



FlowMagic Network Packet Capture, Packet Viewer, Analytics and Export User Guide

Supported Models:

FlowMagic-400

FlowMagic-3200

FlowMagic-3240

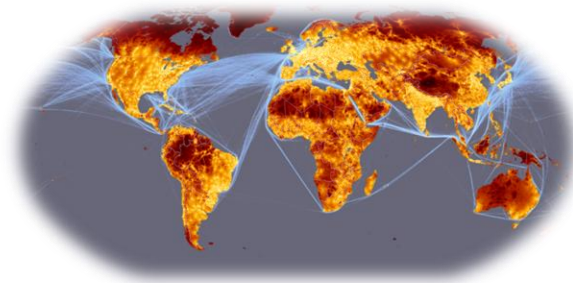
FlowMagic-StorageShelf-3545

RELEASE 1.1.0.00682

Doc. No. UG104

March 30, 2017

INFINICORE INCORPORATED



Copyright © 2010-2017 Infinicore® Incorporated. All rights reserved.

No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, except as may be expressly permitted by the applicable copyright statutes or in writing by the Publisher.

The following are registered trademarks of Infinicore™ Incorporated: Infinicore and the Infinicore logo.

The following are trademarks of Infinicore Corporation: InfiniCore and Infiniload.

All other trademarks and/or registered trademarks are the property of their respective owners.

Infinicore disclaims any express or implied warranty relating to the sale and/ or use of Infinicore products, including liability or warranties relating to fitness for a particular purpose, merchantability or infringement of any patent, copyright or other intellectual property right. Products described in this document are NOT intended for use in medical, life support, or other hazardous uses where malfunction could result in death or bodily injury.

THE INFORMATION CONTAINED IN THIS DOCUMENT IS PROVIDED ON AN “AS IS” BASIS. Infinicore assumes no liability for damages arising directly or indirectly from any use of the information contained in this document.

Publishing Information:

Document Number	UG104
Doc. Release Number	1.1.0.00682
Date	March 30th, 2017

Contact Information:

Infinicore Incorporated
Information: info@infinicoreinc.com
Web Site: http://www.infinicoreinc.com

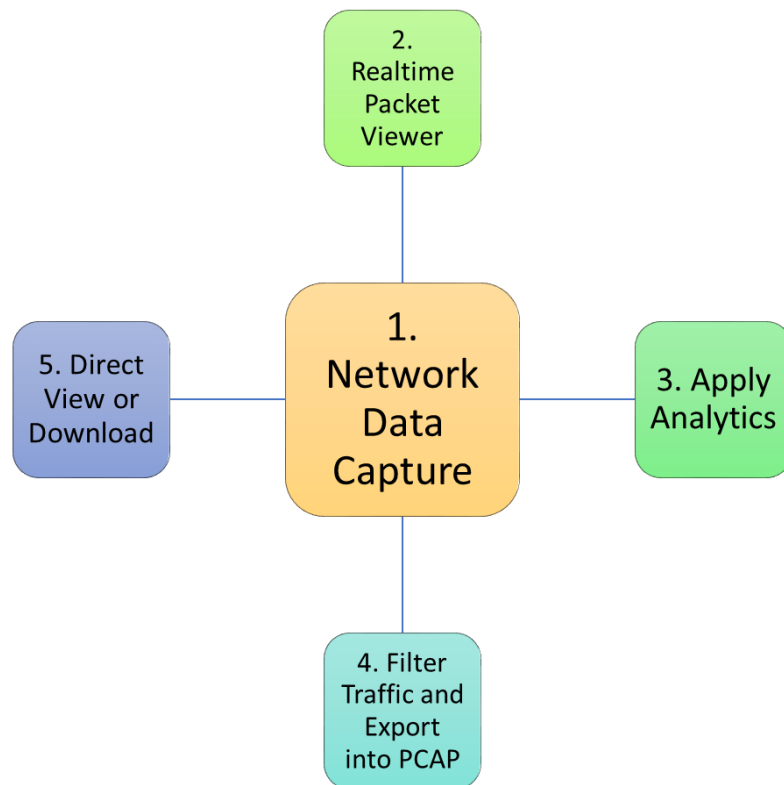
Table of Contents

Chapter 1 Overview of Five Major Operations	4
Chapter 2 Network Data Capture	6
2.1 Check Network Data Storage and Capture Interfaces Speed	6
2.1.1 Check Network Data Storage	6
2.1.2 Check Network Interface Speed	7
2.2 Network Data Capture	7
Chapter 3 Real-time Packet Decoder and Viewer	10
Chapter 4 FlowMagic Analytics Function	11
Chapter 5 Filter and PCAP export	14
5.1 Export Using the Export Dialog	14
5.2 Export Using Row Selection	15
Chapter 6 Recommended Reading Material	16

Chapter 1 Overview of Five Major Operations

Among many functions provided by FlowMagic appliance, there are five operations that are designed to provide packet capture and packet view, network traffic analysis, traffic filter, export, view and export. Together, these operations can greatly improve network administrators' efficiency during incident response and retrospective analysis capabilities.

This user guide is design to give FlowMagic customers an overview of the five most frequently used operation. All five operations can be invoked from FlowMagic's Web User Interface.



- **Network Data Capture**

Network Data Capture Operation will enable FlowMagic to receive traffic from selected network interfaces. Multiple ports can be assigned within a single capture. Each capture creates a named capture domain. The named domain can be used as a handle to access the capture data and start other operations.

- **Direct Packet Viewer**

FlowMagic Appliance has a purposefully designed packet decoder and viewer that can be invoked directly from WEB UI in order to see the traffic. Users can view the traffic from any device with a Web browser.

