

# Synapse Bootcamp - Module 2

## Getting Started - Answer Key

<b>Getting Started - Answer Key</b>	<b>1</b>
<b>Answer Key</b>	<b>2</b>
Fork a View	2
Exercise 1 Answer	2
Lifting Nodes	3
Exercise 2 Answer	3
Exercise 3 Answer	5
Working with Tags	6
Exercise 4 Answer	6
Exercise 5 Answer	8
Exercise 6 Answer	9

---

# Answer Key

## Fork a View

### Exercise 1 Answer

**Objective:**

- Create a fork of your current view.

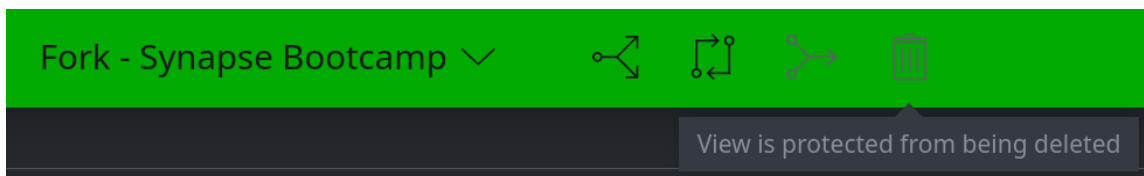
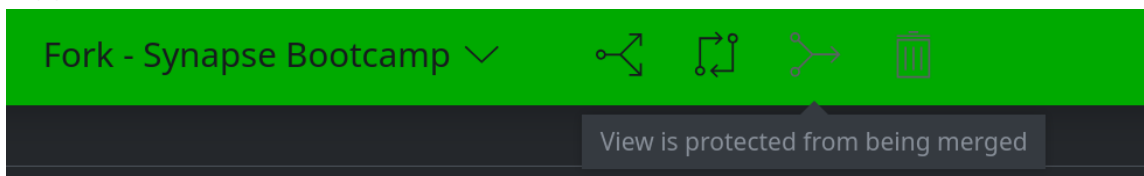
**Question 1:** How did the information displayed in your **Top Bar** change?

- Your **Top Bar** shows that you are in your new **Fork - Synapse Bootcamp** view:



**Tip:** When you fork a view, Synapse automatically switches you into your newly created view (your fork / forked view).

Your **merge** and **delete** icons are also grayed out (because you set the **Protect** toggle to **ON**):



## Lifting Nodes

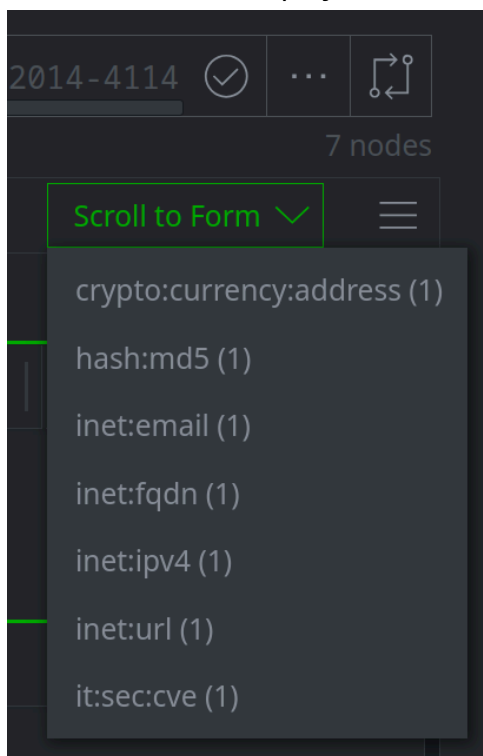
### Exercise 2 Answer

**Objective:**

- Practice lifting nodes using Lookup mode.

