

# Synapse Bootcamp - Module 10

## Filtering in Storm - Answer Key

<b>Filtering in Storm - Answer Key</b>	<b>1</b>
<b>Answer Key</b>	<b>2</b>
Simple Filters	2
Exercise 1 Answer	2
Filters with Mathematical Operators	7
Exercise 2 Answer	7
Filters with Extended Operators	8
Exercise 3 Answer	8

---

# Answer Key

## Simple Filters

### Exercise 1 Answer

**Objective:**

- Use Storm to perform simple filter operations.

#### Part 1

**Question 1:** How can you **add a filter** to your existing query to **only** display the **inet:url** nodes?

- You can filter the nodes with the following Storm:

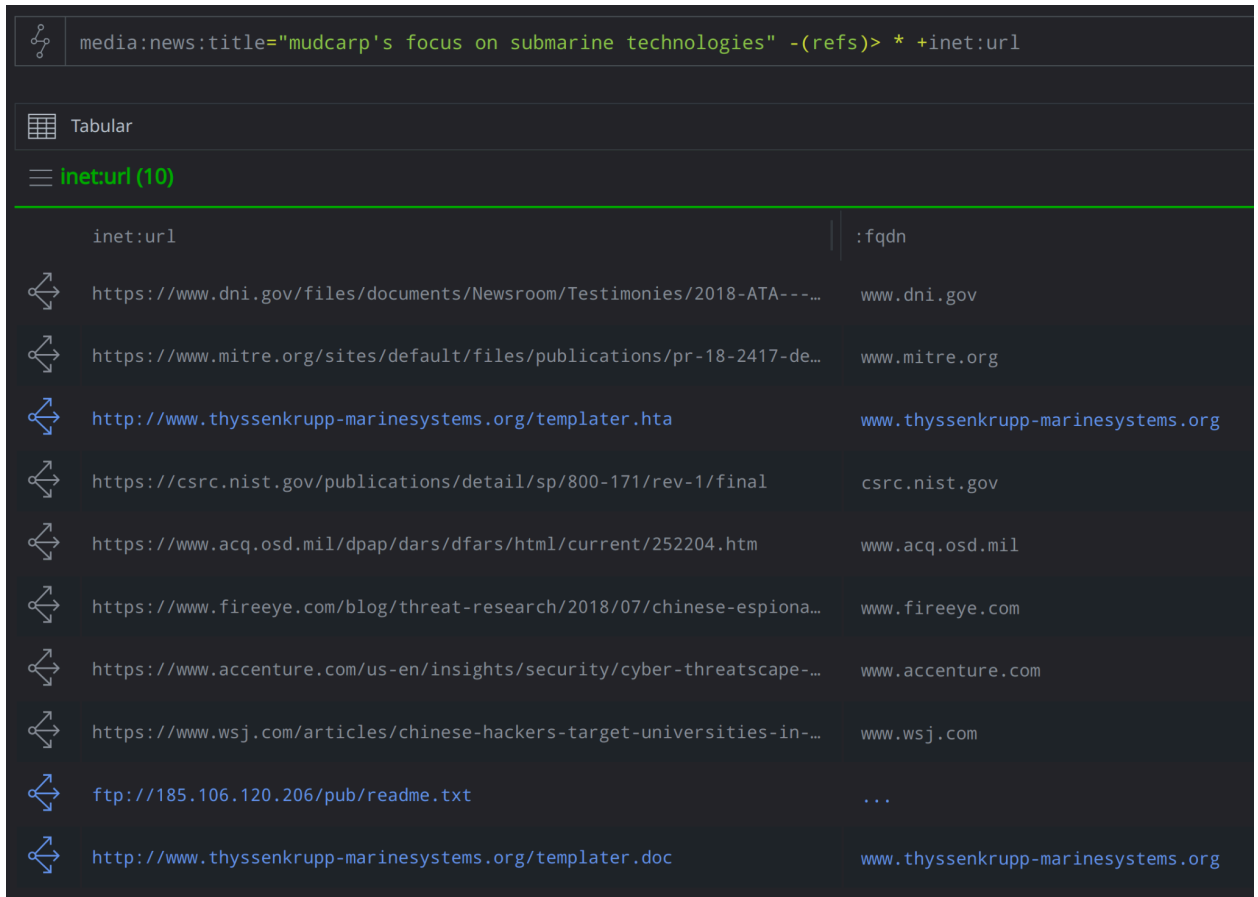
```
media:news:title="mudcarp's focus on submarine technologies"  
-(refs)> * +inet:url
```

You're telling Synapse to limit (downselect) your results to **only include** **inet:url** nodes.

