# 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: <u>https://community.rsa.com/community/products/netwitness/investigator</u>), it needs to be registered before use. Fill out the required information as seen below and click "Submit Registration".

Collection		NetWitness Investigator 10.6	- 🗆 🗙
Al Data       NetWitness Investigator         Collection <ul> <li>A magnetic field</li> <li>Succession y connect, you will automaticany be activated. In enterprise mode, you will have access to a succession y connect of fill out the form below.</li> </ul> Name     Status         Image: The status <ul> <li>Test</li> <li> <li></li></li></ul>	<u>Collection Edit View Bookmarks History H</u> elp		
Collection       • • • • • • • • • • • • • • • • • • •	All Data 🔹 NetWitness	Investigator	le l
Succession of up to 1 TB of packets each. You can close this Registration window at any time to compare the original before activation of up to 1 TB of packets each. You can close this Registration window at any time to compare the text in the compared to the text of the compared to the text of the compared to the compared tote compared tote to the compared tote tote to the compar	Collection 👻 म 🗙	rss Register 🗷	$\triangleleft \triangleright \mathbf{x}$
First Name *       Jon         Last Name *       Nelson         Email Address *       jon.nelson@rsa.com         Organization       Phone         Submit Registration       Image: Comment of the second	Name     Status       Image: Status     -	Successiony connect, you win automaticany be activated. In Enterpri- hundreds of Collections of up to 1 TB of packets each. You can close time. You do not need to fill out the form below. Freeware Activation To activate Investigator as Freeware, please fill out the registration for validate your email before activation can be finalized. In Freeware mo Local Collections. Each Collection can capture or import up to 2 GBs from Freeware activation to Enterprise activation at any time by follow steps. Freeware Registration	se mode, you nave access to e this Registration window at any orm below. You will be required to ode, you will have access to 25 of packets each. You can switch wing the Enterprise activation
	<	First Name *     Jon       Last Name *     Nelson       Email Address *     jon.nelson@rsa.com       Organization       Phone       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:



RS/



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

	NetWitness Investigator 10.6	- • ×
<u>Collection Edit View B</u> ookmarks <u>H</u> istory <u>H</u> elp		
All Data NetWitness	Investigator	88
Collection 👻 🖣 🗙	Register 🛞	4 ▷ ×
Name Status	<b>RSA</b> NetWitness	investigator
	Email Validation Required Please validate your email to finish activating Investigator the activation email, please click the Activate button below then please verify your registration information by <u>clickin</u> Activate Freeware	in Freeware mode. Once you have responded to w. If you did not receive the activation email, g here.

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

NetWitness Investigator 10.6
Congratulations, you have successfully activated the product for Freeware use.
This entitles you to create up to 25 local collections of up to 2 GB each.
ОК

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:

NetWitness Investigator 10.6				
The Demo Collection contains sample data to explore in Investigator.				
Would you like to install it as a local collection?				
Yes No				

#### **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.



NetWitness Investigator 10.6	- 🗆 🗙
: <u>C</u> ollection <u>E</u> dit <u>V</u> iew <u>B</u> ookmarks <u>H</u> istory <u>H</u> elp	
All Data Demo Collection	88
📾 🔤 Register 🗵 👩 Demo Collection 区	4 ▷ ×
ê 💯 📧 123 avc 🗱 🐰 🗂 📼 🔁 🍸 🚫 🚍 拱 😭 🕑	
< 2008-11-14 17:50	2008-11-14 18:06 >
Service Type (9 items)     DNS (20) - OTHER (3) - HTTP (2) - IRC (1) - RTP (1) - TDS (1) - MSN IM (1) - SSL (1) - POP3 (1)	^
Top Level Domains (2 mems) net (23) - com (23)	ession count
Hostname Aliases (12 items)     besespecially.com (4) - protectedreally.com (3) - definitelyfriendly.com (3) - bestremarkably.com (3) - www.netwitness.com (1) - definitelysociable.com (1) - decision-intelligent.com (1) - bright-decision-intelligent.com (1	com (2) - truly-secure.com (1) - securetruly.com (1) - sion.com (1)
Source IP Address (8 items) 10.21.3.35 (20) - 10.21.3.39 (3) - 10.21.2.52 (3) - 192.168.88.4 (1) - 192.168.1.112 (1) - 192.168.1.80 (1) - 192.168.1.7	9 (1) - 64.57.248.132 (1)
Destination IP address (11 items) 68.100.16.30 (20) - 64.78.4.164 (2) - 208.239.76.99 (1) - 192.168.1.70 (1) - 168.75.65.78 (1) - 87.98.217.43 (1) - 68.1.1 (1) - 10.21.3.40 (1)	17.2 (1) - 65.54.228.55 (1) - 63.228.228.8 (1) - 10.21.4.100
Report options	
Sa (1) - joann.sample (1) - bobby (1)	~
	NUM .::

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.

