Vertex

Synapse Bootcamp - Module 11

Building Queries in Storm - Answer Key

© 2025 The Vertex Project, LLC

Answer Key

Storm Commands

Exercise 1 Answer

Objective:

- **Use common Storm commands to help answer analytical questions.**

Question 1: What Storm command can you add to the end of your query to find a file with the **earliest** compile (**`:mime:pe:compiled`**) time?

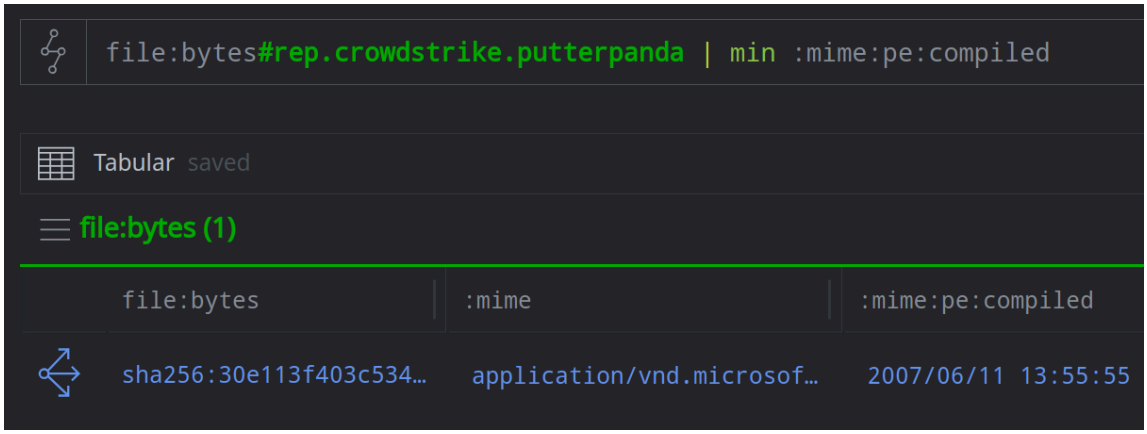
- You can find the earliest compile time with the following query:

```
file:bytes#rep.crowdstrike.putterpanda
  | min :mime:pe:compiled
```

  The **`min`** command returns a node with the lowest / smallest / earliest value for the specified property:

Question 2: What is the earliest compile date/time?

- The earliest compile time is **2007/06/11 13:55:55:**



Question 3: What Storm query / command can you use to determine the total number of indicators (without displaying the nodes)?

- You can determine the total number of Putter Panda indicators with the following query:

```
#rep.crowdstrike.putterpanda | count
```

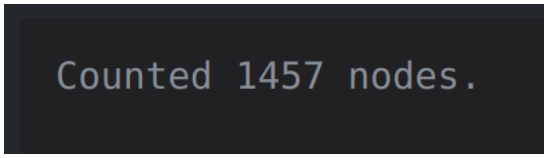
The `count` command tells Synapse to return the total **without** displaying the nodes by default.

The total is displayed in the **Console Tool.**

> **Tip:** You can optionally display both the total (in the Console Tool) **and** the nodes (in the Research Tool) with the `count --yield` command.

Question 4: How many indicators are there?

- There are **1457** indicators:



© 2025 The Vertex Project, LLC

Building a Storm Query

Exercise 2 Answer

Objective:

- **Understand how to build a Storm query step-by-step as you explore data and conduct analysis.**

Question 1: What kinds of nodes are connected to the article?

- The article is connected to various nodes, including:
  - Hashes (**`hash:sha256`**)
  - Email addresses (**`inet:email`**)
  - IPv4 addresses (**`inet:ipv4`**)
  - Servers (**`inet:server`**)
  - URLs (**`inet:url`**)
  - Files (**`file:bytes`**)
  - Software / malware names (**`it:prod:softname`**)
  - Organization / threat names (**`ou:name`**)
  - Threat groups (**`risk:threat`**)
  - Malware / tools (**`risk:tool:software`**)

Question 2: What Storm operation can you add to your original query to only view the **`inet:ipv4`** nodes?

