

# DERANT

Data Analysis Documentation

June 23, 2022

# Contents

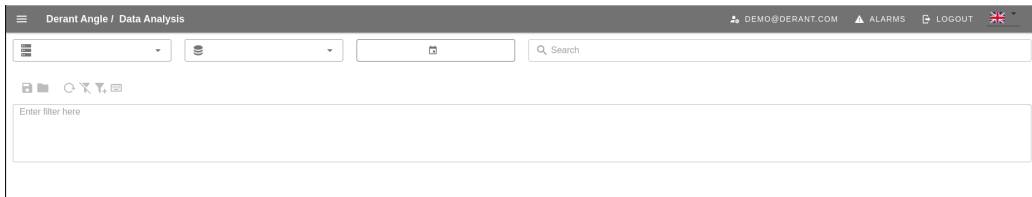
<b>1</b>	<b>Introduction</b>	<b>3</b>
<b>2</b>	<b>Retrieving Data</b>	<b>3</b>
2.1	Choosing Sensor . . . . .	3
2.2	Choosing Log Type . . . . .	4
2.3	Choosing Date . . . . .	4
<b>3</b>	<b>Data Table</b>	<b>5</b>
3.1	Data Presentation . . . . .	5
3.2	Table Settings . . . . .	6
<b>4</b>	<b>Filters, Profiles and Baselineing</b>	<b>7</b>
4.1	Filter Language . . . . .	7
4.2	Saved Filter . . . . .	9
4.3	Applying Filters . . . . .	9
4.4	Profiles . . . . .	10
4.5	Baselineing . . . . .	11

# 1 Introduction

The Data Analysis page is essential to Angle, as it is where the user interacts with the network data; whether it comes from a sensor monitoring a network, a PCAP file, or one of our available preconfigured data sets. Baselining the network, in order to alert on anomalies, will also be done on the Data Analysis page using the filters to build profiles. Additionally, the Data Analysis page is a useful investigation tool when an incident arises, Angle alerts on some traffic or even when verifying configurations in the network.

## 2 Retrieving Data

When navigating to the Data Analysis page for the first time, below image is the sight you will meet. The first thing to do is retrieving some data to work with. Angle will need 3 pieces of information before it can fetch data: The sensor from where to pull the data, the log type specifying which type of data, and finally the date from when the data originates. Notice the 3 boxes in the top left of below image. From left to right, this is where the sensor, the log type and the date is specified. These informations should be filled in from left to right, since available options are loaded when the previous information is specified.



### 2.1 Choosing Sensor

Sensors are created by the users of Angle, and belongs to the company. A company can have multiple sensors of varying types:

- Sensor with **preconfigured** data, created on the Getting Started page.
- Sensor with data from a **PCAP** file uploaded by the user.
- A **sensor** installed on a network, feeding live data into Angle.

Data in Angle is always associated with a sensor.

## 2.2 Choosing Log Type

Data in Angle is categorized into different log types. Choosing a log type means choosing what type of data to retrieve. The log types supported by Angle are those included in Zeek and Suricata. Available log types, depend on what traffic and other information is in your network or on your sensor. When choosing a log type Angle labels 5 specific ones as recommended: conn, dns, http, ssl, and suricata. These are log types that Derant values highly, and expects/suggests users to frequently work with.

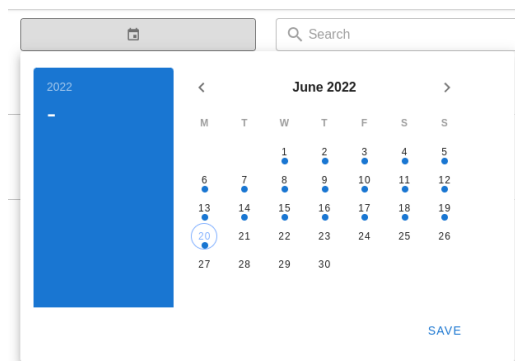
For further information on the log types, we refer to the documentation of Zeek and Suricata:

