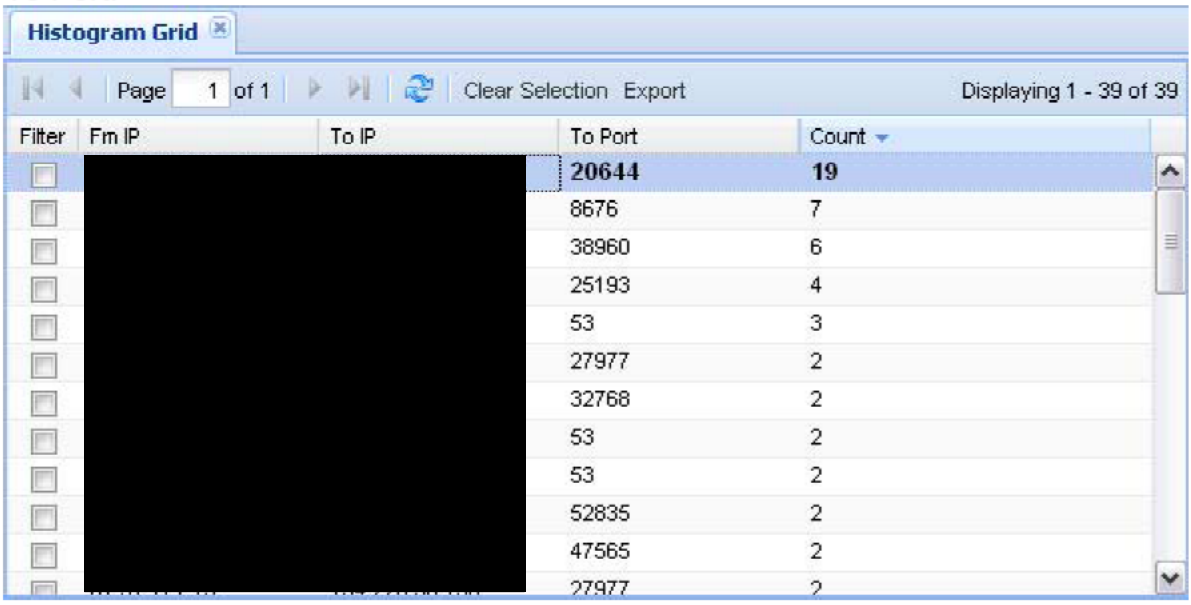
XKEYSCORE HELPER NOTES

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

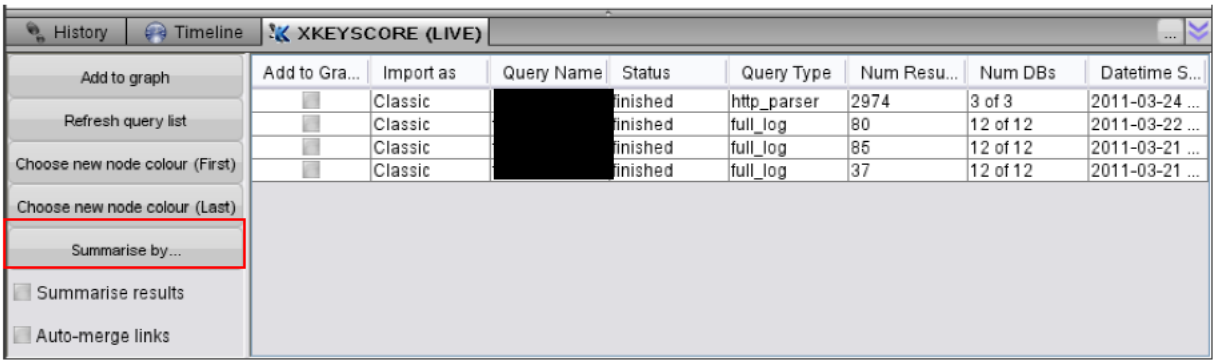
- Summary/Histogram import of data
- Data sourcing for XKEYSCORE queries
- Fixes for UI redraw bugs on query list refresh
- Fixes for disappearing links

Summary import

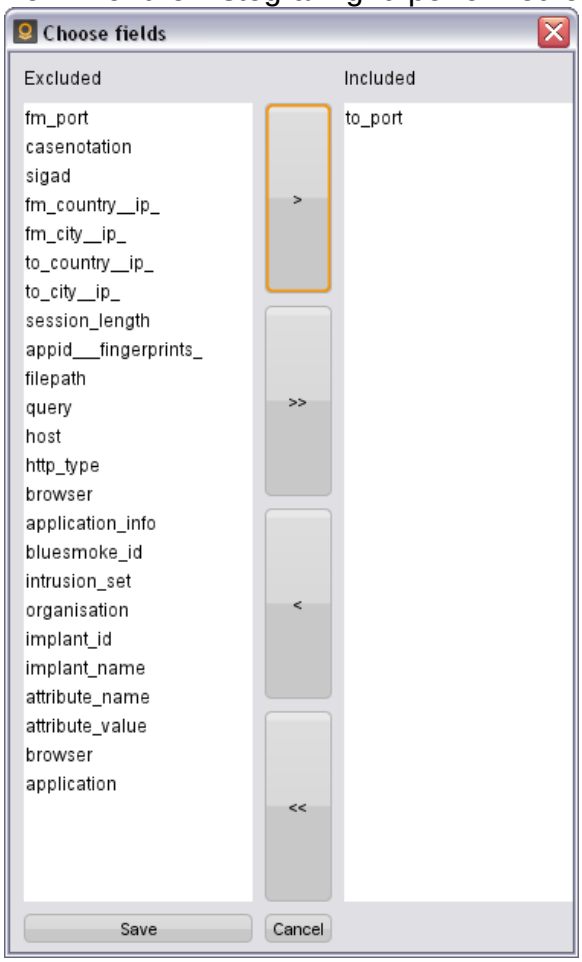
This feature is intended to mirror the functionality in XKEYSCORE for creating histogram grids over a query. It allows for a large dataset to be reduced down in size considerably while still maintaining useful data. As an example this is a histogram grid view over a small query in XKEYSCORE, histogrammed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



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:

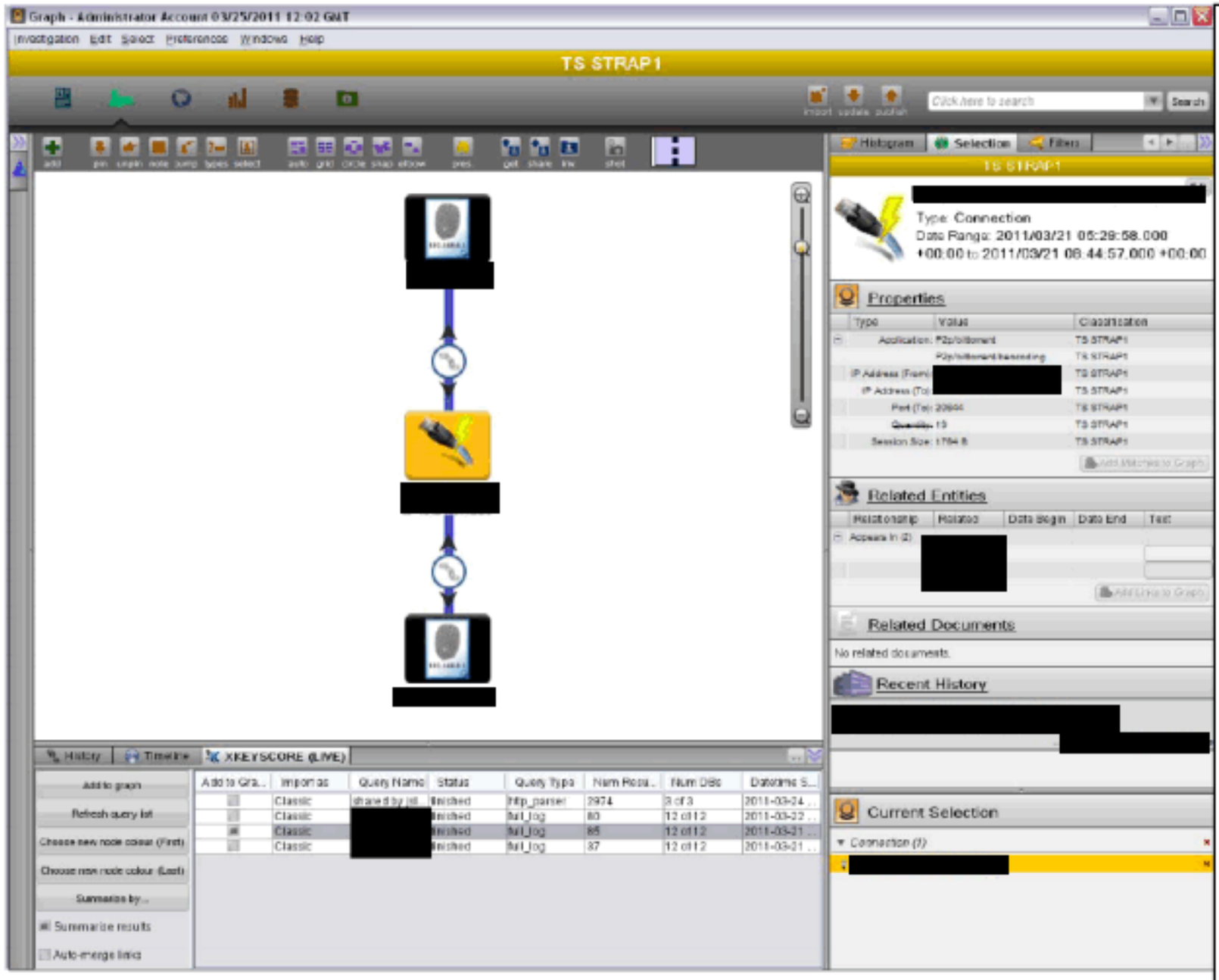


To mirror the histogram grid performed on the data, I've chosen to include to_port:



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

[redacted]



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:

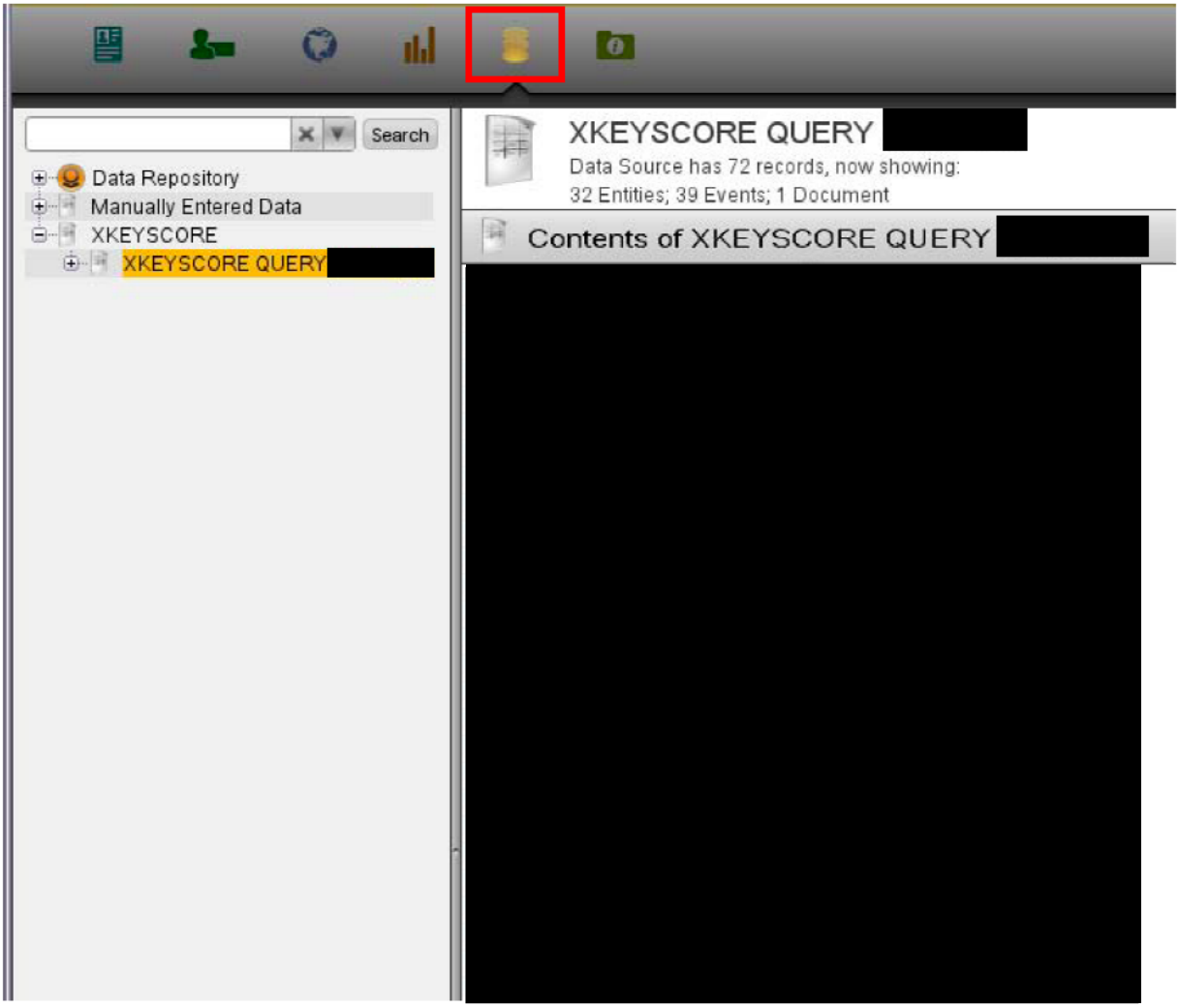
- Quantity records the number of results which matched that histogram criteria (In this case 19). This matches up with the XKEYSCORE histogram grid
- Session size is a sum of all session sizes for this histogrammed piece of data. This allows you to see the total amount of data being sent from one IP 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.

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.

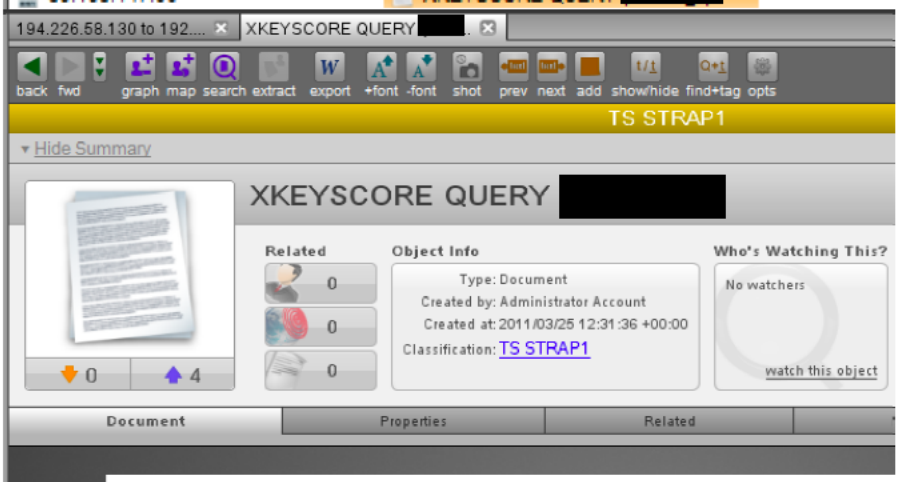
[redacted]

XKEYSCORE QUERY [redacted]

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

Contents of XKEYSCORE QUERY [redacted]

[redacted]

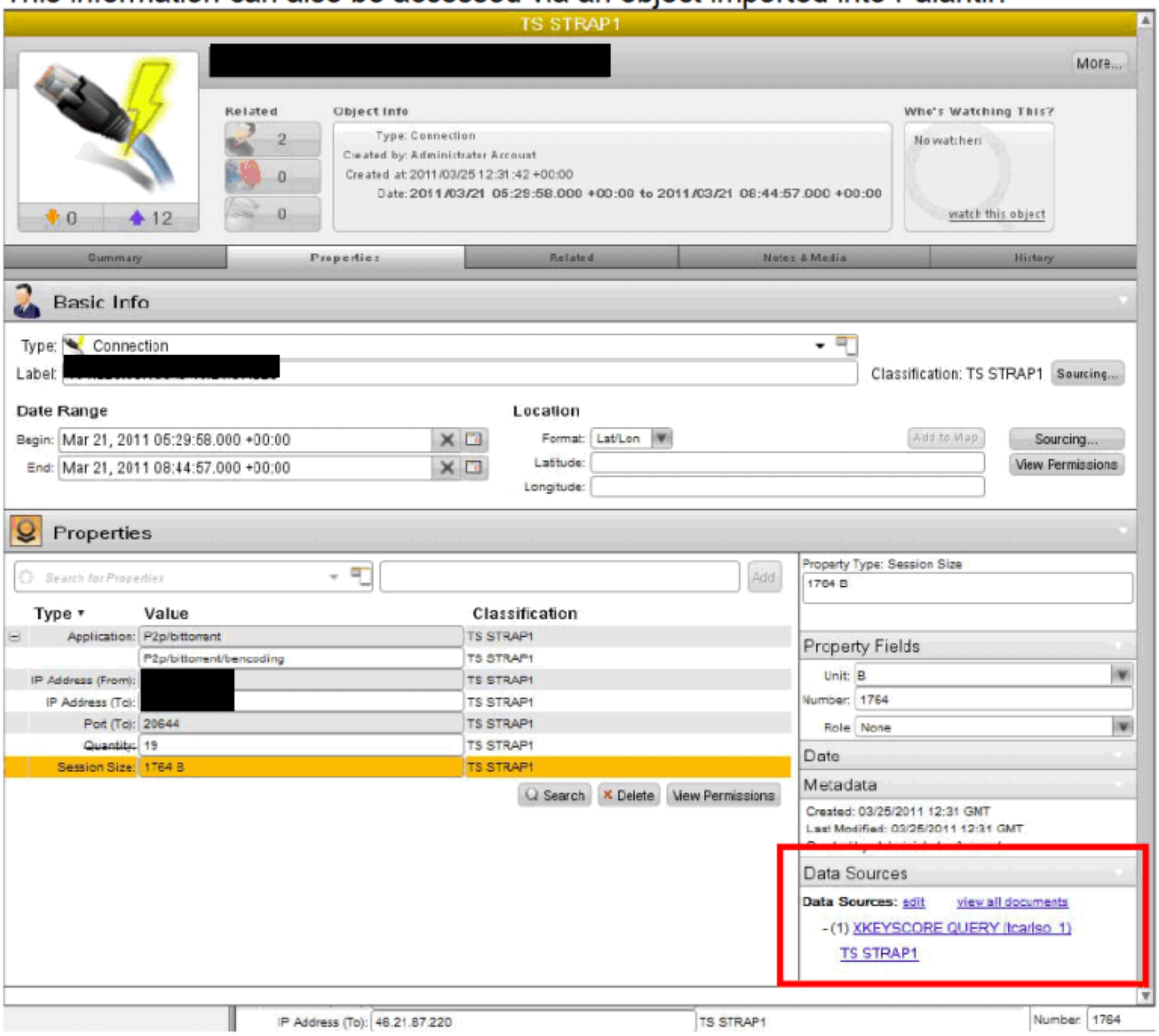


XKEYSCORE QUERY [redacted]

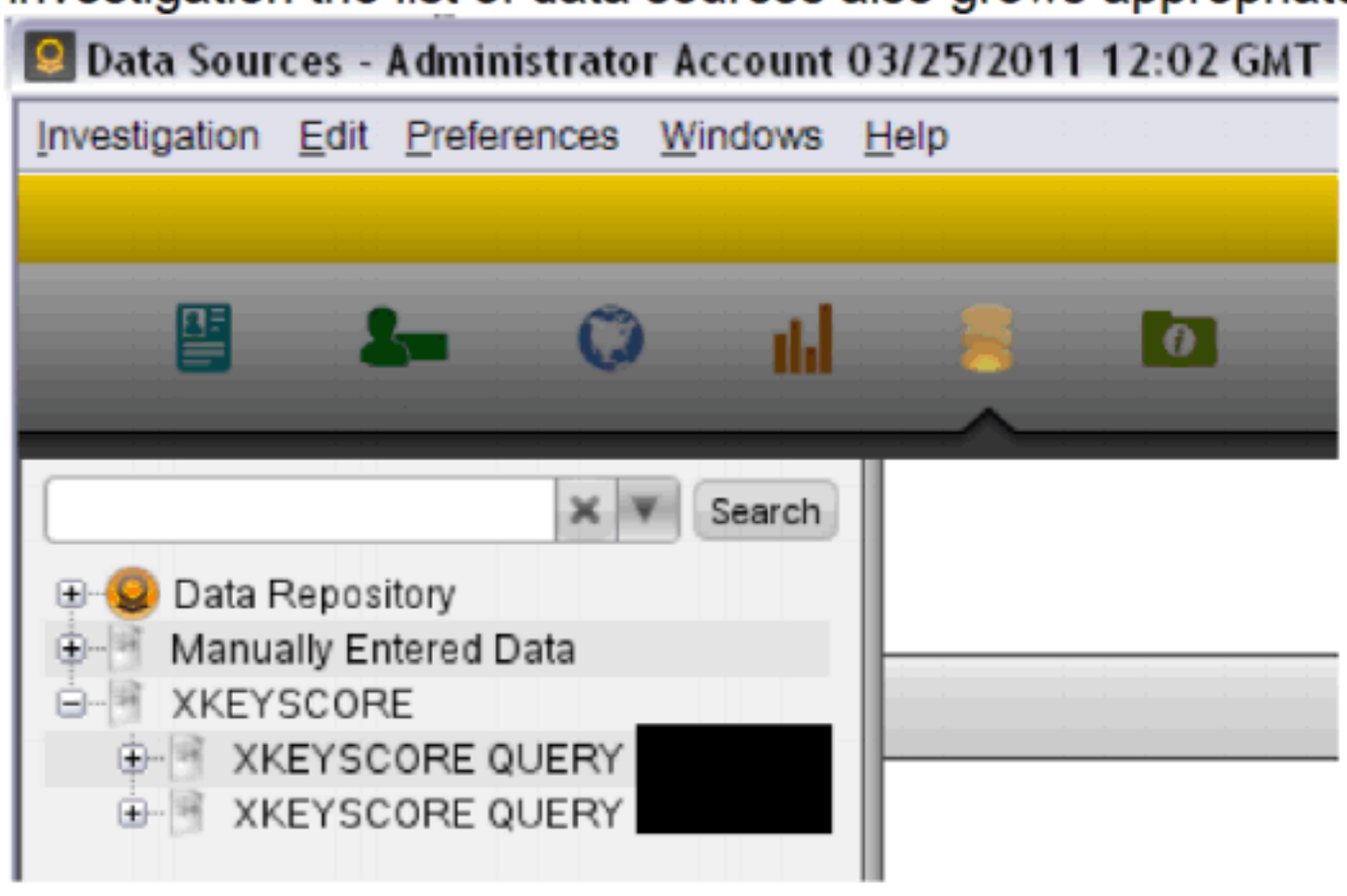
Datetime: 2011-03-21 13:18:35
Output: [redacted]
Query name: [redacted]
DBs: 12 of 12
Hits: 85
Status: 100%

[redacted]

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



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



[redacted]