Vertex

Synapse Bootcamp - Module 18

Reports, Articles, and the Spotlight Tool - Exercises

Objectives

In these exercises you will learn:

- How to use the Spotlight Tool to load, parse, model, and tag a report

> **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.

Using Spotlight to Model Reports

Exercise 1

Objective:
- **Use Synapse Spotlight to load, parse, add, and tag data related to a public report.**

For this exercise, we will use the following blog from Fortinet:

"Guard Your Drive from DriveGuard: Moses Staff Campaigns Against Israeli Organizations Span Several Months"

```
https://www.fortinet.com/blog/threat-research/guard-your-drive-from-driveguard
```

The blog describes activity by a threat group Fortinet calls **Moses Staff.**

To get started:

- **Open** the blog link in your web browser.

Part 1 - Load the Report

- In the **Spotlight Tool,** click the **+ New Document** button.

- In the **New Document** dialog, enter the following in the *Name* field:
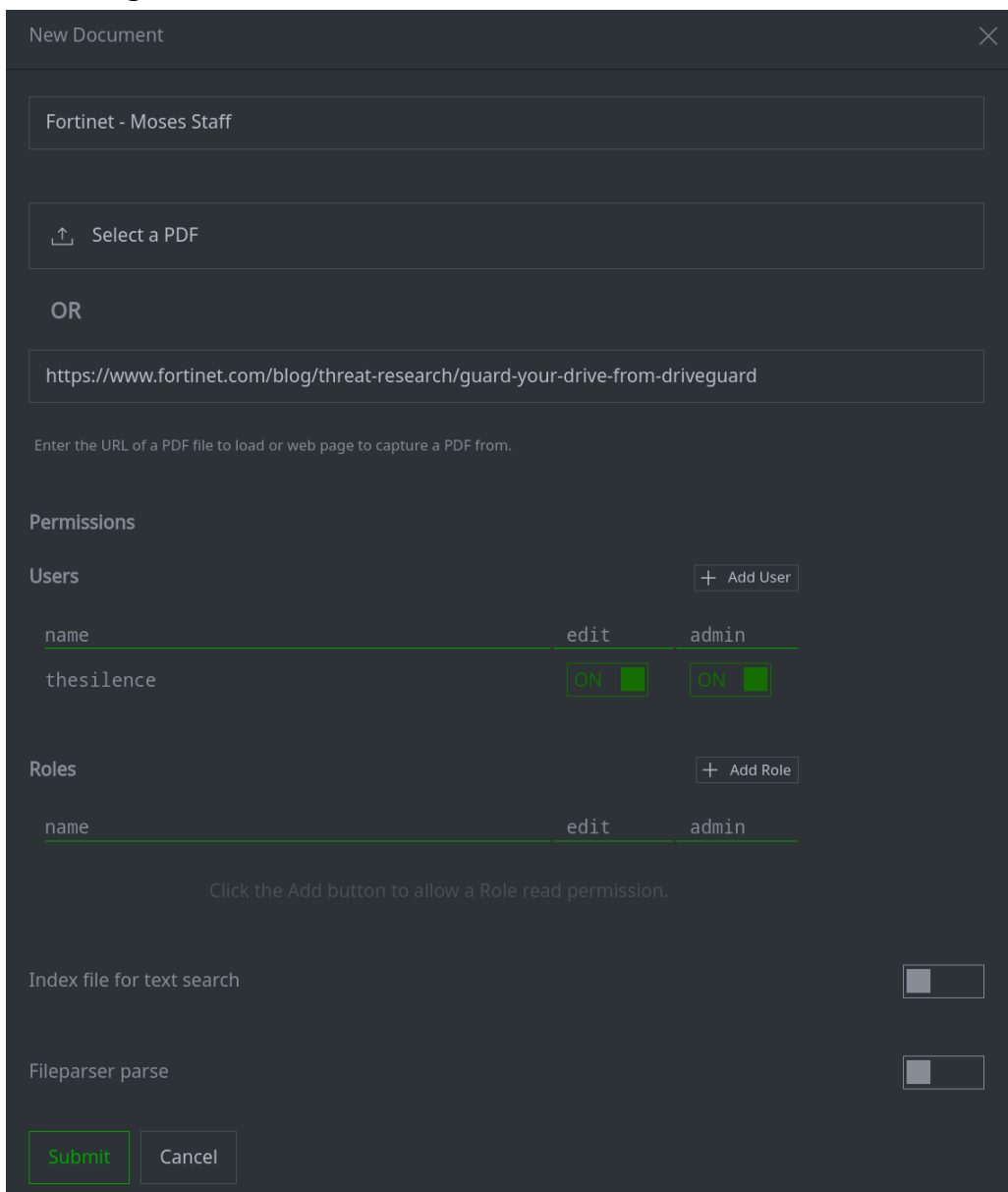
  Fortinet - Moses Staff

- Enter the following in the *URL* field:

https://www.fortinet.com/blog/threat-research/guard-your-drive-from-driveguard

- Set the toggles for **Index file for text search** and **Fileparser parse** to **OFF:**

Index file for text search

Fileparser parse

- The dialog should look similar to this. Click the **Submit** button to continue:

New Document ✕

Fortinet - Moses Staff

⬆ Select a PDF

OR

https://www.fortinet.com/blog/threat-research/guard-your-drive-from-driveguard

Enter the URL of a PDF file to load or web page to capture a PDF from.

Permissions

Users   + Add User

name	edit	admin
thesilence	ON	ON

Roles   + Add Role
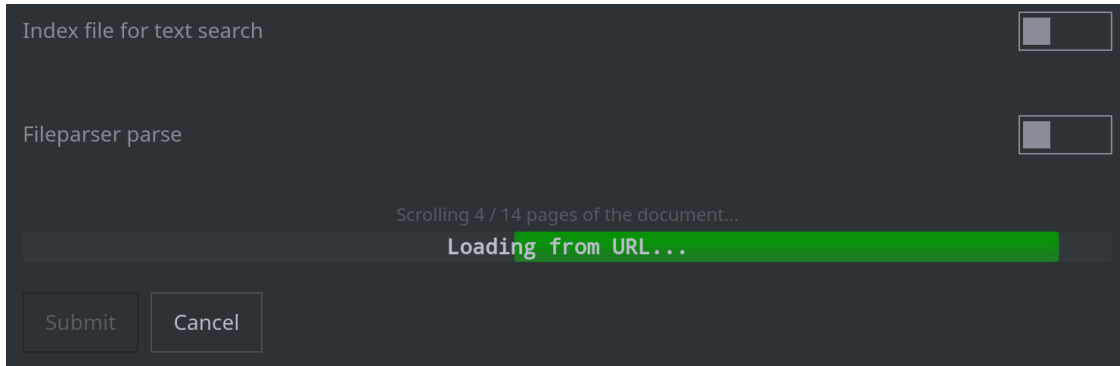
name	edit	admin

Click the Add button to allow a Role read permission.

Index file for text search

Fileparser parse

Submit   Cancel
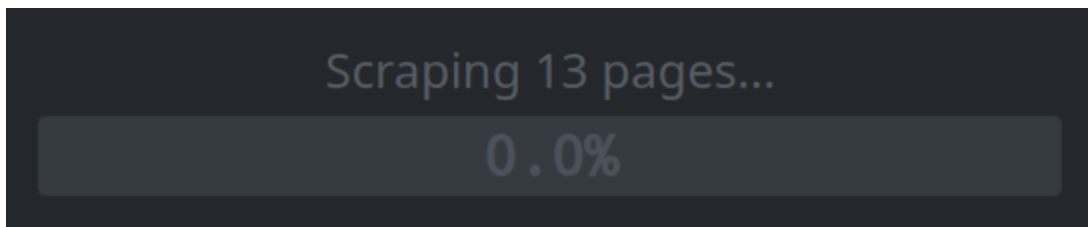
- You will see two progress bars while Spotlight loads the document.