Zeek: <https://docs.zeek.org/en/master/logs/index.html>

Suricata: <https://suricata.readthedocs.io/>

## 2.3 Choosing Date

Finally, Angle requires to know from which time frame data should be retrieved. This is specified in the date selector, found in the last of the 3 boxes. When the sensor and the log type has been selected, the date selector will indicate on which dates data is available by marking them with a blue dot as seen in the image below:



By clicking on a single date, data will be fetched from this day only. It is also possible to fetch data from a range of dates, simply by selecting a start date and an end date. Pressing the save button will tell Angle to fetch the data.

### 3 Data Table

The image below shows the data table filled with the requested data in a well known row/column format. By using the arrow keys, one can navigate the data with the cursor, going horizontally to browse all the available information, and vertically to inspect more data points.

The screenshot shows the Derant Angle Data Analysis interface. At the top, there is a navigation bar with 'Derant Angle / Data Analysis', a user profile 'DEMO@DERANT.COM', and buttons for 'ALARMS', 'LOGOUT', and a flag icon. Below this is a search bar with 'Cobalt-Strike-Activity' selected, a dropdown for 'suricata', a date filter for '2022-06-15', and a search input field. A filter input field is also present. The main area contains a data table with the following columns: 'ts', 'src\_ip', 'src\_port', 'dest\_ip', 'dest\_port', 'alert\_signature', 'alert\_category', 'alert\_severity', and 'followups'. The table displays 20 rows of data, with the first row highlighted in blue. The table is paginated, showing 'Row: 1 / Column: 3', 'Data Size: 5584 (+1584)', and 'Current Subset: 0-1000'. The cursor value is '2022-06-15T13:50:00'. The footer of the interface shows '2022 — www.derant.com'.

ts	src_ip	src_port	dest_ip	dest_port	alert_signature	alert_category	alert_severity	followups
2022-06-15T13:50:00	10.10.10.13	9217	52.98.149.104	443	ET JA3 Hash - [Abuse.ch] Possible Tofsee	Unknown Traffic	3	{files: nan, http_hostname: na...
2022-06-15T13:50:00	10.10.10.13	7483	104.94.26.91	80	ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent	Unknown Traffic	3	{files: [{"filename: "/hwink/", sid...
2022-06-15T13:50:00	10.10.10.13	7302	52.98.149.196	443	ET JA3 Hash - [Abuse.ch] Possible Tofsee	Unknown Traffic	3	{files: nan, http_hostname: na...
2022-06-15T13:50:01	10.10.10.13	1873	52.98.149.205	443	ET JA3 Hash - [Abuse.ch] Possible Tofsee	Unknown Traffic	3	{files: nan, http_hostname: na...
2022-06-15T13:50:01	10.10.10.13	20527	104.94.26.91	80	ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent	Unknown Traffic	3	{files: [{"filename: "/hwink/", sid...
2022-06-15T13:50:01	10.10.10.13	12077	52.98.149.189	443	ET JA3 Hash - [Abuse.ch] Possible Tofsee	Unknown Traffic	3	{files: nan, http_hostname: na...
2022-06-15T13:50:02	10.10.10.13	28712	52.98.149.140	443	ET JA3 Hash - [Abuse.ch] Possible Tofsee	Unknown Traffic	3	{files: nan, http_hostname: na...
2022-06-15T13:50:02	10.10.10.13	25469	104.94.26.91	80	ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent	Unknown Traffic	3	{files: [{"filename: "/hwink/", sid...
2022-06-15T13:50:02	10.10.10.13	863	52.98.149.129	443	ET JA3 Hash - [Abuse.ch] Possible Tofsee	Unknown Traffic	3	{files: nan, http_hostname: na...
2022-06-15T13:50:03	10.10.10.13	4960	52.98.149.172	443	ET JA3 Hash - [Abuse.ch] Possible Tofsee	Unknown Traffic	3	{files: nan, http_hostname: na...
2022-06-15T13:50:03	10.10.10.13	27764	52.98.149.113	443	ET JA3 Hash - [Abuse.ch] Possible Tofsee	Unknown Traffic	3	{files: nan, http_hostname: na...
2022-06-15T13:50:03	10.10.10.13	30887	104.94.26.91	80	ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent	Unknown Traffic	3	{files: [{"filename: "/hwink/", sid...
2022-06-15T13:50:04	10.10.10.13	22521	104.94.26.91	80	ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent	Unknown Traffic	3	{files: [{"filename: "/hwink/", sid...
2022-06-15T13:50:04	10.10.10.13	705	52.98.149.99	443	ET JA3 Hash - [Abuse.ch] Possible Tofsee	Unknown Traffic	3	{files: nan, http_hostname: na...
2022-06-15T13:50:04	10.10.10.13	6373	52.98.149.108	443	ET JA3 Hash - [Abuse.ch] Possible Tofsee	Unknown Traffic	3	{files: nan, http_hostname: na...
2022-06-15T13:50:05	10.10.10.13	4257	52.98.149.59	443	ET JA3 Hash - [Abuse.ch] Possible Tofsee	Unknown Traffic	3	{files: nan, http_hostname: na...
2022-06-15T13:50:05	10.10.10.13	14815	104.94.26.91	80	ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent	Unknown Traffic	3	{files: [{"filename: "/hwink/", sid...

