

# Synapse Bootcamp - Module 18

## Reports, Articles, and the Spotlight Tool - Answer Key

<b>Reports, Articles, and the Spotlight Tool - Answer Key</b>	<b>1</b>
Using Spotlight to Model Reports	2
Exercise 1 Answer	2
Part 1 - Load the Report	2
Part 2 - Set Document (media:news node) Properties	3
Part 3 - Create and Tag Indicators	5
Part 4 - Highlight and Add Nodes with Quick Forms	6
Part 5 - Review Suggested Nodes	7

---

# Using Spotlight to Model Reports

## Exercise 1 Answer

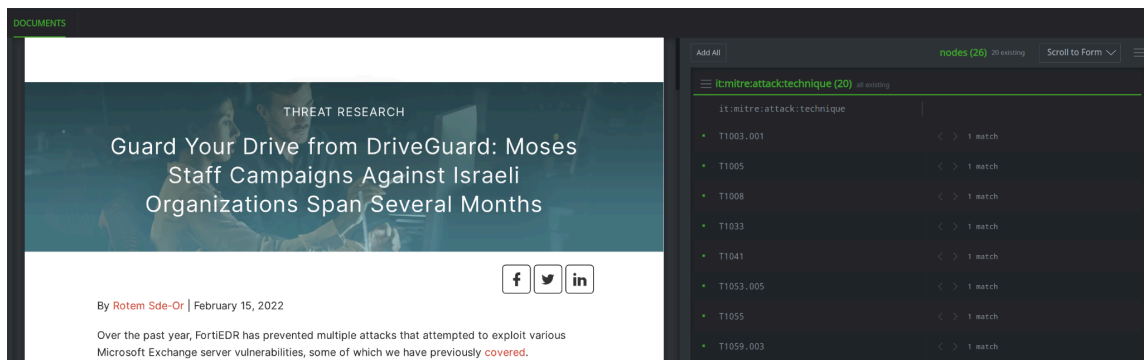
### Objective:

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

### Part 1 - Load the Report

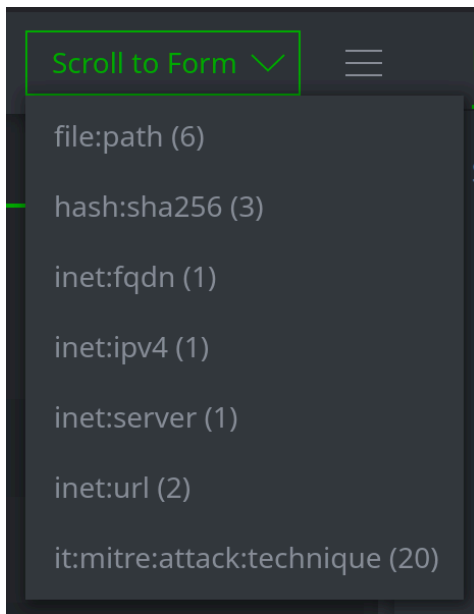
#### Question 1: What does Spotlight display after loading the PDF?

- Once the file has loaded, you should see the report in the left hand panel, and extracted indicators in the center (Results) panel:



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

- Spotlight (using Synapse's 'scrape' functionality) was able to recognize the following indicators:



These include:

- File paths (**file:path**)
- Hashes (**hash:sha256**)
- Domains (**inet:fqdn**)
- IP addresses (**inet:ipv4**)
- Servers (**inet:server**)
- URLs (**inet:url**)
- MITRE ATT&CK techniques (**it:mitre:attack:technique**)

---

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

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

- The **Title** and **Summary** properties are set, based on the text you highlighted.
- The **URL** and **file** properties are set by Spotlight when it creates the PDF content (file) of the URL you specified:

Edit Document media:news node ✕

Title  
guard your drive from driveguard: mores staff campaigns against israelistaff ca

Summary  
Over the past year, FortiEDR has prevented multiple attacks that attempted to exploit various Microsoft Exchange server vulnerabilities, some of which we have previously covered. Among these attacks, we identified a campaign operated by Moses Staff, a geo-political motivated threat group believed to be sponsored by the Iranian government. After tracking this campaign for the

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

Organization  
media:news:publisher:name

Published  
media:news:published

.created  
2023/11/28 15:56:21.251

File  
sha256:a892309cb6f1cfe663444af8063b5254308e8b39f798ffa70149e61ae4415

---

**Question 4:** What does your `media:news` node look like after setting the document properties in Spotlight?

- Your **media:news** node should look similar to the following:

```
▪ media:news
  840e1ddd0db3bbd3baed68f9df139f8e

▪ :file          sha256:a892309cb6f1cfe663444af80...
▪ :published     2022/02/15 00:00:00
▪ :publisher:name fortinet
▪ :summary       Over the past year, FortiEDR has...
▪ :title         guard your drive from driveguard...
▪ :url           https://www.fortinet.com/blog/th...
▪ :url:fqdn      www.fortinet.com
▪ .created       2023/11/28 15:56:21.251
```