- Add the following Storm operation to show the IPv4s referenced in the article:

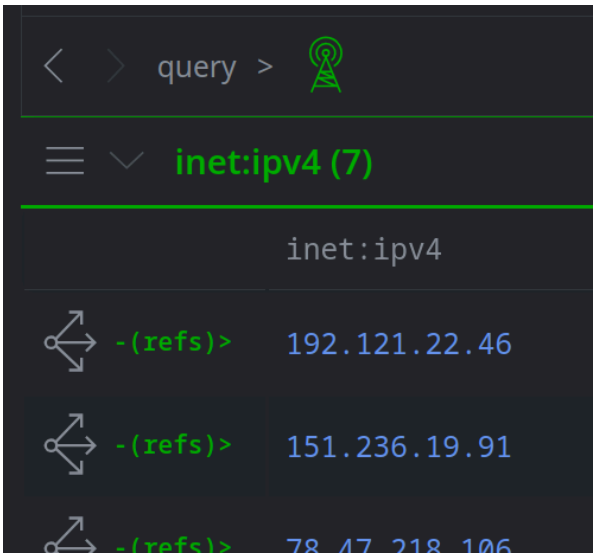
```
media:news:title^=crambus -(refs)> inet:ipv4
```

  You added an **edge traversal** operation to your Storm query.

© 2025 The Vertex Project, LLC

Tip: when you use the **Explore** button, the **link column** appears. The value in the link column shows how you arrived at these target nodes from your source nodes.

In this case, the link column shows the **inet:ipv4** nodes are linked to the **media:news** node by a **-(refs)>** edge:

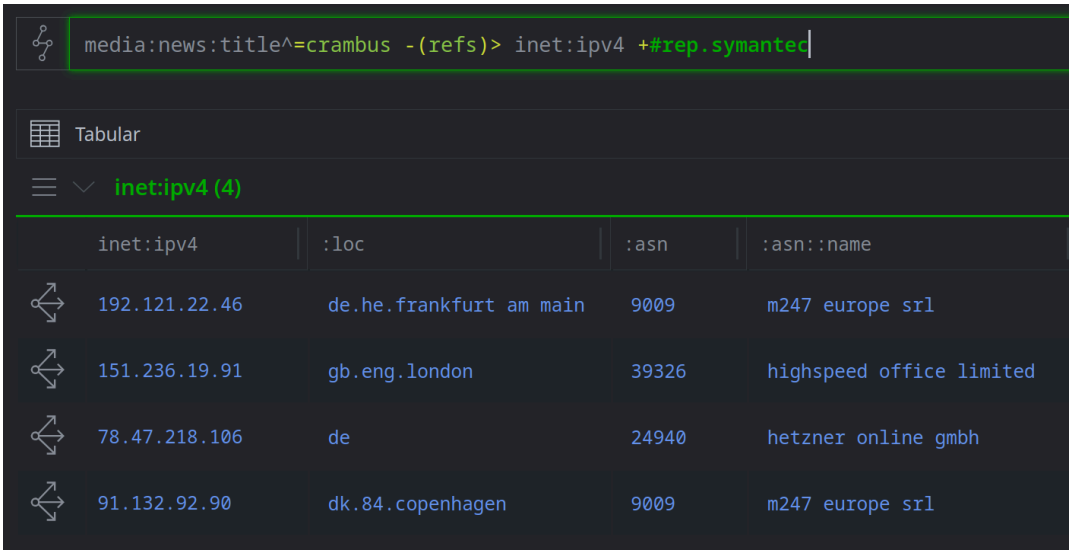


Question 3: What Storm operation can you add to this query to **only** view the IOCs reported by Symantec (**rep.symantec**)?

- Add the following Storm operation to only show the IOCs:

```
media:news:title^=crambus -(refs)> inet:ipv4 +#rep.symantec
```

© 2025 The Vertex Project, LLC



You added a **filter** operation to your Storm query.

Question 4: What Storm operation can you add to your query to **pivot** to the **`inet:server`** nodes?

- Add the following Storm operation to pivot to the **`inet:server`** nodes:

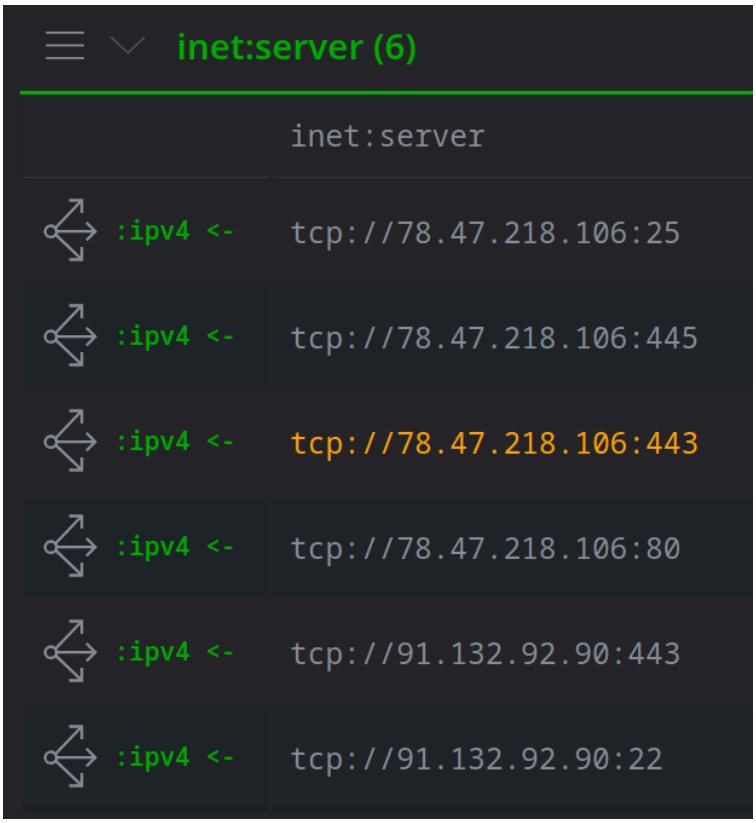
```
media:news:title^=crambus -(refs)> inet:ipv4 +#rep.symantec
  -> inet:server
```

© 2025 The Vertex Project, LLC

You added a **pivot** operation to your Storm query.

© 2025 The Vertex Project, LLC

Once again the **link column** showed how the target (**`inet:server`**) nodes are linked to the source nodes (**`inet:ipv4`**) nodes:



In this case, the pivot "arrow" symbol shows the nodes are linked by a property **pivot** (vs. an edge **traversal**). The "arrow" points to the left because the **`inet:server:ipv4`** property "points to" the **`inet:ipv4`** nodes we Explored from.

Note that regardless of the "direction" of the arrow in the link column, we use a "right pointing" arrow in our Storm query because all Storm pivots navigate from "left to right".

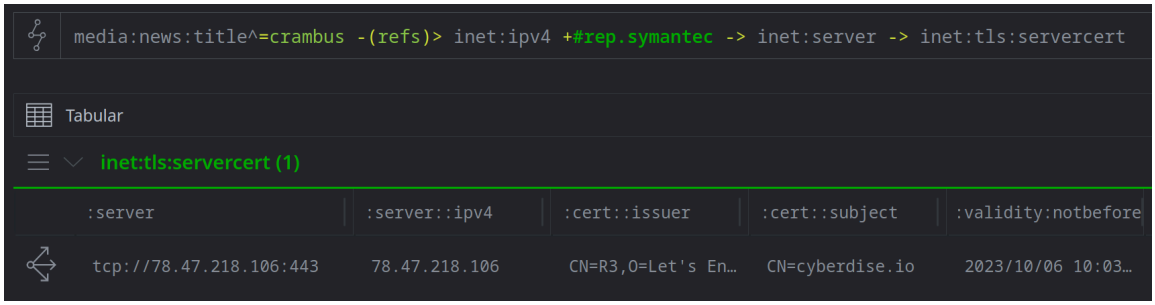
(The only exception is the left-pointing "wildcard pivot in" where the target **must** be the wildcard (*) symbol.)

Question 5: What Storm operation can you add to your query to **pivot** to the **`inet:tls:servercert`** node?

© 2025 The Vertex Project, LLC

- Add the following Storm operation to pivot to the **inet:tls:servercert** node:

```
media:news:title^=crambus -(refs)> inet:ipv4 +#rep.symantec
  -> inet:server -> inet:tls:servercert
```



You added another **pivot** operation to your query.

Working with Bookmarks

Exercise 3 Answer

Objective:
- **Save a useful query as a bookmark.**
- **Add the bookmark to your Favorites for easy access.**

Question 1: How many files did your query find?

- The query identified **179** files.

> **Note:** This answer is based on the baseline Synapse demo instance. Your answer may vary depending on the data that has been added to your demo instance so far in this course.