NetWitness Investigator 10.6	5 – 🗆 🗙				
Edit View Bookmarks History Help					
Register         Image: Second Se	4 Þ ×				
§ < 2008-11-14 17:50	2008-11-14 18:06 >				
Service Type (9 items)     DNS (20) - OTHER (3) - HTTP (2) - IRC (1) - RTP (1) - TDS (1) - MSN IM (1) - SSL (1) - POR3 (1)     Apply Drill i     Apply Drill i     Apply Drill i	n New Tab				
Image: Top Level Domains (2 items)     Apply 1200       net (23) - com (23)     Apply 1200       Image: Aligned	ALS Drill in New Tab				
Postname Allases (12 items)     besespecially.com (4) - protectedreally.com (3) - definitelyfriendly.com (3) - bestre     securereally.com (1) - resolution-sharp.com (1) - definitelysociable.com (1) - decis     Google	Whois for IPs and Hostnames om (1) - securetruly.com (1) -				
Source IP Address (8 items)         Google Keyword Search           10.21.3.35 (20) - 10.21.3.39 (3) - 10.21.2.52 (3) - 192.168.88.4 (1) - 192.168.1112         Google Malware Diagnostic for IPs and Hostnames					
Destination IP address (11 items)         McAree Site           68.100.16.30 (20) - 64.78.4.164 (2) - 208.239.76.99 (1) - 192.168.1.70 (1) - 168.75 (1) - 10.21.3.40 (1)         MyNetWatch	Iman IP Incidents (1) - 63.228.228.8 (1) - 10.21.4.100				
Action Event (5 items)         SamSpade           login (3) - get (3) - sendto (2) - sendfrom (2) - attach (2)         NETSTAT					
User Account (3 items)     Sa (1) - Joann.sample (1) - bobby (1)	n Actions				



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.



NetWitness Investig	jator 10.6 – 🗆 🗙
: <u>C</u> ollection <u>E</u> dit <u>V</u> iew <u>B</u> ookmarks <u>H</u> istory <u>H</u> elp	
All Data  T Demo Collection > POP3	le l
💼 🔤 Register 🗵 🔣 Demo Collection 🕃 🤣 Demo Collection 😰	4 Þ ×
💡 🚟 🔲 123 abc 👔 🚜 🥅 📾 🔁 🍞 🚫 🚔 📕 🤿 🖒 🔊	
	2008-11-14 18:06 >
Destination IP address (1 item)     68.1.17.2 (1)	^
Action Event (4 items) sendto (1) - sendfrom (1) - login (1) - get (1)	
Joann.sample (1)	
Image: Second system     View Sessions in New Tab       jo@investigator.demo (1)	
Content Type (2 items) message/rfc822 (1) - mail (1)	
Creditcards.txt (1)	
Filename [open]	~
	<ul> <li></li></ul>

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.

85A		NetWitness	Investigator 10	.6	- 🗆 ×
: <u>C</u> ollection <u>E</u> dit <u>V</u> iew <u>B</u> o	okmarks <u>H</u> istory <u>H</u> elp				
All Data	Demo Collection	on > POP3 > Sessions for "joa	ann.sample"	0	0
🔚 🛯 🛤 Register 🖂 🔗 Dem	o Collection 💿 👩 Demo Collect	tion 💿 👩 Demo Collectio	n 🔀		4 ▷ ×
					Disclosing 1 and 1
S	Lime	Service	Size	Events	Displaying I - I of I
	2008-Nov-14 17:51:39	IP / TCP / POP3	293.47 KB	00:1F:C6:2B:FA:F6 -> 00:0F:B5:0E:B5:A3	_
The State Address of the State				ali 192.168.88.4 -> 68.1.17.2	
				😡 3594 -> 110 (pop3)	
				ka payload: 281475	
The a new second control and second s				🧑 medium: Ethernet	
Niew				🧑 tcp.flags: 27	
view				🧑 streams: 2	
				🧑 packets: 352	
	See reco	onstructio	n	🧑 lifetime: 18	
			~	🧑 client.payload: 84	
				🧑 client.ub: 30	
				lient.entropy: 0.568278	
				ka client.mcb: 10	
				ka client.mfb: 9	
				🖗 action: login	
				🔊 username: joann.sample	
				assword: mypassword1	
				naction: get	
				aserver.payload: 281391	
				action: sendfrom	
				💽 email: jo@investigator.demo	*
<					>
					NUM .::