  The first shows Spotlight downloading the content from the URL and generating a PDF:

  The second shows Spotlight "scraping" (parsing) the PDF for indicators Synapse can recognize:

> **Note:** this process may take several seconds to complete, depending on the size and format of the HTML document.
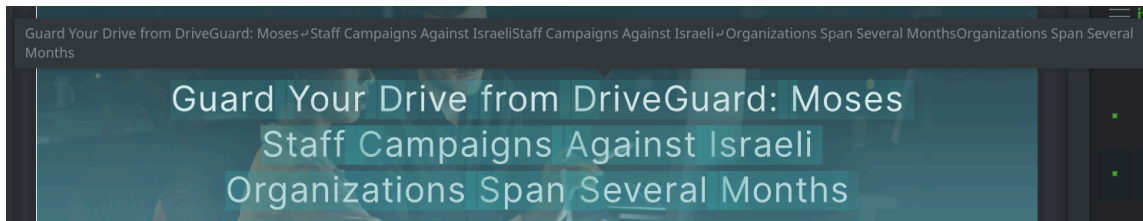
Question 1: What does Spotlight display after loading the PDF?

Question 2: What kinds of indicators (forms) did Spotlight recognize, based on its initial parsing of the PDF?

Part 2 - Set Document (media:news node) Properties

- In the **Spotlight Tool,** in the document window, use your mouse to highlight the text of the article's title:
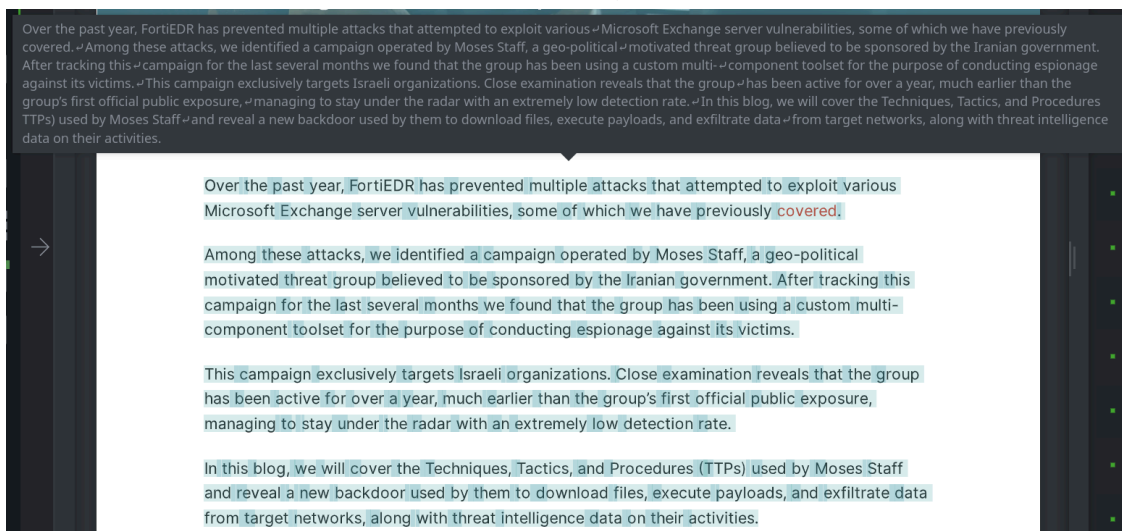
> **Tip:** Synapse will display a tooltip containing the highlighted text.

- **Right-click** the highlighted text and select **document details > set media:news:title:**
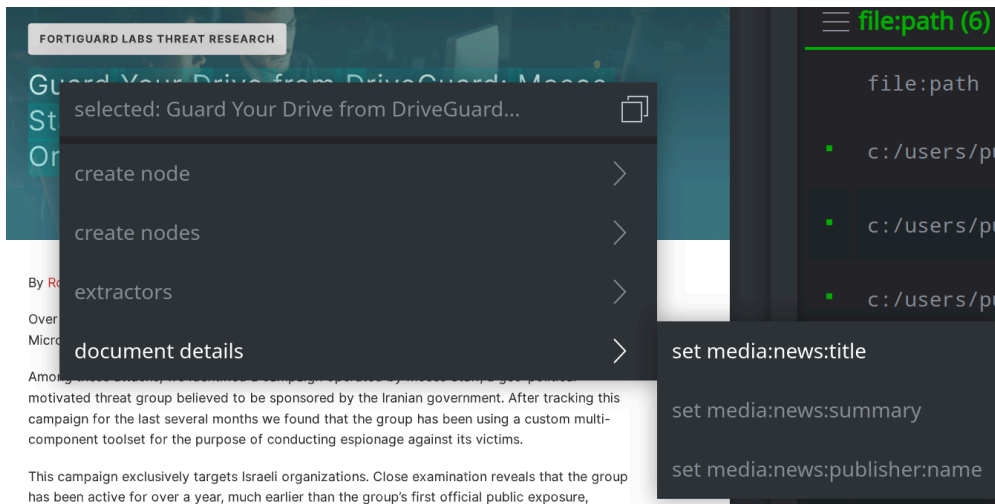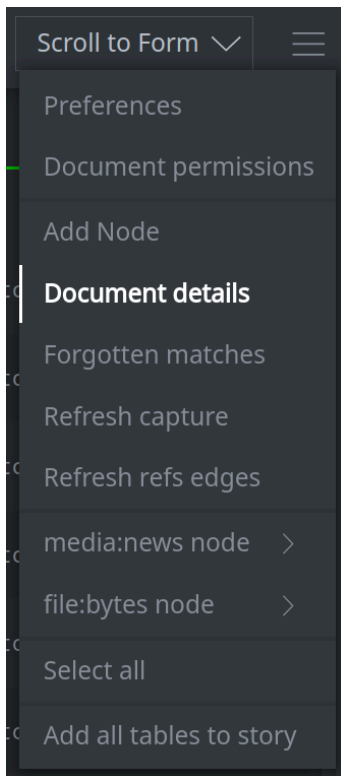

- In the document window, use your mouse to highlight the first four paragraphs of the article (from below the author's name to just above "Affected Platforms"):

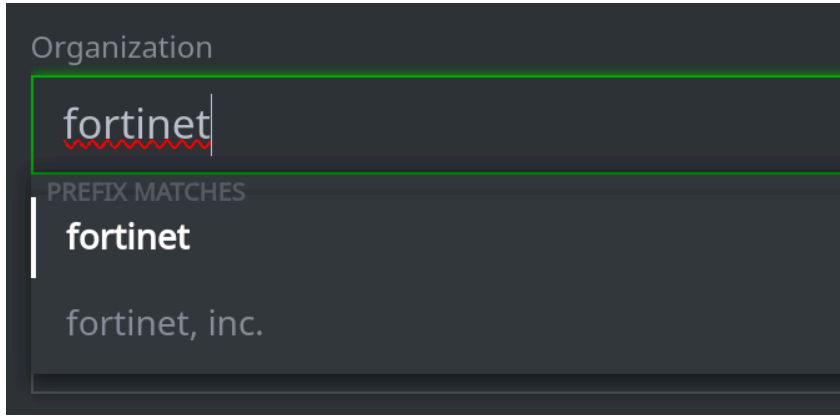- **Right-click** the highlighted text and select **document details > set media:news:summary:**
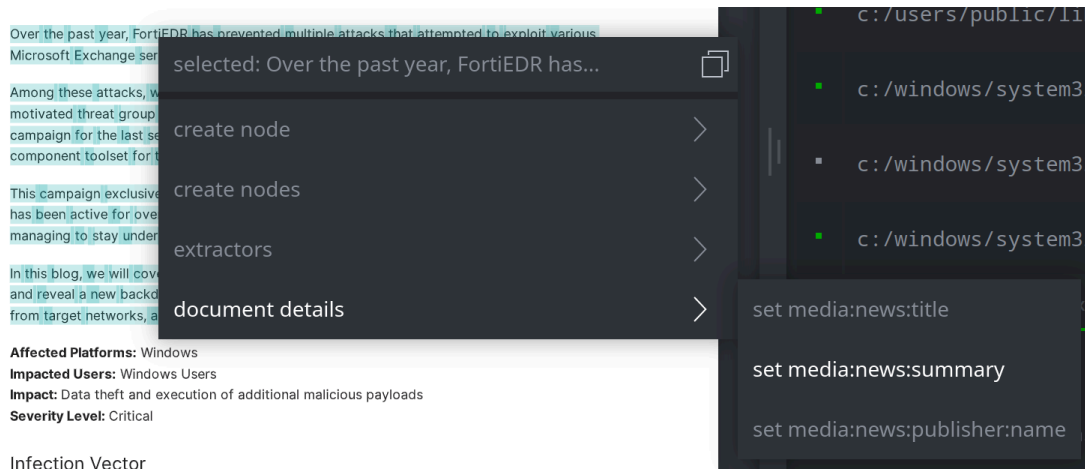
- In the **Spotlight Tool,** click the **main hamburger menu** (next to the **Scroll to Form** button) and select **document details:**

Question 3: What document (media:news) properties are already set?