**Question 1:** How many nodes are displayed in the Results Panel?

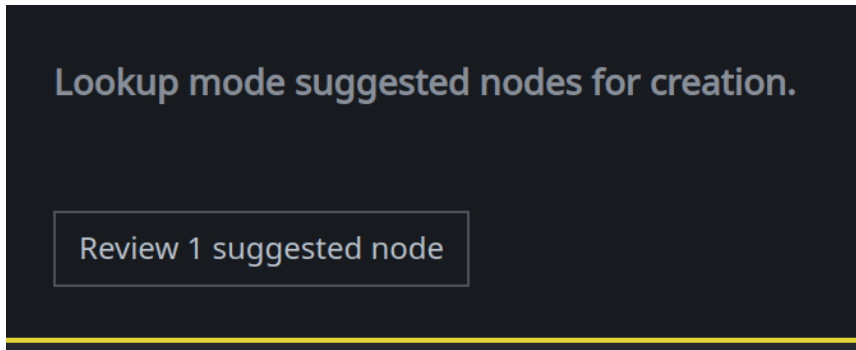
- **Seven** nodes are displayed in the Results Panel:



**Tip:** Synapse is able to recognize the indicators, even though some of them are **defanged**. Synapse automatically "refangs" the indicators to lift them.

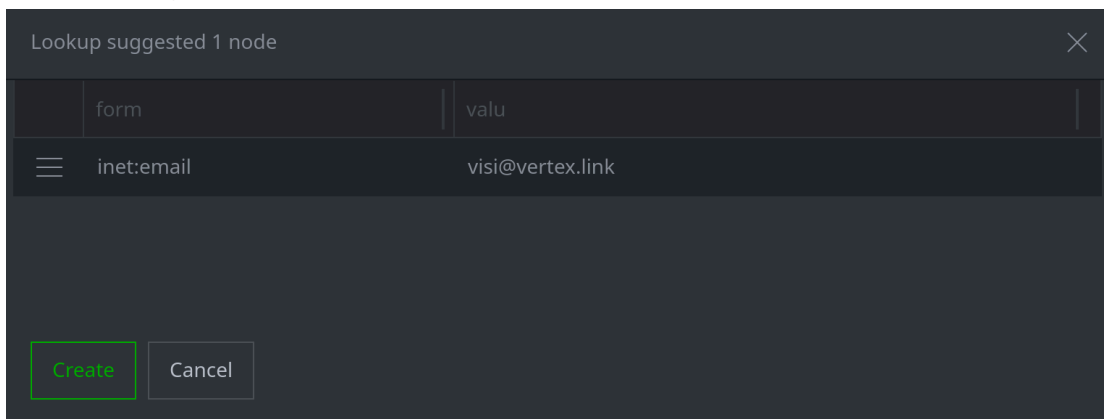
**Question 2:** What happens when you run the query?

- Synapse displayed a popup ("toast") message:



Lookup mode was able to recognize **visi@vertex.link** as a valid email address, but the address does not currently exist in Synapse. Synapse offers to create the node for you.

If you click the **Review 1 suggested node** button, you can use the **suggested nodes** dialog to **Create** the node or **Cancel**:



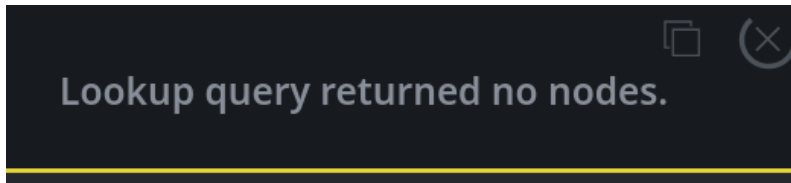
**Tip:** If the toast message disappears, place your cursor in the **Query Bar** and press **Enter** to re-run the query.

In the **Lookup suggested 1 node** dialog, you can use the **hamburger menu** next to each node to **Remove** individual nodes. This is useful when Lookup mode suggests multiple nodes, but you only want to create some of them.

---

**Question 3:** What happens when you run the query?

- When you query the file name **certutil.exe**, Synapse displays a message:



Lookup mode did not find a matching node, and did not know what kind of node to offer to create for you.

Lookup mode does not recognize "file names" - **certutil.exe** does not match the kinds of data that **Lookup** mode knows about.

**Note:** A "file name" is an arbitrary string. It could even "look like" another kind of data, such as an FQDN. Is **command.com** a file name, or a domain, or both?