- [Traffic Analytics](#)

FlowMagic has several built-in analytics that can be used to drill through massive amount of captured data. The results can be displayed on the UI, saved for later access or downloaded as a CSV file. More importantly, operator can create filter from the result and use the filter to export traffic.

- [Filter and Export Traffic in PCAP](#)

Indirectly invoked from the analytics results or directly invoked from the UI, FlowMagic allows customer to filter traffic and export in PCAP format.

- [View and Download Exported PCAP](#)

FlowMagic provides capabilities to directly view exported PCAP or download the PCAP for off-line analysis purpose.

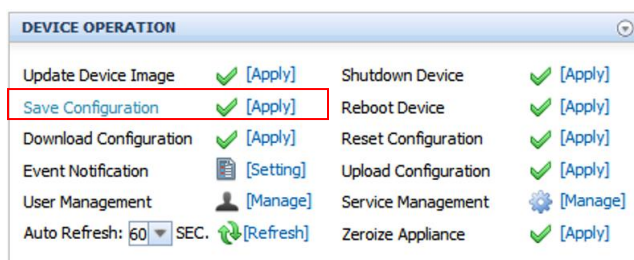
In this user guide, we will provide a series of examples to guide you through the above 5 major operations.

Chapter 2 Network Data Capture

Network Data Capture has been designed to be an easy to follow process. Before starting a packet capture, storage drives needs to be properly enabled and interface speed needs to be selected.

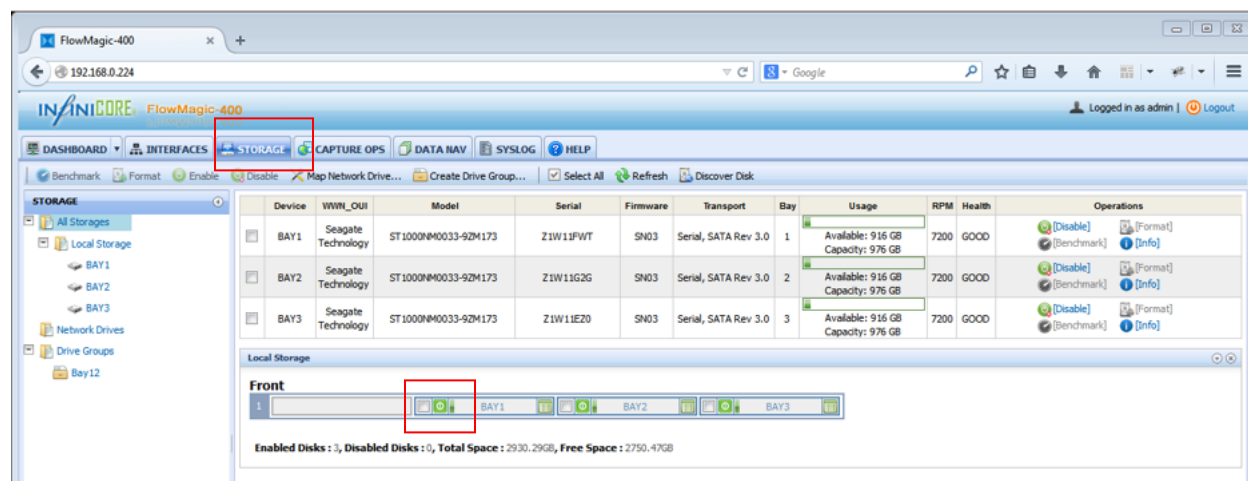
2.1 Check Network Data Storage and Capture Interfaces Speed


Please note that for both data storage and capture interface configuration, the setting only needs to be done once. When saved, the configuration will be automatically applied from power cycle. To save configuration, use the 'Save Configuration' as shown below.

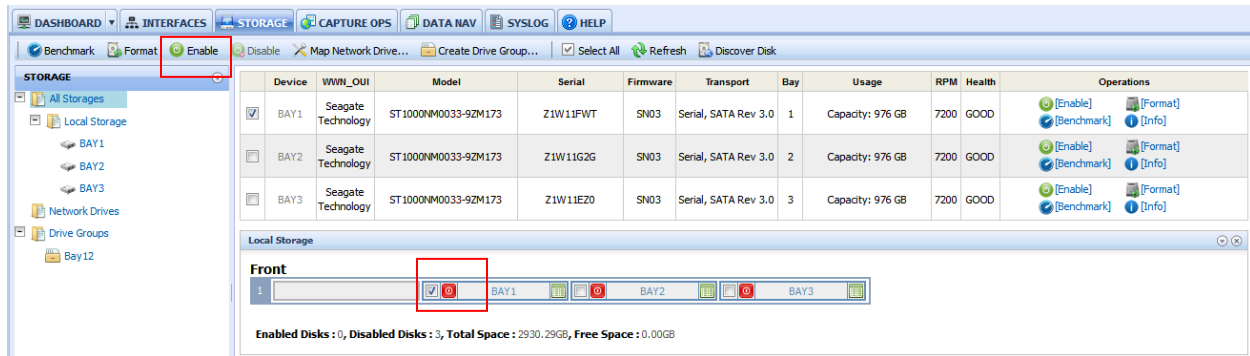


2.1.1 Check Network Data Storage

Each FlowMagic appliance has disk drive bays that are dedicated for the purpose of storing captured traffic data. Drives need to be enabled before they are available for a capture operation. To enable hard drive, please click on the FlowMagic STORAGE tab.