You want to add more information in the **Edit Document media:news node** dialog.

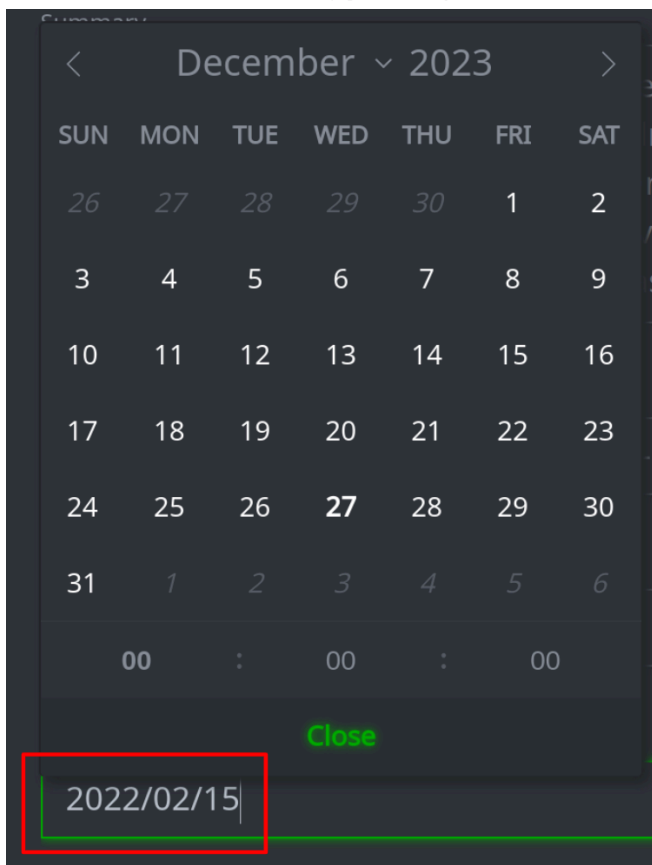- In the **Organization** field, enter the name **fortinet**:

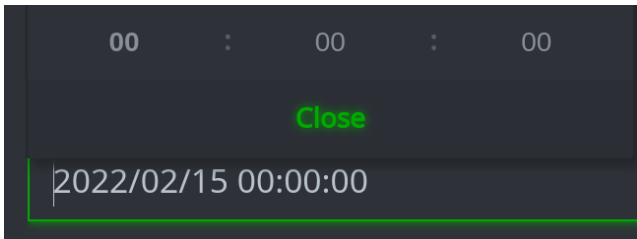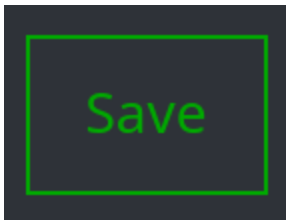- In the **Published** field, **type** the publication date of the blog (**2022/02/15**):

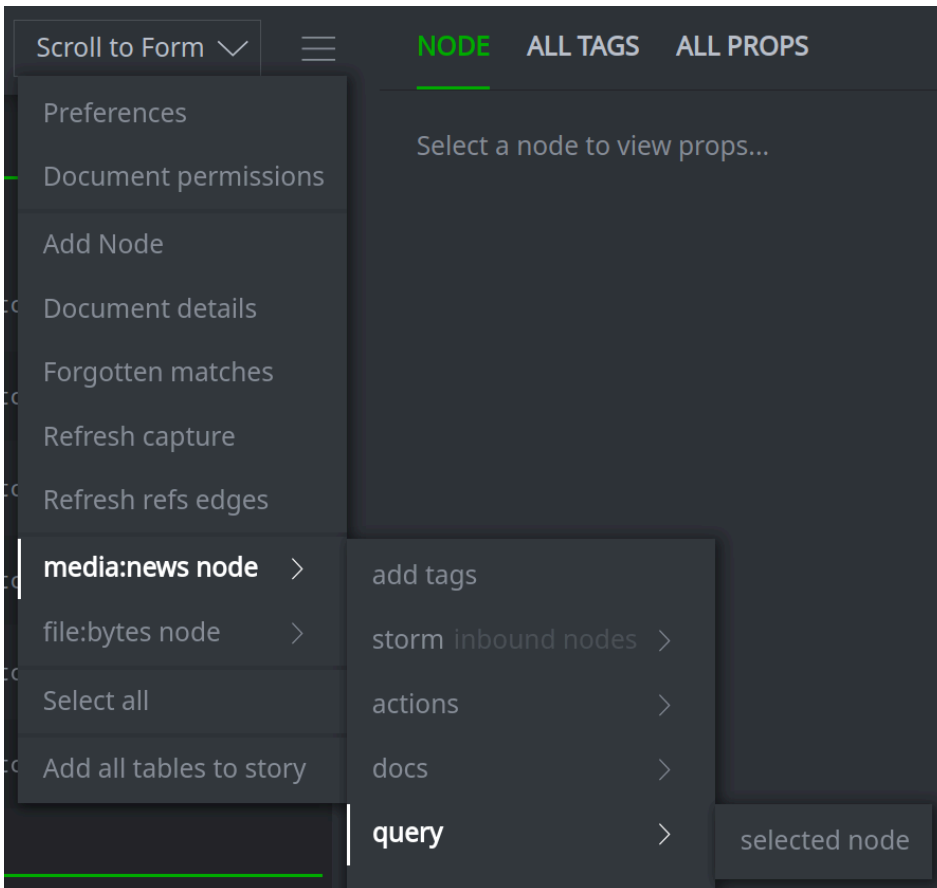(You can also use the **Date Picker** to select the date.)

- Click **Close** to close the Date Picker:

- Click the **Save** button when finished:

- Click the **main hamburger menu** and select the **media:news node > query > selected node** option:

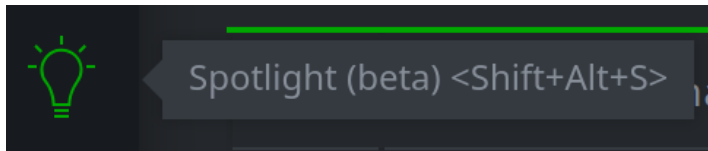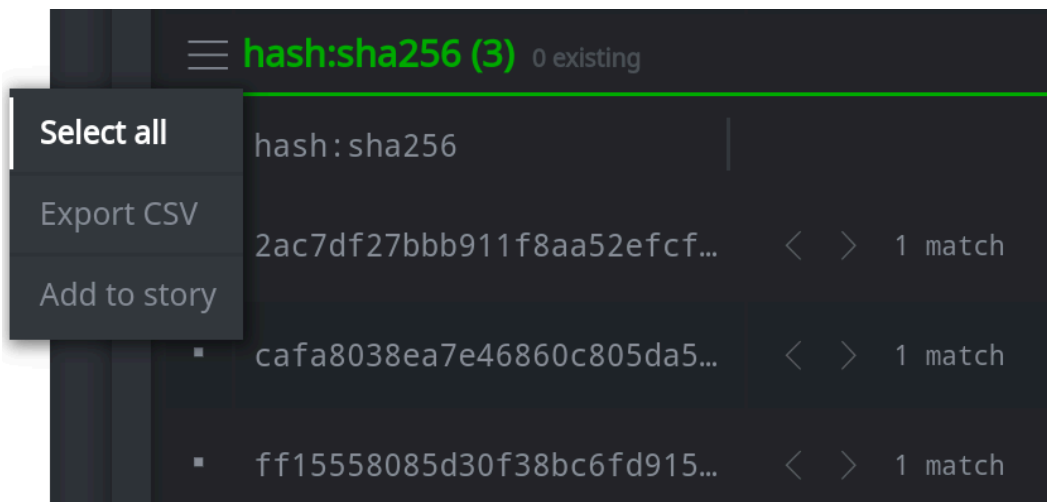- **Select** the `media:news` node and view its properties.

Part 3 - Create and Tag Indicators

We want to add and tag any common indicators before reviewing other data in more detail.