The data in the table can be exported as a csv file using the download button just above the data table:

Shortcuts for creating filters, fetching data, customizing the data table etc. can be found using the shortcuts button just above the data table:

#### 3.1 Data Presentation

Angle will present a subset of 1000 rows of the full amount of available data. In the image above 5584 rows are available, but Angle has only loaded in the first 1000. Only in the unlikely event that a user wants to manually inspect more than a 1000 rows, Angle will fetch additional data. This way the time it takes to present data to the user is decreased. The total amount of data, as well as the current subset of data, is displayed just above the column header in the data table. Additionally the position of the cursor (relative to the full amount of data), and contents of the cell currently marked by the cursor is


also displayed.

Each column in a row will give some information about the data point. This information will vary across different log types, but will have some specific columns in common. Usually, for the logs containing internet traffic, there will be some basic information:

- Timestamp (ts) - The time and date on which the connection occurred.
- Source IP (src\_ip) - The IP address that initiated the connection.
- Source Port (src\_port) - The port on which the communication was sent on.
- Destination IP (dest\_ip) - The IP address that received the connection.
- Destination Port (dest\_port) - The port on which the connection was received.

These specific information might be named slightly differently in another log type, but for network traffic they should generally be there and be easily recognizable.

## 3.2 Table Settings

Customization of the data table is available, and allows the user to adjust the column order, width, and whether it should be visible or not. Column width is adjusted by pulling on the column separators in the header, or by hovering the column with the cursor and using the hotkeys "0" and "+". The order of the columns are arranged by placing the cursor on a column and moving it with the "8" and "9" keys. Finally, hiding and showing columns can be done in the menu for this, by clicking the following button: , or alternatively placing the cursor on a column and pressing the "h" button to toggle visibility.

Angle has default settings for the data table, which applies to all users who have not made their own customization. After saving the changes to the table, Angle will remember them for next time. Customizations apply only for the log type they have been created for. The first 3 buttons just above the table are used to interact with the table layout:

- ☒ Saves the current layout of the table for the current log type.
- ☒ Opens the menu for hiding and showing columns.
- ☒ Resets the table layout to the default layout in Angle.

## 4 Filters, Profiles and Baselining

Filters and profiles are an essential part of working with data in Angle, and specifically when creating a baseline for a network. Filters give a way of filtering (as the name suggests) the data in the table; zooming in on specific data of interest or removing insignificant rows. Multiple filters can be collected into a profile, that models the traffic that is expected to be seen from the host or the network. Below image shows a simple filter being applied on the data, zooming in on traffic going to 52.98.149.104 on port 443.