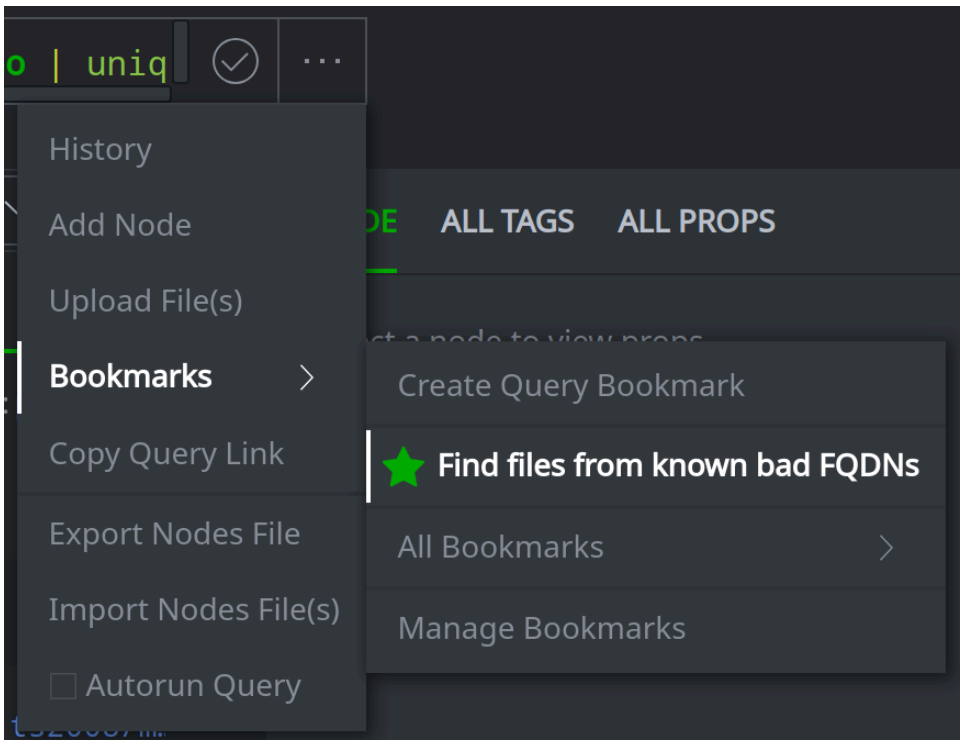
Some of the files have **rep** tags (from companies like Trend Micro or VirusTotal). But they do not have **cno** tags, which means they have not been reviewed or tagged internally by Vertex. We may want to do things like:
- Confirm the files are malicious and tag them **cno.mal**
- Associate the files with various malware families (**cno.mal.***)

© 2025 The Vertex Project, LLC

- Attribute the files to various threat clusters (**cno.threat.***)

Question 2: Where is your bookmarked query located now?

- When you add the bookmarked query to your Favorites, it is accessible directly from the **Bookmarks** menu:



For reference, the following table breaks down the Bookmarked Storm query step-by-step:

Query Element	Operation
`inet:fqdn#rep`	**Lift** all malicious FQDNs reported by third-parties (tagged `rep`)
`inet:fqdn#cno`	**Lift** all malicious FQDNs tracked internally by Vertex (tagged `cno`)
`| uniq`	**Deduplicate** the results
`| :zone -> inet:fqdn:zone`	**Pivot** to any / all subdomains of those FQDNs

© 2025 The Vertex Project, LLC

Query Element	Operation
	• includes the original FQDNs themselves • includes any untagged subdomains
`| uniq`	**Deduplicate** the results
`| -> inet:dns:request`	**Pivot** to any DNS requests for those FQDNs
`-> file:bytes`	**Pivot** to any files associated with those DNS queries
`-#cno`	**Filter** out files that are already tracked by Vertex
`| uniq`	**Deduplicate** the results

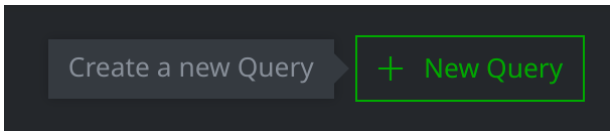
Working with Storm Editor

Exercise 4 Answer

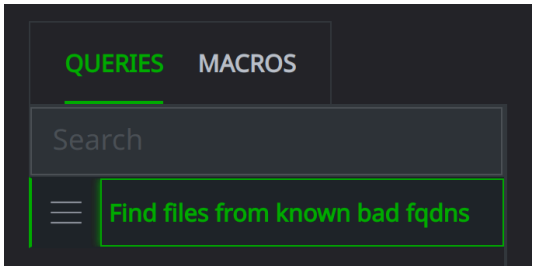
Objective:
- **Use Storm Editor to write and test a Storm query.**
- **Add comments to the query.**

For this exercise, examine the features of the Storm Editor Tool and its ability to compose, test, save, and run Storm queries.