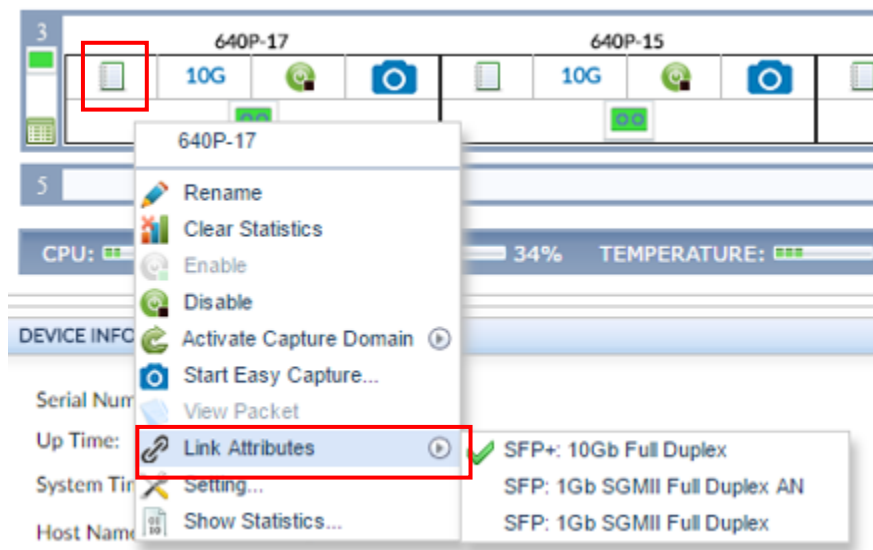


When a drive is enabled, green drive indicator  will be displayed. Otherwise the drive bay will be shown as RED. To enable a drive, simply click to select the drive and click enable.



2.1.2 Check Network Interface Speed

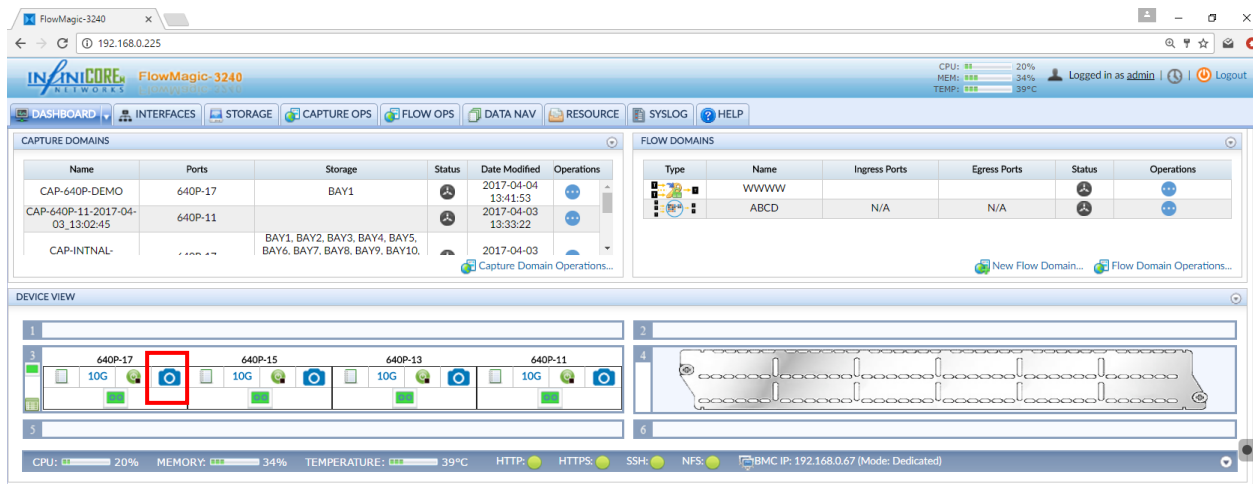
Depending on the traffic modules, FlowMagic Capture Port is capable of operating at 1Gbps speed or 1Gbps/10Gbps or 40Gbps/100Gbps speed. The speed of interface needs to match what its peer offers so that link can be brought up. The interface speed can be changed using the following drop down menu found on the top left corner of each port.