**Tip:** Lookup mode makes it easy to lift (ask about) many **common** indicators. Later we'll learn how the Storm query language expands our ability to "ask about" additional kinds of data!

---

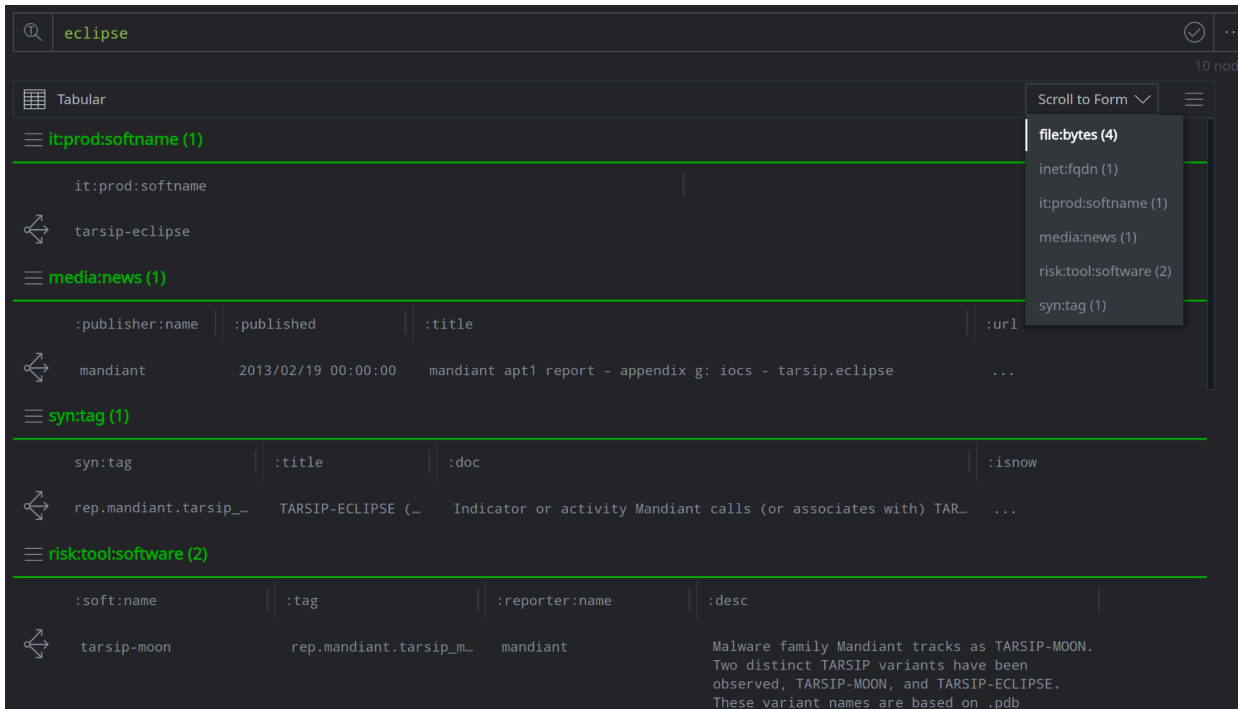
## Exercise 3 Answer

**Objective:**

- Practice lifting nodes using Text Search mode.

**Question 1:** What kinds of nodes are returned by your search?

- Synapse returns several kinds of nodes:



The screenshot shows a search interface for the term 'eclipse'. The results are categorized into several tags:

- it:prod:softname (1)**: A single result with the value 'tarsip-eclipse'.
- media:news (1)**: A single result with the title 'mandiant apt1 report - appendix g: iocs - tarsip.eclipse' and a published date of '2013/02/19 00:00:00'.
- syn:tag (1)**: A single result with the title 'TARSIP-ECLIPSE (...)' and a description: 'Indicator or activity Mandiant calls (or associates with) TAR...'.
- risk:tool:software (2)**: Two results, one of which is 'tarsip-moon' with a description: 'Malware family Mandiant tracks as TARSIP-MOON. Two distinct TARSIP variants have been observed, TARSIP-MOON, and TARSIP-ECLIPSE. These variant names are based on .pdb'.