(This is called a **filter by form**).

Technically, you can **modify** your original query to only traverse the **refs** edge to any **inet:url** nodes in the first place (which is actually a bit more efficient). But we want to practice with filters!

- Running this query will produce the following:



```
media:news:title="mudcarp's focus on submarine technologies" -(refs)> * +inet:url
```

Tabular

inet:url (10)

inet:url	:fqdn
<a href="https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---...">https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---...</a>	www.dni.gov
<a href="https://www.mitre.org/sites/default/files/publications/pr-18-2417-de...">https://www.mitre.org/sites/default/files/publications/pr-18-2417-de...</a>	www.mitre.org
<a href="http://www.thyssenkrupp-marinesystems.org/templater.hta">http://www.thyssenkrupp-marinesystems.org/templater.hta</a>	www.thyssenkrupp-marinesystems.org
<a href="https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final">https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final</a>	csrc.nist.gov
<a href="https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm">https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm</a>	www.acq.osd.mil
<a href="https://www.fireeye.com/blog/threat-research/2018/07/chinese-espiona...">https://www.fireeye.com/blog/threat-research/2018/07/chinese-espiona...</a>	www.fireeye.com
<a href="https://www.accenture.com/us-en/insights/security/cyber-threatscape-...">https://www.accenture.com/us-en/insights/security/cyber-threatscape-...</a>	www.accenture.com
<a href="https://www.wsj.com/articles/chinese-hackers-target-universities-in-...">https://www.wsj.com/articles/chinese-hackers-target-universities-in-...</a>	www.wsj.com
<a href="ftp://185.106.120.206/pub/readme.txt">ftp://185.106.120.206/pub/readme.txt</a>	...
<a href="http://www.thyssenkrupp-marinesystems.org/templater.doc">http://www.thyssenkrupp-marinesystems.org/templater.doc</a>	www.thyssenkrupp-marinesystems.org

**Question 2:** How can you **add a filter** to your query to **only** display URLs that Accenture reported?

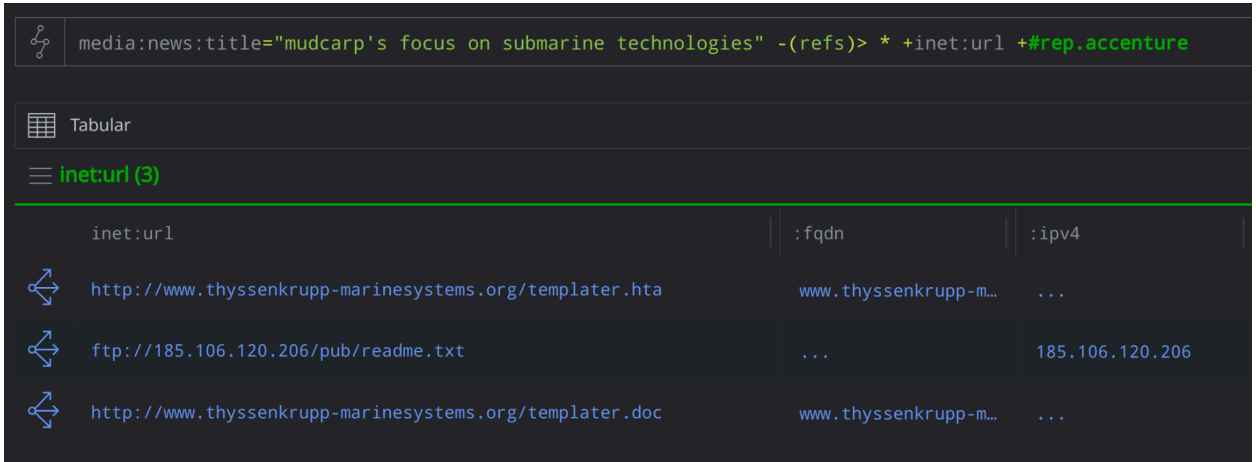
- You can filter the nodes with the following Storm:

```
media:news:title="mudcarp's focus on submarine technologies"
-(refs)> * +inet:url +#rep.accenture
```