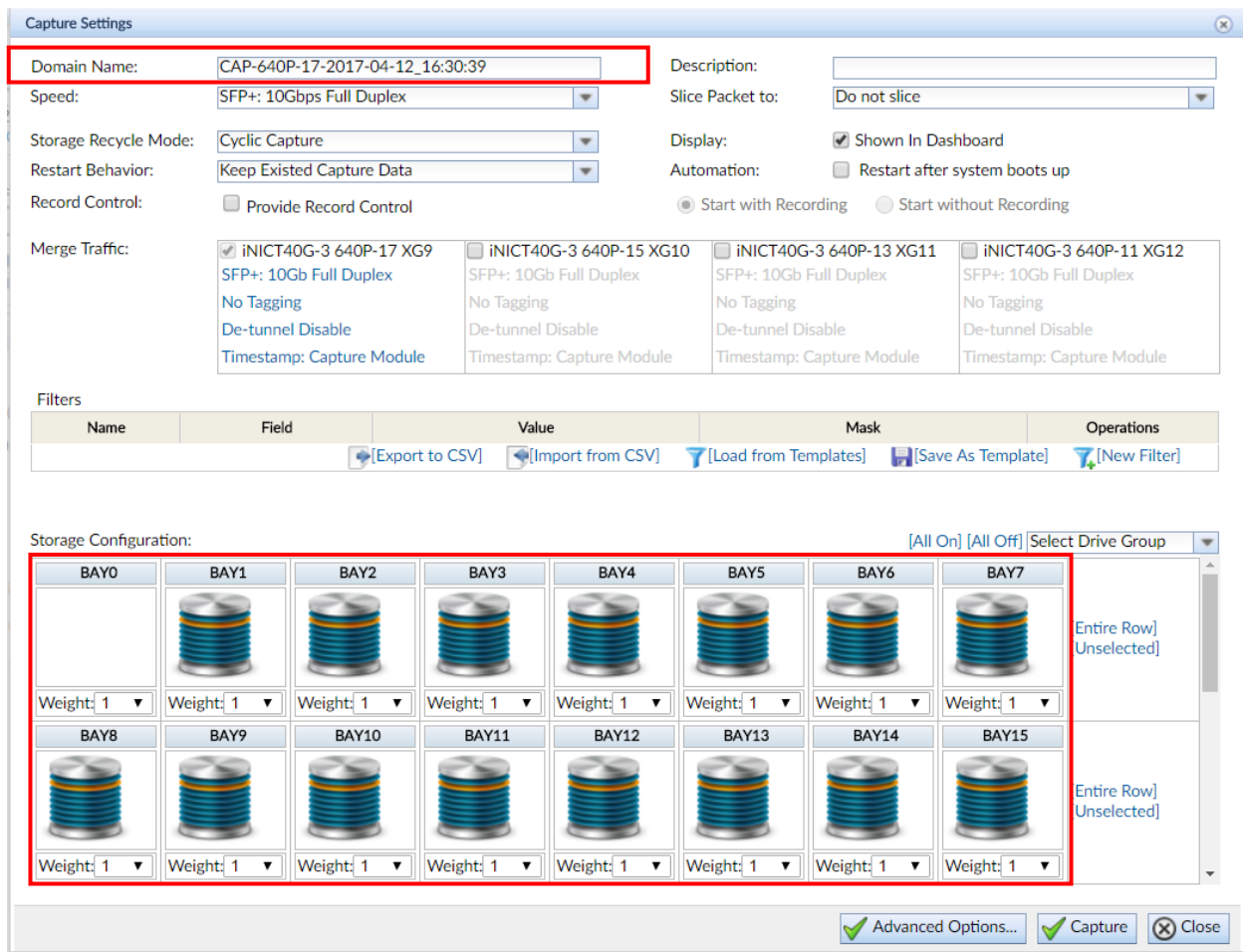
When speed is properly set, link should be turning up and the port will be shown as green.

2.2 Network Data Capture

Network Data Capture can be invoked directly from Dashboard. There is an icon  on the top right corner of each port as shown below.



Click the 'Start Easy Capture...' button will bring out the following dialog.

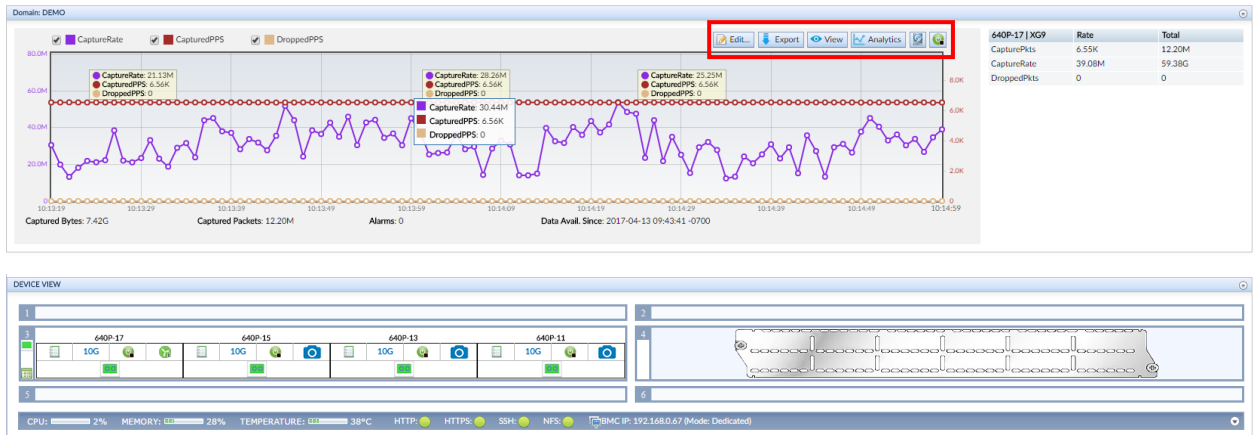


Normally user might want to change the domain name to something useful. And select the storage configuration by clicking on the disk drive icon. To max the capture to disk speed, all drives can be

selected. Drive can be reused for different capture operation if the capture performance is not at major concern.

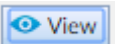
To merge the traffic from a different port, click on the interface shown in the ‘Merge Traffic’ section on the same dialog.

Once the capture starts, a progress dialog will be displayed and the captured data graph will be shown on the dashboard.