- Return to the **Spotlight Tool:**

- In the **Spotlight Results,** click the **hamburger menu** next to the **hash:sha256** header and choose **Select all**:

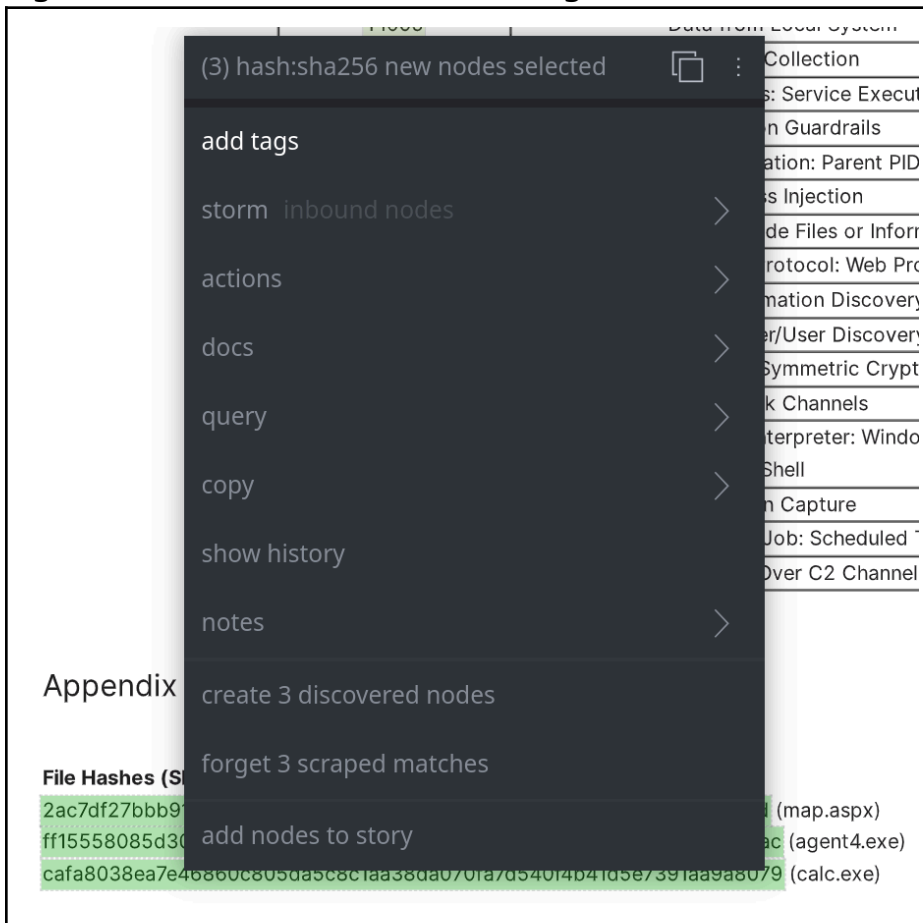- Spotlight shows you the hashes in the document:

Appendix B: IOCs

File Hashes (SHA256)
2ac7df27bbb911f8aa52efcf67c5dc0e869fcd31ff79e86b6bd72063992ea8ad (map.aspx)
ff15558085d30f38bc6fd915ab3386b59ee5bb655cbccbeb75d021fdd1fde3ac (agent4.exe)
cafa8038ea7e46860c805da5c8c1aa38da070fa7d540f4b41d5e7391aa9a8079 (calc.exe)

We want to create the hashes and tag them to show Fortinet associates them with Moses Staff. Tagging the nodes will also create them.

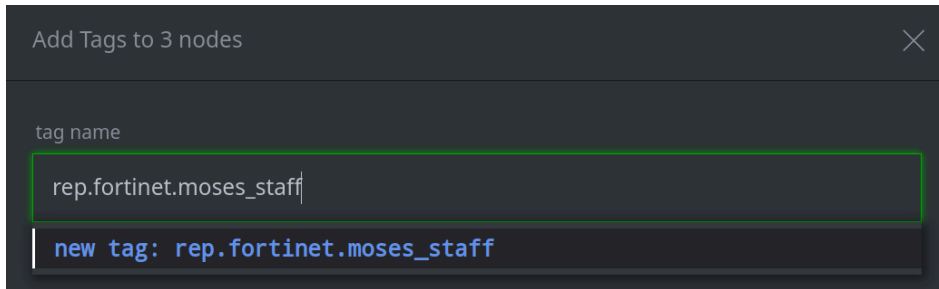- **Right-click** the hashes and select **add tags:**

- In the **Add Tags** dialog, enter the new tag **rep.fortinet.moses_staff:**
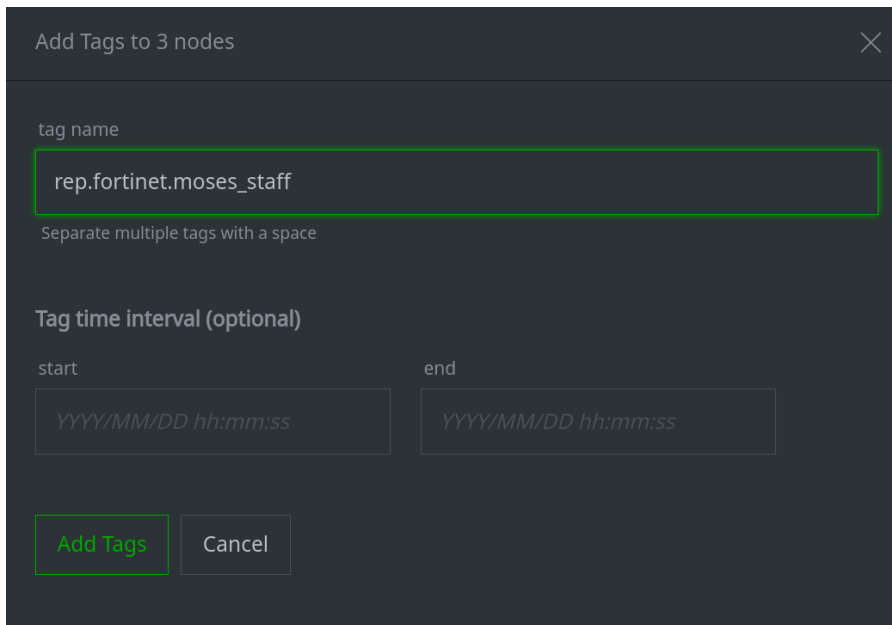
Add Tags to 3 nodes ✕

tag name

rep.fortinet.moses_staff

new tag: rep.fortinet.moses_staff

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

Add Tags to 3 nodes ✕

tag name

rep.fortinet.moses_staff

Separate multiple tags with a space

Tag time interval (optional)

start

YYYY/MM/DD hh:mm:ss

end

YYYY/MM/DD hh:mm:ss

Add Tags   Cancel

Question 4: What happened to the hashes?

We want to add the rest of the indicators from Fortinet's IOC list.

- In the document use **Shift-click and drag** to draw a box around the IP address, Domains, and URLs:

Domains
techzenspace[.]com

URLs
hxxp://87.120.8.210:80/RVP/index3.php
hxxp://techzenspace.com:80/RVP/index8.php
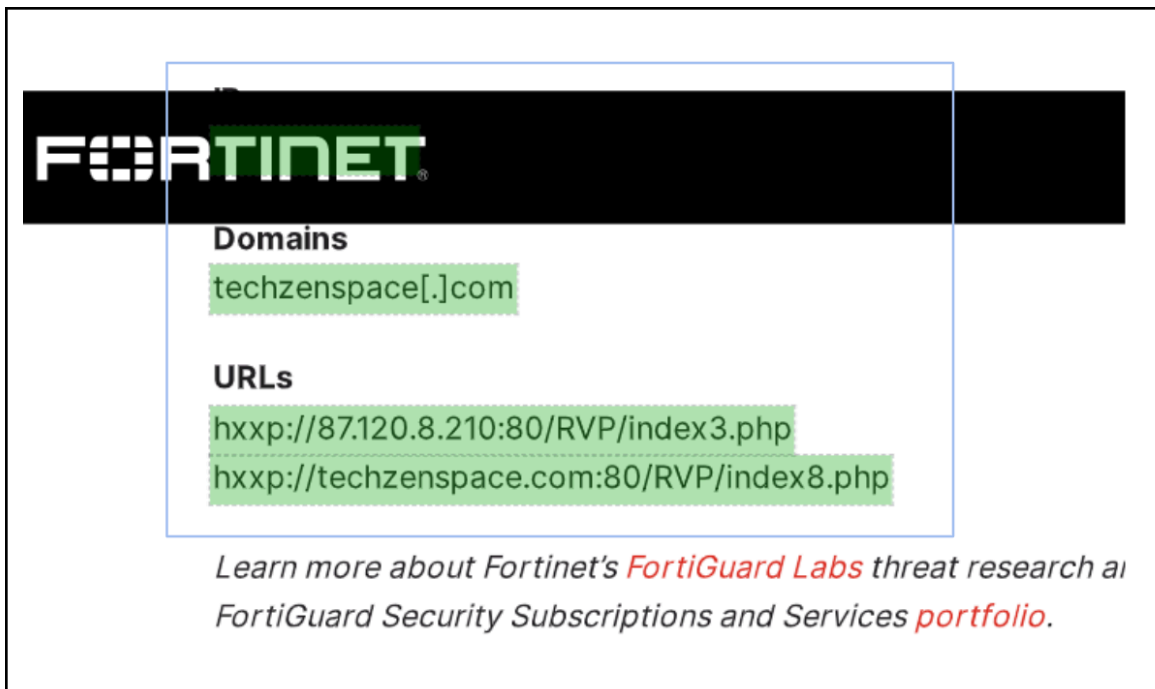
Learn more about Fortinet's *FortiGuard Labs* threat research ar
FortiGuard Security Subscriptions and Services *portfolio.*

You can also use **ctrl-click** to multi-select the indicators.

