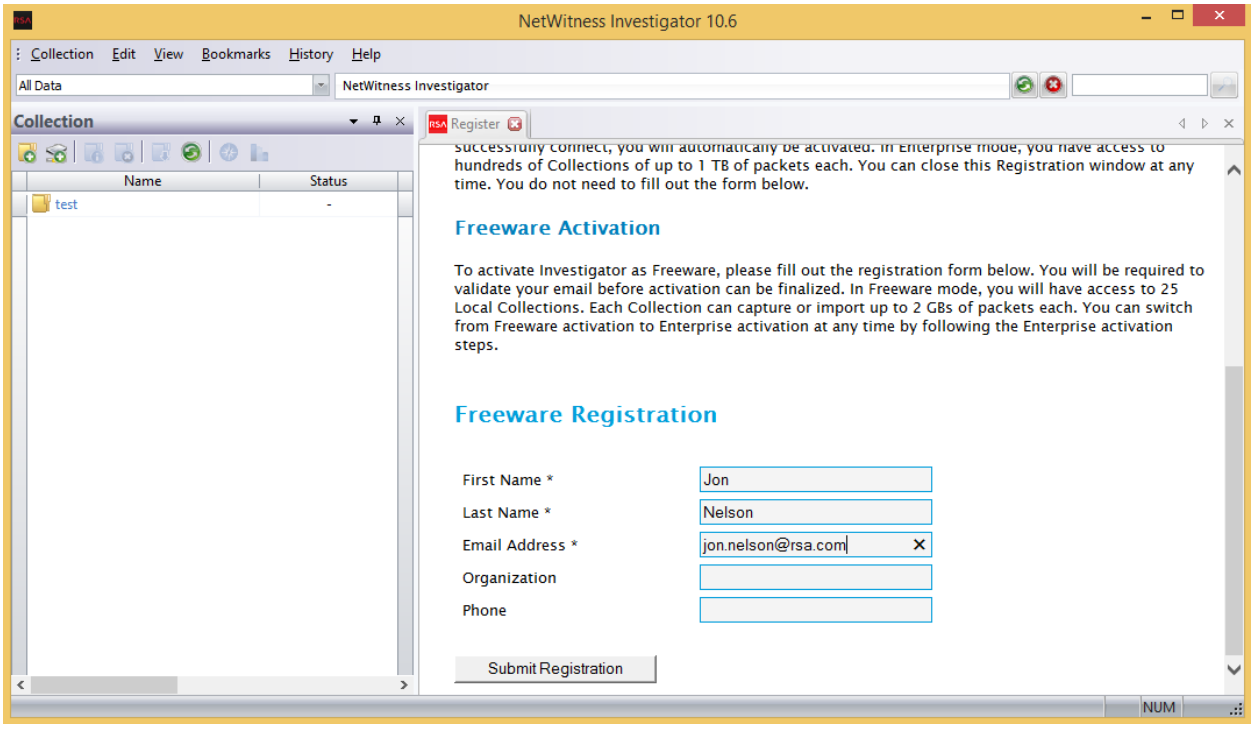
RSA Netwitness Investigator Freeware Client Quick Start Guide

Introduction

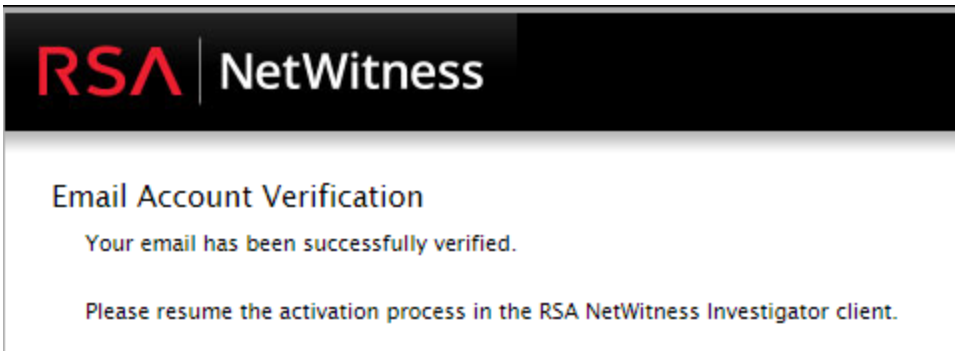
This Quick start Guide was written to provide users the very basics to get up and running with the RSA Netwitness Investigator Freeware Client. For more detailed information please consult the RSA Netwitness Investigator 9.8 User Guide (https://community.rsa.com/community/products/netwitness/investigator).

Registration

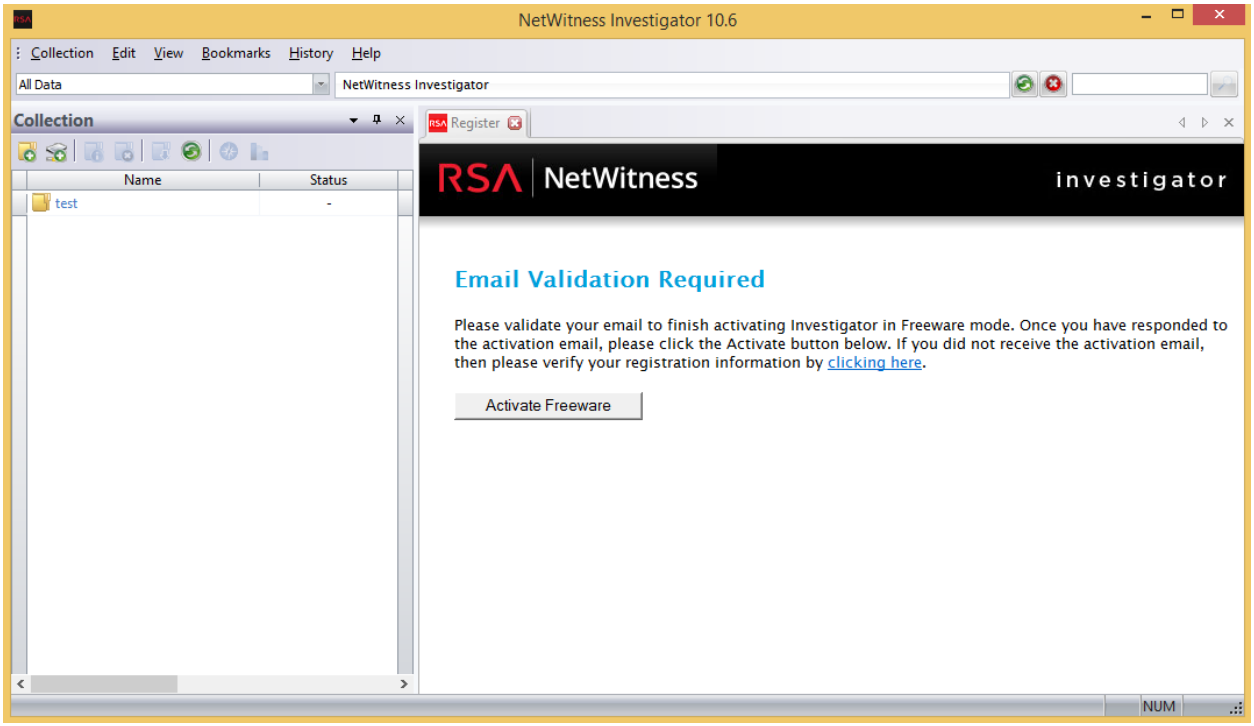
After you have installed the RSA Netwitness Investigator client (available here: https://community.rsa.com/community/products/netwitness/investigator), it needs to be registered before use. Fill out the required information as seen below and click “Submit Registration”.



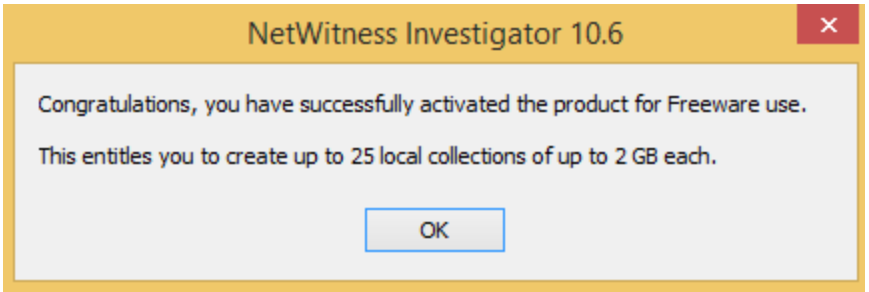
An email will be sent to the address provided with a link to verify the address. After clicking the link you should see the following in a browser:



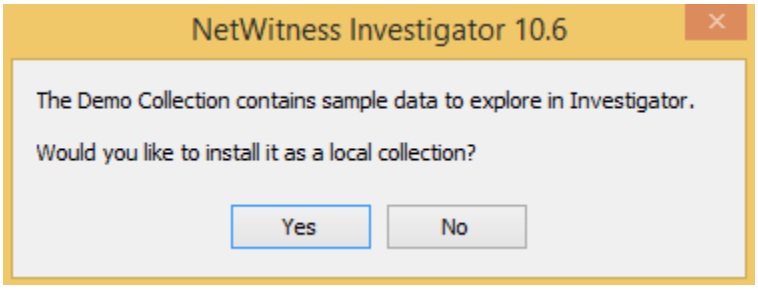
Once verified you can click the "Activate Freeware" as seen below.



You should then see the following popup indicating that the RSA Netwitness Investigator is activated:

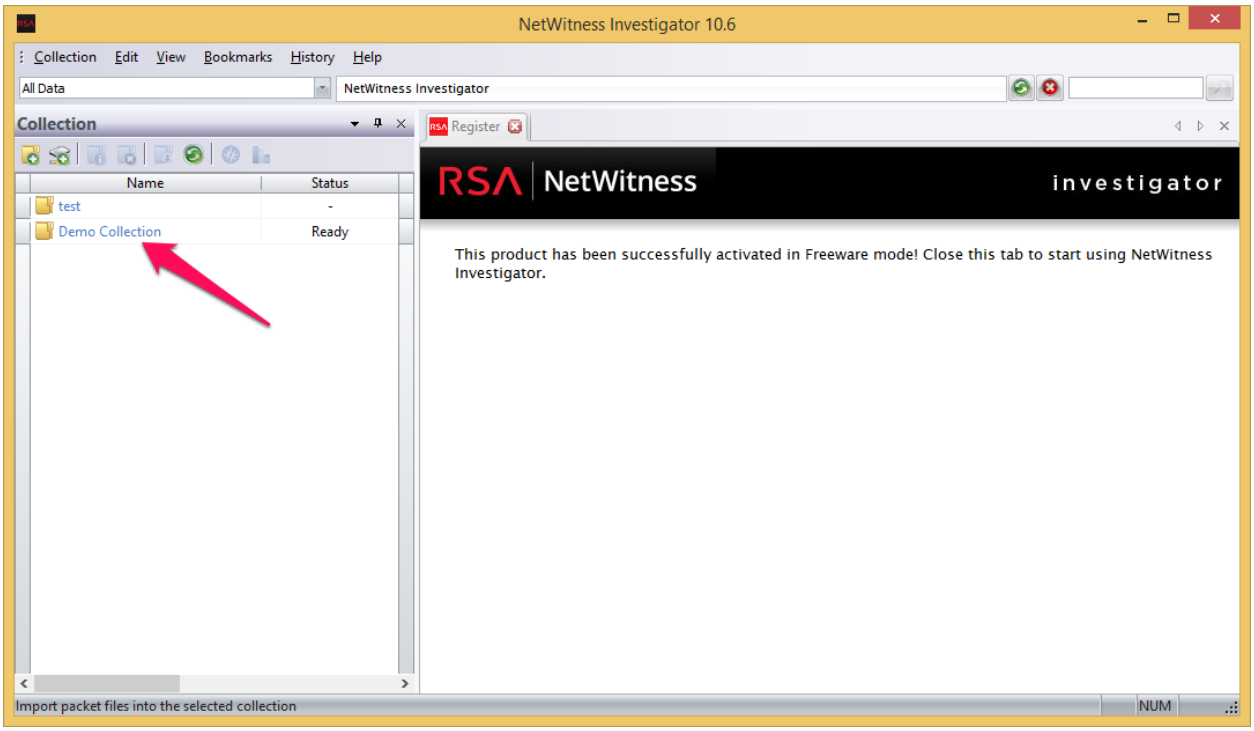


The RSA Netwitness Investigator freeware client comes with demo data to help you get used to the interface, and conducting investigations. If you want to import that data Choose “Yes” as seen below:



Basic navigation

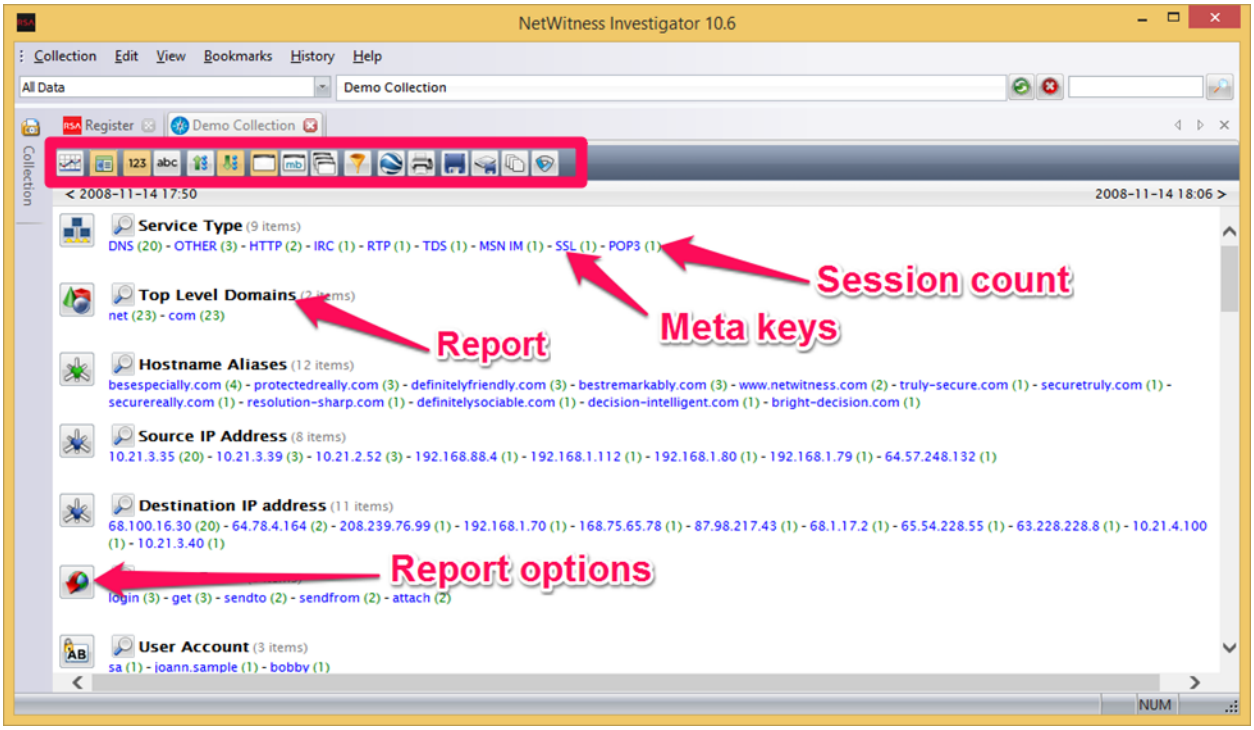
To access the demo data, double-click on the “Demo Collection” in the collection pane as shown below:



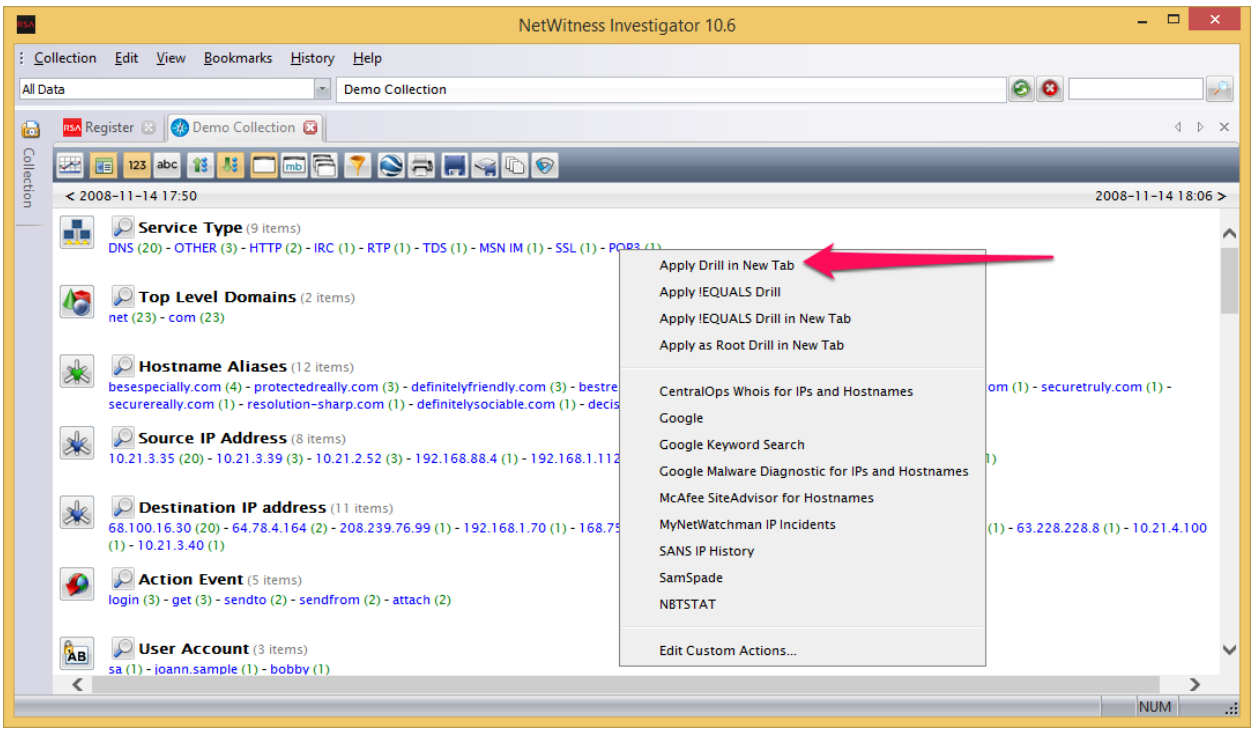
Once the collection is opened you will see the Navigation window for RSA Netwitness Investigator. Here we see Reports (meta categories in the web client), which are collections of meta values. Each meta values have an associated session count to indicate how many network sessions this key is found in.

The list of icons across the top of the Navigate pane gives you the ability view a timeline, sort the data in different ways, and export sessions and files.

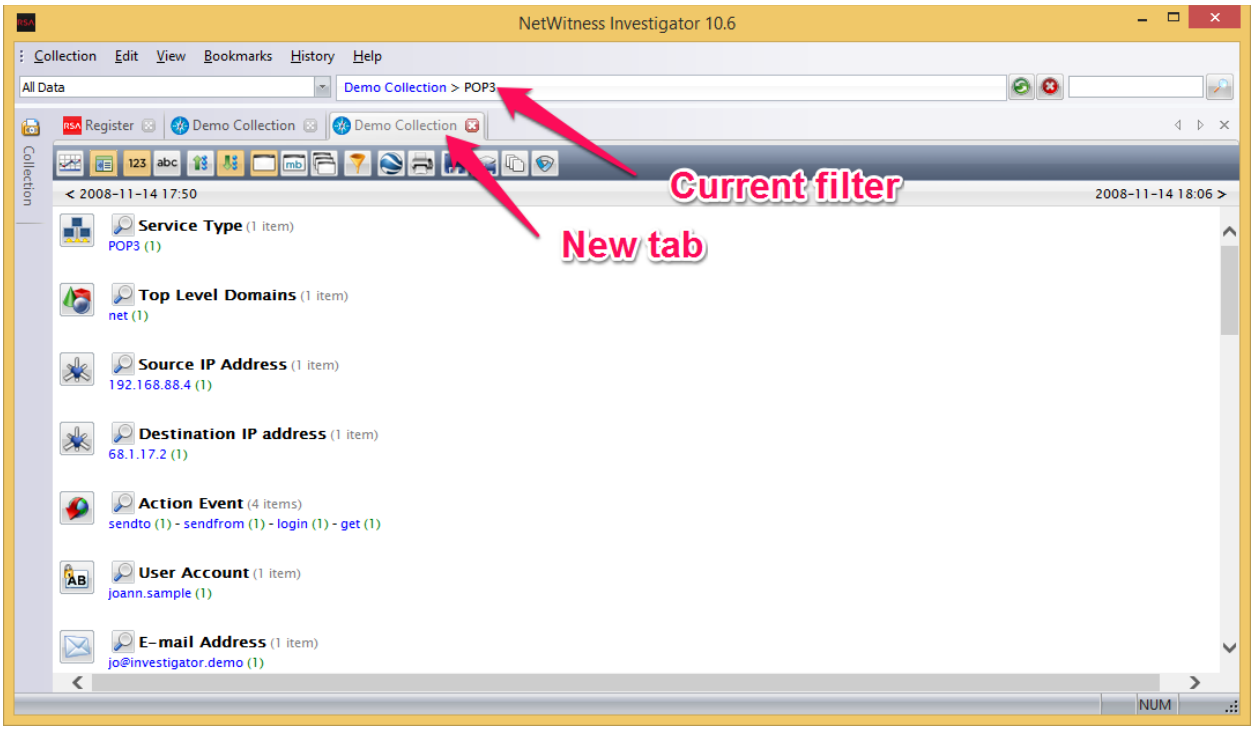
Investigations are conducted by leveraging the vast amount of metadata that RSA Netwitness Investigator provides to quickly narrow your focus to packets of interest.



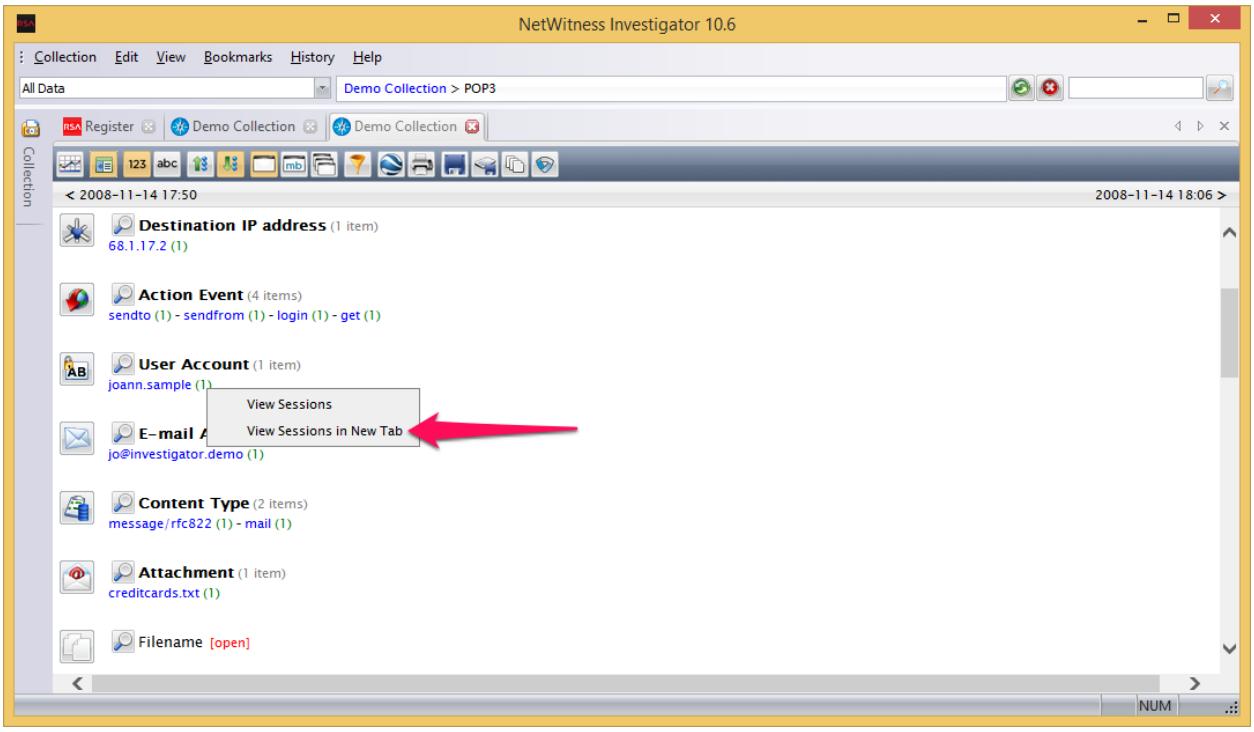
To add a layer of filtration to the data, or drill, click on one of the meta keys. Or you can right-click on the key and open the drill in a new tab. We are demonstrating this below with the POP3 meta key.



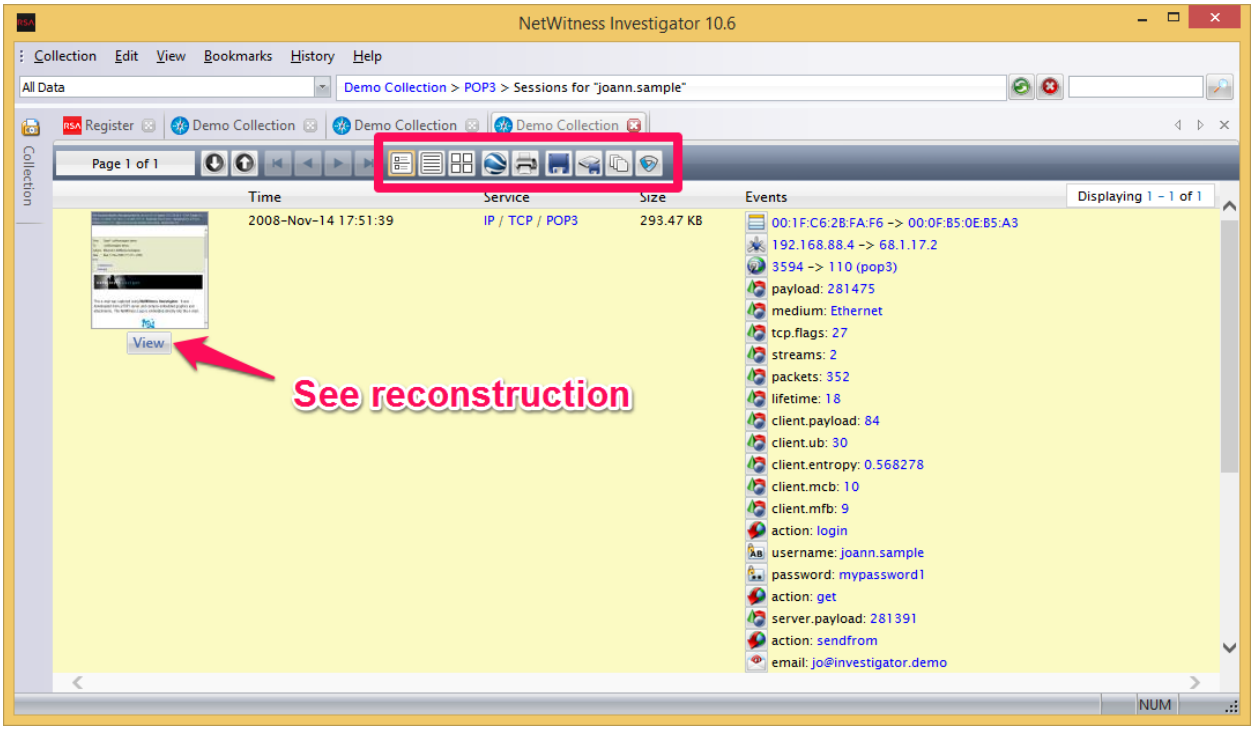
Now you can see that we have opened a new tab and we are drilled into just POP3 traffic and the associated metadata. It should be noted that RSA Netwitness Investigator does not rely on destination port to determine the protocol of a given session. RSA Netwitness Investigator looks inside the packets and looks at the actual packets to determine the protocol.



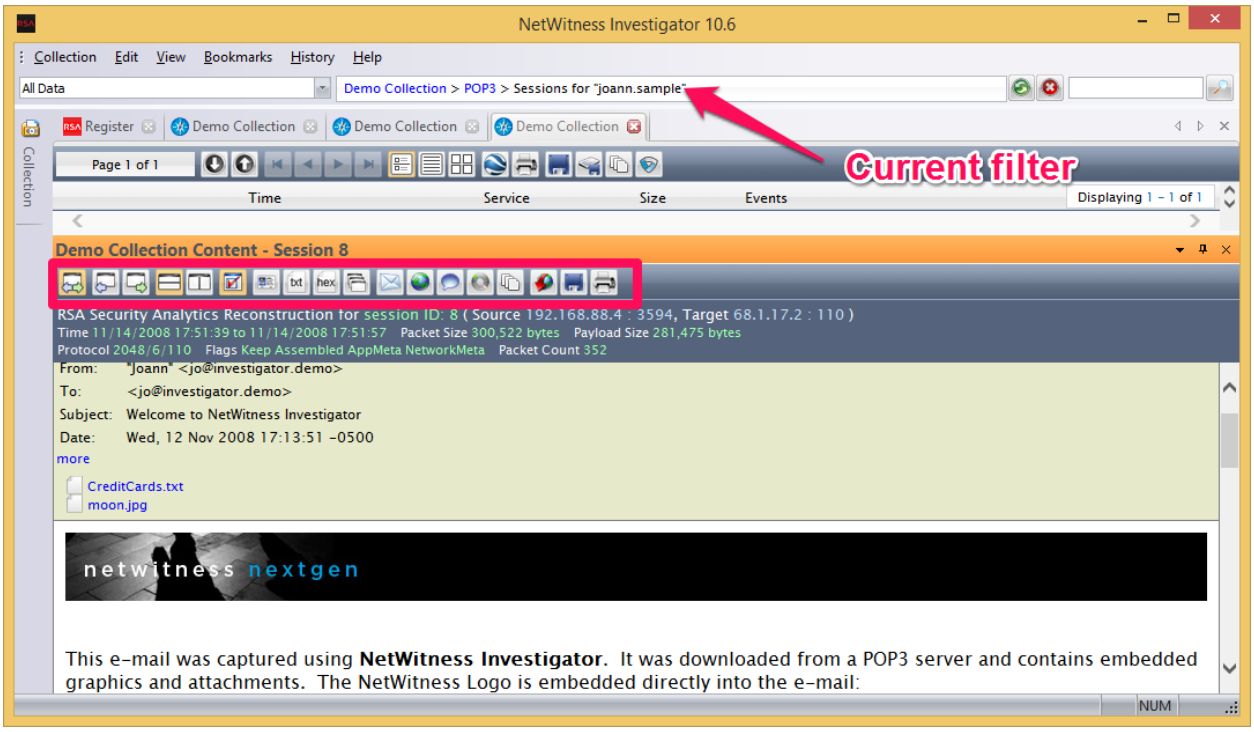
Once you have leveraged the metadata to focus on packets of interest, you can take a look at the actual packet data by clicking on the session count. Below, we have right clicked on the session count for the "joann.sample" meta key so we can open it in a new tab.



Below you can see that we have the one session shown in Hybrid view with other views available shown in the box. Since this is an email, RSA Netwitness Investigator will reconstruct it so you can see what the end user saw.

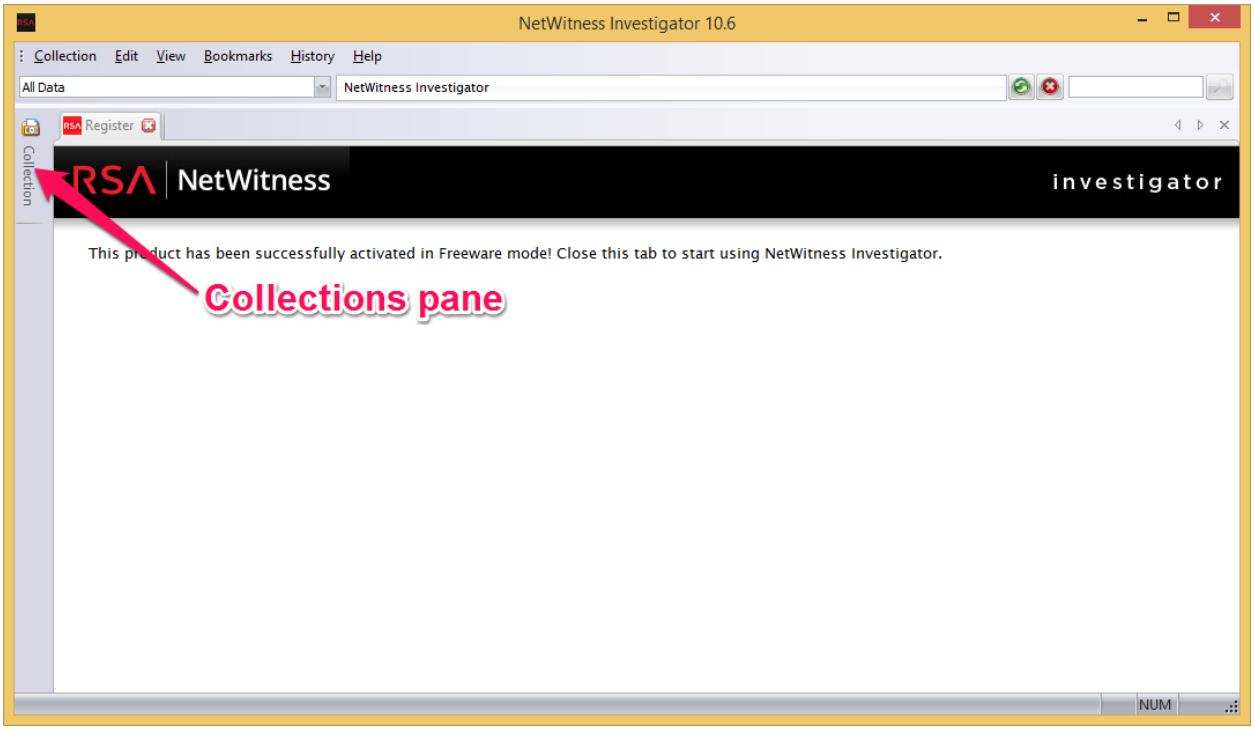


Below is the reconstructed email. There are also other views, ways to export data, and navigation options shown in the box.

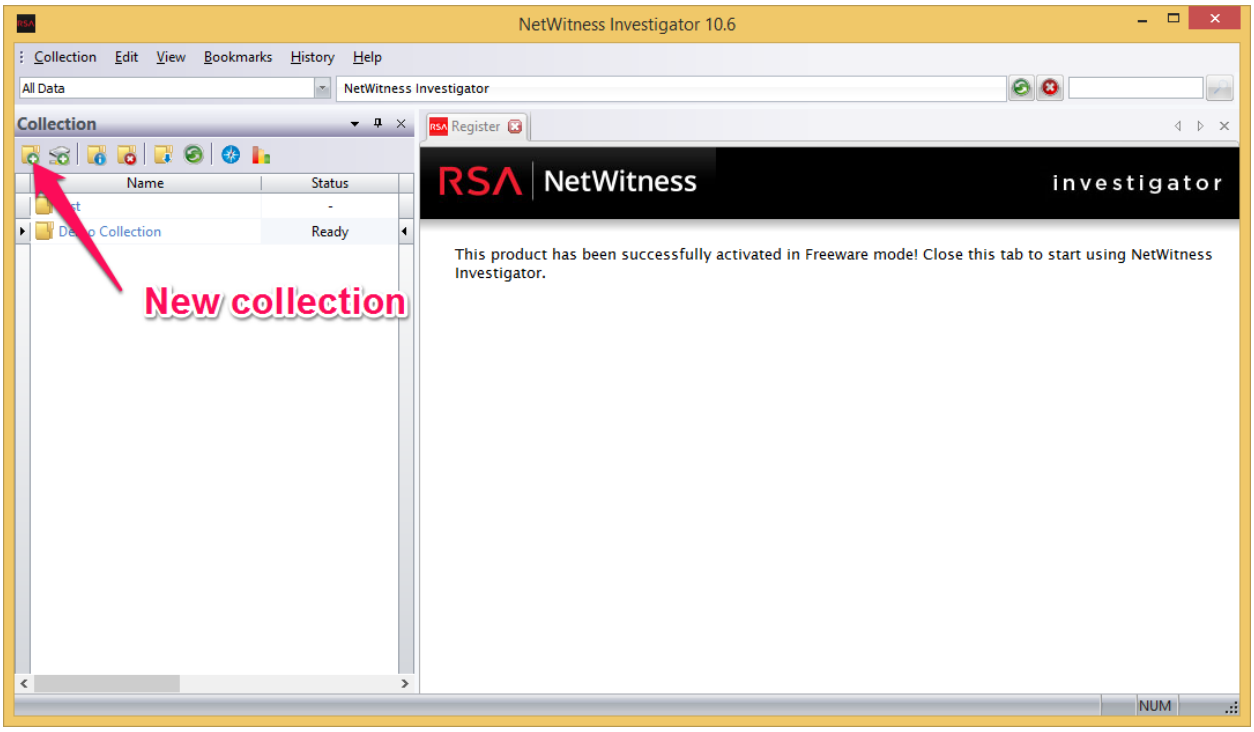


Importing PCAPs

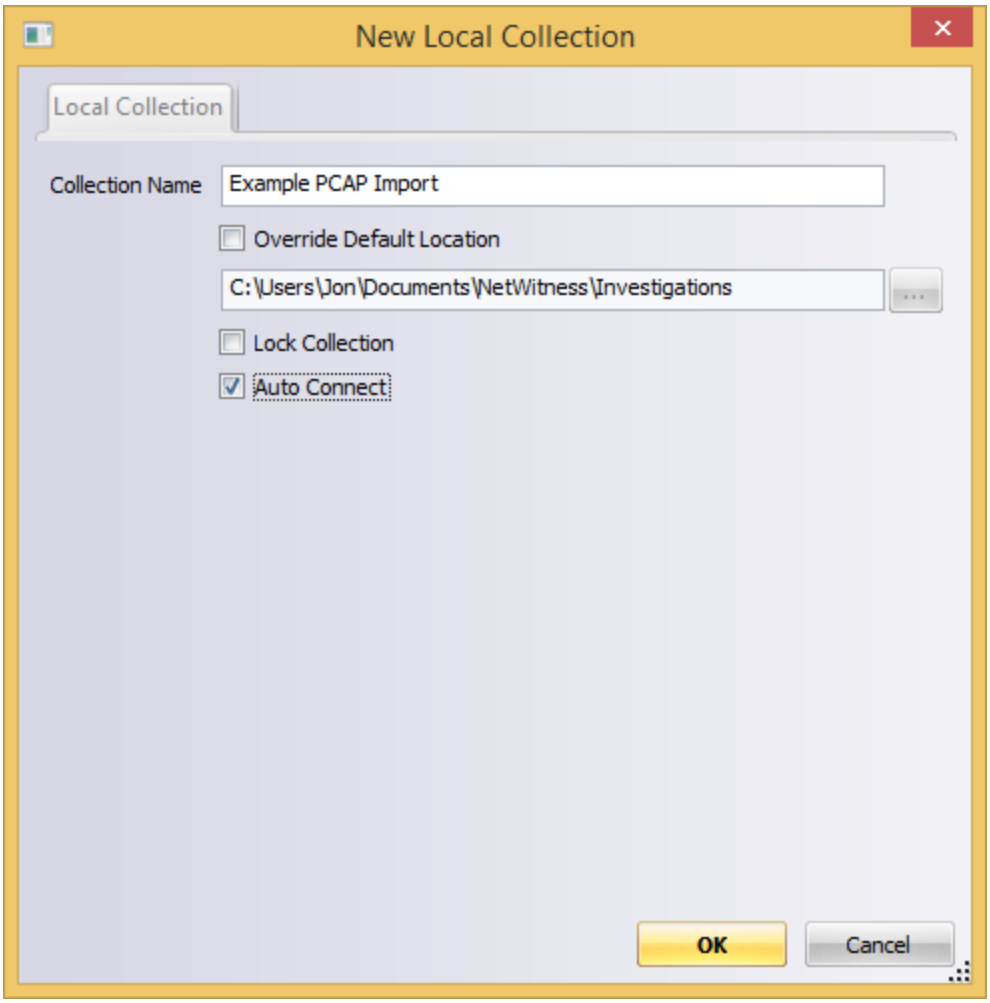
Now that you have an idea of how to use Netwitness Investigator, lets look at how you can import your own PCAPs. First, you need to open the collections pane.



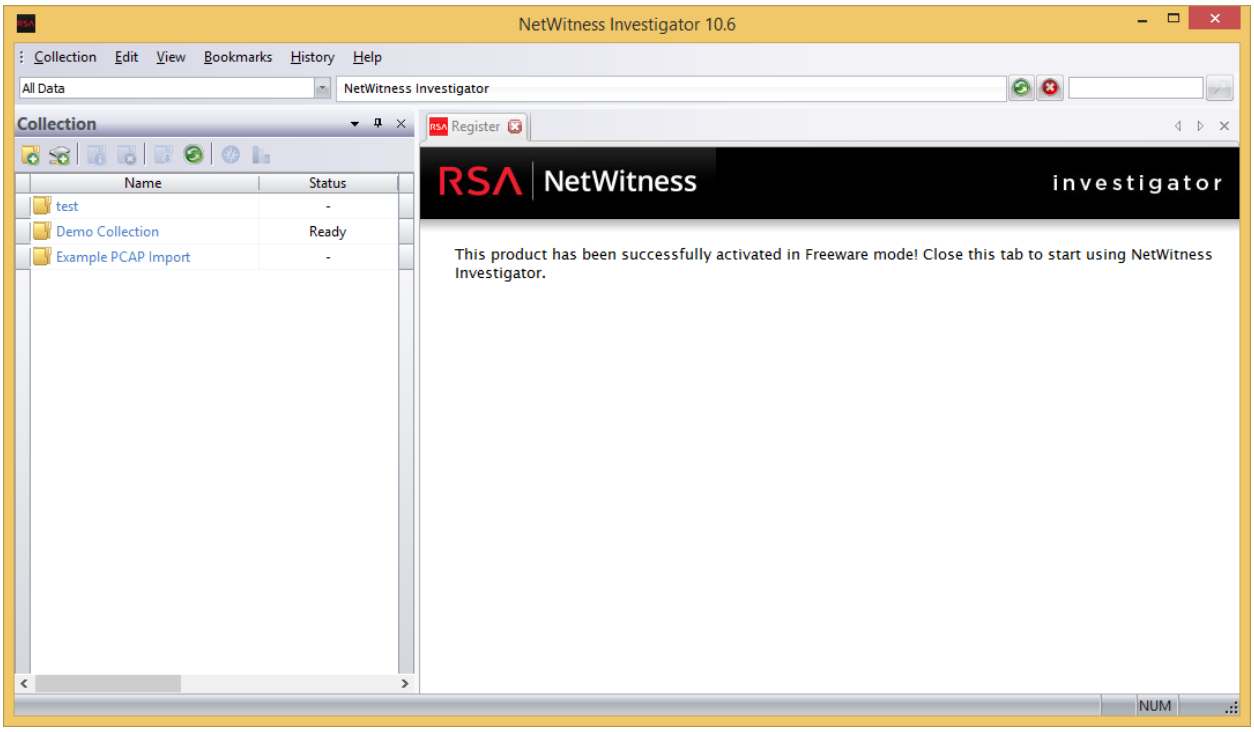
Then click the “New local collection” icon. You can have up to 25 collections in the freeware version.



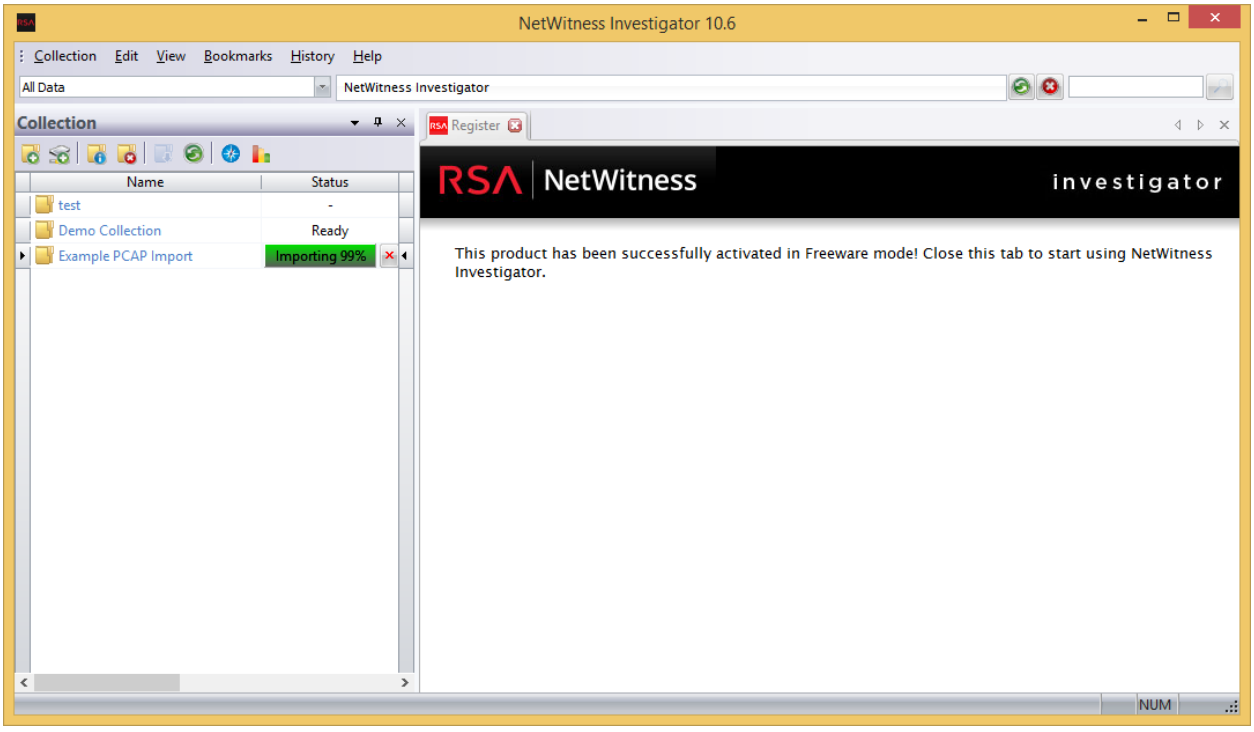
Give your collection a name, and choose “Auto Connect”. This option will automatically connect to the collection when the RSA Netwitness Investigator is opened. Then click “OK”.



Now you will see your collection listed in the collection pane. Double click it to connect to it, and you should see “Ready” in status column.



Then right-click on your collection and choose “Import packets”. You can import any number of PCAPs as long as their total size does not exceed 2GB, which is a limitation of the Freeware version. When you have started importing PCAPs you will see a progress bar like that seen below:



Once the processing is complete double-click on the collection to open it as we saw with the demo data.

Basic configuration

In the main interface choose Edit -> Options to see the dialog below. More can be read about the options in the RSA RSA Netwitness Investigator 9.8 User Guide (https://community.rsa.com/community/products/netwitness/investigator)