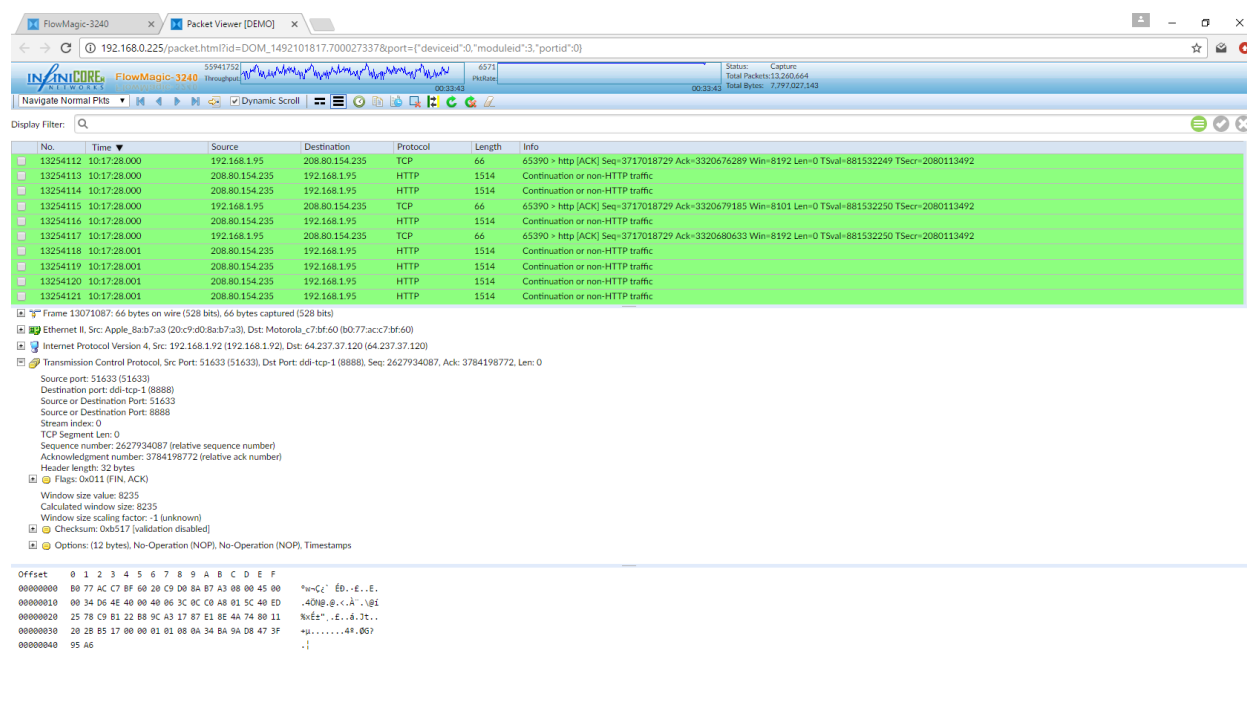


Please note that there will be three shortcuts available on the lower right corner of real time graph. They can be used to invoke the real time packet viewer and analytics function.

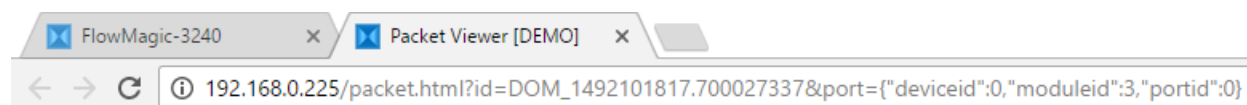
Chapter 3 Real-time Packet Decoder and Viewer


FlowMagic appliance has an integrated packet decoder that operator can use to take a direct look into the traffic. To invoke real time packet decoder, click  View button.

The real time packet viewer will be displayed on a separate TAB together with the original UI so that user can easily switch between the two.

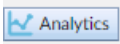


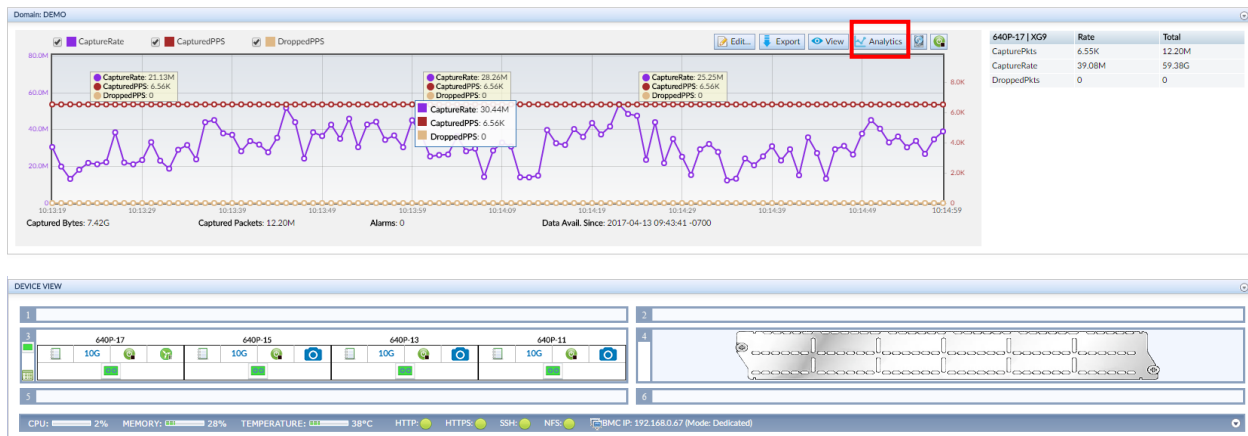
Please note the link shown on the address bar is a link that can be shared. Simply copy and paste into browser the same view will be opened and displayed.



