

# TOP SECRET STRAP 1

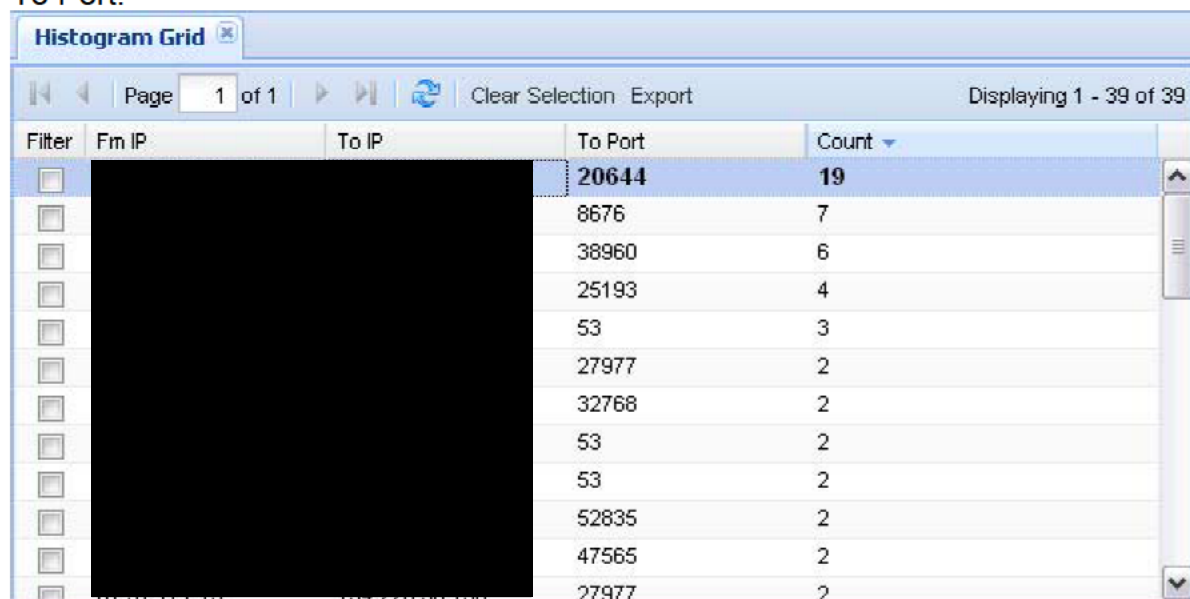
## XKEYSCORE HELPER NOTES

There are several new and updated features in this release of the XKEYSCORE Palantir helper:

- Summary/Histogram import of data
- Data sourcing for XKEYSCORE queries
- Fixes for UI redraw bugs on query list refresh
- Fixes for disappearing links

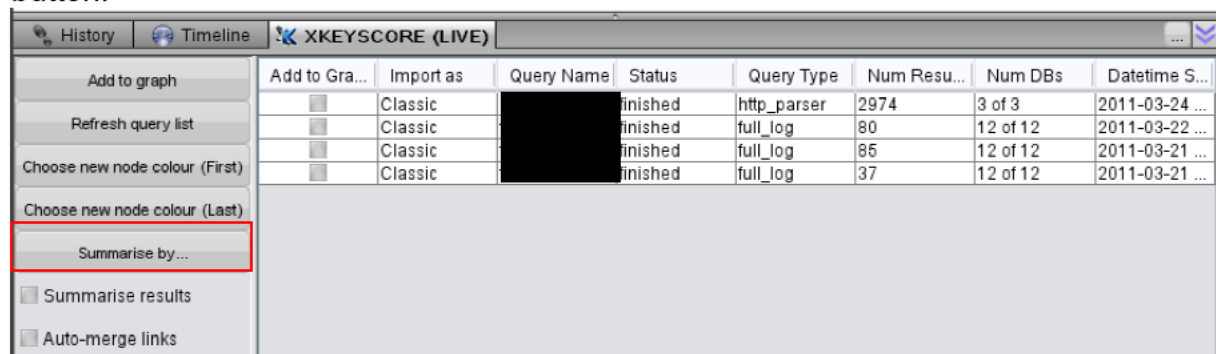
### Summary import

This feature is intended to mirror the functionality in XKEYSCORE for creating histogram grids over a query. It allows for a large dataset to be reduced down in size considerably while still maintaining useful data. As an example this is a histogram grid view over a small query in XKEYSCORE, histogrammed by From IP, To IP and To Port:



Filter	From IP	To IP	To Port	Count
<input type="checkbox"/>			20644	19
<input type="checkbox"/>			8676	7
<input type="checkbox"/>			38960	6
<input type="checkbox"/>			25193	4
<input type="checkbox"/>			53	3
<input type="checkbox"/>			27977	2
<input type="checkbox"/>			32768	2
<input type="checkbox"/>			53	2
<input type="checkbox"/>			53	2
<input type="checkbox"/>			52835	2
<input type="checkbox"/>			47565	2
<input type="checkbox"/>			27977	2

As you can see, there are 19 entries for the top line here. In the old XKEYSCORE helper this would create 19 new events. While you still have the option of importing every row in an XKEYSCORE query as a new connection, the summary import lets you cut this down a little. Once logged in to the helper, choose the “Summarise by...” button:

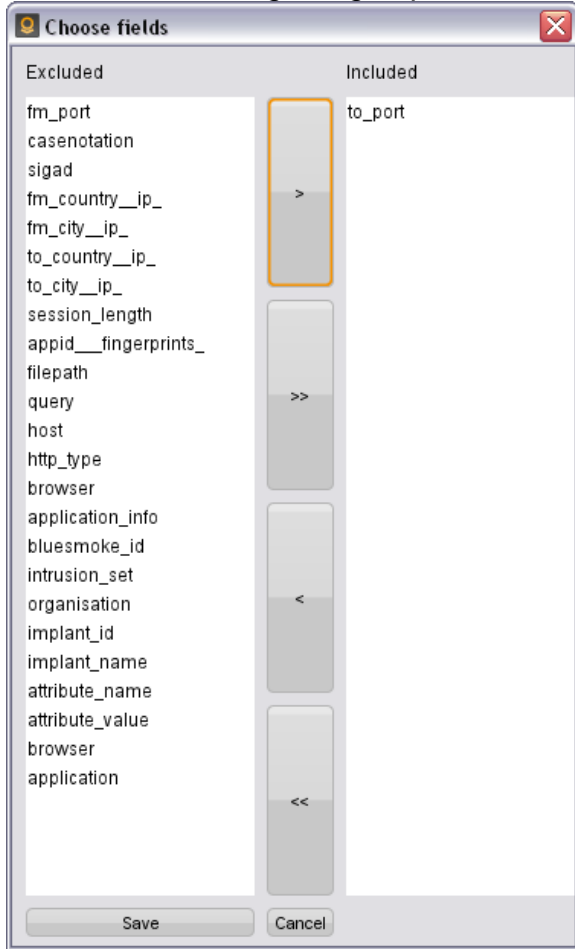


Add to Gra...	Import as	Query Name	Status	Query Type	Num Resu...	Num DBs	Datetime S...
<input type="checkbox"/>	Classic		inished	http_parser	2974	3 of 3	2011-03-24 ...
<input type="checkbox"/>	Classic		inished	full_log	80	12 of 12	2011-03-22 ...
<input type="checkbox"/>	Classic		inished	full_log	85	12 of 12	2011-03-21 ...
<input type="checkbox"/>	Classic		inished	full_log	37	12 of 12	2011-03-21 ...

Summarise by...

# TOP SECRET STRAP 1

To mirror the histogram grid performed on the data, I've chosen to include to\_port:



Note that when doing a summary import, summarisations will be done on source and destination IP in addition to any included fields.

# TOP SECRET STRAP 1

The screenshot shows the Graph application interface. The main window displays a network diagram with two nodes (represented by fingerprint icons) connected by a central link. The link is highlighted in yellow, indicating it is the current selection. The right-hand side of the interface contains a properties panel for the selected connection. The properties panel includes a histogram view, a selection list, and a table of properties. The properties table is as follows:

Type	Value	Classification
Application	P2p/BitTorrent	TS STRAP1
Application	P2p/BitTorrent	TS STRAP1
IP Address (From)	[Redacted]	TS STRAP1
IP Address (To)	[Redacted]	TS STRAP1
Port (To)	20004	TS STRAP1
Quantity	19	TS STRAP1
Session Size	1754 B	TS STRAP1

Below the properties panel, there are sections for Related Entities, Related Documents, and Recent History. The bottom of the interface shows a query history table with columns for Query Name, Status, Query Type, Num Rows, Num DBs, and Date/Time. The table contains three rows of query results.

In this example, I removed all the other data from the input from the graph.

