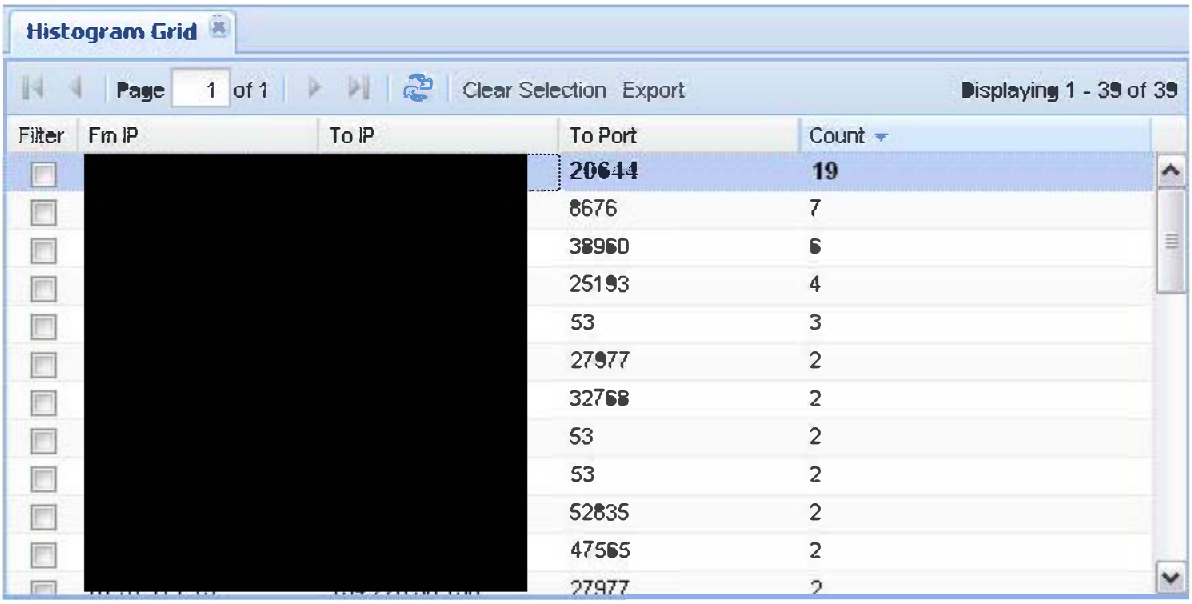
XKEYSCORE HELPER NOTES

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

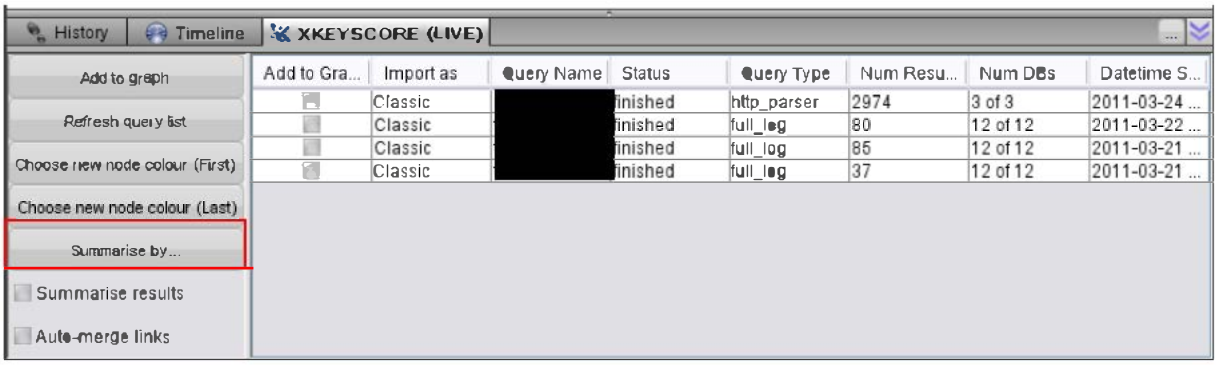
Summary import

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	Frn IP	To IP	To Port	Count
☐	[redacted]	[redacted]	20644	19
☐	[redacted]	[redacted]	8676	7
☐	[redacted]	[redacted]	38960	6
☐	[redacted]	[redacted]	25193	4
☐	[redacted]	[redacted]	53	3
☐	[redacted]	[redacted]	27977	2
☐	[redacted]	[redacted]	32768	2
☐	[redacted]	[redacted]	53	2
☐	[redacted]	[redacted]	53	2
☐	[redacted]	[redacted]	52835	2
☐	[redacted]	[redacted]	47565	2
☐	[redacted]	[redacted]	27977	2

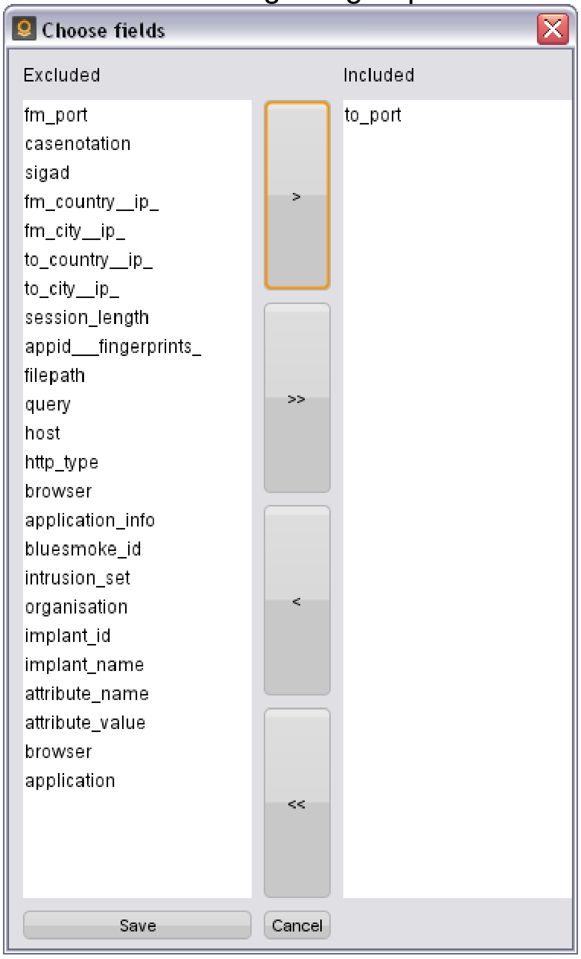
As you can see, there are 19 entries for the top line here. In the old XKEYSCORE helper this would create 19 new events. While you still have the option of importing every row in an XKEYSCORE query as a new connection, the summary import lets you cut this down a little. Once logged in to the helper,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



Add to Gra...	Import as	Query Name	Status	Query Type	Num Resu...	Num DBs	Datetime S...
☐	Classic	[redacted]	inished	http_parser	2974	3 of 3	2011-03-24 ...
☐	Classic	[redacted]	inished	full_log	80	12 of 12	2011-03-22 ...
☐	Classic	[redacted]	inished	full_log	85	12 of 12	2011-03-21 ...
☐	Classic	[redacted]	inished	full_log	37	12 of 12	2011-03-21 ...

[redacted]

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



Excluded

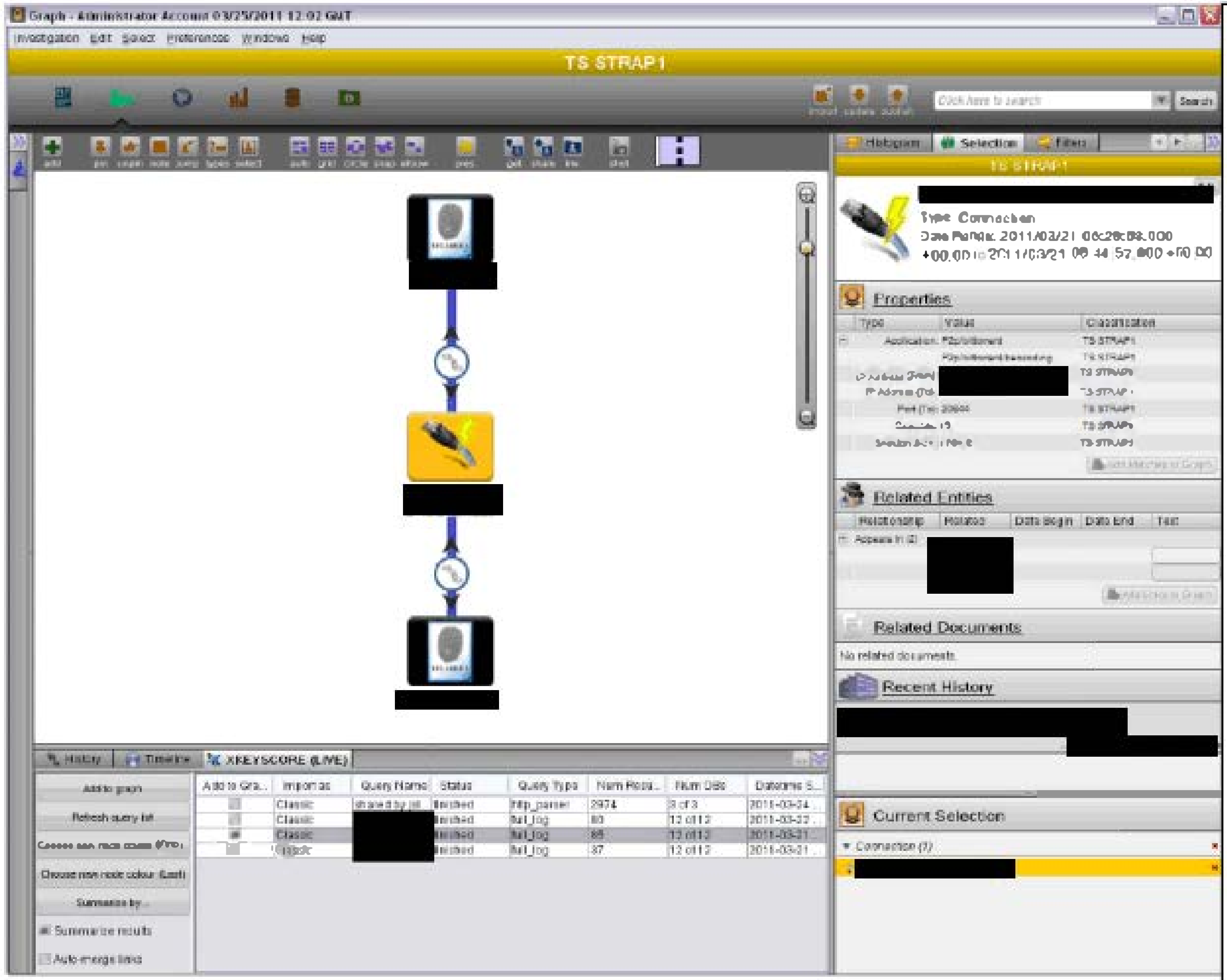
fm_port
casenotation
sigad
fm_country__ip_
fm_city__ip_
to_country__ip_
to_city__ip_
session_length
appid___fingerprints_
filepath
query
host
http_type
browser
application_info
bluesmoke_id
intrusion_set
organisation
implant_id
implant_name
attribute_name
attribute_value
browser
application

Included

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]



Graph - Administrator Account 03/25/2011 12:02 GMT

Investigation Edit Select Preferences Windows Help
TS STRAP1
Import Update Submit
Click here to search
Search
Histogram Selection Filters
TS STRAP1

[redacted]

Type: Connection
Date Range: 2011/03/21 06:28:08.000 +00:00 to 2011/03/21 08:44:57.000 +00:00

Properties

Type	Value	Classification
Application	P2p/bittorrent	TS STRAP1
	P2p/bittorrent/seeding	TS STRAP1
IP Address (From)	[redacted]	TS STRAP1
IP Address (To)	[redacted]	TS STRAP1
Port (To)	20000	TS STRAP1
Quantity	19	TS STRAP1
Session Size	[illegible]	TS STRAP1

Related Entities

Relationship	Related	Date Begin	Date End	Text
Appears In (2)	[redacted]			

Related Documents

No related documents.

Recent History

[redacted]

Current Selection

Connection (1)

[redacted]

History Timeline XKEYSCORE (LIVE)
Add to graph
Refresh query list
Choose new node colour (From)
Choose new node colour (Last)
Summarise by...
Summarise results
Auto-merge links

Add to Gra...	Import as	Query Name	Status	Query Type	Num Reco...	Num DBs	Datetime S...
☐	Classic	shared by [illegible]	finished	http_parser	2974	3 of 3	2011-03-24 ...
☐	Classic	[redacted]	finished	full_log	80	12 of 12	2011-03-22 ...
☑	Classic	[redacted]	finished	full_log	85	12 of 12	2011-03-21 ...
☐	Classic	[redacted]	finished	full_log	37	12 of 12	2011-03-21 ...

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 "too" and "bar" as applications
- Time metadata is preserved in that you can view the first time this event occurred and the last.

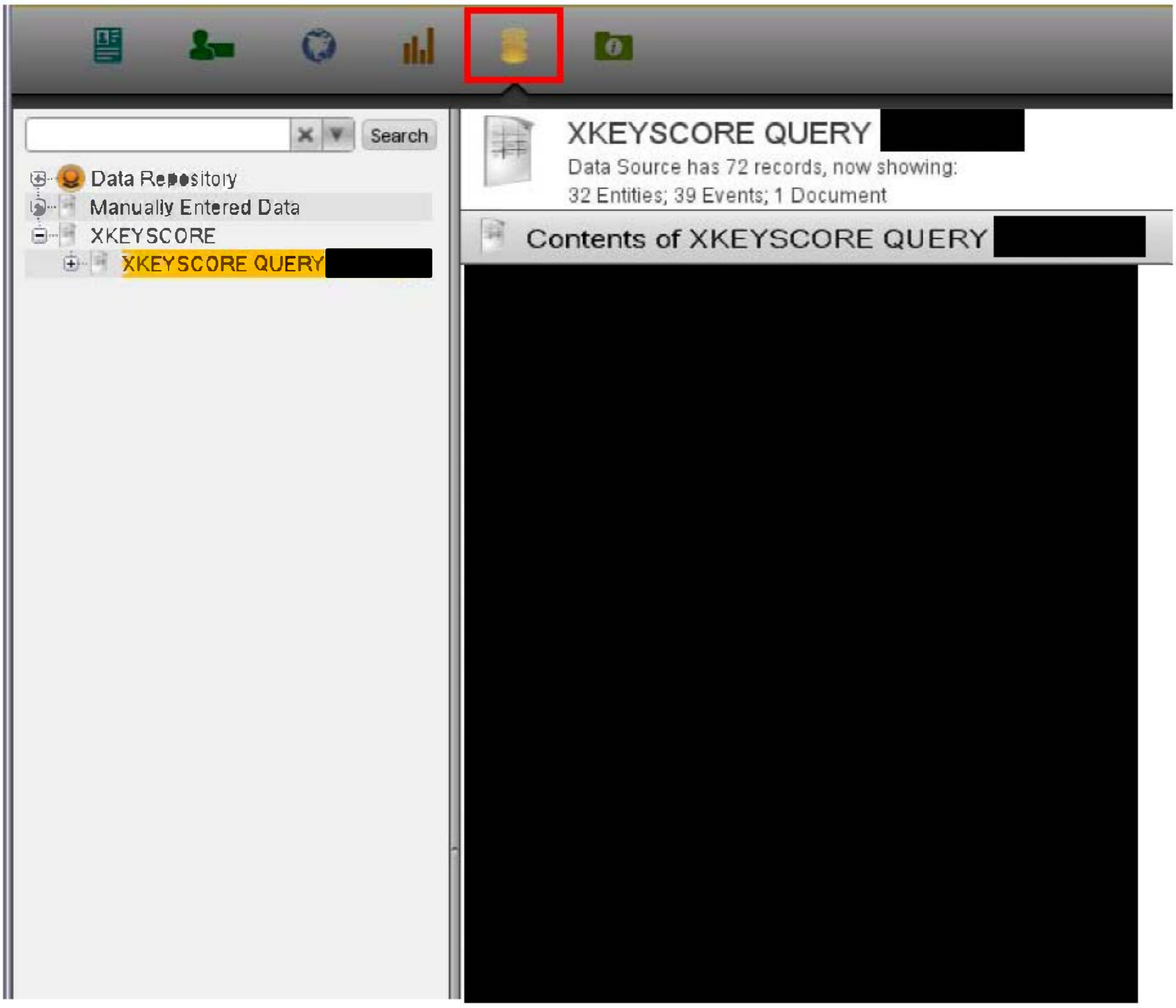
[redacted]

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:



Data Repository
Manually Entered Data
XKEYSCORE
XKEYSCORE QUERY [redacted]

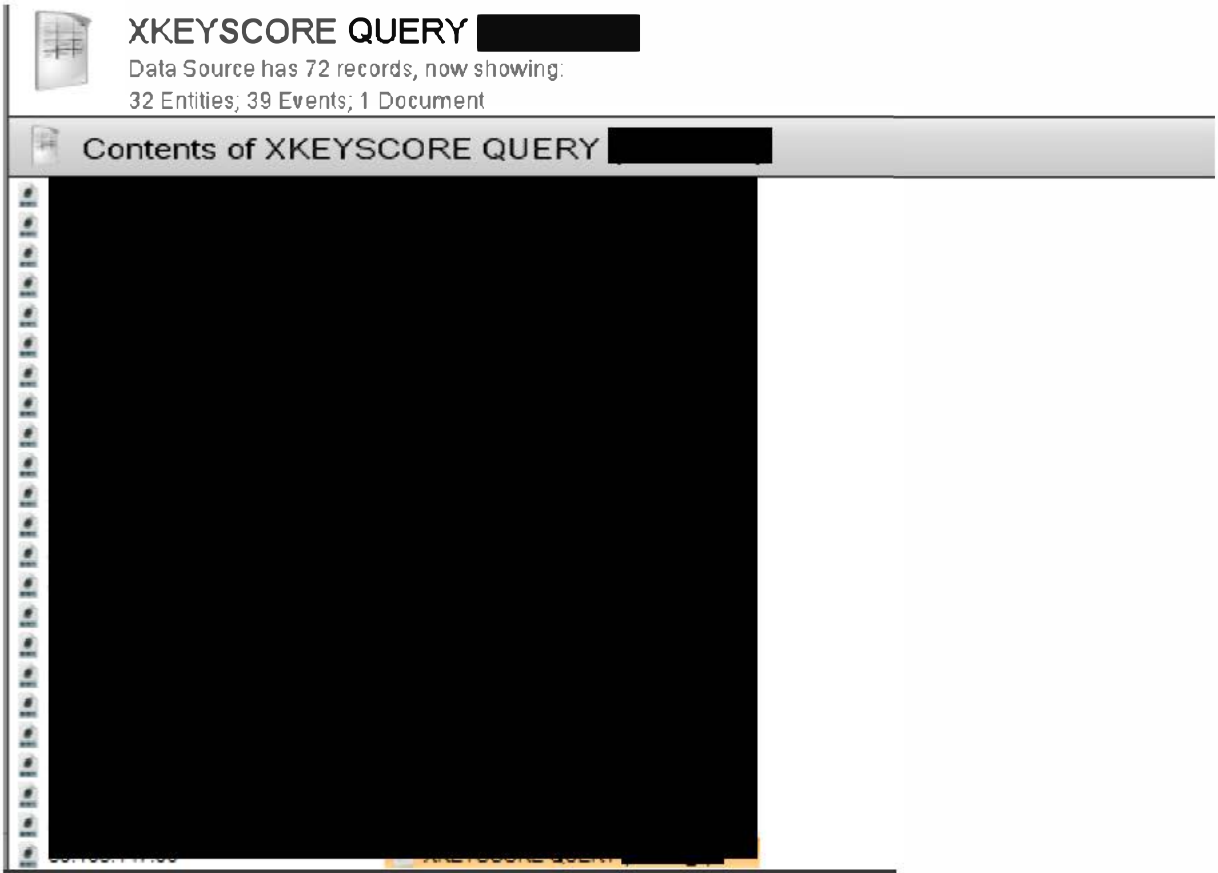
XKEYSCORE QUERY [redacted]
Data Source has 72 records, now showing:
32 Entities; 39 Events; 1 Document

Contents of XKEYSCORE QUERY [redacted]

[redacted]

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]

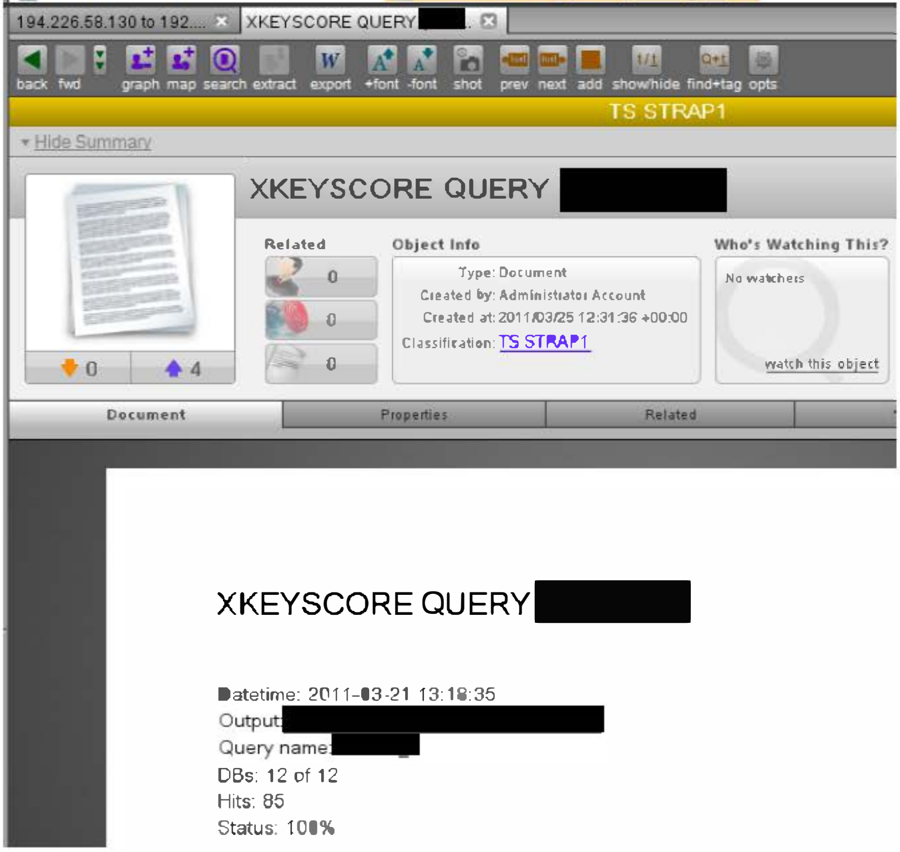


XKEYSCORE QUERY [redacted]

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

Contents of XKEYSCORE QUERY [redacted]

[redacted]



XKEYSCORE QUERY [redacted]

Related

0
0
0

0 4

Object Info

Type: Document
Created by: Administrator Account
Created at: 2011/03/25 12:31:36 +00:00
Classification: TS STRAP1

Who's Watching This?

No watchers

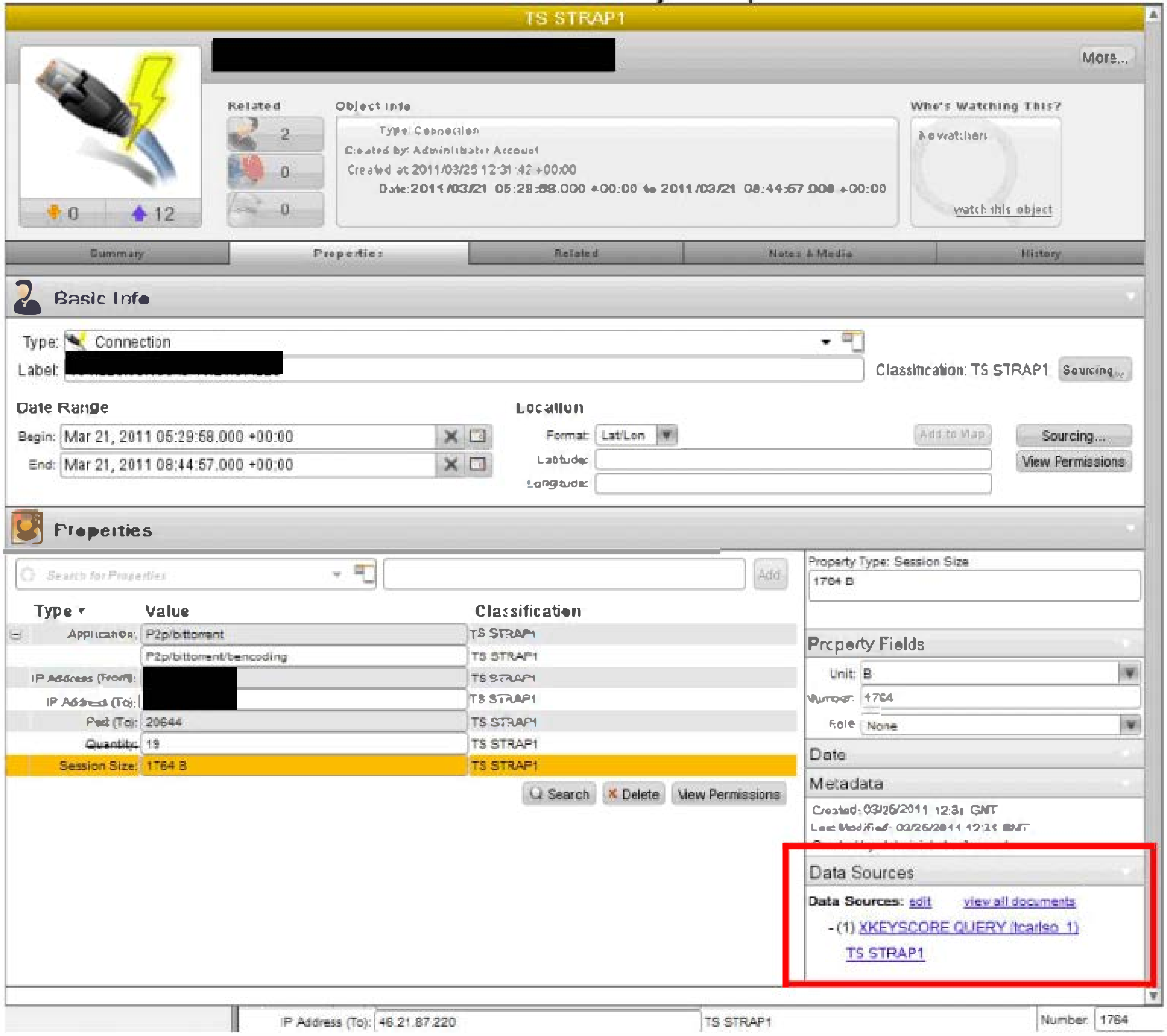
watch this object

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:



TS STRAP1

[redacted]

Object Info

Type: Connection
Created by: Administrator Account
Created at 2011/03/25 12:31:42 +00:00
Date: 2011/03/21 05:29:58.000 +00:00 to 2011/03/21 08:44:57.000 +00:00

Who's Watching This?

No watchers

Basic Info

Type: Connection

Label: [redacted]

Classification: TS STRAP1

Date Range

Begin: Mar 21, 2011 05:29:58.000 +00:00

End: Mar 21, 2011 08:44:57.000 +00:00

Location

Format: Lat/Lon

Latitude:

Longitude:

Properties

Type	Value	Classification
Application:	P2p/bittorrent	TS STRAP1
	P2p/bittorrent/bencoding	TS STRAP1
IP Address (From):	[redacted]	TS STRAP1
IP Address (To):	[redacted]	TS STRAP1
Port (To):	20644	TS STRAP1
Quantity:	19	TS STRAP1
Session Size:	1764 B	TS STRAP1

Property Type: Session Size

1764 B

Property Fields

Unit: B

Number: 1764

Role: None

Date

Metadata

Created: 03/25/2011 12:31 GMT

Last Modified: 03/25/2011 12:31 GMT

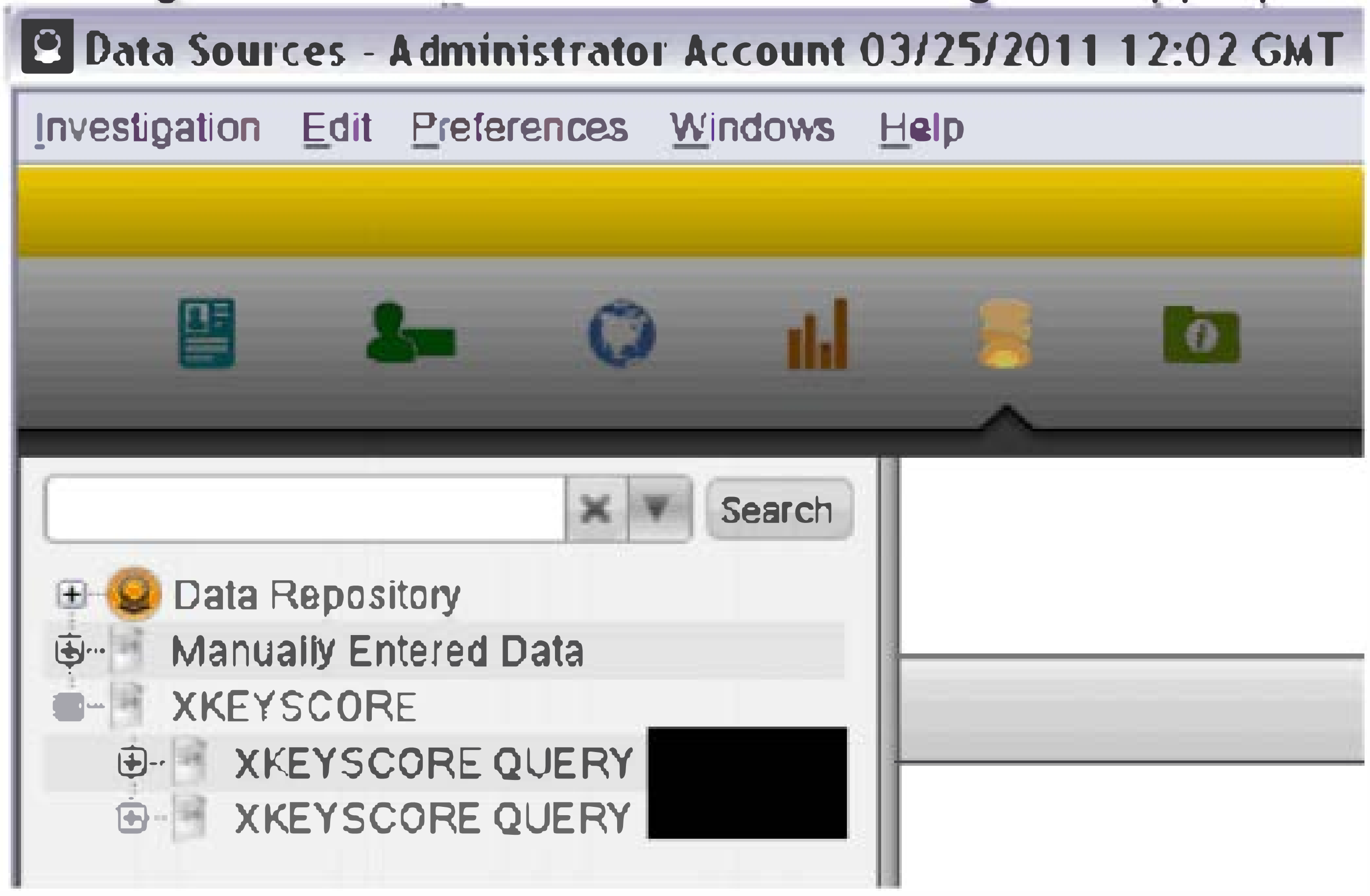
Data Sources

Data Sources: edit view all documents

- (1) XKEYSCORE QUERY (tcarlso_1)
  TS STRAP1

IP Address (To): 46.21.87.220 TS STRAP1 Number: 1764

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



Data Sources - Administrator Account 03/25/2011 12:02 GMT

- Data Repository
- Manually Entered Data
- XKEYSCORE
  - XKEYSCORE QUERY [redacted]
  - XKEYSCORE QUERY

[redacted]