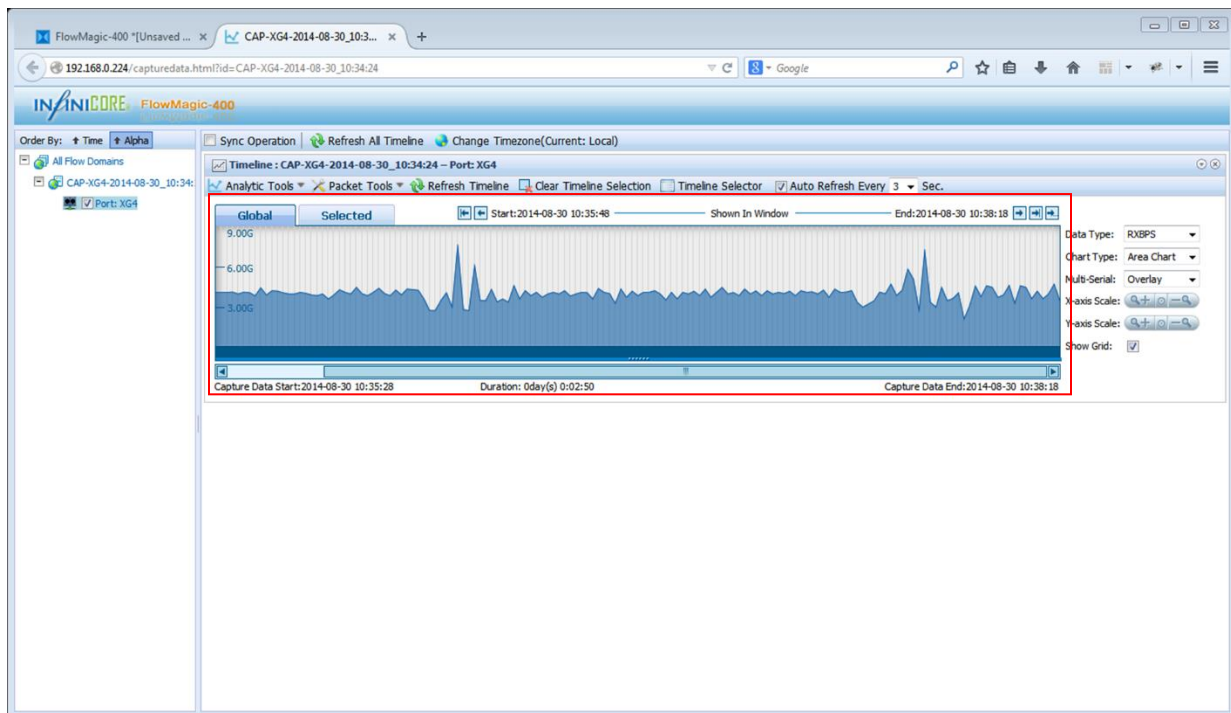
The packet viewer is a wireshark alike view into the packet data. When  Show New Captured Packets is checked, the viewer will automatically scrolled to the new captured packets. Uncheck or click on any packet will stop the scrolling and goes into manual check mode.

Chapter 4 FlowMagic Analytics Function

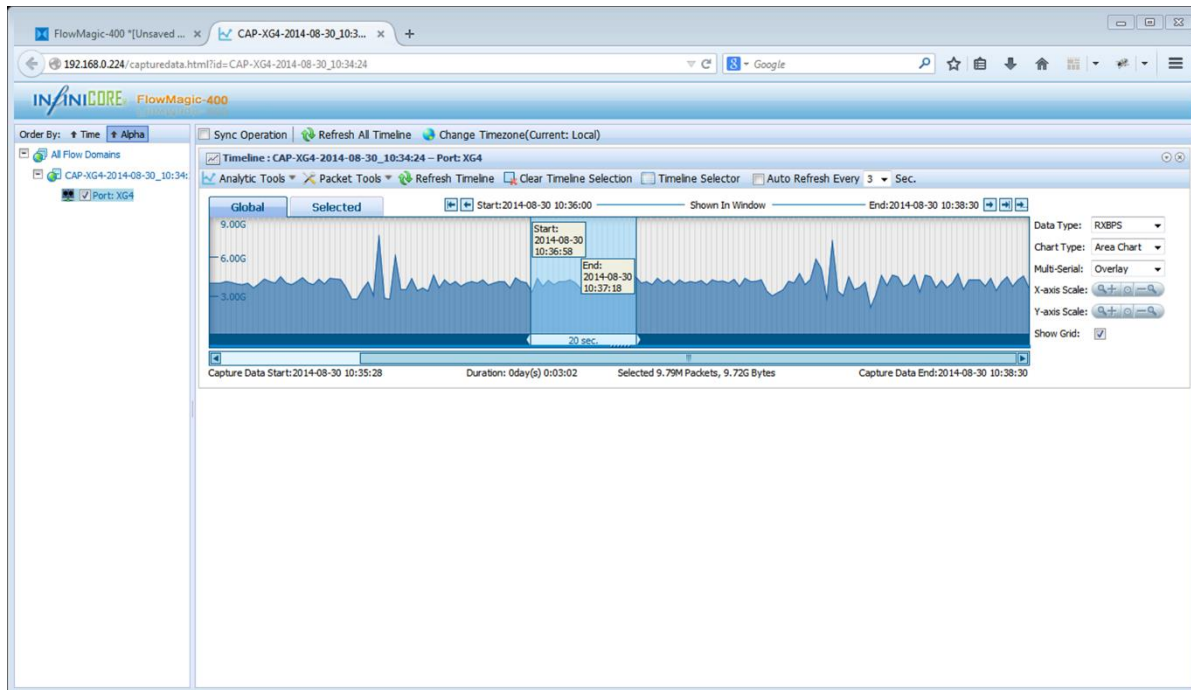
FlowMagic embeds several useful analytics functions within its software. To invoke analytics function, first invoke the analytics UI page by clicking on the  Analytics button.



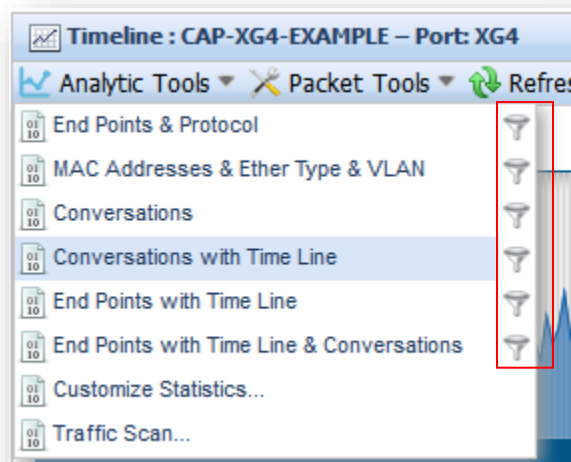
After Analytics UI loaded, one can see the following web page. InfiniCORE implements a timeline based analytic model. All the analytics function starts with a selection of time period. The time period defines the data period that the analytic function will run through.



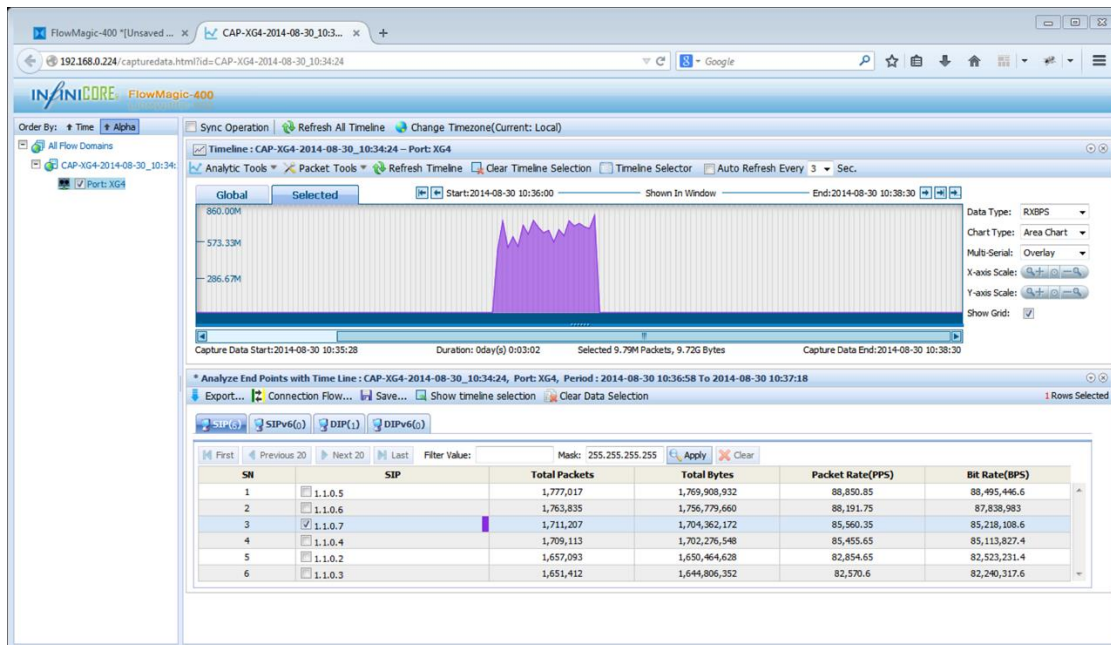
There are two ways to define time period. The first method is to use drag and drop interface. Click on the graph, hold the mouse left button and release the left mouse button when enough data is selected. After selection, the timeline window will be displayed similar to what shown below.



After time period is selected, one can use the tools shown in the **Analytic Tools** menu to invoke analytics function. One can also configure the filter function that will be applied to control the packet reading process.



After the analytics runs to the end, the analytics' result will be displayed below the time line window. The following screen shot shows what the result looks like.

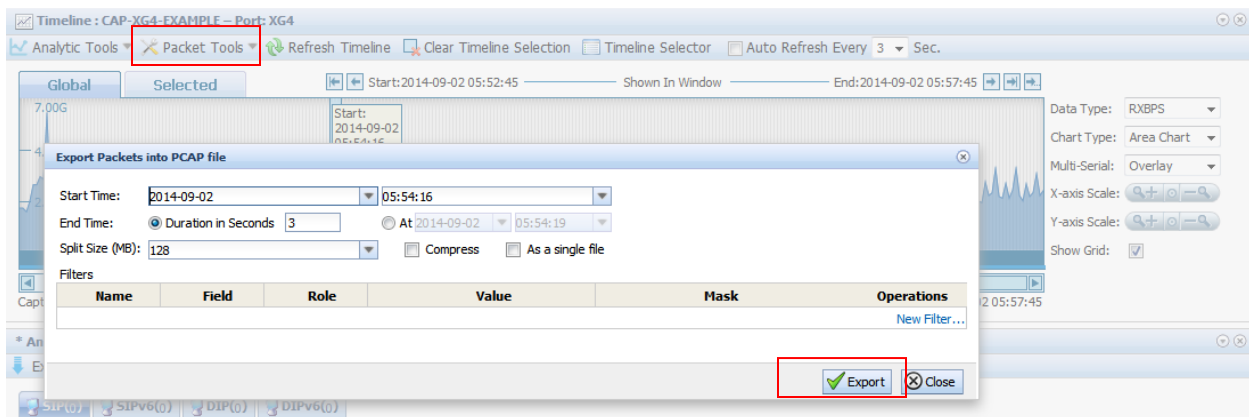


Chapter 5 Filter and PCAP export

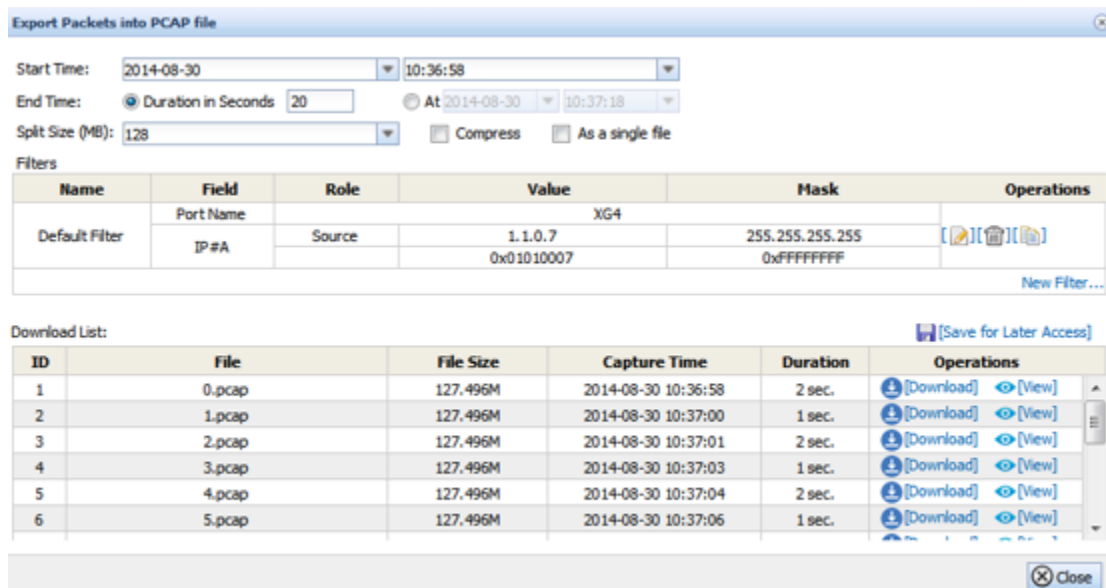
FlowMagic has an easy to use filter system. One can invoke it either within the export dialog or select rows from the analytic result to export. In the later case, FlowMagic will configure the filter automatically for the export process.

5.1 Export Using the Export Dialog

Please click on the packet tools→ Export menu item to start the export dialog.



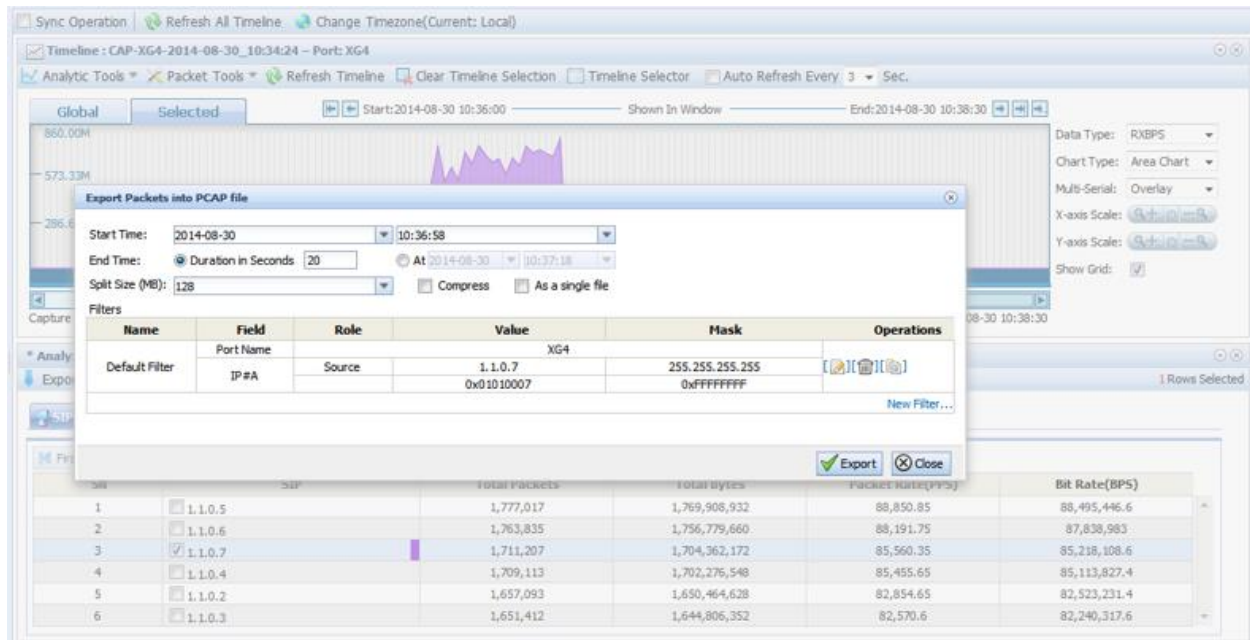
When export finishes, the result will be shown right below the original dialog.



One can choose to download a PCAP file or use view button to directly view it in the PCAP viewer.

5.2 Export Using Row Selection

One can also export packet data into the PCAP file by click on the rows shown within analytic results.



With this method, the filter is automatically configured and with a single click, one can export the traffic that matches the selected row.

Chapter 6 Recommended Reading Material

The following list provides further reading materials when users find the need to gain in-depth knowledge in specific area.

- [UG-100 FlowMagic Hardware Owner Manual and Getting Started Guide](#)
- [UG-101 FlowMagic Firmware Update Guide](#)
- [UG-102 FlowMagic System Recovery Guide](#)
- [UG-103 FlowMagic-400 Rack Mounting Guide](#)
- [UG-104 FlowMagic Network Packet Capture Analysis and Export Guide](#)
- [UG-105 FlowMagic Hard Disk Drive Selection and Storage Management Guide](#)