Note: Depending on how Spotlight captured Fortinet's website, a banner may cover some of the IOCs. In the image above, the IPv4 address is "behind" the banner but still recognized by Spotlight.

- Note that Spotlight also **selects** the four nodes in the Results:

inet:fqdn (1) 0 existing

| inet:fqdn | |
| techzenspace.com | < > 3 matches |

inet:ipv4 (1) 0 existing

| inet:ipv4 | |
| 87.120.8.210 | < > 2 matches |

inet:server (1) 0 existing

| inet:server | |
| tcp://87.120.8.210:80 | < > 1 match |

inet:url (2) 0 existing

inet:url	
http://87.120.8.210:80/R…	< > 1 match
http://techzenspace.com:…	< > 1 match

- **Right-click** any of the selected nodes and choose **add tags:**
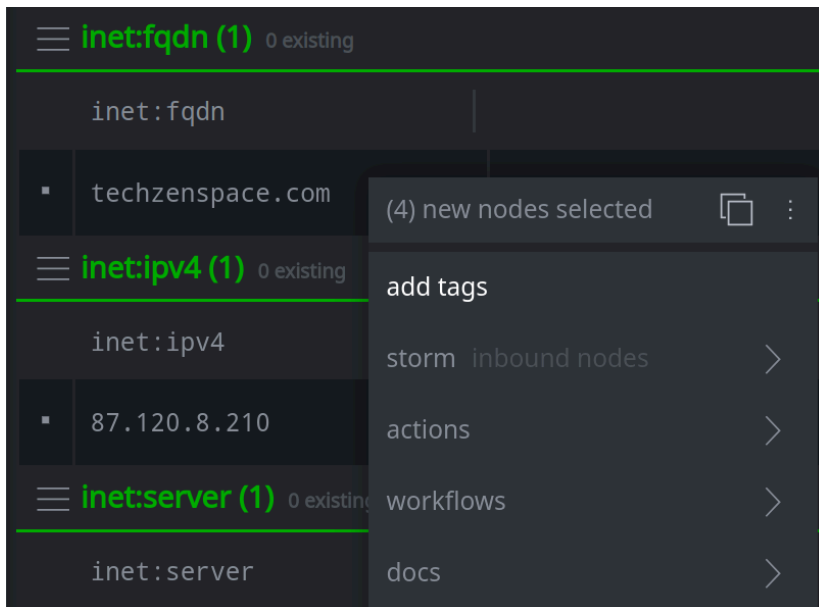
- Use the **Add Tags** dialog to add the tag **rep.fortinet.moses_staff**:
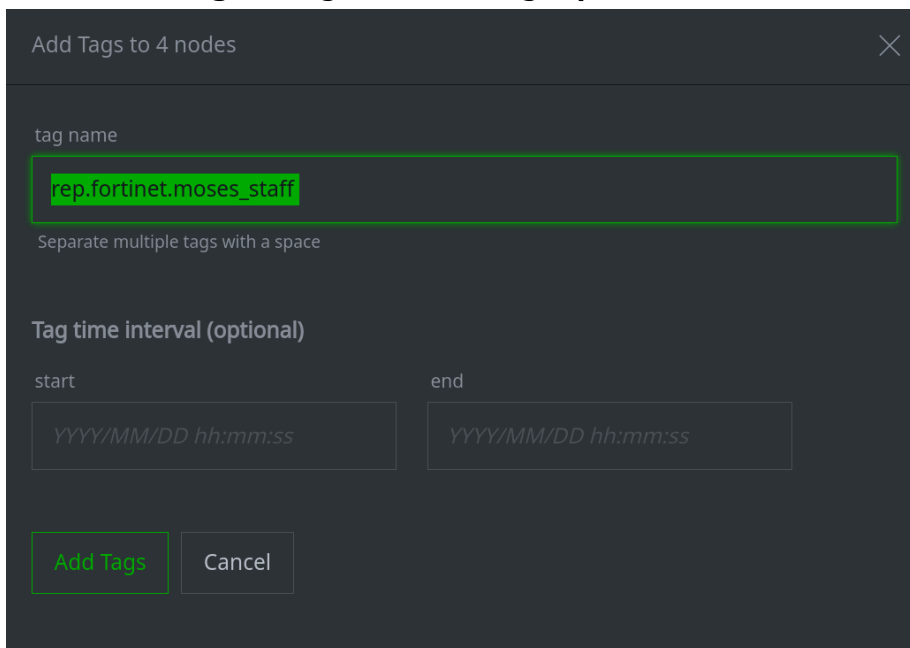
Part 4 - Highlight and Add Nodes with Quick Forms

The IOCs include a list of file names. Spotlight cannot recognize ("scrape") file names, so we need to create them manually.

Spotlight can recognize 'lists' of forms, so we can create all the file names (`file:base` nodes) at once.

- In the document, **click and drag** to highlight the file names:

- **Right-click** the highlighted text and select **create nodes > file:base**:
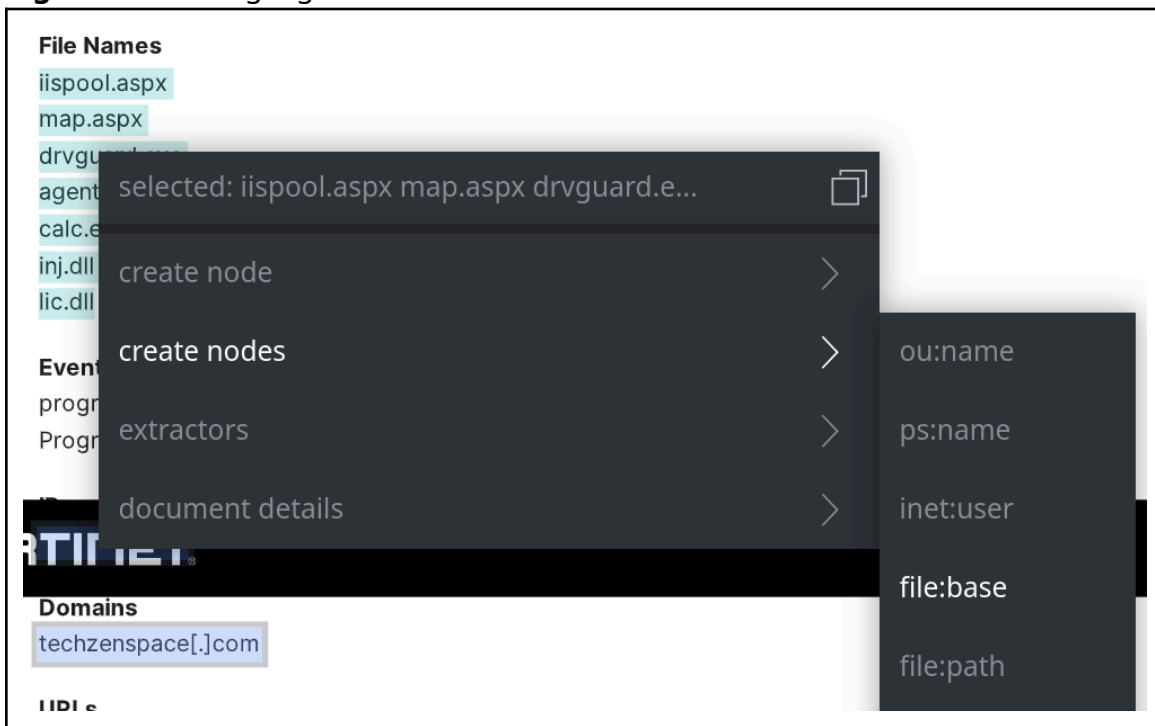
Question 5: What happened? Did Spotlight create the `file:base` nodes?