**Note:** Spotlight generates an arbitrary guid for the **media:news** node. Your guid value will differ.

---

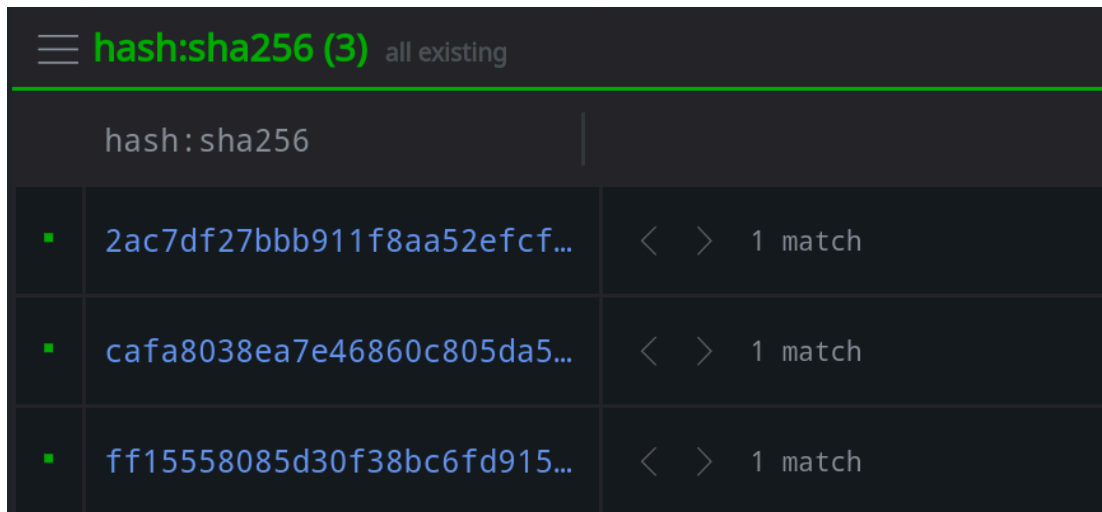
### Part 3 - Create and Tag Indicators

#### Question 4: What happened to the hashes?

- The hashes in the document are highlighted in **blue** (to match our tag color rules):

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

- In the Results, the **hash:sha256** nodes are also blue, and the toggle dot next to each node is now **green** to show that the nodes have been created:



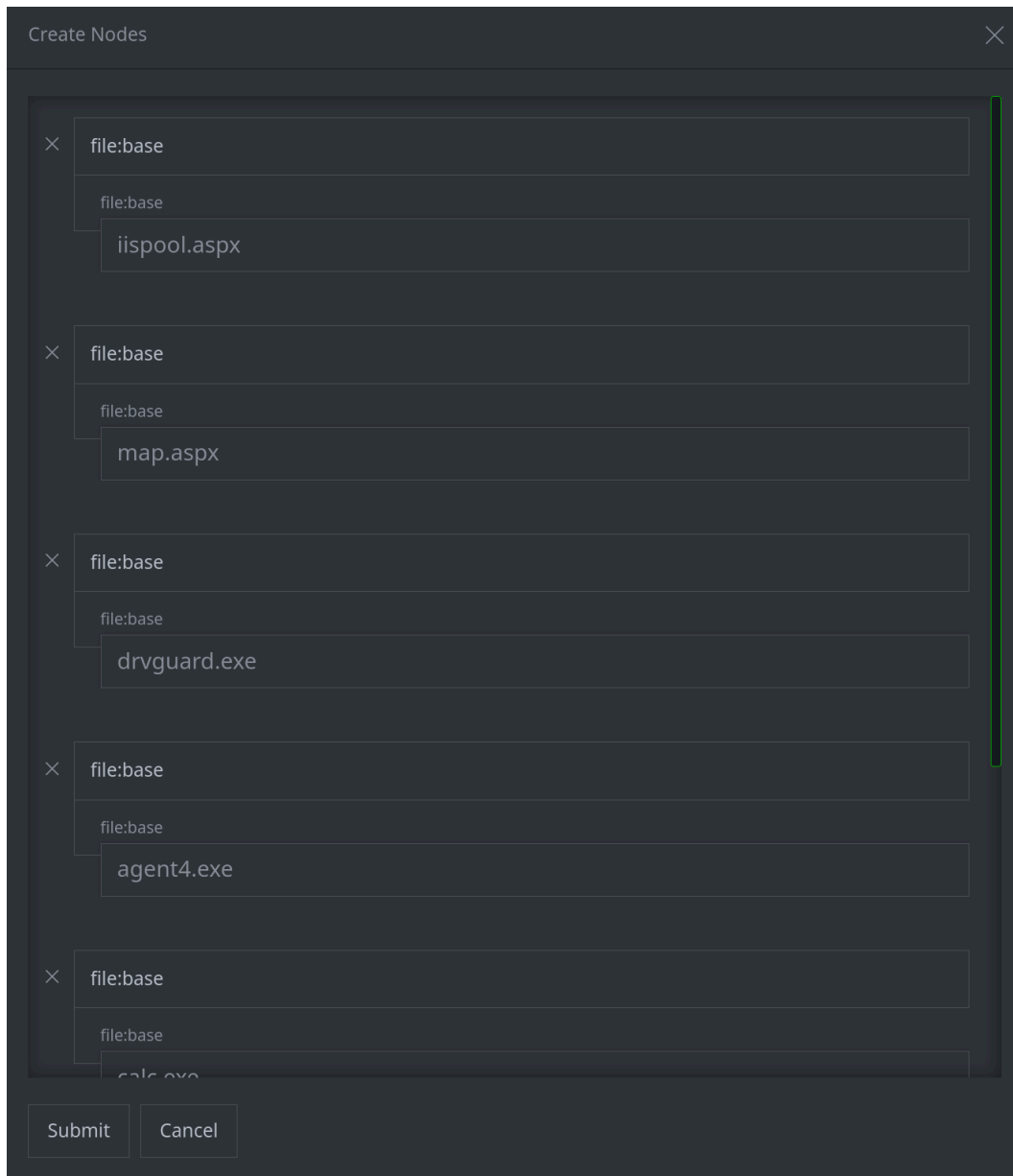
hash:sha256 (3) all existing	
hash:sha256	
▪ 2ac7df27bbb911f8aa52efcf...	< > 1 match
▪ cafa8038ea7e46860c805da5...	< > 1 match
▪ ff15558085d30f38bc6fd915...	< > 1 match