- The **+ New Query** button allows you to create a new query:



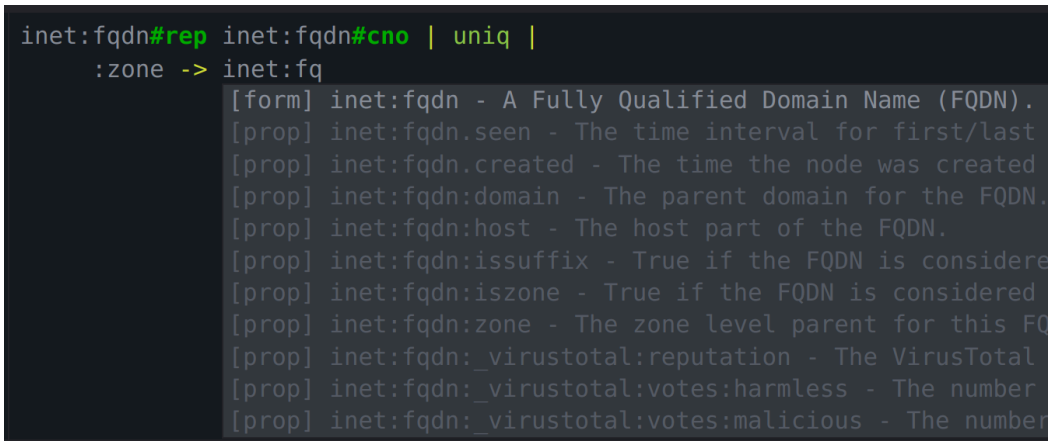
- You must specify a name for the query:



  Once the name is saved, it cannot be changed.

  Note: if you need to rename a query, use the query's **hamburger menu** to **Make a copy** and give the copy a name you like. You can then **Delete** the original query.

- **As you type,** Synapse will generate **auto-complete suggestions** wherever it is able to identify them:

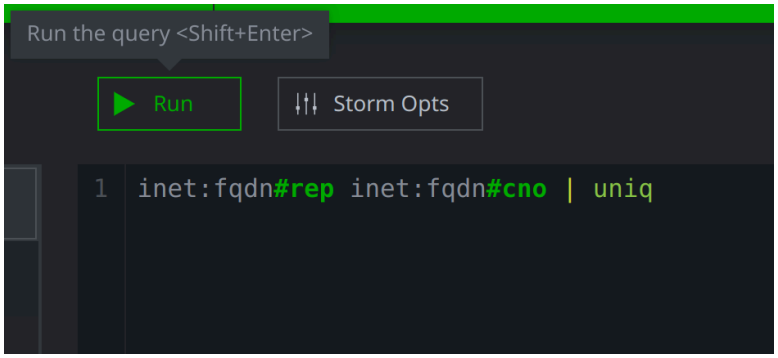


  Auto-complete will attempt to match:
  - Form names
  - Property names
  - Tag names
  - Storm commands
  - Storm library names
  - Variable names
  - Macro names

  Auto-complete suggestions will get more specific as you type.

© 2025 The Vertex Project, LLC

- The **Run** button will execute your query in its current state (as will pressing the **Shift-Enter** key combination):



This makes it easy to test your query. Synapse will let you know of any problems (such as a syntax error). If the query runs, Synapse will display any results in the console window underneath the Storm Editor window.

> **NOTE:** Your query runs **for real.** if your query simply lifts data and returns nodes, that is not a problem. But **use caution** with any queries that make changes! We strongly recommend that you test queries in a **forked view** before deciding they are ready for production.

- You can add comments throughout the query:

```
1  /*
2  First we'll lift the FQDNs tagged with #rep and #cno, and remove
3  duplicates
4  */
5  inet:fqdn#rep inet:fqdn#cno | uniq |
6  /*
7  Then we'll pivot to lift any related FQDNS, again removing duplicates
8  */
9       :zone -> inet:fqdn:zone | uniq |
10 /*
11 Then we'll pivot to DNS requests
12 */
13     -> inet:dns:request
14 /*
15 This is a lot of commenting. I think I need a snack.
16 */
17     -> file:bytes -#cno | uniq
18
```

© 2025 The Vertex Project, LLC