You're telling Synapse to limit (downselect) your results to only **include** nodes reported by Accenture (e.g., as associated with the MUDCARP threat group or a malware family).

(This is called a **filter by tag**).

- Running this query will give you the following results:



```
media:news:title="mudcarp's focus on submarine technologies" -(refs)> * +inet:url +#rep.accenture
```

Tabular

ineturl (3)

inet:url	:fqdn	:ipv4
<a href="http://www.thyssenkrupp-marinesystems.org/templater.hta">http://www.thyssenkrupp-marinesystems.org/templater.hta</a>	www.thyssenkrupp-m...	...
<a href="ftp://185.106.120.206/pub/readme.txt">ftp://185.106.120.206/pub/readme.txt</a>	...	185.106.120.206
<a href="http://www.thyssenkrupp-marinesystems.org/templater.doc">http://www.thyssenkrupp-marinesystems.org/templater.doc</a>	www.thyssenkrupp-m...	...

## Part 2

**Question 3:** How can you **add a filter** to the above query to **only** show IPv4s on AS 25820?

- You can filter the nodes with the following Storm:

```
inet:fqdn#rep.microsoft.brass_typhoon -> inet:dns:a  
-> inet:ipv4 | uniq | +:asn=25820
```

After switching back to Storm query mode with the **pipe** character ( | ), you're telling Synapse to **include** only those IPv4s whose **:asn** value is 25820.

(This is called a **filter by property value**).

- Running this query will produce the following:

```
inet:fqdn#rep.microsoft.brass_typhoon -> inet:dns:a -> inet:ipv4 | uniq | +:asn=25820
```

Tabular

inet:ipv4 (17)

inet:ipv4	:loc	:asn	:asn::name	:dns:rev
74.120.175.144	us.ca.los angel...	25820	it7net	74.120.175.144.16c...
104.243.19.49	us.ca.los angel...	25820	it7net	104.243.19.49.16cl...
74.82.201.8	us.ca.los angel...	25820	it7net	74.82.201.8.16clou...
198.35.45.105	us.ca.los angel...	25820	it7net	198.35.45.105.16cl...

**Tip:** you only need to provide the **relative property name (:asn)** for the filter. Synapse knows that the nodes that are "inbound" to the filter operation are **inet:ipv4** nodes, so you don't need to include the form name.

The filter will work the same way if you use the **full property name (+inet:ipv4:asn=25820)**, but using the **relative** name saves you some typing!

**Question 4:** How can you add a filter to your query to view **only** those IPs reported by Microsoft (**rep.microsoft**)?

- You can filter the nodes with the following Storm:

```
inet:fqdn#rep.microsoft.brass_typhoon -> inet:dns:a
-> inet:ipv4 | uniq | +:asn=25820 +#rep.microsoft
```

You're telling Synapse to only **include** indicators tagged **rep.microsoft**.

(This is called a **filter by tag**).

- Incorporating this filter reduces our results from 17 `inet:ipv4` nodes to 7:

inet:ipv4 (7)					
	inet:ipv4	:loc	:asn	:asn::name	:dns:rev
↔	74.82.201.8	us.ca.los angeles	25820	it7net	74.82.201.8.16c1ou...
↔	104.224.185.36	us.ca.los angeles	25820	it7net	104.224.185.36.16c...
↔	104.36.69.105	us.ca.los angeles	25820	it7net	104.36.69.105.16cl...
↔	65.49.192.74	us.ca.los angeles	25820	it7net	65.49.192.74.16clo...
↔	176.122.162.149	us.ca.los angeles	25820	it7net	176.122.162.149.16...
↔	107.182.18.149	us.ca.los angeles	25820	it7net	107.182.18.149.16c...
↔	176.122.188.254	us.ca.los angeles	25820	it7net	176.122.188.254.16...