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



RSA		NetW	itness Investigator	10.6		- 🗆 ×
: <u>C</u> o	llection <u>E</u> dit <u>V</u> iew <u>B</u> ookmarks <u>H</u> ist	ory <u>H</u> elp				
All D	ita	Demo Collection > POP3 > Session	s for "joann.sample"		<b>O</b>	
6	🛤 Register 💿 🚷 Demo Collection 💿	🛛 🛞 Demo Collection 💿 🛞 Demo C	Collection 区			4 Þ ×
Colle	Page 1 of 1 0 0 💌 🗸				<b>Current filter</b>	-
ction	Time	Service	Size	Events		Displaying 1 – 1 of 1 🗘
	<					>
	Demo Collection Content - Sessi	on 8				<b>→</b> ₽ ×
		hex 🖻 🖂 🥥 🗩 🔕 🗅 🏈	<b>a a</b>			_
	RSA Security Analytics Reconstructi Time 11/14/2008 17:51:39 to 11/14/20 Protocol 2048/6/110 Flags Keep Assen	on for session ID: 8 ( Source 192.) 08 17:51:57 Packet Size 300,522 bytes ibled AppMeta NetworkMeta Packet Cou	168.88.4 : 3594, Tai Payload Size 281,475 unt 352	rget 68.1.17.2 : 1 bytes	10)	
	From: "Joann" < jo@investigator.de To: < io@investigator.demo>	no>				~
	Subject: Welcome to NetWitness Inve	stigator				
	Date: Wed, 12 Nov 2008 17:13:51 -0500					
	more					
	CreditCards.txt					
	netwitness next	g e n				
	This e-mail was captured u	sing NetWitness Investig	ator. It was do	wnloaded fro	m a POP3 server and contai	ins embedded 🗸 🧹
	graphics and attachments.	The Netwitness Logo is em	ibedded directl	y into the e-r	naii:	NUM
						1401WI

## 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.

<b>NA</b>		NetWitness Investigator 10.6	X
<u>Collection Edit View Bookma</u>	rks <u>H</u> istory <u>H</u> elp		
All Data	<ul> <li>NetWitness I</li> </ul>	Investigator	Ø 8
Collection	<b>▲</b> û ×	Register 😰	d Þ ×
Name	- Status	<b>KS</b> Netwitness	investigator
De o Collection	Ready 4		
New c	ollection	This product has been successfully activat Investigator.	ed in Freeware mode! Close this tab to start using NetWitness
			NUM .:

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".

New Local Collection     ×
Local Collection
Collection Name Example PCAP Import Override Default Location C:\Users\Jon\Documents\WetWitness\Investigations
<ul> <li>Lock Collection</li> <li>Auto Connection</li> </ul>
OK Cancel

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.



RSA

85A		NetWitness Investigator 10.6	- 🗆 🗙
: <u>C</u> ollection <u>E</u> dit <u>V</u> iew <u>B</u> ookmarks	<u>H</u> istory <u>H</u> elp		
All Data	<ul> <li>NetWitness</li> </ul>	Investigator	
Collection	<b>→ ‡</b> ×	Register 😰	d ⊳ ×
Name	Status	<b>RSA</b> NetWitness	investigator
Demo Collection	- Ready		
Example PCAP Import	-	This product has been successfully activate	d in Freeware mode! Close this tab to start using NetWitness
		Investigator.	
4	>		
		1	NUM .:

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:

rsA		NetWitness Investigator 10.6	- 🗆 🗙
: <u>C</u> ollection <u>E</u> dit <u>V</u> iew <u>B</u> ookmar	rks <u>H</u> istory <u>H</u> elp		
All Data	<ul> <li>NetWitness I</li> </ul>	Investigator	8 8
Collection	<b>→ ů</b> ×	Register 🔀	4 ▷ ×
6 8 6 6 8 9 9			
Name	Status	<b>RSA</b> NetWitness	investigator
Demo Collection	Ready		
Example PCAP Import	Importing 99% × 4	This product has been successfully activation	ted in Freeware mode! Close this tab to start using NetWitness
		investigator.	
<	>		NUM

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)

Options ×						
General Display Reports C	Capture Process	Audio Codecs	Advanced 4			
Default Collection Path	ers\Jon\Documents\	NetWitness\Invest	igations 🔁			
Automatically Check for Updates						
Allow Investigator to Reach Internet						
Show Welcome Page on Application Startup						
Smart Hide Collections Page						
Show Descriptive Tooltips						
Reset Warning Prompts	If at any point in the disable a warning pr re-enable all warnin	e application you h rompt, clicking this l g dialogs.	ave opted to button will			
Restore Default Settings	Reset Investigator (	Settings to the Def	ault Settings.			
		ОК	Cancel			