The screenshot shows the Derant Angle Data Analysis interface. At the top, there's a search bar with the filter query: `dest_ip = "52.98.149.104" AND dest_port = "443"`. Below the search bar, a table of traffic data is displayed. The table has columns for timestamp (ts), source IP (src\_ip), source port (src\_port), destination IP (dest\_ip), destination port (dest\_port), alert signature, alert category, alert severity, and leftovers. The data is filtered to show only traffic going to 52.98.149.104 on port 443. The table shows 16 rows of data, all with the same alert signature: "ET JA3 Hash - [Abuse.ch] Possible ToFsee".

ts	src_ip	src_port	dest_ip	dest_port	alert_signature	alert_category	alert_severity	leftovers
2022-06-15T13:50:00	10.10.10.13	9217	52.98.149.104	443	ET JA3 Hash - [Abuse.ch] Possible ToFsee	Unknown Traffic	3	{files: nan, http_hostname: na...
2022-06-15T13:56:25	10.10.10.13	17370	52.98.149.104	443	ET JA3 Hash - [Abuse.ch] Possible ToFsee	Unknown Traffic	3	{files: nan, http_hostname: na...
2022-06-15T14:04:38	10.10.10.13	28120	52.98.149.104	443	ET JA3 Hash - [Abuse.ch] Possible ToFsee	Unknown Traffic	3	{files: nan, http_hostname: na...
2022-06-15T14:05:53	10.10.10.13	31905	52.98.149.104	443	ET JA3 Hash - [Abuse.ch] Possible ToFsee	Unknown Traffic	3	{files: nan, http_hostname: na...
2022-06-15T14:08:08	10.10.10.13	2738	52.98.149.104	443	ET JA3 Hash - [Abuse.ch] Possible ToFsee	Unknown Traffic	3	{files: nan, http_hostname: na...
2022-06-15T14:08:26	10.10.10.13	3247	52.98.149.104	443	ET JA3 Hash - [Abuse.ch] Possible ToFsee	Unknown Traffic	3	{files: nan, http_hostname: na...
2022-06-15T14:11:43	10.10.10.13	25834	52.98.149.104	443	ET JA3 Hash - [Abuse.ch] Possible ToFsee	Unknown Traffic	3	{files: nan, http_hostname: na...
2022-06-15T14:12:16	10.10.10.13	27277	52.98.149.104	443	ET JA3 Hash - [Abuse.ch] Possible ToFsee	Unknown Traffic	3	{files: nan, http_hostname: na...
2022-06-15T14:14:27	10.10.10.13	22746	52.98.149.104	443	ET JA3 Hash - [Abuse.ch] Possible ToFsee	Unknown Traffic	3	{files: nan, http_hostname: na...
2022-06-15T14:14:28	10.10.10.13	4813	52.98.149.104	443	ET JA3 Hash - [Abuse.ch] Possible ToFsee	Unknown Traffic	3	{files: nan, http_hostname: na...
2022-06-15T14:14:13	10.10.10.13	7907	52.98.149.104	443	ET JA3 Hash - [Abuse.ch] Possible ToFsee	Unknown Traffic	3	{files: nan, http_hostname: na...
2022-06-15T14:17:06	10.10.10.13	22235	52.98.149.104	443	ET JA3 Hash - [Abuse.ch] Possible ToFsee	Unknown Traffic	3	{files: nan, http_hostname: na...
2022-06-15T14:17:32	10.10.10.13	25825	52.98.149.104	443	ET JA3 Hash - [Abuse.ch] Possible ToFsee	Unknown Traffic	3	{files: nan, http_hostname: na...
2022-06-15T14:19:52	10.10.10.13	1297	52.98.149.104	443	ET JA3 Hash - [Abuse.ch] Possible ToFsee	Unknown Traffic	3	{files: nan, http_hostname: na...
2022-06-15T14:20:13	10.10.10.13	26956	52.98.149.104	443	ET JA3 Hash - [Abuse.ch] Possible ToFsee	Unknown Traffic	3	{files: nan, http_hostname: na...
2022-06-15T14:20:21	10.10.10.13	23658	52.98.149.104	443	ET JA3 Hash - [Abuse.ch] Possible ToFsee	Unknown Traffic	3	{files: nan, http_hostname: na...