**Tip:** you only need to specify "enough" of the tag to get what you want. In this case "things reported by Microsoft" all fall under the `rep.microsoft` portion of the tag tree. This includes `rep.microsoft.brass_typhoon` but would also include `rep.microsoft.midnight_blizzard`, for example.

Using the "higher level" tag in your filter gets you what you want without having to individually specify any / all leaf tags.

**Question 5:** How can you add a filter to your query to view **only** those IPs reported by Microsoft (`rep.microsoft`) and Mandiant (`rep.mandiant`)? How many IPs were reported by both organizations?

- You can filter the nodes with the following Storm:

```
inet:fqdn#rep.microsoft.brass_typhoon -> inet:dns:a
-> inet:ipv4 | uniq | +:asn=25820 +#rep.microsoft
+#rep.mandiant
```

One IPv4 address was reported by both Microsoft (as Brass Typhoon) and Mandiant (as APT41):

```

≡ inet:ipv4 (1)
┌───────────┬───────────┬───────────┬───────────┬───────────┐
│ inet:ipv4  │ :loc       │ :asn       │ :asn::name  │             │
│ ↔          │ 74.82.201.8 │ us.ca.los angeles │ 25820       │ it7net      │
└───────────┴───────────┴───────────┴───────────┴───────────┘

```

## Filters with Mathematical Operators

### Exercise 2 Answer

**Objective:**

- Use mathematical operators to perform filter operations with Storm.

**Question 1:** How can you **add a filter** to your query to **only** display WhoIs records created **before** January 11, 2014 (the date Kleissner & Associates registered / sinkholed the domain)?

- You can filter the WhoIs records with the following Storm:

```
inet:fqdn=hugesoft.org -> inet:whois:rec +:created<2014/01/11
```

You're telling Synapse to **include** whois records with a registration (**:created**) date **less than** (earlier than) January 11, 2014:

```

≡ inet:whois:rec (57)
┌───────────┬───────────┬───────────┬───────────┬───────────┬───────────┐
│ :fqdn      │ :asof      │ :created   │ :updated   │ :expires   │             │
│ ↔         │ hugesoft.org │ 2008/11/20 0... │ 2004/10/25 0... │ 2008/09/25 0... │ 2009/10/25 0... │
│ ↔         │ hugesoft.org │ 2005/07/25 0... │ 2004/10/25 0... │ 2005/07/18 0... │ 2005/10/25 0... │
│ ↔         │ hugesoft.org │ 2009/06/08 0... │ 2004/10/25 0... │ 2009/03/31 1... │ 2010/10/25 0... │
│ ↔         │ hugesoft.org │ 2009/02/11 0... │ 2004/10/25 0... │ 2009/01/17 0... │ 2009/10/25 0... │
└───────────┴───────────┴───────────┴───────────┴───────────┴───────────┘

```

Because Synapse stores dates as integer values, we can easily perform mathematical comparisons and mathematical operations using date/time values!

