GRASSMARLIN User Guide

Document Control #: QS-AS017-001

Prepared for the National Security Agency

by

The GRASSMARLIN Team

September 26, 2014

(U) Revision History

Version	Date	Summary of changes
1.0	02 March 2012	GRASSMARLIN Version 1.0 User Guide: Initial release. Included logical view, live capture, PCAP import, and summary statistics as well as event and network manager models.
1.1	19 April 2012	GRASSMARLIN Version 1.1 User Guide: Physical view, session management, active scans, additional options.
1.2	18 October 2012	GRASSMARLIN Version 1.2 User Guide Separated version description guide and installation guide.
1.2.4	26 June 2013	GRASSMARLIN VERSION 1.2.4 User Guide Updated for new features. New appendix for How to make a Fingerprint
2.0	09 June 2014	GRASSMARLIN Version 2.0 Updated for new features

(U) Reference Documents

Document	Version
GRASSMARLIN Installation Guide	2.0
GRASSMARLIN How-To-Guide for fingerprints	1.0

Table of Contents

List of Figures

List of Tables

1. Product Description

GRASSMARLIN is a software prototype that provides a method for discovering and cataloging SCADA (Supervisory Control and Data Acquisition) and ICS (Industrial Control System) systems on IP-based networks. GRASSMARLIN uses a variety of sources to generate this data, including PCAP files, router and switch configuration files, CAM tables and live network packet captures. The tool can automatically determine the available networks and generate the network topology as well as visualize the communication between hosts. GRASSMARLIN is still in a prototype phase.

1.1. Versioning Schema

The official prototype is named as follows:

GRASSMARLIN v#.#.#

The version numbers include the major number, minor number, and patch number. The major number increases for fundamental or significant changes to the baseline. The minor number increases when less significant changes are made to the baseline.

1.2. Supported Platforms (32-bit and 64-bit)

Operating System – MS Windows 7, Fedora 18, or Ubuntu 12.04

2. GRASSMARLIN Start Up

When GRASSMARLIN loads, the welcome screen prompts the user to start a new session or open a previous session (Figure 1). For a new session, the GRASSMARLIN user interface will open with no data (Figure 2).

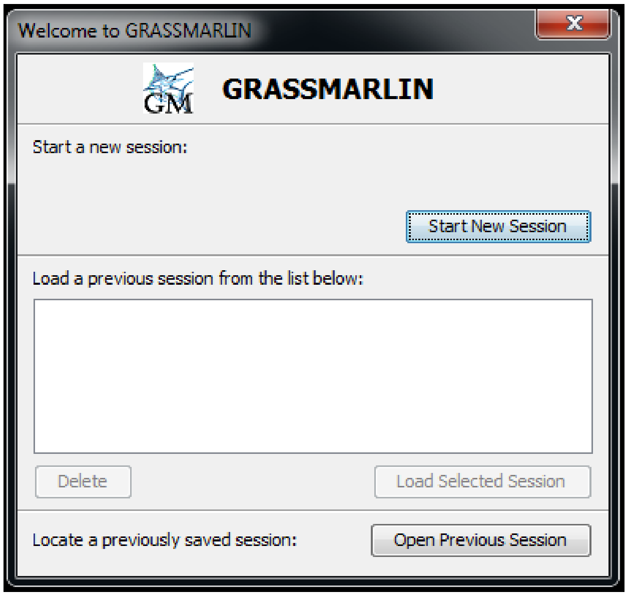
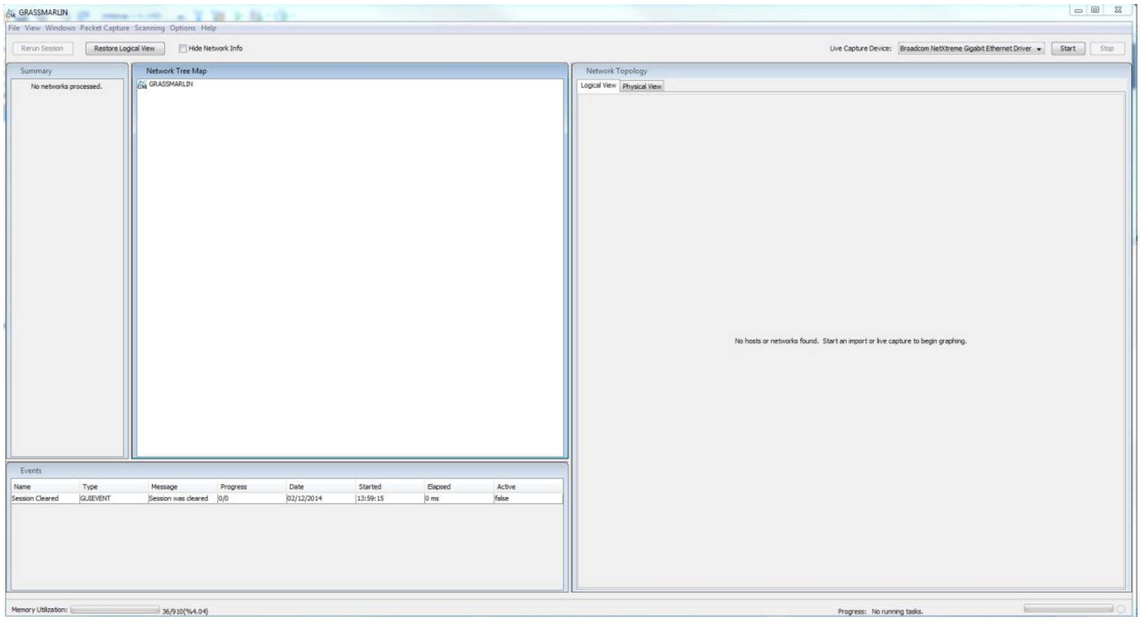


Figure 1: Welcome to GRASSMARLIN



Live Capture Device: Broadcom NetXtreme Gigabit Ethernet Driver

No networks processed.

No hosts or networks found. Start an import or live capture to begin graphing.

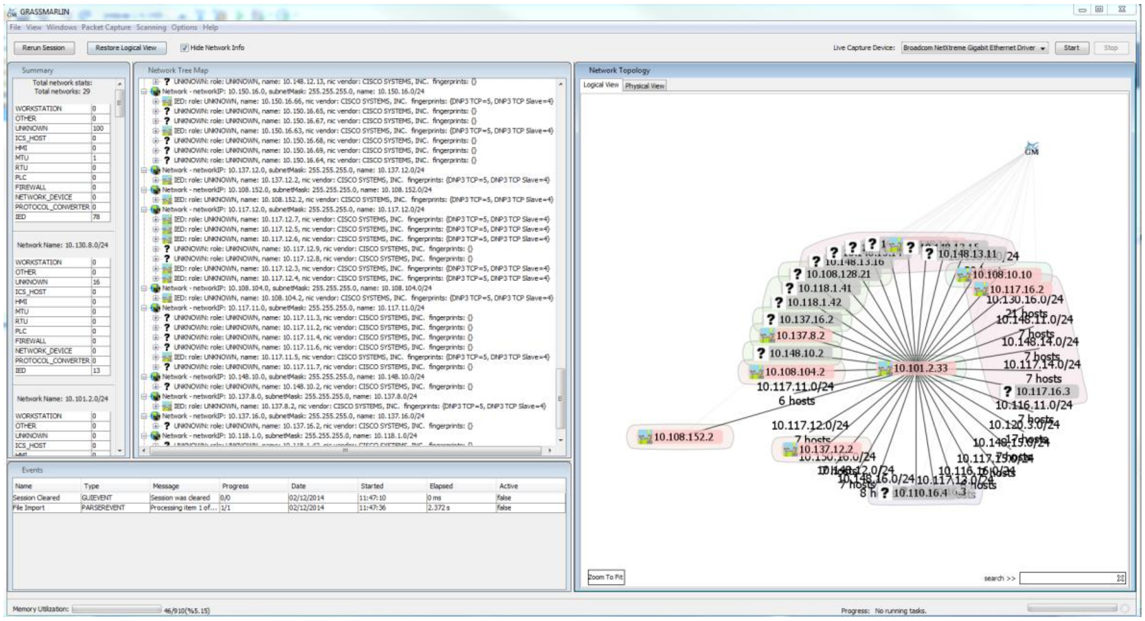
Name	Type	Message	Progress	Date	Started	Elapsed	Active
Session Cleared	GUIEVENT	Session was cleared	0/0	02/12/2014	13:59:15	0 ms	false

Memory Utilization: 36/910(%4.04)

Progress: No running tasks.

Figure 2: New GRASSMARLIN Session

GRASSMARLIN can also load all of the data from a previous 2.0 saved session into the user interface (Figure 3). **Note: Saved sessions from previous versions of GRASSMARLIN are not compatible with newer versions.** For either a new session or a loaded session, the initial view will update with new network and host information as it is imported into GRASSMARLIN.



Live Capture Device: Broadcom NetXtreme Gigabit Ethernet Driver

Total network stats:
Total networks: 29

WORKSTATION	0
OTHER	0
UNKNOWN	100
ICS_HOST	0
HMI	0
MTU	1
RTU	0
PLC	0
FIREWALL	0
NETWORK_DEVICE	0
PROTOCOL_CONVERTER	0
IED	78

Network Name: 10.130.8.0/24

WORKSTATION	0
OTHER	0
UNKNOWN	16
ICS_HOST	0
HMI	0
MTU	0
RTU	0
PLC	0
FIREWALL	0
NETWORK_DEVICE	0
PROTOCOL_CONVERTER	0
IED	13

Network Name: 10.101.2.0/24

WORKSTATION	0
OTHER	0
UNKNOWN	0
ICS_HOST	0

```
    ? UNKNOWN: role: UNKNOWN, name: 10.148.12.13, nic vendor: CISCO SYSTEMS, INC.  fingerprints: {}
Network - networkIP: 10.150.16.0, subnetMask: 255.255.255.0, name: 10.150.16.0/24
    IED: role: UNKNOWN, name: 10.150.16.66, nic vendor: CISCO SYSTEMS, INC.  fingerprints: {DNP3 TCP=5, DNP3 TCP Slave=4}
    ? UNKNOWN: role: UNKNOWN, name: 10.150.16.65, nic vendor: CISCO SYSTEMS, INC.  fingerprints: {}
    ? UNKNOWN: role: UNKNOWN, name: 10.150.16.67, nic vendor: CISCO SYSTEMS, INC.  fingerprints: {}
    IED: role: UNKNOWN, name: 10.150.16.63, nic vendor: CISCO SYSTEMS, INC.  fingerprints: {DNP3 TCP=5, DNP3 TCP Slave=4}
    ? UNKNOWN: role: UNKNOWN, name: 10.150.16.68, nic vendor: CISCO SYSTEMS, INC.  fingerprints: {}
    ? UNKNOWN: role: UNKNOWN, name: 10.150.16.69, nic vendor: CISCO SYSTEMS, INC.  fingerprints: {}
    ? UNKNOWN: role: UNKNOWN, name: 10.150.16.64, nic vendor: CISCO SYSTEMS, INC.  fingerprints: {}
Network - networkIP: 10.137.12.0, subnetMask: 255.255.255.0, name: 10.137.12.0/24
    IED: role: UNKNOWN, name: 10.137.12.2, nic vendor: CISCO SYSTEMS, INC.  fingerprints: {DNP3 TCP=5, DNP3 TCP Slave=4}
Network - networkIP: 10.108.152.0, subnetMask: 255.255.255.0, name: 10.108.152.0/24
    IED: role: UNKNOWN, name: 10.108.152.2, nic vendor: CISCO SYSTEMS, INC.  fingerprints: {DNP3 TCP=5, DNP3 TCP Slave=4}
Network - networkIP: 10.117.12.0, subnetMask: 255.255.255.0, name: 10.117.12.0/24
    IED: role: UNKNOWN, name: 10.117.12.7, nic vendor: CISCO SYSTEMS, INC.  fingerprints: {DNP3 TCP=5, DNP3 TCP Slave=4}
    IED: role: UNKNOWN, name: 10.117.12.5, nic vendor: CISCO SYSTEMS, INC.  fingerprints: {DNP3 TCP=5, DNP3 TCP Slave=4}
    IED: role: UNKNOWN, name: 10.117.12.6, nic vendor: CISCO SYSTEMS, INC.  fingerprints: {DNP3 TCP=5, DNP3 TCP Slave=4}
    ? UNKNOWN: role: UNKNOWN, name: 10.117.12.9, nic vendor: CISCO SYSTEMS, INC.  fingerprints: {}
    ? UNKNOWN: role: UNKNOWN, name: 10.117.12.8, nic vendor: CISCO SYSTEMS, INC.  fingerprints: {}
    IED: role: UNKNOWN, name: 10.117.12.3, nic vendor: CISCO SYSTEMS, INC.  fingerprints: {DNP3 TCP=5, DNP3 TCP Slave=4}
    IED: role: UNKNOWN, name: 10.117.12.4, nic vendor: CISCO SYSTEMS, INC.  fingerprints: {DNP3 TCP=5, DNP3 TCP Slave=4}
Network - networkIP: 10.108.104.0, subnetMask: 255.255.255.0, name: 10.108.104.0/24
    IED: role: UNKNOWN, name: 10.108.104.2, nic vendor: CISCO SYSTEMS, INC.  fingerprints: {DNP3 TCP=5, DNP3 TCP Slave=4}
Network - networkIP: 10.117.11.0, subnetMask: 255.255.255.0, name: 10.117.11.0/24
    ? UNKNOWN: role: UNKNOWN, name: 10.117.11.3, nic vendor: CISCO SYSTEMS, INC.  fingerprints: {}
    ? UNKNOWN: role: UNKNOWN, name: 10.117.11.2, nic vendor: CISCO SYSTEMS, INC.  fingerprints: {}
    ? UNKNOWN: role: UNKNOWN, name: 10.117.11.4, nic vendor: CISCO SYSTEMS, INC.  fingerprints: {}
    ? UNKNOWN: role: UNKNOWN, name: 10.117.11.6, nic vendor: CISCO SYSTEMS, INC.  fingerprints: {}
    IED: role: UNKNOWN, name: 10.117.11.5, nic vendor: CISCO SYSTEMS, INC.  fingerprints: {DNP3 TCP=5, DNP3 TCP Slave=4}
    ? UNKNOWN: role: UNKNOWN, name: 10.117.11.7, nic vendor: CISCO SYSTEMS, INC.  fingerprints: {}
Network - networkIP: 10.148.10.0, subnetMask: 255.255.255.0, name: 10.148.10.0/24
    ? UNKNOWN: role: UNKNOWN, name: 10.148.10.2, nic vendor: CISCO SYSTEMS, INC.  fingerprints: {}
Network - networkIP: 10.137.8.0, subnetMask: 255.255.255.0, name: 10.137.8.0/24
    IED: role: UNKNOWN, name: 10.137.8.2, nic vendor: CISCO SYSTEMS, INC.  fingerprints: {DNP3 TCP=5, DNP3 TCP Slave=4}
Network - networkIP: 10.137.16.0, subnetMask: 255.255.255.0, name: 10.137.16.0/24
    ? UNKNOWN: role: UNKNOWN, name: 10.137.16.2, nic vendor: CISCO SYSTEMS, INC.  fingerprints: {}
Network - networkIP: 10.118.1.0, subnetMask: 255.255.255.0, name: 10.118.1.0/24
```

Name	Type	Message	Progress	Date	Started	Elapsed	Active
Session Cleared	GUIEVENT	Session was cleared	0/0	02/12/2014	11:47:10	0 ms	false
File Import	PARSEREVENT	Processing item 1 of...	1/1	02/12/2014	11:47:36	2.372 s	false

Memory Utilization: 46/910(%5.15)

Progress: No running tasks.