There are a few things to note from the results of this import:

- Quantity records the number of results which matched that histogram criteria (In this case 19). This matches up with the XKEYSCORE histogram grid
- Session size is a sum of all session sizes for this histogrammed piece of data. This allows you to see the total amount of data being sent from one IP to another, in this case also summarised by destination port.
- "Application" shows the different fingerprints hit on for this summary event. For example, if X contacts Y and it is picked up by fingerprints foo on connection 1 and bar on connection 2, the summarised connection between X and Y will list "foo" and "bar" as applications
- Time metadata is preserved in that you can view the first time this event occurred and the last.

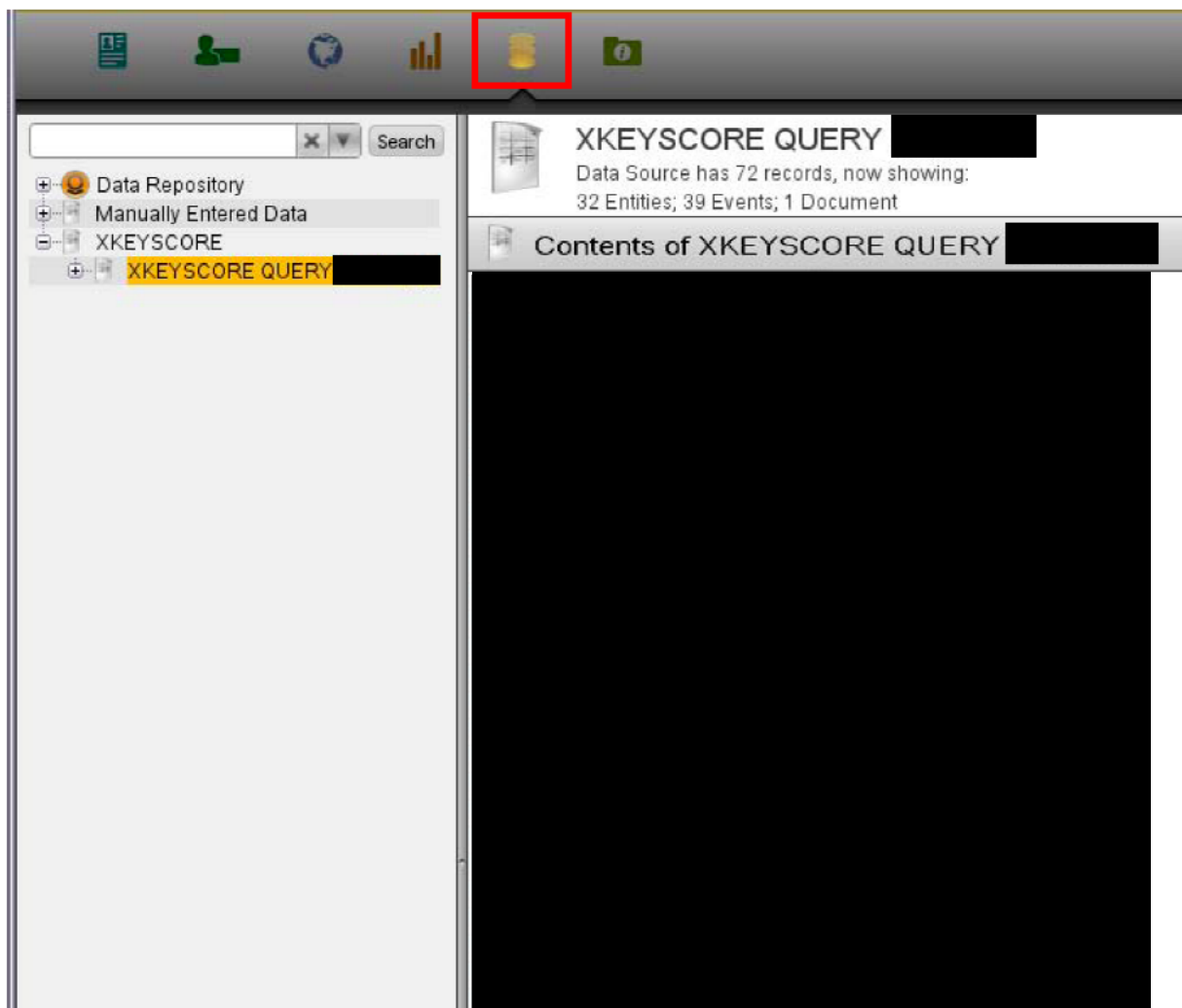
# TOP SECRET STRAP 1

Preferences for which fields to summarise by, whether you wish to summarise and whether you wish to automatically merge links between IP addresses and connections are saved per-user, so if you have a common histogram import then you don't need to re-select the fields to histogram on every time.