## Filters with Extended Operators

### Exercise 3 Answer

**Objective:**

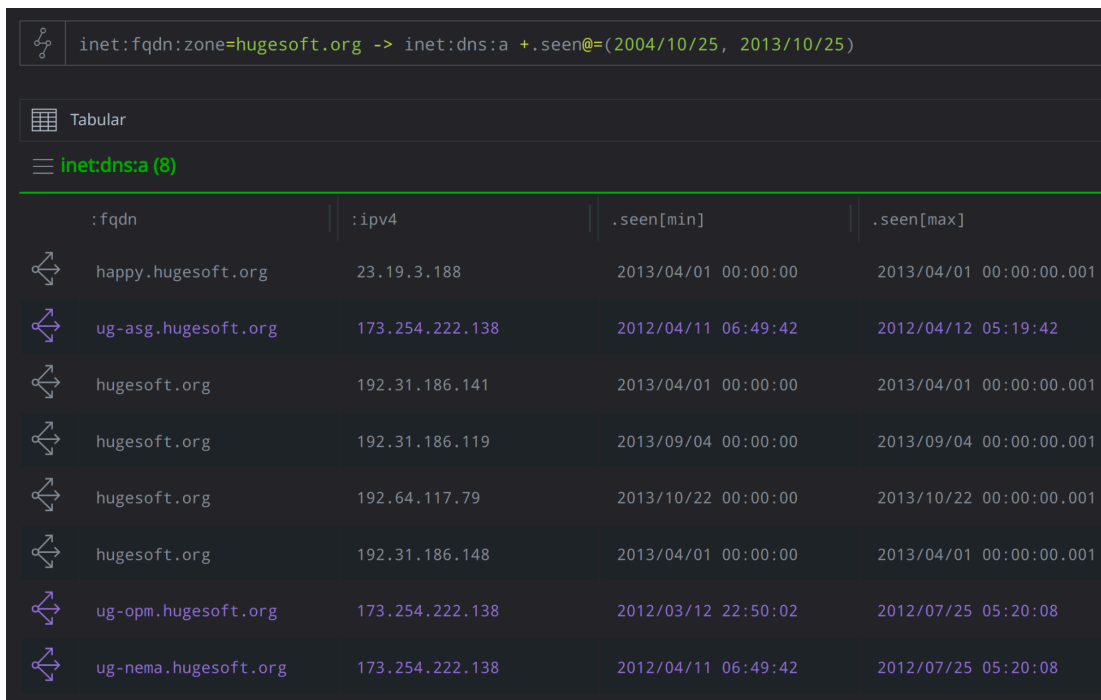
- Use extended operators to perform filter operations in Storm.

**Question 1:** How can you **add a filter** to the query above to **only** display DNS A records observed (**.seen**) between those dates?

- You can filter the DNS A records with the following Storm:

```
inet:fqdn:zone=hugesoft.org -> inet:dns:a
+.seen@=(2004/10/25, 2013/10/25)
```

You're using Synapse's **time / interval operator** to tell Synapse to **include** only those records seen between the specified dates:



The screenshot shows a Synapse query interface. At the top, the query is: `inet:fqdn:zone=hugesoft.org -> inet:dns:a +.seen@=(2004/10/25, 2013/10/25)`. Below the query, the view is set to 'Tabular' and shows 8 results for the query `inet:dns:a (8)`. The results are displayed in a table with the following columns: `:fqdn`, `:ipv4`, `.seen[min]`, and `.seen[max]`.

:fqdn	:ipv4	.seen[min]	.seen[max]
happy.hugesoft.org	23.19.3.188	2013/04/01 00:00:00	2013/04/01 00:00:00.001
ug-asg.hugesoft.org	173.254.222.138	2012/04/11 06:49:42	2012/04/12 05:19:42
hugesoft.org	192.31.186.141	2013/04/01 00:00:00	2013/04/01 00:00:00.001
hugesoft.org	192.31.186.119	2013/09/04 00:00:00	2013/09/04 00:00:00.001
hugesoft.org	192.64.117.79	2013/10/22 00:00:00	2013/10/22 00:00:00.001
hugesoft.org	192.31.186.148	2013/04/01 00:00:00	2013/04/01 00:00:00.001
ug-opm.hugesoft.org	173.254.222.138	2012/03/12 22:50:02	2012/07/25 05:20:08
ug-nema.hugesoft.org	173.254.222.138	2012/04/11 06:49:42	2012/07/25 05:20:08



**Tip:** Synapse understands many formats for date/time values. When entering dates in **YYYY/MM/DD** format, we include the forward slashes ( / ) for clarity, but they are not required. The following format also works: **+ .seen@=(20041025, 20131025)**.

---

**Question 2:** How many DNS A records are in your results after adding the filter operation?

- After adding the filter there are **eight** DNS A records (from more than 300 originally).
-