A dropdown menu is visible on the right side of the interface, listing the following tags and their counts:

- file:bytes (4)
- inet:fqdn (1)
- it:prod:softname (1)
- media:news (1)
- risk:tool:software (2)
- syn:tag (1)

The results include:

- **Files (file:bytes)**, where 'eclipse' appears in the file's PDB path and exports library name;
- **Domains (inet:fqdn)** that include the string 'eclipse';
- **Software (malware) names (it:prod:softname)** that include 'eclipse';
- **Articles (media:news)** that contain 'eclipse' in their title or summary;
- **Software (risk:tool:software)** that contain 'eclipse' in their description; and
- **Tags (syn:tag)** that contain 'eclipse'.

## Working with Tags

### Exercise 4 Answer

#### Objective:

- View and understand the tags on a node.

**Question 1:** What do the **tags** on this node tell us about the IP address?

- The tags show that:

- The IP is (or was) a **TOR exit node** (between 2023/05/08 and at least 2024/04/17).
- **PwC** (PricewaterhouseCoopers) associates the IP with **APT10**.
- **PwC** associates the IP with **Cloud Hopper**.

```
■ seen (2023/05/08 14:30:51, 2024/04/17 17:37:10.001) ...  
  TOR Exit Node  
  An IP address, server, or host acting as a TOR exit node.  
■ #cno.infra.anon.tor.exit  
  (2023/05/08 14:30:51, 2024/04/17 17:37:10.001)  
■ #rep.pwc.apt10  
■ #rep.pwc.cloud_hopper
```

---

**Question 2:** What **publicly reported** threat group is this FQDN associated with?

- The FQDN **satellitebbs.com** is associated with the **APT1** threat group, according to Mandiant (**rep.mandiant.apt1**):

```
APT1 (Mandiant)  
Indicator or activity Mandiant calls (or associates with) APT1.  
■ #rep.mandiant.apt1
```

Vertex uses the **rep** ("reported") tag tree to record information or assessments reported by third parties.

---

**Question 3:** What **internally tracked** threat group is this FQDN associated with? When did that threat group control the FQDN?

- The FQDN is associated with Vertex internal threat group **T15**:

```
▪ #cno.threat.t15.own  
(2009/10/22 00:00:00, 2013/10/22 00:00:00)
```

- Vertex indicates that T15 controlled the FQDN between **October 22, 2009 and October 22, 2013** (2009/10/22 - 2013/10/22).

Vertex uses the **cno** ("computer network operations") tag tree to record our own first-hand assessments.

---

**Question 4:** When was the FQDN **first sinkholed**? What organization sinkholed it?

- The FQDN was first sinkholed on **January 10, 2014** (2014/01/10) by **Kleissner & Associates** (aka Virus Tracker):

```
▪ #cno.infra.dns.sink.holed.kleissner  
(2014/01/10 00:00:00, 2017/01/10 00:00:00)  
▪ #cno.infra.dns.sink.holed.snk1  
(2017/03/30 00:00:00, 2018/03/30 00:00:00)
```

---

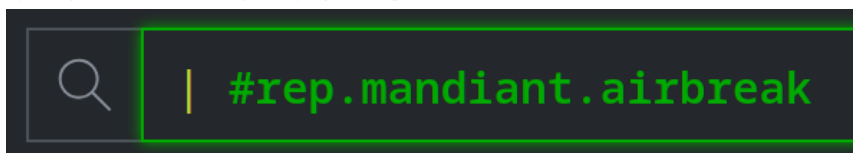
Exercise 5 Answer

**Objective:**

- Lift nodes using tags.

