Synapse Bootcamp

Module 3

Exploring and Filtering Data

v0.4 - May 2024

Objectives

- Understand the Synapse Explore feature
- Use Explore in Tabular mode to examine data
- Use Explore in Force Graph mode to examine data
- Use the `pivot` menu to view connected data
- Filter your display using column filters
- Downselect results using the `select` and `query` menus

Exploring Data in Synapse

Exploring in Synapse

- The **Explore** feature allows you to navigate data in Synapse
- Synapse's data model represents:
  - Objects (**nodes**)
  - Their **connections** or relationships in the real world
- **Explore** allows you to see **all** the connections
  - Regardless of **how** they're connected
- View connections you expect
  - FQDN to DNS A to IPv4
- **Discover** connections you didn't know about
  - "This email used for phishing is also the technical contact for a netblock in Belarus"

Explore Demo

The Pivot Menu

Using the Pivot Menu

- The **Explore** button shows you **all** connections
- The **pivot** menu shows you a **particular** connection
  - Focus your navigation more narrowly
- Allows you to view:
  - Related nodes
    - “Pivot from a DNS A record to its associated IPv4 address”
  - Nodes that share a property value
    - “Pivot from a file to all files with the same imphash value”

Pivot Menu Demo

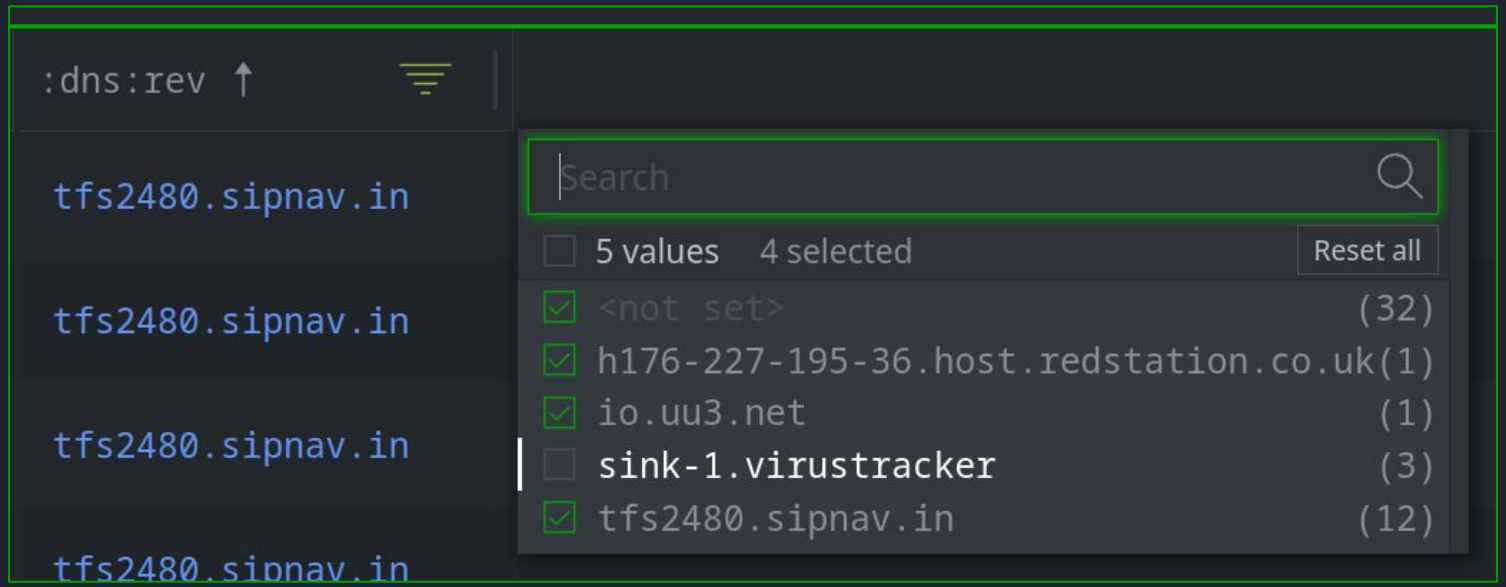
Filtering Data in Synapse

Filtering

- When you **filter** data, you take a set of results and "reduce" it
  - **Include** (keep) the things you want
  - **Exclude** (remove) the things you don't care about
- Two ways to filter in the Synapse UI
  - Column filters
  - Menu options (query, select)

Column Filters

- Limit or focus your **display**
  - Results don't **change** - some are simply **hidden**



Menu "Filters"

- **Change** the focus of your analysis / results
- Menu options allow you to:
  - Easily run a **new** query
  - "Restart" your navigation from the data that interests you
- **`query`** menu
- **`select`** menu

Filtering Demo

Summary

- Synapse's **Explore** feature allows you to easily view "connected" nodes
  - Examine data and relationships
  - See **all** connections
- Navigate more specific connections using the `pivot` menu
  - Pivot on a selected property, while maintaining breadcrumbs
- The `query` menu allows you to:
  - **Filter** existing results by resetting your query
  - Remove breadcrumbs and start over
  - The `select` menus help you choose nodes to query
- **Column filters** allow you to filter your display
  - Combine with `pivot` and / or `query` for flexible navigation