## Data sourcing

Data imported into Palantir using the updated XKEYSCORE helper now has data sourcing.

There are a couple of places this can be seen, the most evident is the "Data sources" application within Palantir. So, when you open up Data Sourcing:



At the top level in this screenshot you can see there are three folders. The XKEYSCORE folder contains a list of the IP addresses and connection events associated with the query. Double clicking the document within this datasource opens up some metadata about the query run.

# TOP SECRET STRAP 1

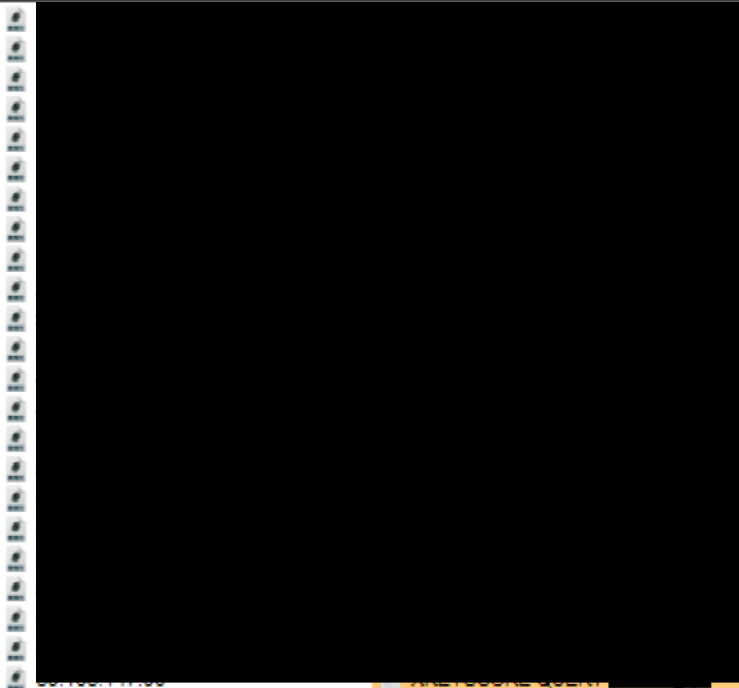


## XKEYSCORE QUERY [REDACTED]

Data Source has 72 records, now showing:  
32 Entities; 39 Events; 1 Document



## Contents of XKEYSCORE QUERY [REDACTED]




194.226.58.130 to 192... x XKEYSCORE QUERY [REDACTED] x




back fwd graph map search extract export +font -font shot prev next add showhide find+tag opts

**TS STRAP1**

Hide Summary



XKEYSCORE QUERY [REDACTED]

Related	Object Info	Who's Watching This?
 0	Type: Document Created by: Administrator Account Created at: 2011/03/25 12:31:36 +00:00 Classification: <a href="#">TS STRAP1</a>	No watchers <a href="#">watch this object</a>
 0		
 0		

Document Properties Related

## XKEYSCORE QUERY [REDACTED]

Datetime: 2011-03-21 13:18:35  
Output: [REDACTED]  
Query name: [REDACTED]  
DBs: 12 of 12  
Hits: 85  
Status: 100%

# TOP SECRET STRAP 1

This information can also be accessed via an object imported into Palantir:

The screenshot shows the Palantir interface for an object named 'TS STRAP1'. The object is a 'Connection' type, created by the 'Administrator Account' on 2011/03/25 12:31:42 +00:00. It covers the date range from 2011/03/21 05:29:58.000 +00:00 to 2011/03/21 08:44:57.000 +00:00. The 'Properties' section lists several attributes, with 'Session Size' highlighted in yellow, showing a value of 1764 B. The 'Data Sources' section, highlighted with a red box, shows a single data source: '(1) XKEYSCORE QUERY (carloso\_1) TS STRAP1'. The interface also includes tabs for 'Summary', 'Properties', 'Related', 'Notes & Media', and 'History', and a 'Basic Info' section with fields for 'Type', 'Label', 'Date Range', and 'Location'.

After multiple imports of XKEYSCORE data have been done within the same investigation the list of data sources also grows appropriately:

The screenshot shows the 'Data Sources' panel in Palantir, titled 'Data Sources - Administrator Account 03/25/2011 12:02 GMT'. The panel displays a list of data sources under the 'XKEYSCORE' category. The list includes 'XKEYSCORE QUERY' followed by a redacted name, and another 'XKEYSCORE QUERY' followed by another redacted name. The interface includes a search bar and navigation icons for 'Investigation', 'Edit', 'Preferences', 'Windows', and 'Help'.