---

#### Part 4 - Highlight and Add Nodes with Quick Forms

**Question 5:** What happened? Did Spotlight create the **file:base** nodes?

- Spotlight opens a **Create Nodes** dialog:



When you select **create nodes** Spotlight interprets your highlighted text as a newline-separated list. Use the **Create Nodes** dialog to review the nodes and make any changes before creating them.

---

## Part 5 - Review Suggested Nodes

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

Three things happen:

- The file path in the document is now blue (because of our tag colors):

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 Details Panel shows the **file:path** node and the tag:

```
• file:path
  c:/windows/system32/broker.exe

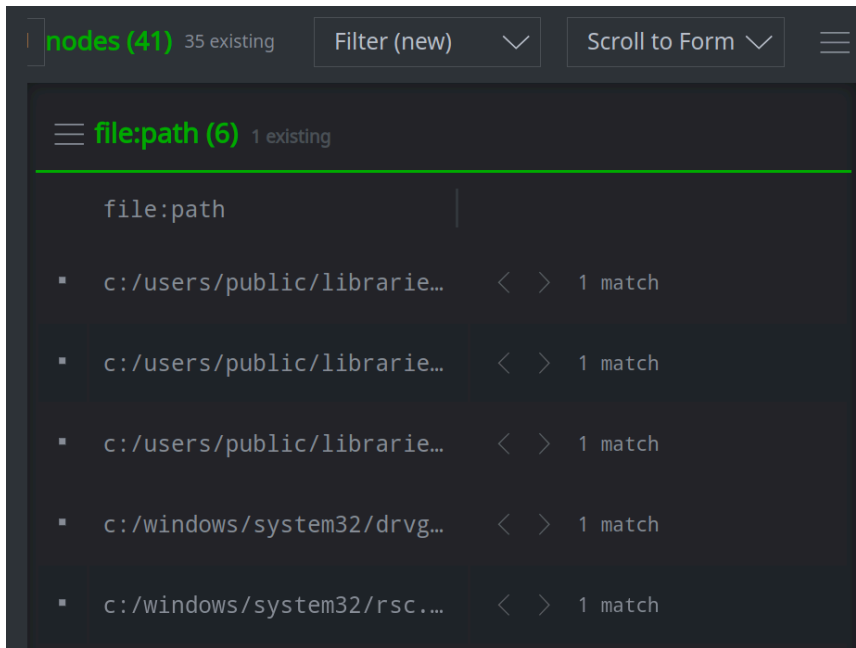
▪ :base      broker.exe
▪ :base:ext  exe
▪ :dir       c:/windows/system32
▪ .created   2023/11/30 19:33:41 ...

+ Add Tags

▪ rep.fortinet.moses_staff
```



- In the Results, the node is **no longer visible**:



The **Filter (new)** option only shows **suggested** nodes. Once we create the **file:path** node, it is removed from the "new" list. This helps us focus on the nodes we still need to review.

Note that the **file:path** header still shows the **total** number of nodes (6 total, 1 existing, but only five displayed).