- In the **Create Nodes** dialog, review the suggested nodes. Click **Submit** to create the nodes:
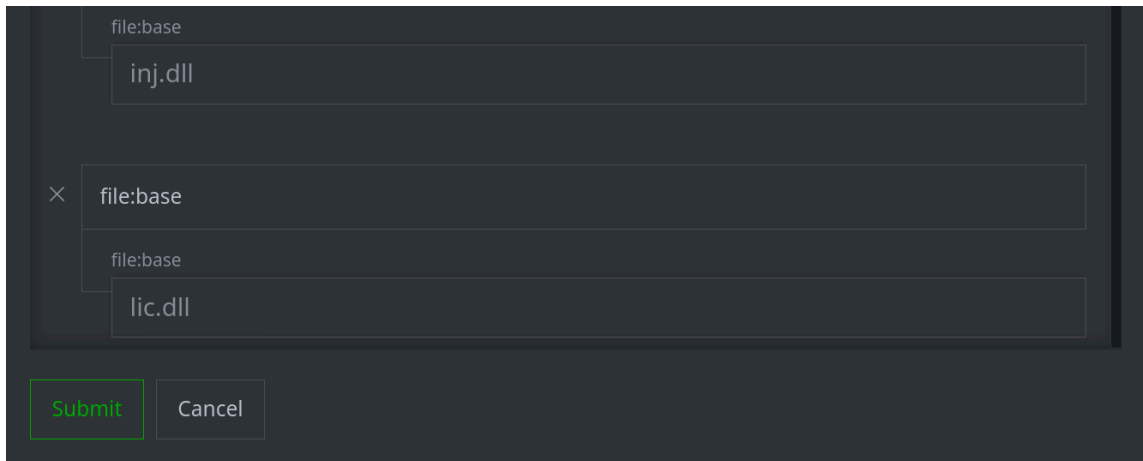
- Spotlight created and selected the seven `file:base` nodes:

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

- Use the **Add Tags** dialog to add the tag **rep.fortinet.moses_staff**:

Part 5 - Review Suggested Nodes

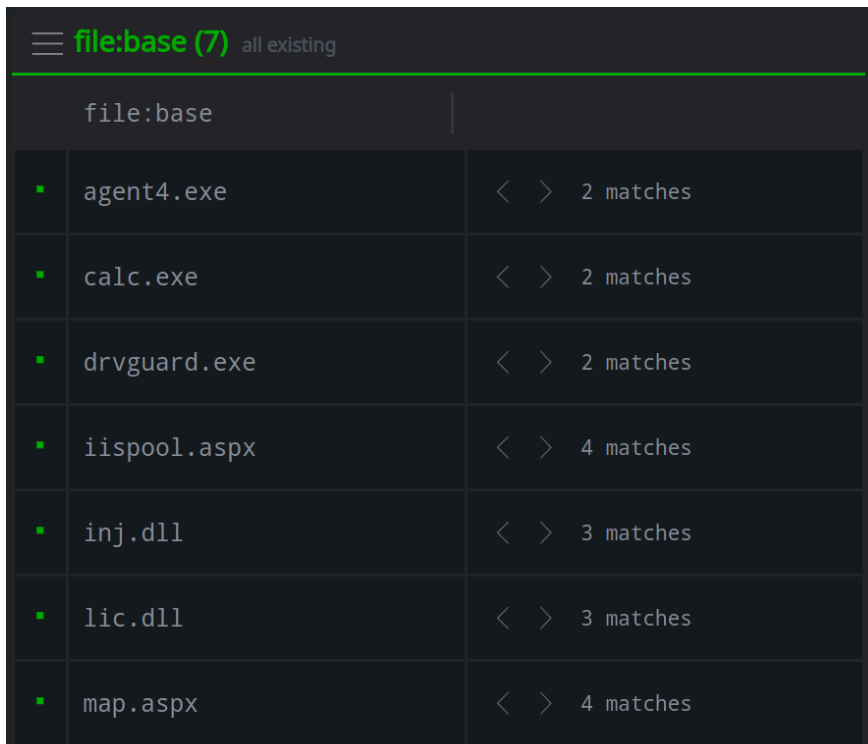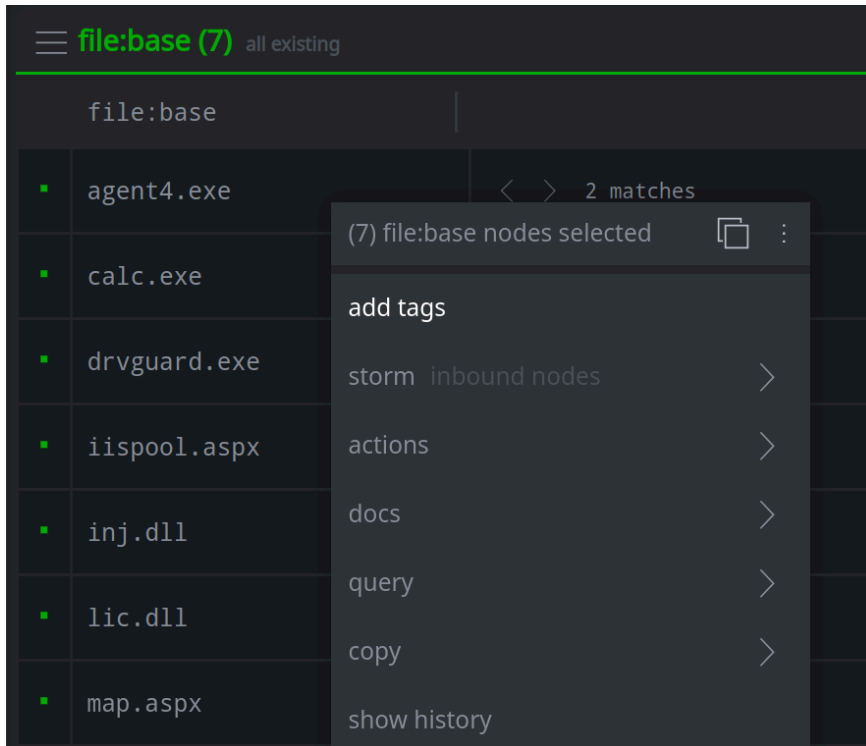You want to review additional nodes that Spotlight scraped and suggested.

- In the Spotlight **Results**, click the **Filter** button and select **new (7)** to only display new (suggested) nodes:

Filter (all) ⌄	Scroll to Form ⌄
all (41)	
existing (34)	
new (7)	Display only new nodes
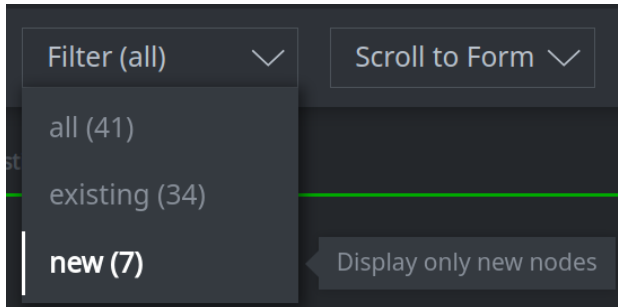
The numbers on your menu may vary slightly depending on the data in your demo instance.