### 4.1 Filter Language

Writing a filter in Angle can be done either by free typing the text, or by using the hotkeys. Clicking the button: ☒ or pressing "f", switches between the two input methods. Shortcuts for creating filters with the hotkey method,

can be found using the shortcuts button just above the data table: . Below image shows an example of a filter created by typing the text freely.



---

```
NOT( id_resp_h = "194.187.99.236" AND id_resp_p = 9091 AND service = "ssl" )
```

---

A filter in Angle is much like an SQL statement. In fact it is the where-clause of the SQL statement where the **SELECT** columns and the **FROM** log type parts are handled by Angle and the user provides the filter:

```
SELECT columns FROM log type WHERE filter
```

Before a filter is applied it is validated by a parser. If the parser does not understand the filter it will not be applied, and an error message will occur. Filters are built up of comparisons on columns and logical operators. Comparisons have the column name on the left, operator in the middle and the value in quotes at the end:

```
column_name '⊗' "value"
```

The operator  $\otimes$  can be any of the following: =, >=, >, <=, <, <>, !=, LIKE. Multiple comparisons are put together using OR or AND, while NOT can negate. All this can be seen in the filter example above. For comparisons using LIKE, "%" is a wildcard matching zero or more characters and "\_" matches exactly one character. This can be useful for creating filters on ranges of IP addresses. Say we wanted to create a filter excluding all traffic going to an IP in the range 51.103.0.0 - 51.104.255.255:



```
NOT( id_resp_h LIKE "51.103.%" OR id_resp_h LIKE "51.104.%" )
```

Another example could be to create a filter fetching all traffic coming from a local IP address in the range 10.0.0.0 - 10.255.255.255, and going to another local IP address in the range 192.168.0.20 - 192.168.0.29:

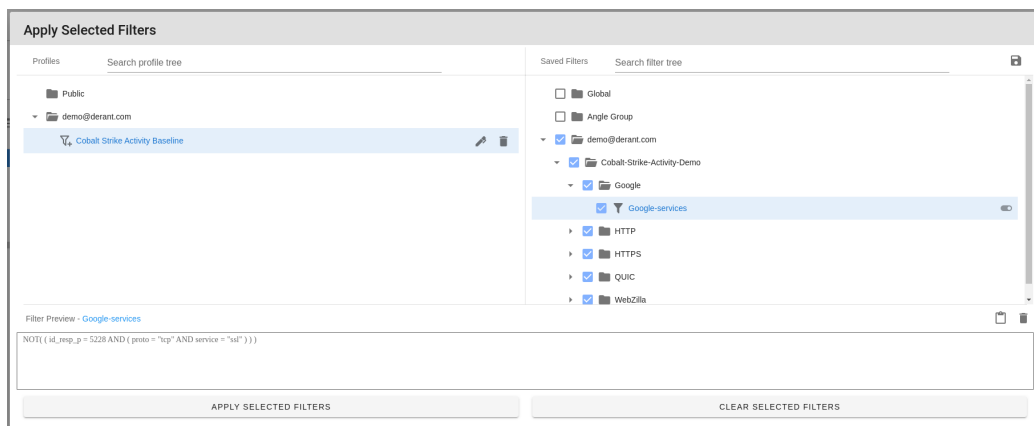
```
id_orig_h LIKE 10.% AND id_resp_h LIKE "192.168.0.2_"
```



## 4.2 Saved Filter


Filters can be saved for later use, as well as shared within the company or even with your associated group. They are saved only for one log type. Clicking "s" or  above the filter will save the current filter. An overview (as below) of all the available filters can be found by clicking "F" or using the  button above the filter. On the right side of the overview the filters are displayed, and separated into 3 main folders:

- Global - Filters shared with everyone, created only by Derant.
- Group - Filters created by and shared with companies within the group.
- Company - Filters created by and shared with users within the company.



