LiveAction

LiveWire 24.3.0 New Features

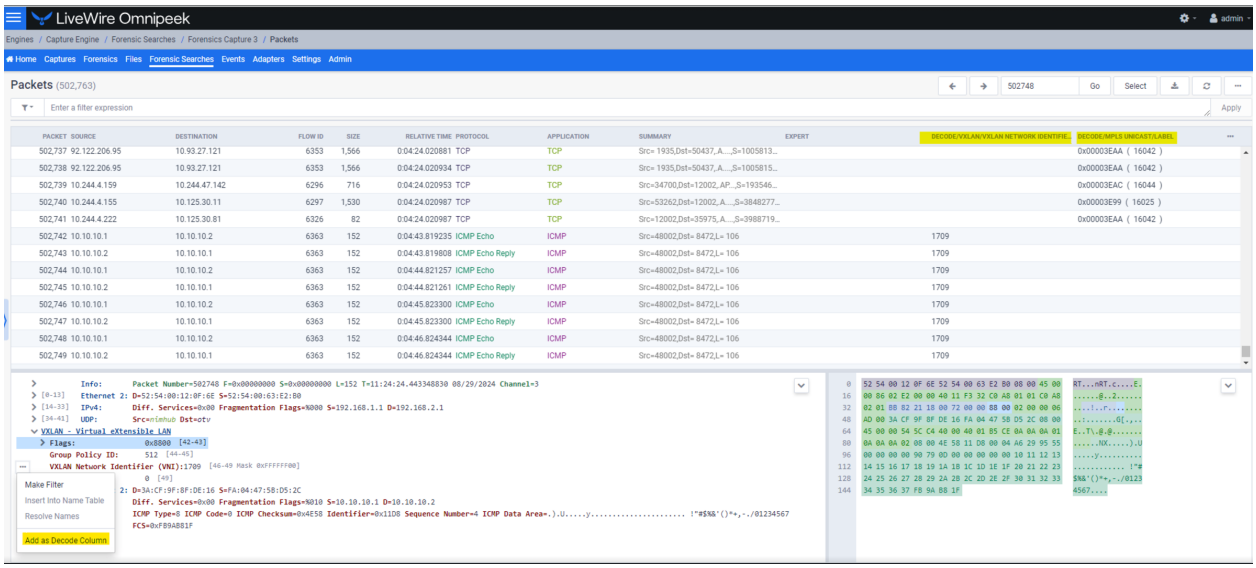
QUICK GUIDE

ver. 24.3.0a

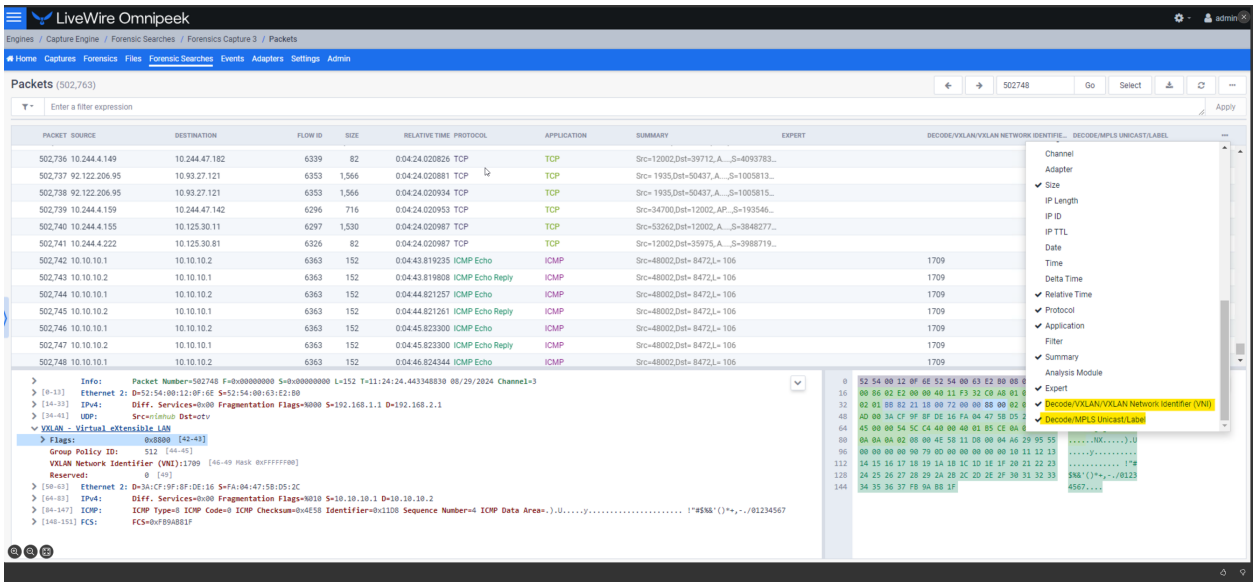
Enable Decode VXLAN Column in LiveWire Omnipeek

Here are the steps to enable the Decode VXLAN column:

1. Enable "Decode /MPLS/VXLAN Network Identifier" in *Expert* > *Packets*.
2. Click the flag for VXLAN > Click the ellipsis and Select "Add as Decode Column".