- In the Spotlight **Results,** locate the `file:path` nodes:

file:path (6) 0 existing

file:path		
c:/users/public/libraries/async.dat will be …	‹ ›	1 match
c:/users/public/libraries/cfg.dat. the encry…	‹ ›	1 match
c:/users/public/libraries/tmp.bin before	‹ ›	1 match
c:/windows/system32/broker.exe	‹ ›	1 match
c:/windows/system32/drvguard.exe. when execu…	‹ ›	1 match
c:/windows/system32/rsc.dat and restoring it…	‹ ›	1 match
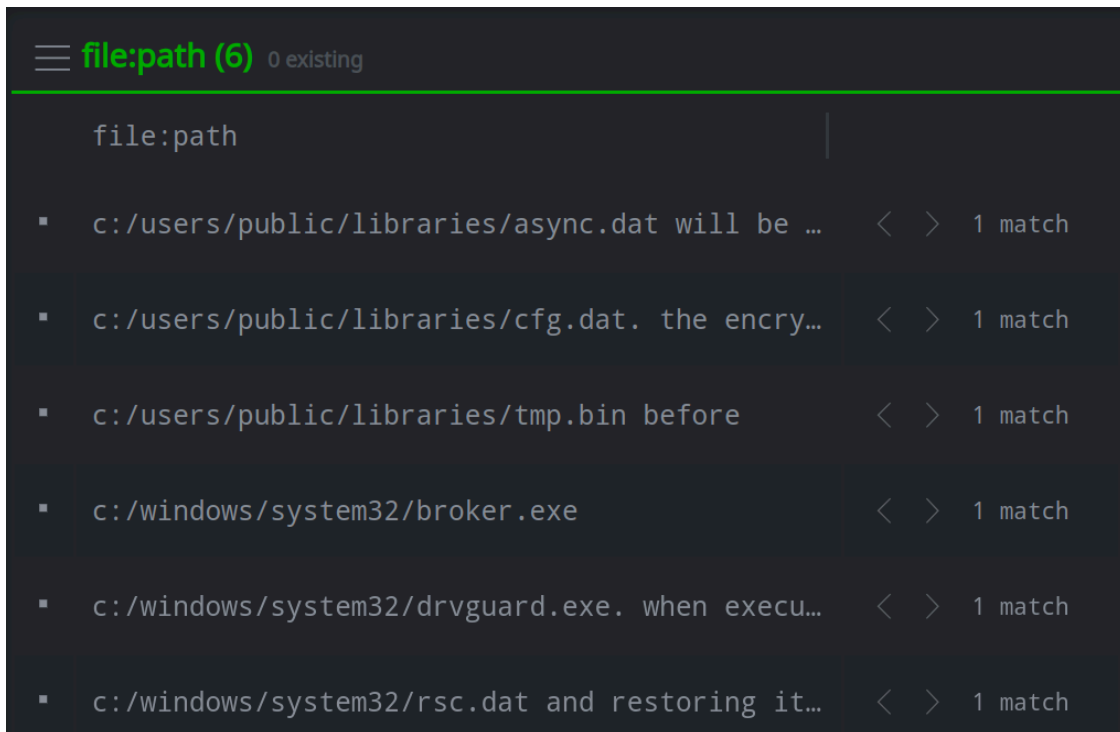
Note that only **one** suggested node is a valid file path.

- **Select** the node for the file path **c:/windows/system32/broker.exe:**

```
▪   c:/users/public/libraries/cfg.dat. the encrypt…     <

▪   c:/users/public/libraries/tmp.bin before           <

▪   c:/windows/system32/broker.exe                      <

▪   c:/windows/system32/drvguard.exe. when execute…     <
```
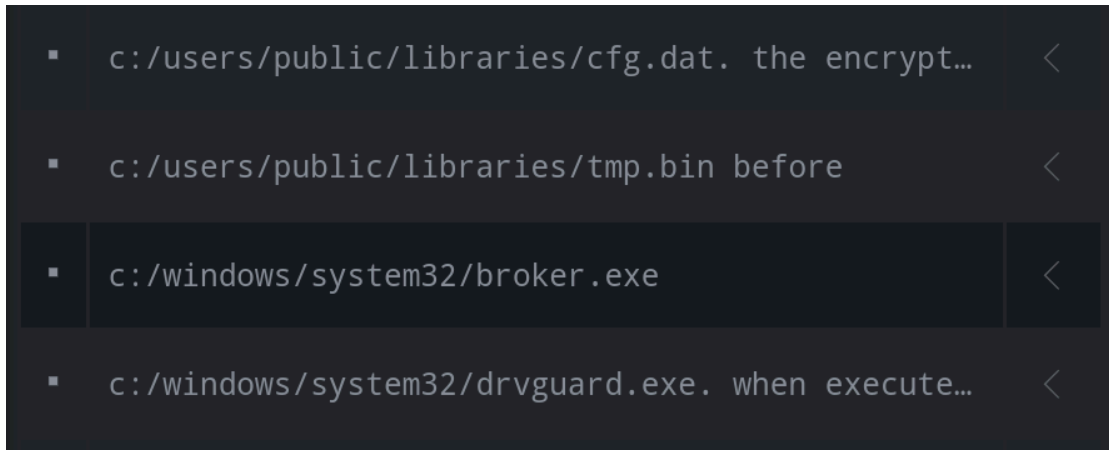
Note that Spotlight takes you to the location of this path within the document:

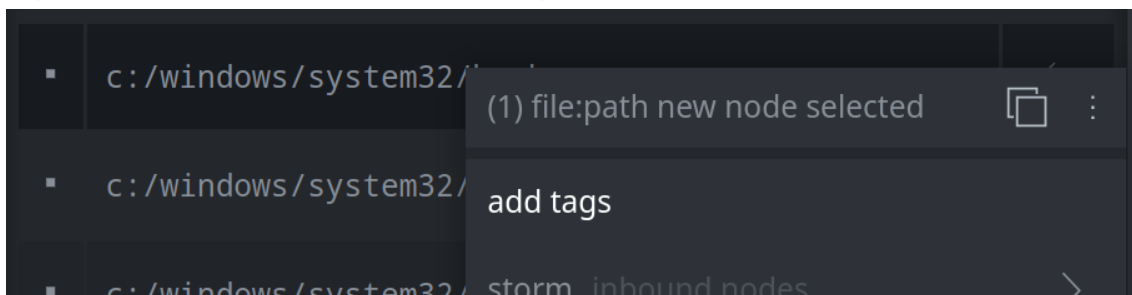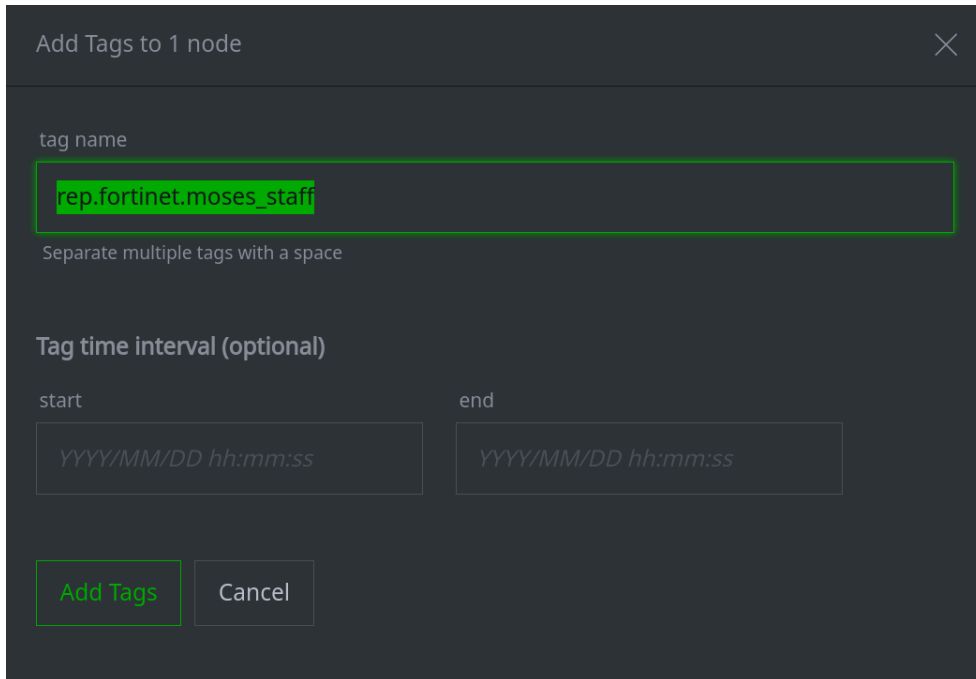> If the backdoor does not exist on the disk, the loader creates it by reading the content of
> C:\Windows\System32\rsc.dat and restoring its DOS header magic value to 4D 5A 90. The valid executable is
> written to disk at C:\Windows\System32\broker.exe

The path is the location of a backdoor used by Moses Staff. We want to add the node to Synapse and tag it.