**Question 1:** What query did Synapse load and run in the Query Bar?

- Synapse ran the query | **#rep.mandiant.airbreak:**



```
| #rep.mandiant.airbreak
```

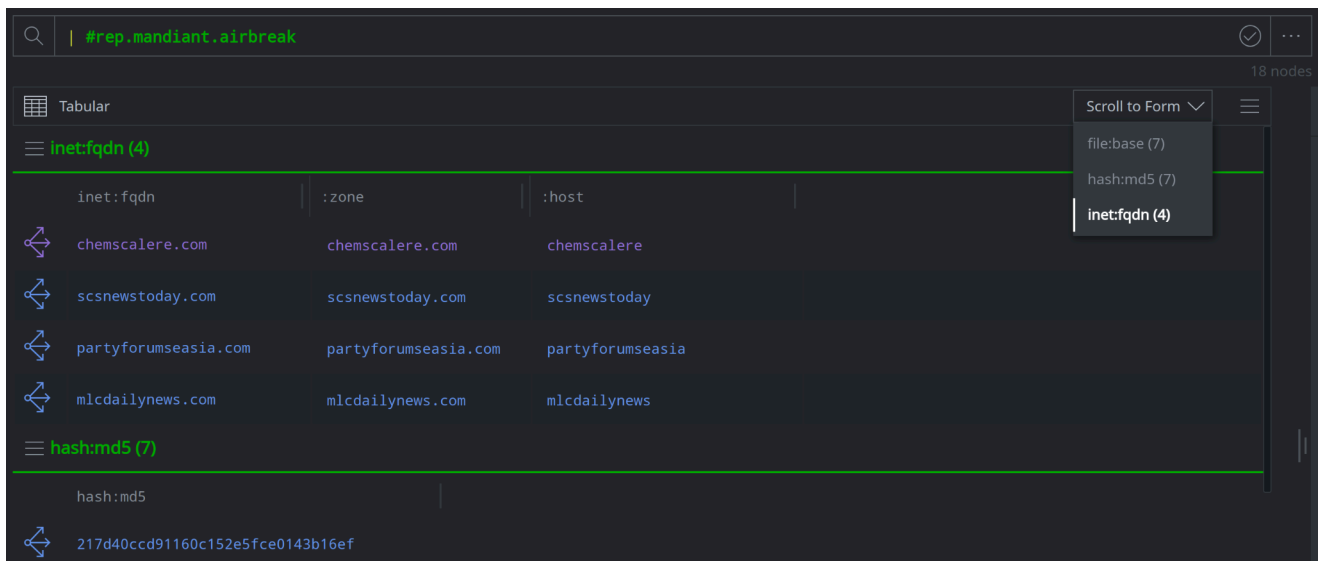


**Tip:** Synapse uses the **hashtag** symbol ( # ) to represent a tag applied to a node.

Synapse uses the pipe character ( | ) to run a **Storm** query even though we are in **Lookup** mode. We'll learn more about this when we start learning Storm!

## Question 2: What kinds of nodes are returned by the query?

- The query returns **18 nodes** that Mandiant associates with AIRBREAK. These include:
  - **Domains** (**inet:fqdn**)
  - **MD5 hashes** (**hash:md5**)
  - **File names** (**file:base**)



The screenshot shows the Synapse interface with the query `#rep.mandiant.airbreak`. The results are displayed in a tabular view with columns for schema, value, and host. A dropdown menu is open, showing options to scroll to 'file:base (7)', 'hash:md5 (7)', and 'inet:fqdn (4)'. The results are as follows:

inet:fqdn (4)	:zone	:host
chemscalere.com	chemscalere.com	chemscalere
scsnewstoday.com	scsnewstoday.com	scsnewstoday
partyforumseasia.com	partyforumseasia.com	partyforumseasia
mlcdailynews.com	mlcdailynews.com	mlcdailynews

hash:md5 (7)
217d40ccd91160c152e5fce0143b16ef

## Exercise 6 Answer

### Objective:

- Lift nodes using tags from Tag Explorer.

## Question 1: How many nodes are returned by the query?

- The query returns **three** files:

🔍 | #rep.vt.upx

📄 Tabular

☰ ▼ file:bytes (3)

file:bytes	:mime	:mime:pe:compiled
↔ sha256:d6556996c2170b2c662dbda1650...	application/vnd.microsoft.porta...	2011/01/29 07:13:48
↔ sha256:24e37c38410ee2173b1a0988ed0...	application/vnd.microsoft.porta...	2003/01/14 20:27:18
↔ sha256:43ec5100c93603542ed476023a2...	application/vnd.microsoft.porta...	2012/04/24 09:59:18