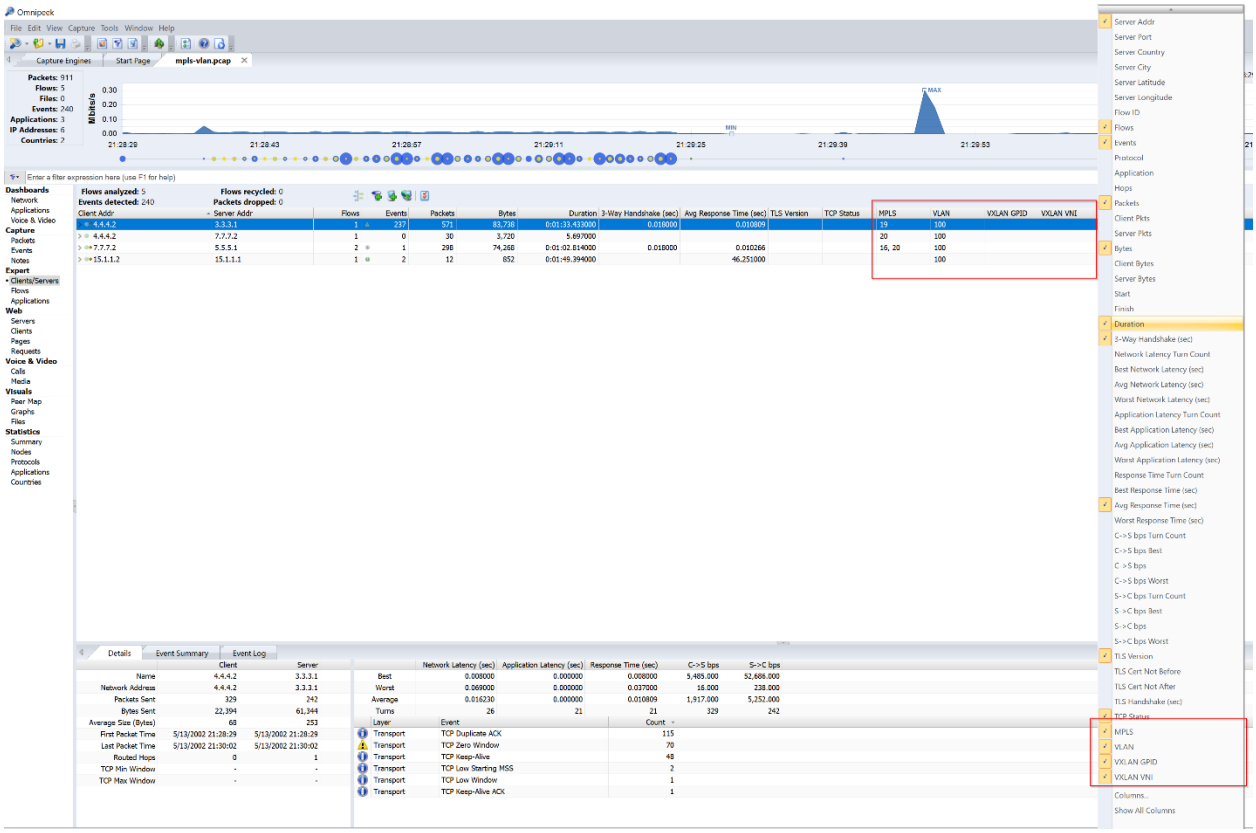


3. A new column will appear in the column on the far right of the Expert/Packets page.



Enable MPLS, VLAN, and VXLAN Expert Events in Omnipeek Windows

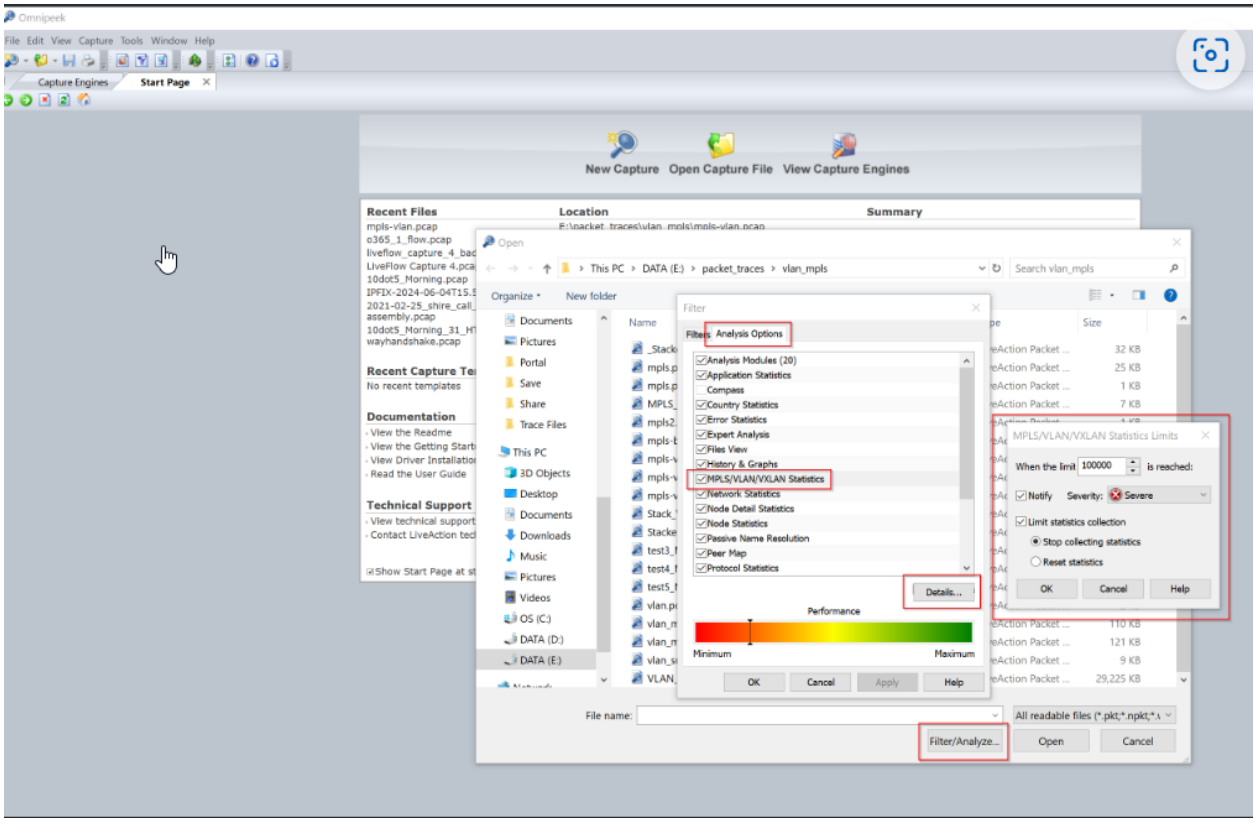
Right-click the Column header in Expert Events and enable all four options as shown at the bottom of the screenshot below:



Enable MPLS, VLAN, and VXLAN Statistics in Omnipeek Windows

Local Files

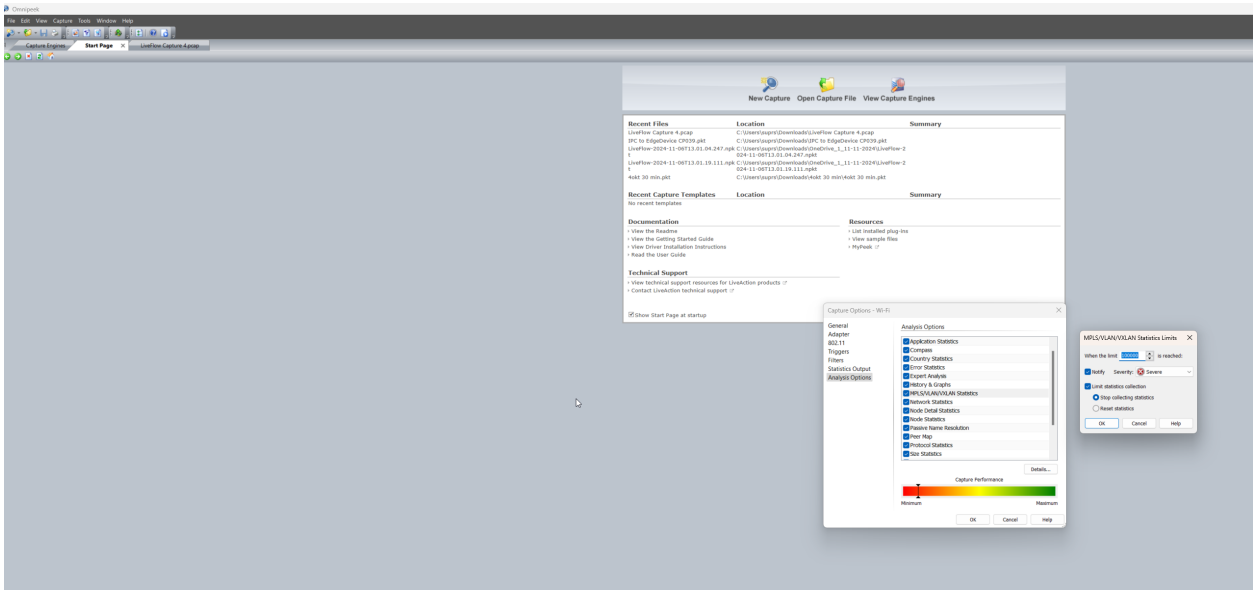
When opening a packet file in Omnipeek Windows, the user may click the Filter/Analyze... button in the open file dialog to see the list of analysis options that will be used to analyze the packet file. A new option will be present called "MPLS/VLAN/VXLAN Statistics" which will represent this new MPLS/VLAN/VXLAN Statistics view. Enabling this option will show the MPLS/VLAN/VXLAN Statistics view in the file window, while disabling this option will hide the MPLS/VLAN/VXLAN Statistics view. Clicking the "Details..." button when the "MPLS/VLAN/VXLAN Statistics" item is selected will display the MPLS/VLAN/VXLAN Statistics Limits dialog and allow the user to modify the statistics limits for this MPLS/VLAN/VXLAN Statistics view.



Capture

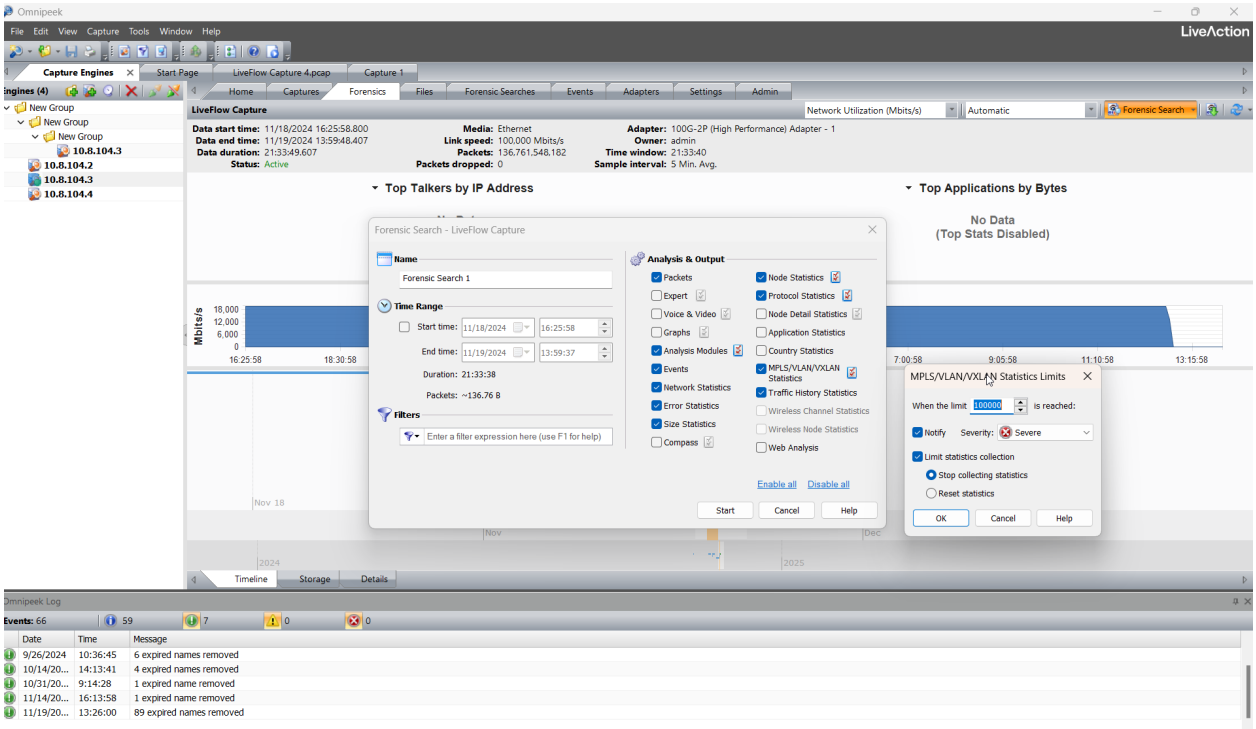
When creating a capture in Omnipeek Windows, the user may click the "Analysis Options" tab in the capture options dialog to see the list of analysis options that will be used to analyze the packets. A new option will be present called "MPLS/VLAN/VXLAN Statistics" which will represent this new MPLS/VLAN/VXLAN Statistics view. Enabling this option will show the MPLS/VLAN/VXLAN Statistics view in the capture window, while disabling this option will hide the MPLS/VLAN/VXLAN Statistics view. Clicking the "Details..." button when the "MPLS/VLAN/VXLAN

Statistics" item is selected will display the MPLS/VLAN/VXLAN Statistics Limits dialog and allow the user to modify the statistics limits for this MPLS/VLAN/VXLAN Statistics view.



Forensic Search

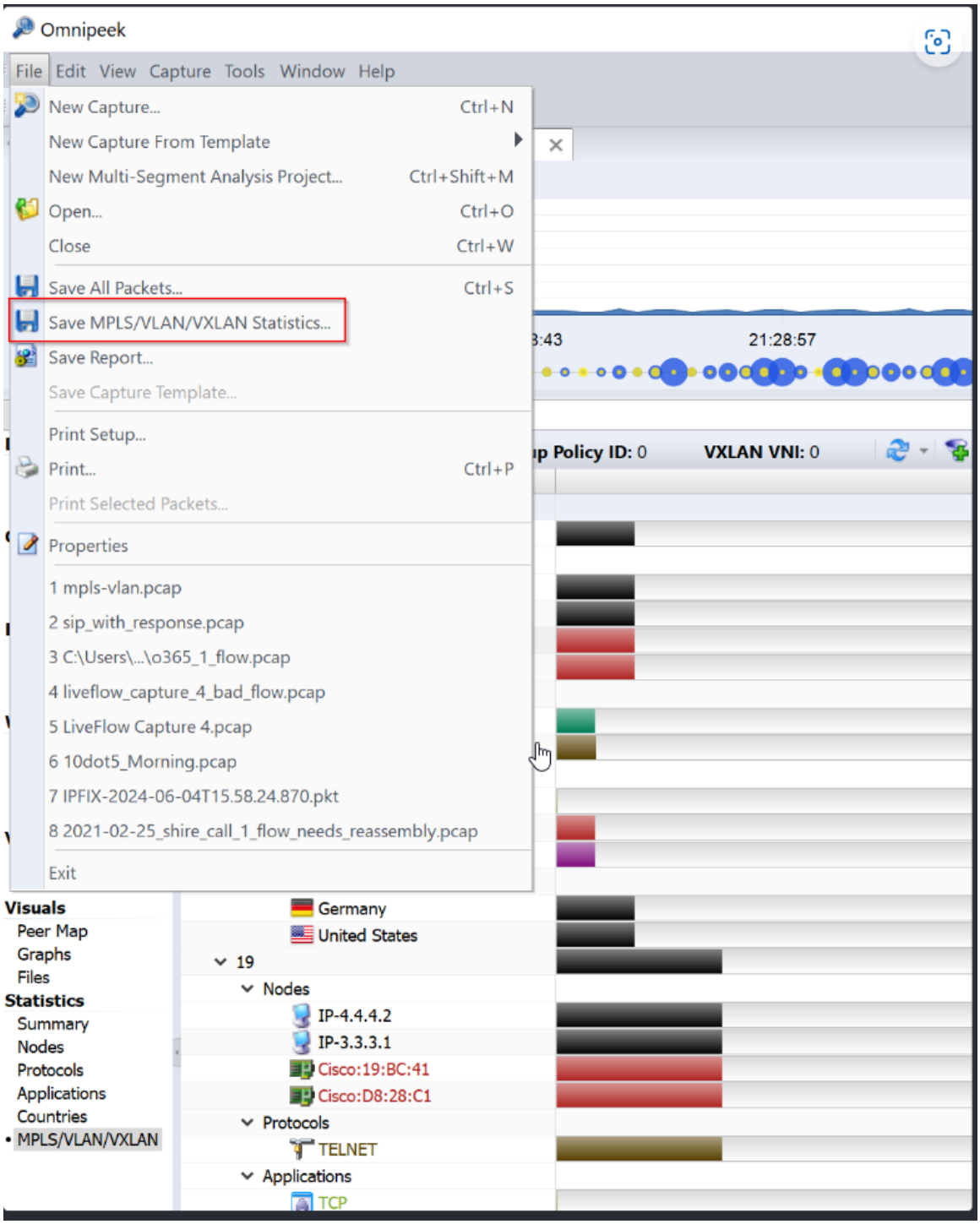
When creating a forensic search in Omnipeek Windows, a new option will be present called "MPLS/VLAN/VXLAN Statistics" which will represent this new MPLS/VLAN/VXLAN Statistics view. Enabling this option will show the MPLS/VLAN/VXLAN Statistics view in the forensic search window, while disabling this option will hide the MPLS/VLAN/VXLAN Statistics view. Clicking the configuration button next to the "MPLS/VLAN/VXLAN Statistics" item will display the MPLS/VLAN/VXLAN Statistics Limits dialog and allow the user to modify the statistics limits for this MPLS/VLAN/VXLAN Statistics view.



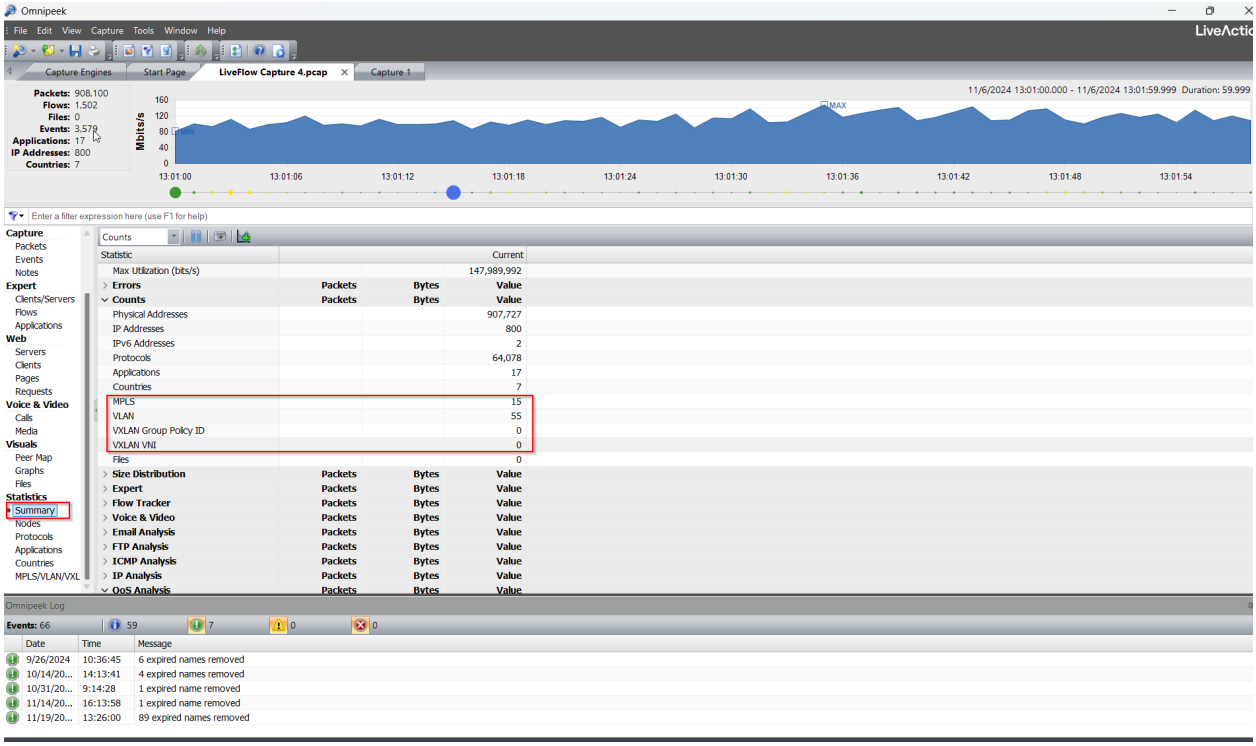
Statistics Limits

The statistics limits work the same way as the other statistics limits work for other statistic views (such as Nodes, Node Details, Protocols, etc...). The only difference is that for MPLS/VLAN/VXLAN Statistics, the limit pertains to the total number of Nodes for all MPLS Labels, VLAN IDs, VXLAN Group Policy IDs and VXLAN VNIs.

Saving/Exporting MPLS/VLAN/VXLAN Statistics to a text file

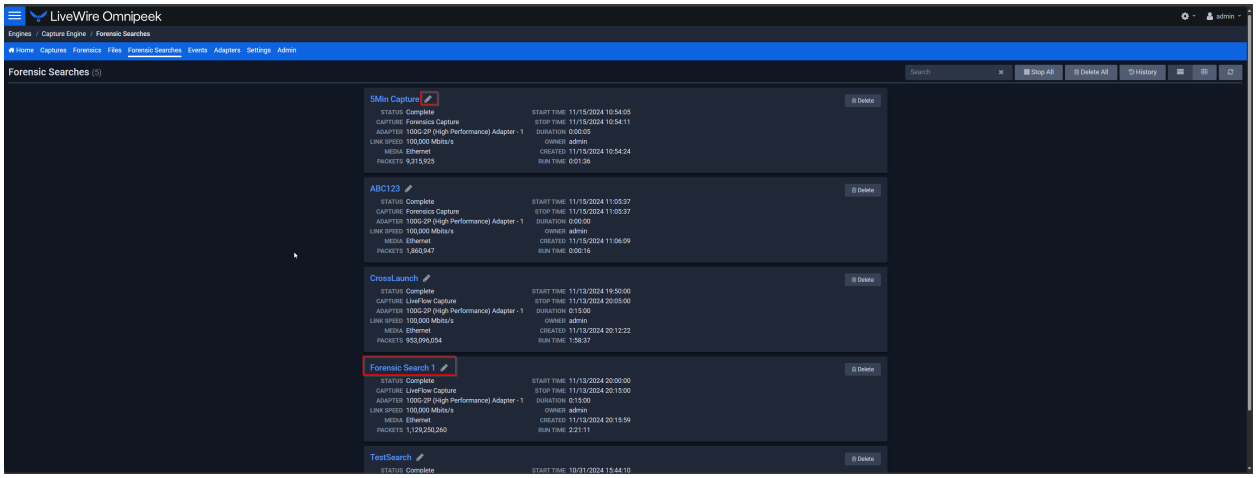


Statistics Summary page for MPLS/VLAN/VXLAN



Rename Forensic Search after creating/running the search

- Click the pencil next to the name of the Forensic Search you want to change the name of. In the screenshot below, the name of Forensic Search was changed to *5Min Capture*.

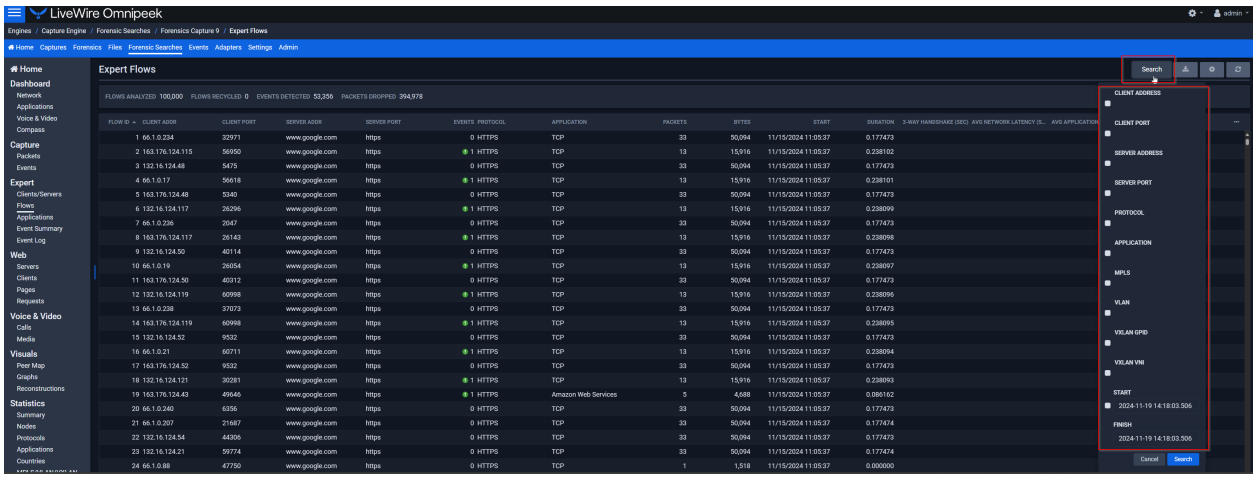


Specific Expert Flows in LiveWire Omnipeek

Here are the steps to search for specific flows in the *Expert Flows* section in LiveWire Omnipeek.

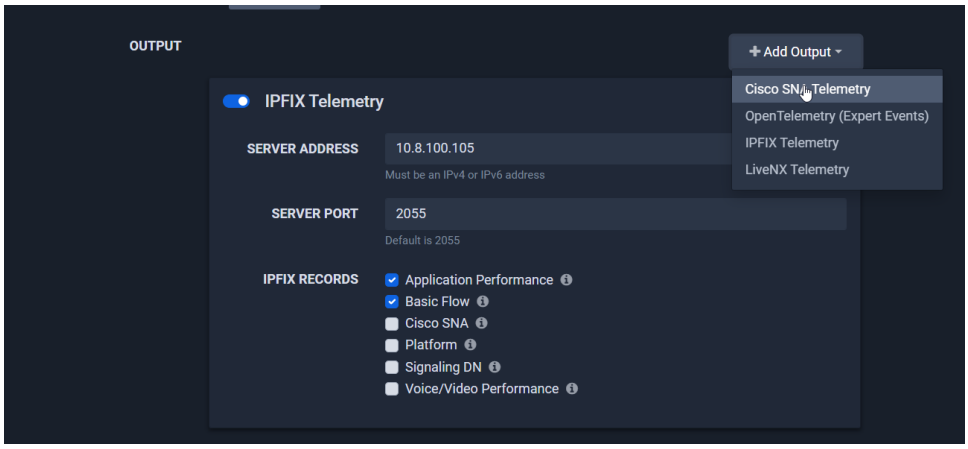
Go to Forensic *Search* > *Expert* > *Flows* > *Search* in the upper right corner of the screen.

From there you can search by specific network data in the flow that you want to see instead of searching the flows manually.



Send IPFIX Flow data to multiple targets

You can configure multiple locations/targets to send IPFIX/Flow data to. Either IPv4 or IPv6 IP addresses must be entered in the *Server Address* field.



You can also specify more than one location to send IPFIX flow data to.

You'll be able to configure LiveNX, IPFIX, OpenTelemetry, and Cisco SNA Telemetry instead of just a singular location.

LiveWire Group Authentication

LiveWires can be added to a "group" that shares the same authentication settings, allowing access without needing to enter or save a username and password.

The primary use case for this feature is to make using Distributed Forensic Search and the Multi-Engine feature easier.

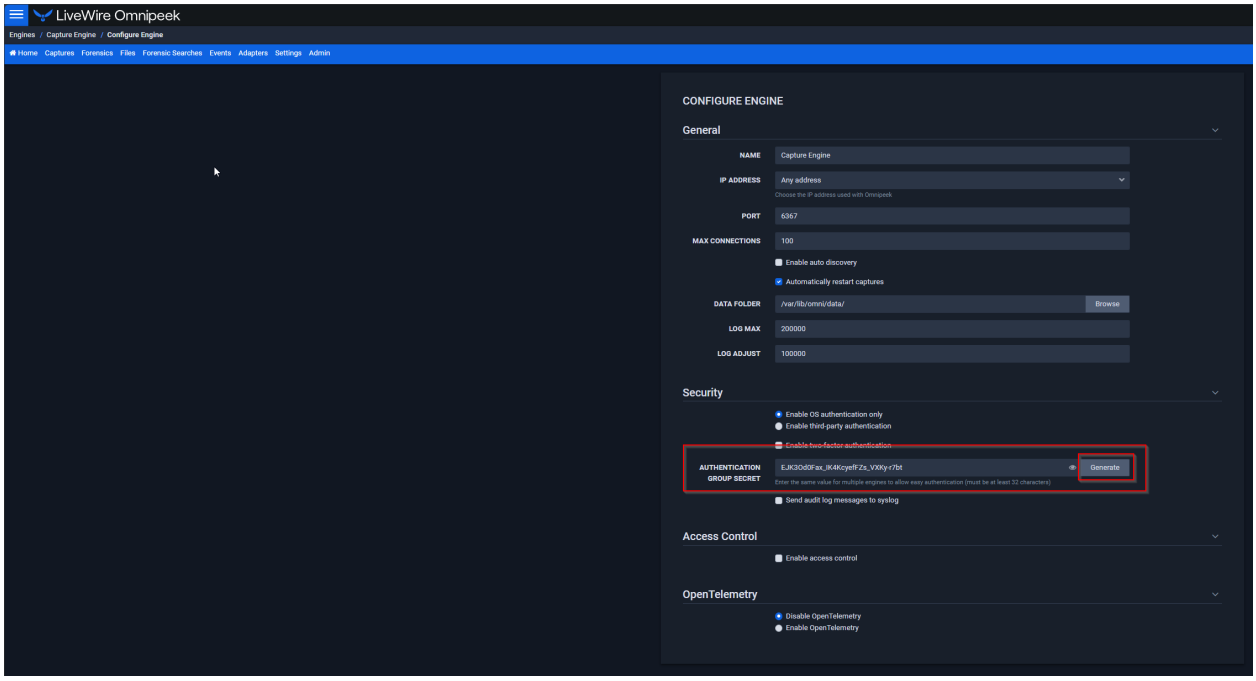
This feature was introduced in LiveWire 24.3 and requires this version or higher for LiveWires accessed remotely from the primary LiveWire.

> **Note** This feature is only available in the LiveWire Omnipeek and is not present in Omnipeek Windows.

Configuration

Set up the Authentication Group Secret

On the **Configure Engine** page for your primary engine (the one you connect to directly), enter or generate an Authentication Group Secret. The primary engine maintains the list of engines you connect to remotely.



Apply the Secret to Other Engines

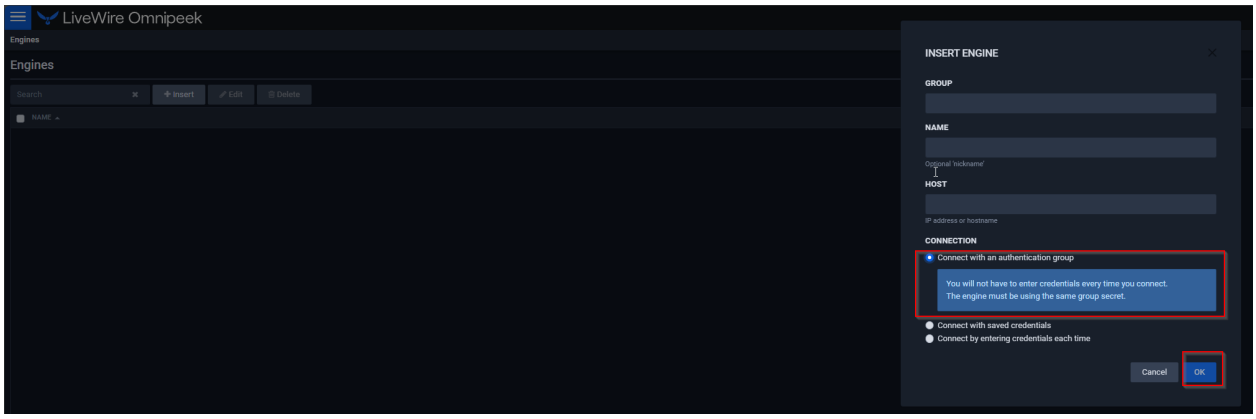
Next, enter the same Authentication Group Secret in the settings for each additional engine you want to access remotely from the primary engine. You can either:

- Use **Apply to Other Engines** to push the same settings (including other authentication and access control settings) to multiple engines, or
- Visit the **Configure Engine** page for each engine individually.

LiveWires are part of the same "authentication group" when they have the same Authentication Group Secret.

Enable Authentication Group Connection

Finally, enable **Connect with an authentication group** when inserting or editing an engine in the **Engines** list of the primary engine.



Use

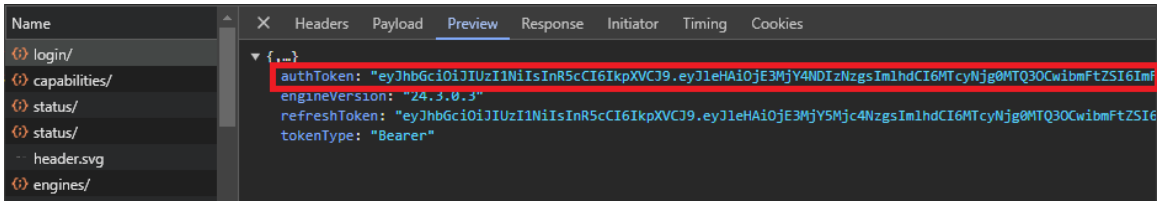
- **Seamless Remote Connection**
  Connect to remote engines from the primary engine without being prompted for a username or password.
- **Effortless Distributed Features**
  Use Distributed Forensic Search or Multi-Segment Analysis without the need to re-enter authentication details.

Implementation Details

The LiveWire Omnipeek UI and back-end now use *JSON Web Tokens (JWTs)*, a widely adopted technology in modern web applications. These tokens contain information such as the expiration time (`exp`), the time the token was issued (`iat`), a username (`name`), a not-valid-before time (`nbf`), a session id (`sess`), and a user id (`sub`). JWTs are signed to verify authenticity.

Example

In this screenshot of the Chrome Developer Tools Network Tab, the login API returns a JWT for the `authToken` in the response along with the `tokenType` "Bearer". This is otherwise known as an **access token**.



The complete JWT returned is `eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE3MjY4NDIzNzgsImlhdCI6MTcyNjg0MTQ3OCwibmFtZSI6ImFkbWluIiwibmJmIjoxNzI2ODQxNDc4LCJzZXNzIjoiNjY5M2UzN2FhNDQ2ZDlkNjBkNmUxYTMyNGYzMzk2OTUiLCJzdWIiOiJhZG1pbiJ9.HHTNCdyWKe7inqS8ZA2D5hzWLySRHp4IbXqgbsj5pC4.`

The token is in 3 parts: the header, payload, and signature. It is signed using the Authentication Group Secret, `mGyHk81TmH4YwIN_qxaFQASKPI9QusfY`.

The token can decoded and verified online https://jwt.io/#debugger-io?token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE3MjY4NDIzNzgsImlhdCI6MTcyNjg0MTQ3OCwibmFtZSI6ImFkbWluIiwibmJmIjoxNzI2ODQxNDc4LCJzZXNzIjoiNjY5M2UzN2FhNDQ2ZDlkNjBkNmUxYTMyNGYzMzk2OTUiLCJzdWIiOiJhZG1pbiJ9.HHTNCdyWKe7inqS8ZA2D5hzWLySRHp4IbXqgbsj5pC4.

Compatibility

JWTs are now the default authentication method for the LiveWire Web UI by requesting a `tokenType` of "Bearer" in the login API. However, the previous authentication method is still supported by engines that do not support JWTs, ensuring backward compatibility.

Security

Since JWTs carry sensitive information, they are always transmitted over encrypted channels (TLS) to prevent eavesdropping. However, if an attacker gains access to a JWT, they could use it to obtain unauthorized access. To mitigate this risk, JWTs used by LiveWire have a short expiration time (15 minutes) and must be periodically renewed using a "refresh token".

Expiration & Refresh Tokens

When the LiveWire UI requests a JWT from the login API, the engine returns an access token with a short expiration time (15 minutes by default) along with a "refresh token". The refresh token is used to obtain new access tokens when the current one nears expiration. The web UI will automatically request a new access token about 1 minute before the current token expires.

- **Remote Engine Connections**
  The access token is used to connect to remote engines, with the session identified by the session ID in the token. The session will remain active even after a new token is issued.
- **Refresh Token Lifetime**
  The refresh token also has an expiration time, typically set to 1 day. Both the refresh token and access token lifetimes can be configured in *omni.conf* by adjusting the `refreshtokenlifetime` and `accesstokenlifetime` settings, respectively.

References

JWT RFC

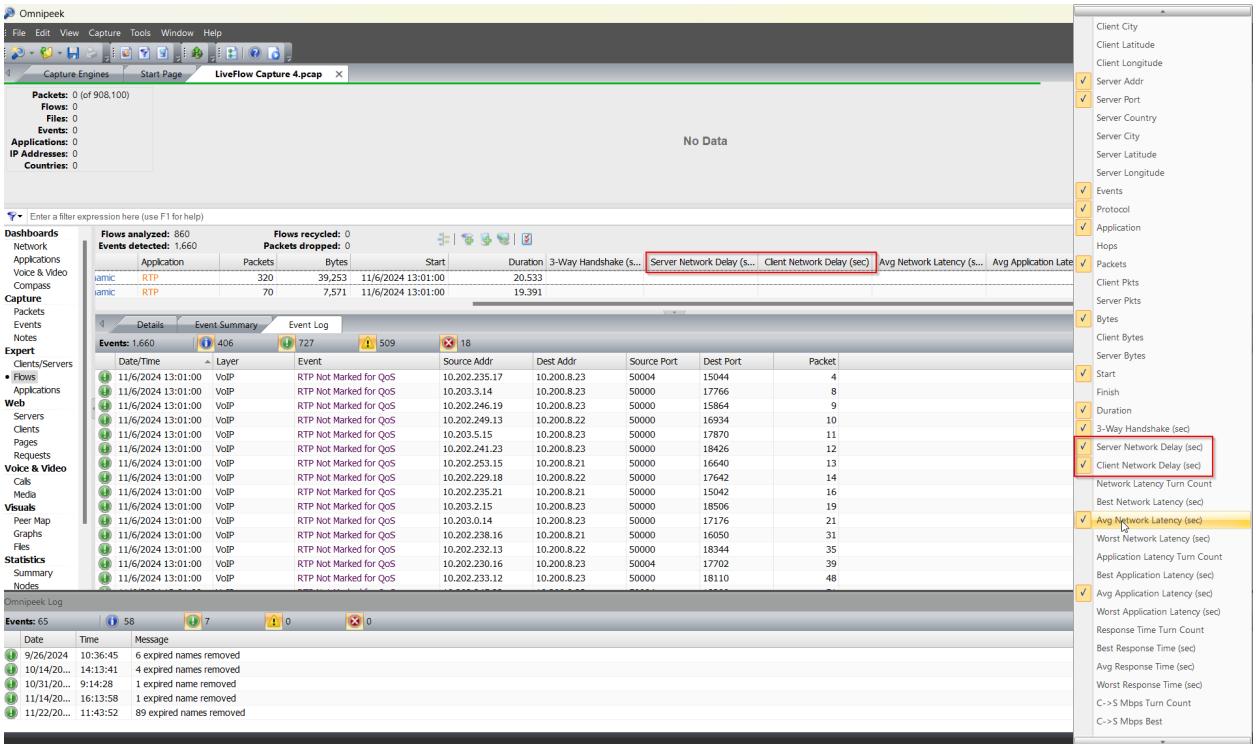
Token Best Practices

Refresh Tokens

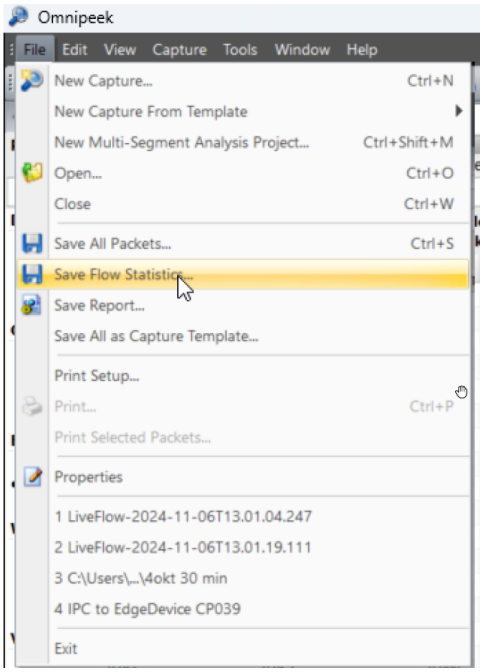
New Expert Events have been added to Omnipeek Windows

The following values have been added to Expert:

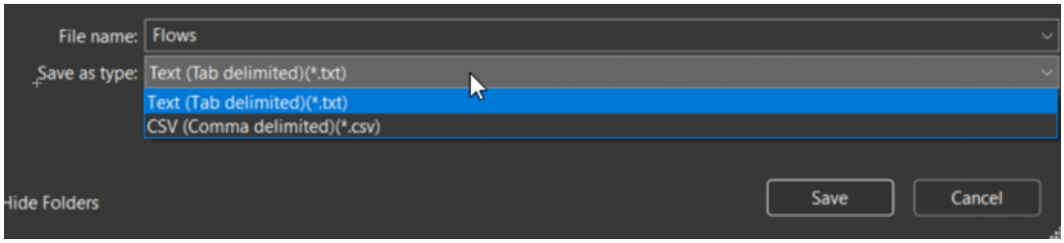
- *Server Network Delay (sec)* - the packet time difference between the TCP SYN packet and the TCP SYN-ACK packet in a TCP 3-way Handshake
- *Client Network Delay (sec)* - the packet time difference between the TCP SYN-ACK packet and the TCP ACK packet in a TCP 3-way Handshake



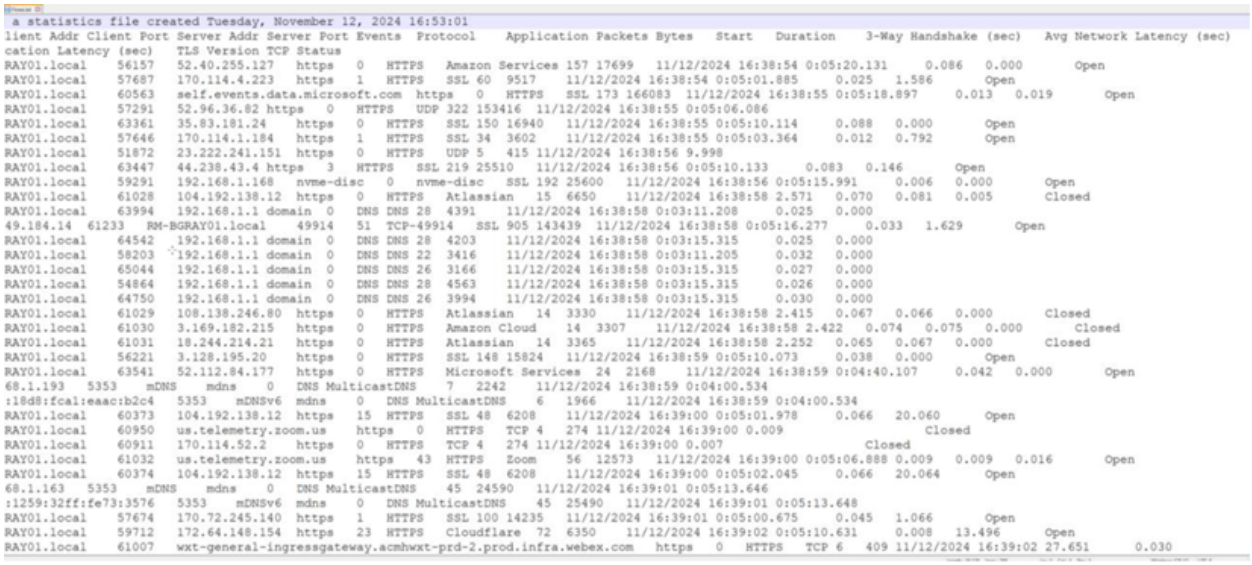
You can also export the data in *Save Flow Statistics* in the **File** menu.



This will save the Server/Network Delay statistics in a comma separated value file or text file.



Example of flows.text file contents:



```
 a statistics file created Tuesday, November 12, 2024 16:53:01
lient Addr Client Port Server Addr Server Port Events  Protocol    Application Packets Bytes   Start   Duration    3-Way Handshake (sec)   Avg Network Latency (sec)
cation Latency (sec)   TLS Version TCP Status
RAY01.local    56157   52.40.255.127   https   0   HTTPS   Amazon Services 157 17699   11/12/2024 16:38:54 0:05:20.131     0.086   0.000       Open
RAY01.local    57687   170.114.4.223   https   1   HTTPS   SSL 60  9517    11/12/2024 16:38:54 0:05:01.885     0.025   1.586       Open
RAY01.local    60563   self.events.data.microsoft.com  https   0   HTTPS   SSL 173 166083  11/12/2024 16:38:55 0:05:18.897     0.013   0.019       Open
RAY01.local    57291   52.96.36.82 https   0   HTTPS   UDP 322 153416  11/12/2024 16:38:55 0:05:06.086
RAY01.local    63361   35.83.181.24    https   0   HTTPS   SSL 150 16940   11/12/2024 16:38:55 0:05:10.114     0.088   0.000       Open
RAY01.local    57646   170.114.1.184   https   1   HTTPS   SSL 34  3602    11/12/2024 16:38:55 0:05:03.364     0.012   0.792       Open
RAY01.local    51872   23.222.241.151  https   0   HTTPS   UDP 5   415 11/12/2024 16:38:56 9.998
RAY01.local    63447   44.238.43.4 https   3   HTTPS   SSL 219 25510   11/12/2024 16:38:56 0:05:10.133     0.083   0.146       Open
RAY01.local    59291   192.168.1.168   nvme-disc   0   nvme-disc   SSL 192 25600   11/12/2024 16:38:56 0:05:15.991     0.006   0.000       Open
RAY01.local    61028   104.192.138.12  https   0   HTTPS   Atlassian   15  6650    11/12/2024 16:38:58 2.571   0.070   0.081   0.005       Closed
RAY01.local    63994   192.168.1.1 domain  0   DNS DNS 28  4391    11/12/2024 16:38:58 0:03:11.208     0.025   0.000
49.184.14  61233   RM-BGRAY01.local    49914   51  TCP-49914   SSL 905 143439  11/12/2024 16:38:58 0:05:16.277     0.033   1.629       Open
RAY01.local    64542   192.168.1.1 domain  0   DNS DNS 28  4203    11/12/2024 16:38:58 0:03:15.315     0.025   0.000
RAY01.local    58203   192.168.1.1 domain  0   DNS DNS 22  3416    11/12/2024 16:38:58 0:03:11.205     0.032   0.000
RAY01.local    65044   192.168.1.1 domain  0   DNS DNS 26  3166    11/12/2024 16:38:58 0:03:15.315     0.027   0.000
RAY01.local    54864   192.168.1.1 domain  0   DNS DNS 28  4563    11/12/2024 16:38:58 0:03:15.315     0.026   0.000
RAY01.local    64750   192.168.1.1 domain  0   DNS DNS 26  3994    11/12/2024 16:38:58 0:03:15.315     0.030   0.000
RAY01.local    61029   108.138.246.80  https   0   HTTPS   Atlassian   14  3330    11/12/2024 16:38:58 2.415   0.067   0.066   0.000       Closed
RAY01.local    61030   3.169.182.215   https   0   HTTPS   Amazon Cloud    14  3307    11/12/2024 16:38:58 2.422   0.074   0.075   0.000       Closed
RAY01.local    61031   18.244.214.21   https   0   HTTPS   Atlassian   14  3365    11/12/2024 16:38:58 2.252   0.065   0.067   0.000       Closed
RAY01.local    56221   3.128.195.20    https   0   HTTPS   SSL 148 15824   11/12/2024 16:38:59 0:05:10.073     0.038   0.000       Open
RAY01.local    63541   52.112.84.177   https   0   HTTPS   Microsoft Services  24  2168    11/12/2024 16:38:59 0:04:40.107     0.042   0.000       Open
68.1.193   5353    mDNS    mdns    0   DNS MulticastDNS    7   2242    11/12/2024 16:38:59 0:04:00.534
:18d8:fca1:eaac:b2c4   5353    mDNSv6  mdns    0   DNS MulticastDNS    6   1966    11/12/2024 16:38:59 0:04:00.534
RAY01.local    60373   104.192.138.12  https   15  HTTPS   SSL 48  6208    11/12/2024 16:39:00 0:05:01.978     0.066   20.060      Open
RAY01.local    60950   us.telemetry.zoom.us    https   0   HTTPS   TCP 4   274 11/12/2024 16:39:00 0.009                   Closed
RAY01.local    60911   170.114.52.2    https   0   HTTPS   TCP 4   274 11/12/2024 16:39:00 0.007                   Closed
RAY01.local    61032   us.telemetry.zoom.us    https   43  HTTPS   Zoom    56  12573   11/12/2024 16:39:00 0:05:06.888 0.009   0.009   0.016       Open
RAY01.local    60374   104.192.138.12  https   15  HTTPS   SSL 48  6208    11/12/2024 16:39:00 0:05:02.045     0.066   20.064      Open
68.1.163   5353    mDNS    mdns    0   DNS MulticastDNS    45  24590   11/12/2024 16:39:01 0:05:13.646
:1259:32ff:fe73:3576   5353    mDNSv6  mdns    0   DNS MulticastDNS    45  25490   11/12/2024 16:39:01 0:05:13.648
RAY01.local    57674   170.72.245.140  https   1   HTTPS   SSL 100 14235   11/12/2024 16:39:01 0:05:00.675     0.045   1.066       Open
RAY01.local    59712   172.64.148.154  https   23  HTTPS   Cloudflare  72  6350    11/12/2024 16:39:02 0:05:10.631     0.008   13.496      Open
RAY01.local    61007   wxt-general-ingressgateway.acmhwxt-prd-2.prod.infra.webex.com   https   0   HTTPS   TCP 6   409 11/12/2024 16:39:02 27.651      0.030
```