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

```
▪   c:/windows/system32/
                              (1) file:path new node selected    ⧉   ⋮

▪   c:/windows/system32/
                              add tags

▪   c:/windows/system32/      storm  inbound nodes               >
```

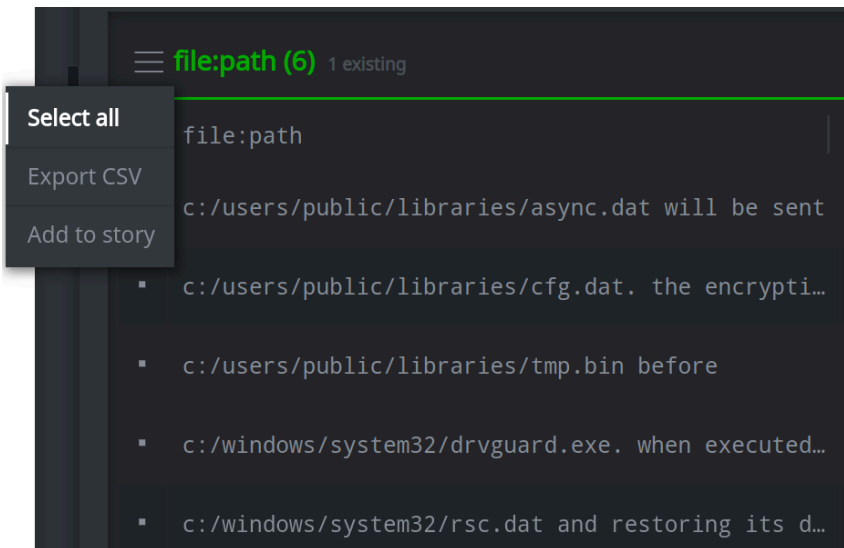- Use the **Add Tags** dialog to apply the tag **rep.fortinet.moses_staff:**

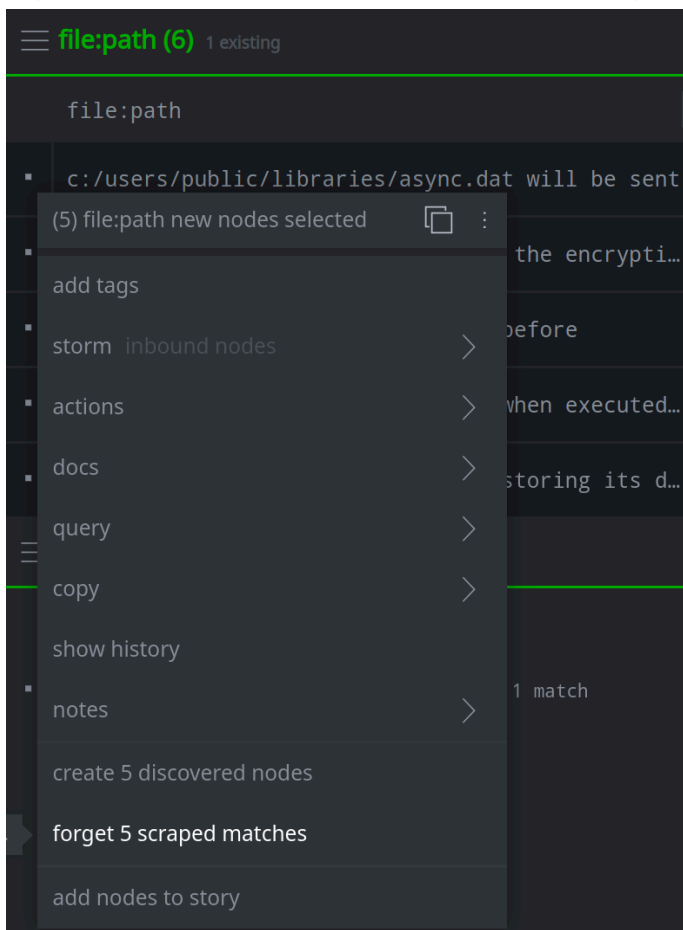**Question 6:** What happens when you tag and create the node?

We want to "forget" the rest of the `file:path` nodes. Spotlight included extra text that is not part of the path.
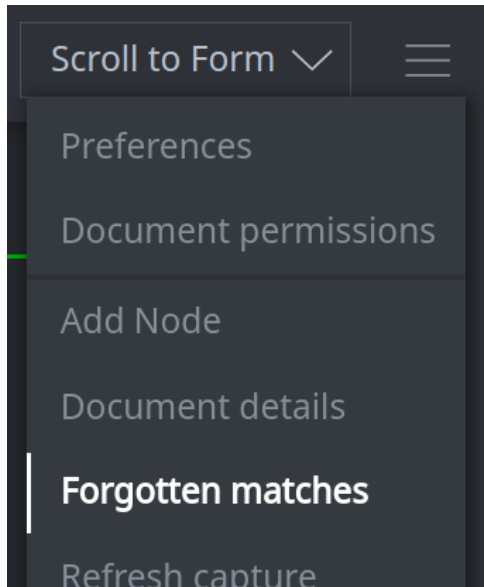
- In the Results, click the **hamburger menu** next to the **file:path** header and choose **Select all:**

- **Right-click** any selected node and choose **forget 5 scraped matches:**

The nodes are removed from the **Filter (new)** list. You can view (and re-add) "forgotten" nodes by clicking the Spotlight **hamburger menu** and selecting **Forgotten Matches:**
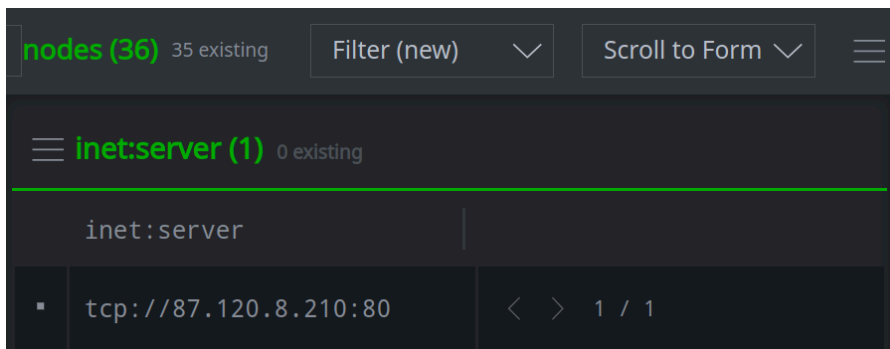

Part 6 - If Time Allows

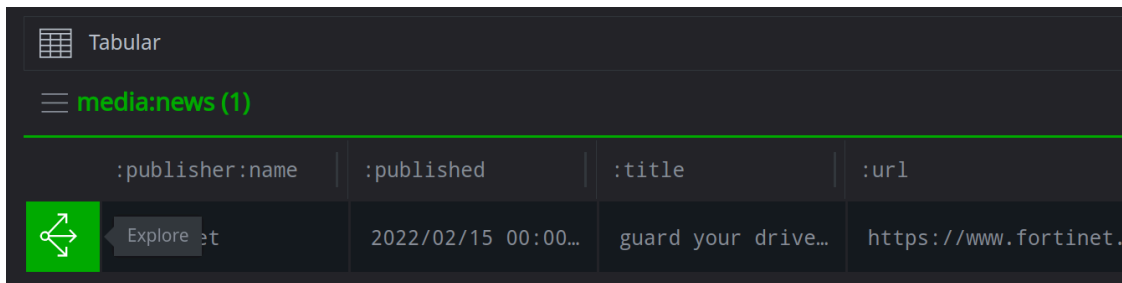If you still have time, continue to practice using Spotlight!

- **Review** (and create or forget) the last "suggested" node:

- Use Spotlight's **Quick Forms** to highlight and create the `file:path` nodes that were scraped incorrectly:

| sc** | Capture a screenshot, saving it to C:\Users\Public\Libraries\tmp.bin before sending it unencrypted to the C2. |
| kl** | The command name and its operation imply keylogger functionality. The first time this command is received, the malware will download a DLL from the C2 and execute it using LoadLibrary, calling its "strt" export. Upon subsequent receipts of this command, the contents of C:\Users\Public\Libraries\async.dat will be sent |

selected: C:\Users\Public\Libraries\async.dat

create node >

extractors >

document details >

file:base
file:path
it:cmd
it:dev:str
it:dev:mutex
it:dev:regkey
it:prod:softname
other

- **Lift** the `media:news` node in the **Research Tool**. Click the **hamburger menu** and select **media:news node > query > selected node.** In the Research Tool, **Explore** from the `media:news` node to view your connected nodes:

Tabular

media:news (1)

	:publisher:name	:published	:title	:url
Explore et		2022/02/15 00:00…	guard your drive…	https://www.fortinet.

- Use **Node Actions** to enrich the indicators: