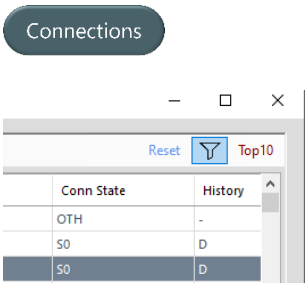
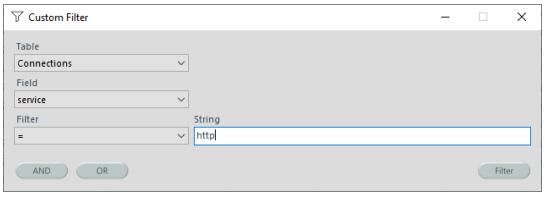
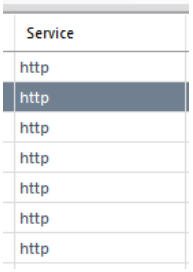
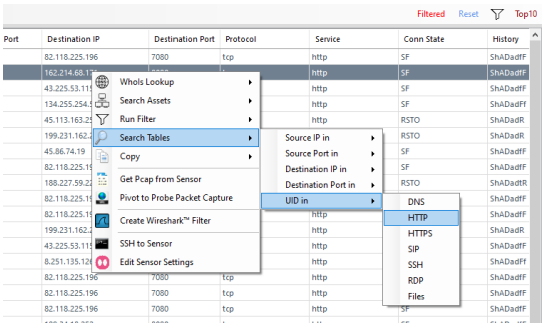
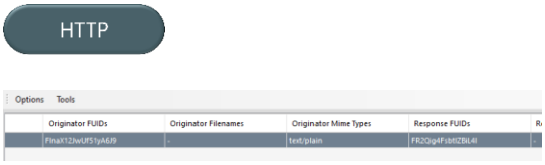
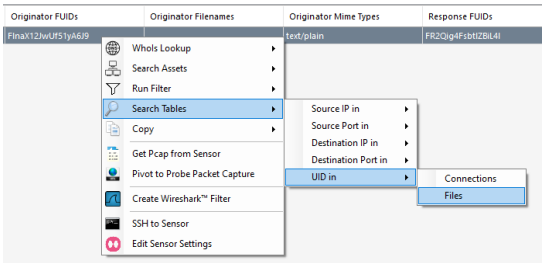
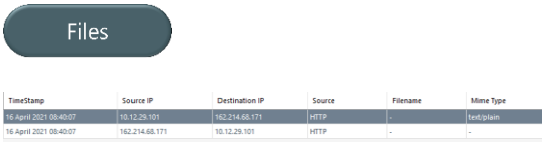
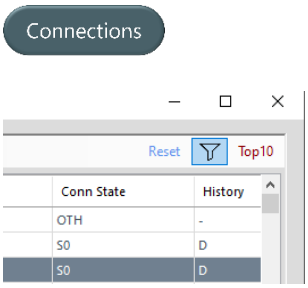
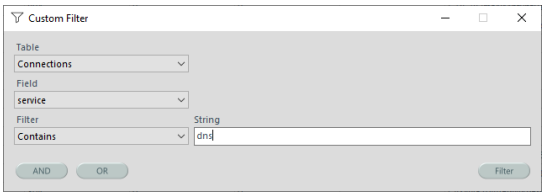
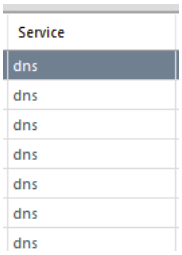
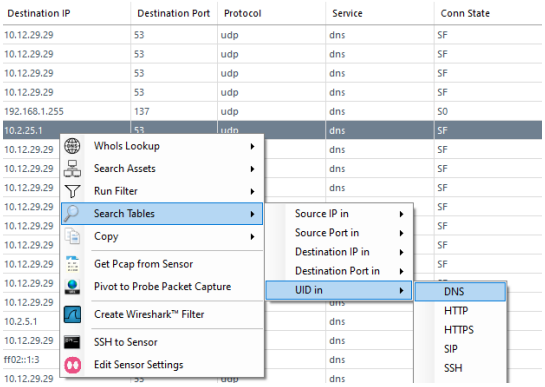
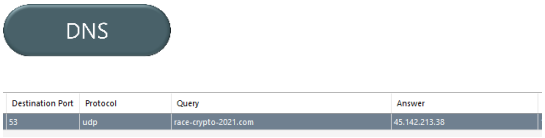
Sniffa Runbook
Filtering, Searching and Pivoting Across Associated Zeek™ Log Files

Serial	Instruction
	Overview. Zeek™ is an opensource network monitoring tool that quietly and unobtrusively observes network traffic being processed by a network interface card (typically from a switch span or mirrored port). Zeek™ interprets what it sees and creates compact, high-fidelity transaction logs, file content, and fully customized output, suitable for manual review on disk. Sniffa Sensors are configured to forward Zeek™ transaction logs via the Syslog protocol, from the local disk on a Sensor to a centralised database server accessible by 1 or more Sensor Manager Applications. Sensor Manager Application users are then able to access the database in a user friendly Microsoft™ Windows Graphical User Interface (GUI) and analyse the traffic logs for patterns of attack and indications of compromise. The Sensor Manager Application builds upon the unique way in which the Zeek™ application associates separate traffic logs by service, originator, responder and connection id, in order to provide users the ability to search, filter and pivot across associated traffic log data using a Windows GUI. Being able to quickly search, filter and pivot across associated traffic log data, enables analysts to quickly visualise network activity and significantly reduce the time to resolve network incidents and alerts. This runbook includes examples of how to Filter, Search and Pivot across Zeek™ traffic log data, using the Sniffa Sensor Manager Application.
1.	**Example 1** Select the ‘Connections’ Panel. Click on the button in the top right-hand corner, marked with the Funnel icon to open the ‘Custom Filter’ window. 
2.	Choose ‘Connections’ from the Table drop down list. Choose ‘service’ from the Field drop down list. Choose ‘=’ from the Filter drop down list. Add the text ‘http’ into the String textbox. Click the button marked ‘Filter’ to execute filter. 

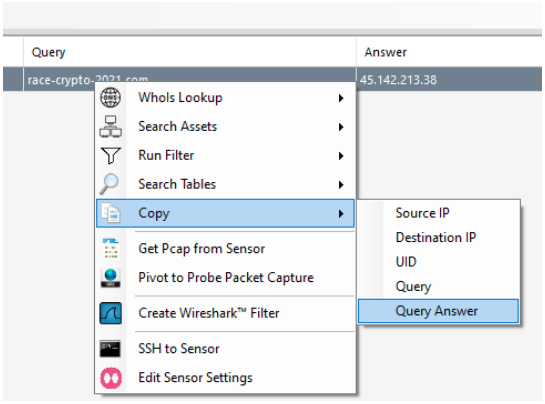
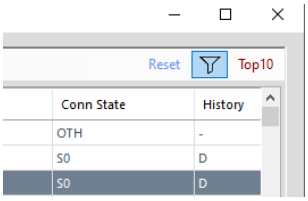
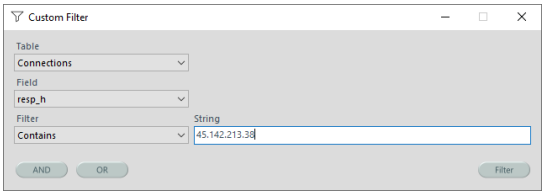
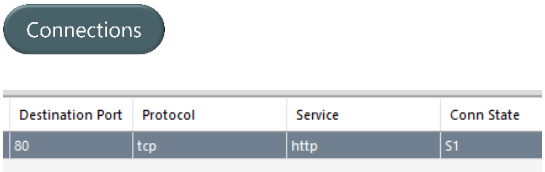
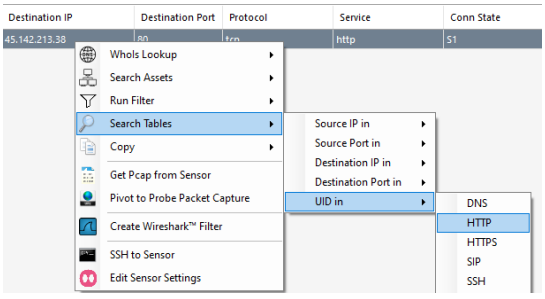
Sniffa Runbook
Filtering, Searching and Pivoting Across Associated Zeek™ Log Files

