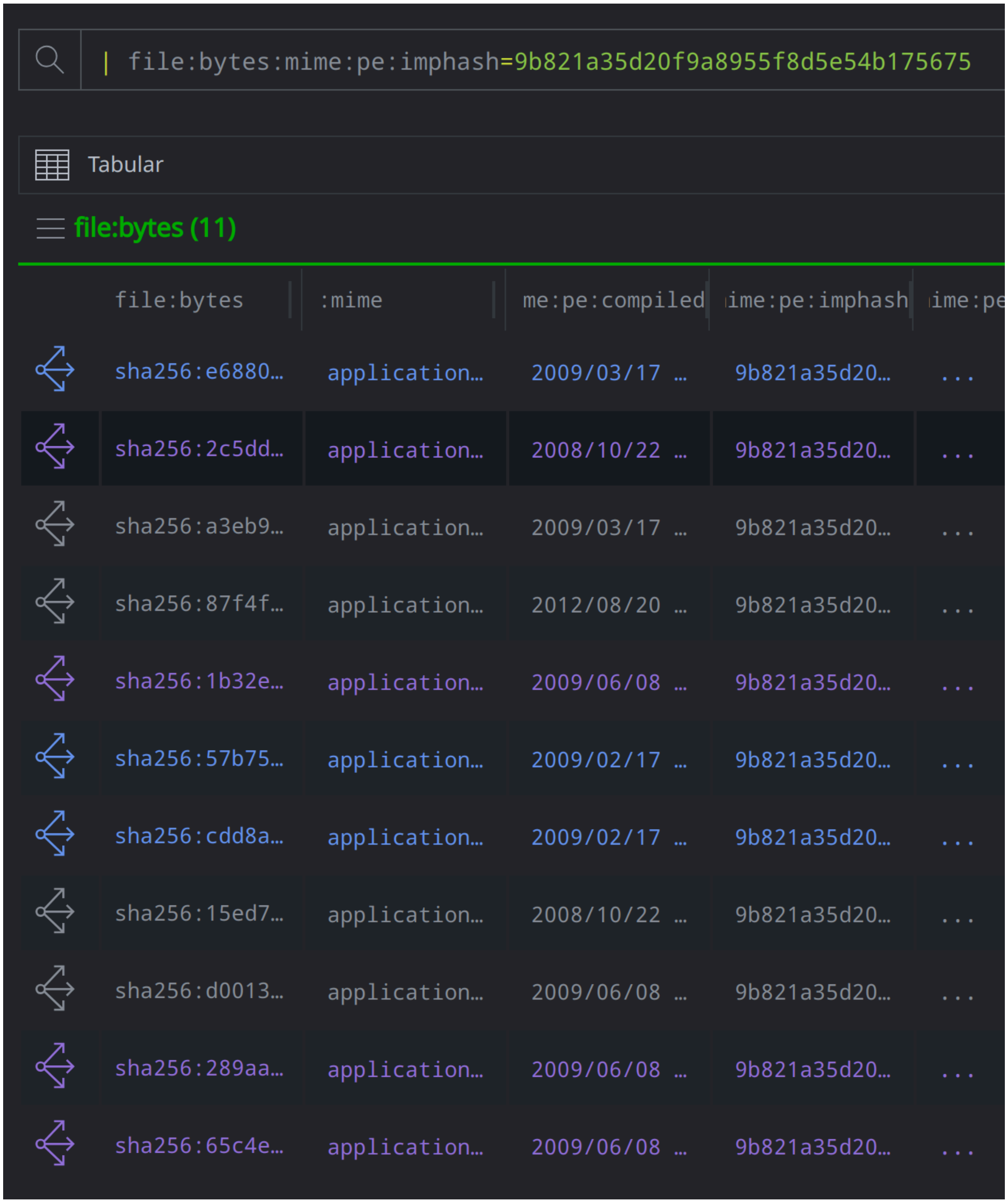
- Synapse creates a new Storm query to select (**lift**) any file with the PE import hash (**`:mime:pe:imphash`**) value **`9b821a35d20f9a8955f8d5e54b175675`**:



```
| file:bytes:mime:pe:imphash=9b821a35d20f9a8955f8d5e54b175675
| file:bytes:mime:pe:imphash=9b821a35d20f9a8955f8d5e54b175675
```

Question 7: How many files are returned when you run this query?

- There are **eleven** files with the same import hash value:



```
| file:bytes:mime:pe:imphash=9b821a35d20f9a8955f8d5e54b175675
```

Tabular

file:bytes (11)

file:bytes	:mime	me:pe:compiled	ime:pe:imphash	ime:pe
sha256:e6880…	application…	2009/03/17 …	9b821a35d20…	...
sha256:2c5dd…	application…	2008/10/22 …	9b821a35d20…	...
sha256:a3eb9…	application…	2009/03/17 …	9b821a35d20…	...
sha256:87f4f…	application…	2012/08/20 …	9b821a35d20…	...
sha256:1b32e…	application…	2009/06/08 …	9b821a35d20…	...
sha256:57b75…	application…	2009/02/17 …	9b821a35d20…	...
sha256:cdd8a…	application…	2009/02/17 …	9b821a35d20…	...
sha256:15ed7…	application…	2008/10/22 …	9b821a35d20…	...
sha256:d0013…	application…	2009/06/08 …	9b821a35d20…	...
sha256:289aa…	application…	2009/06/08 …	9b821a35d20…	...
sha256:65c4e…	application…	2009/06/08 …	9b821a35d20…	...