When saving a filter first thing to do is select either you company folder, or group folder. Then the path of the filter should be specified. Forward slash is used to separate folders, making the last part of the path the actual name of the filter. Say we want to save the Google-services filter in the company folder of demo@derant.com under the sub folders seen in the image above. We then select demo@derant.com as the folder, and specify Cobalt-Strike-Activity-Demo/Google/Google-services as the path.

## 4.3 Applying Filters

In the simplest form a filter can be applied directly from the filter input box, indicated by the blue  icon in the image below. When the filter is

inactive, the icon will change to ✖. Filters in the filter box can also be applied temporarily, without saving the filter by clicking 🚩. One such filter is applied in the example below, named Temp Filter 1, and hovered over to show the actual filter. Applying saved filters will show as their names in a blue oval just above the filter box.

The screenshot shows a log viewer interface. At the top, there are four filter buttons: "Google-services", "QUIC-Generic", "WebZilla-ssl", and "Temp Filter 1". Below these is a filter box containing the query: `NOT(( id_resp_p = 443 AND proto = "tcp" ))`. A tooltip for "Temp Filter 1" shows the query: `NOT(( id_resp_p = 80 AND proto = "tcp" ))`. Below the filter box is a table with the following columns: Log\_Type, ts, id\_orig\_h, id\_orig\_p, id\_resp\_h, id\_resp\_p, proto, and service. The table contains five rows of log entries.

Log_Type	ts	id_orig_h	id_orig_p	id_resp_h	id_resp_p	proto	service
conn	2022-06-15T14:02:33	10.10.10.13	52444	193.162.153.164	53	udp	dns
conn	2022-06-15T14:02:43	10.10.10.13	8	204.79.197.200	0	icmp	
conn	2022-06-15T14:08:21	10.10.10.13	52617	74.124.193.14	8080	tcp	
conn	2022-06-15T14:08:31	10.10.10.13	52617	74.124.193.14	8081	tcp	
conn	2022-06-15T14:08:42	10.10.10.13	52617	74.124.193.14	9080	tcp	

When multiple filters are applied, whether it is current, temporary or saved filters, they are combined with the AND logical operator. This is important to note, in order to understand what data is being shown in the table. One pitfall is to create two filters selecting one specific thing each. In example:

Filter 1: `id_resp_h = "193.162.153.164"`

Filter 2: `id_resp_h = "204.79.197.200"`

Applying both Filter 1 and Filter 2 separately will give no results as they are combined with AND, and no rows have both IP addresses as the responding host.

## 4.4 Profiles

Filters can be collected into profiles, and saved for later use. A profile works only for a single log type, just as filters. An overview of the profiles can be found along side the filters by clicking "F" or using the 📁 button above the filter. Profiles are shared with the company, and can be used and edited by users within this company. Hovering a filter profile will indicate what filters

it contains, while clicking it will select the filters for application. Profiles are commonly used to model the traffic in hosts and networks, also known as baselining.

## 4.5 Baselining

Building a baseline is to define what traffic is legitimate and usually seen in the network or on one host. In order to do this a good amount of sample data is needed. The more available data, the more complete of a baseline.

First step towards building a baseline in Angle is to create filters that remove legitimate traffic. This could be traffic from Google-Playstore, A mail server, a known ssh connection, and much more. Once left with only traffic that is suspicious, collect all the filters into a profile. This profile now works as the baseline, but only for one log type. It is a good idea to test the baseline on data that it was not built on. In example, if a baseline is built using traffic from the month of June, testing should be done with data from July and onwards.

Finally, when the baseline is built and tested, create a trigger using this profile. Angle will then periodically apply the filters/profile to the new incoming data, and create alerts on anything that is not accounted for: these are called anomalies.