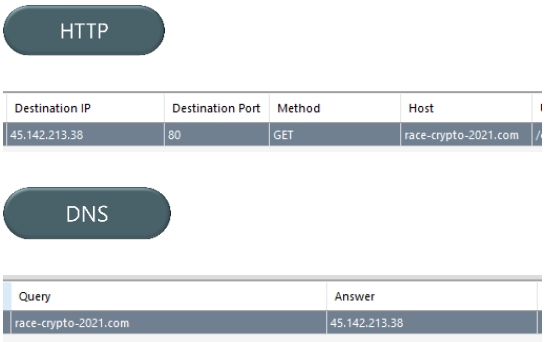
3.	Note that the view has been filtered for connections that are service equals ‘http’.	
4.	Right click on a single connection log entry row. Select ‘Search Tables’ menu item. Select ‘UID in’ menu item. Select ‘HTTP’ menu item.	
5.	Review all HTTP log details in the HTTP panel, that relate to the associated connection selected from the Connections panel. Check for any Files identifiers that indicate the upload or download of files relating to the associated connection (originator or responder FUID).	
6.	Right click the associated HTTP log entry. Select ‘Search Tables’ menu item. Select ‘UID in’ menu item. Select ‘Files’ menu item.	
7.	Review all Files log details in the Files panel, that relate to the associated connection selected from the HTTP and Connections panel.	

Sniffa Runbook
Filtering, Searching and Pivoting Across Associated Zeek™ Log Files

8.	**Example 2** Select the 'Connections' Panel. Click on the button in the top right-hand corner, marked with the Funnel icon to open the 'Custom Filter' window.	
9.	Choose 'Connections' from the Table drop down list. Choose 'service' from the Field drop down list. Choose '=' from the Filter drop down list. Add the text 'dns' into the String textbox. Click the button marked 'Filter' to execute filter.	
10.	Note that the view has been filtered for connections that are service equals 'http'.	
11.	Right click on a single connection log entry row. Select 'Search Tables' menu item. Select 'UID in' menu item. Select 'DNS' menu item.	
12.	Review all DNS log details in the DNS panel, that relate to the associated connection selected from the Connections panel.	

Sniffa Runbook
Filtering, Searching and Pivoting Across Associated Zeek™ Log Files

13.	Right click the associated DNS log entry. Select 'Copy' menu item. Select 'Query Answer' menu item.	
14.	Click on the button in the top right-hand corner, marked with the Funnel icon to open the 'Custom Filter' window.	
15.	Choose 'Connections' from the Table drop down list. Choose 'resp_h' from the Field drop down list. Choose '=' from the Filter drop down list. Paste the Query Answer into the String textbox. Click the button marked 'Filter' to execute filter. *Note:* *You can use Ctrl + V to paste text into String textbox.*	
16.	Note the service that is related to the associated connection.	
17.	**If the service is 'http'.** Right click on a single connection log entry row. Select 'Search Tables' menu item. Select 'UID in' menu item. Select 'HTTP' menu item.	

18.	Review all HTTP log details in the HTTP panel, that relate to the associated connection selected from the Connections panel. Confirm that the 'Query' noted in the DNS panel is the same as the 'Host' in the HTTP panel.	
19.	End of Runbook.	