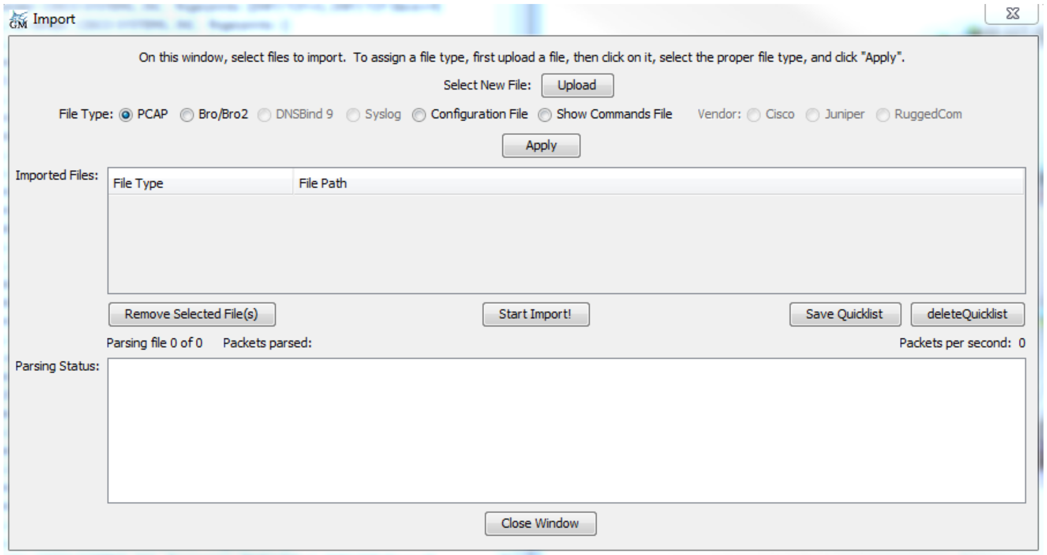
Figure 3: Loaded Session

2.1. Importing Data

To import data, the user must go to File → Import. The Import Dialog will appear and the user will be prompted to select files for upload (Figure 4). Once a file(s) is selected, the user will need to select the file type (Figure 5). The user is presented with the following types:

- PCAP
- Bro (Version 1 and 2)
- *DNSBind 9 (unsupported)*
- *Syslog (unsupported)*
- Configuration File
- Show Commands File

The Configuration and Show Commands files are for reading text-based information obtained from a network device and will require the user to specify the appropriate vendor of the device. Currently, only Cisco and RuggedCom devices are supported at this time.



Import

On this window, select files to import. To assign a file type, first upload a file, then click on it, select the proper file type, and click "Apply".

Select New File: Upload

File Type: ● PCAP ○ Bro/Bro2 ○ DNSBind 9 ○ Syslog ○ Configuration File ○ Show Commands File Vendor: ○ Cisco ○ Juniper ○ RuggedCom

Apply

Imported Files:

File Type	File Path

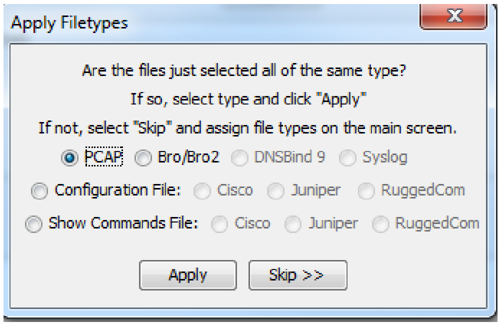
Remove Selected File(s) Start Import! Save Quicklist deleteQuicklist

Parsing file 0 of 0 Packets parsed: Packets per second: 0

Parsing Status:

Close Window

Figure 4: Import Dialog



Apply Filetypes

Are the files just selected all of the same type?
If so, select type and click "Apply"
If not, select "Skip" and assign file types on the main screen.

● PCAP ○ Bro/Bro2 ○ DNSBind 9 ○ Syslog

○ Configuration File: ○ Cisco ○ Juniper ○ RuggedCom

○ Show Commands File: ○ Cisco ○ Juniper ○ RuggedCom

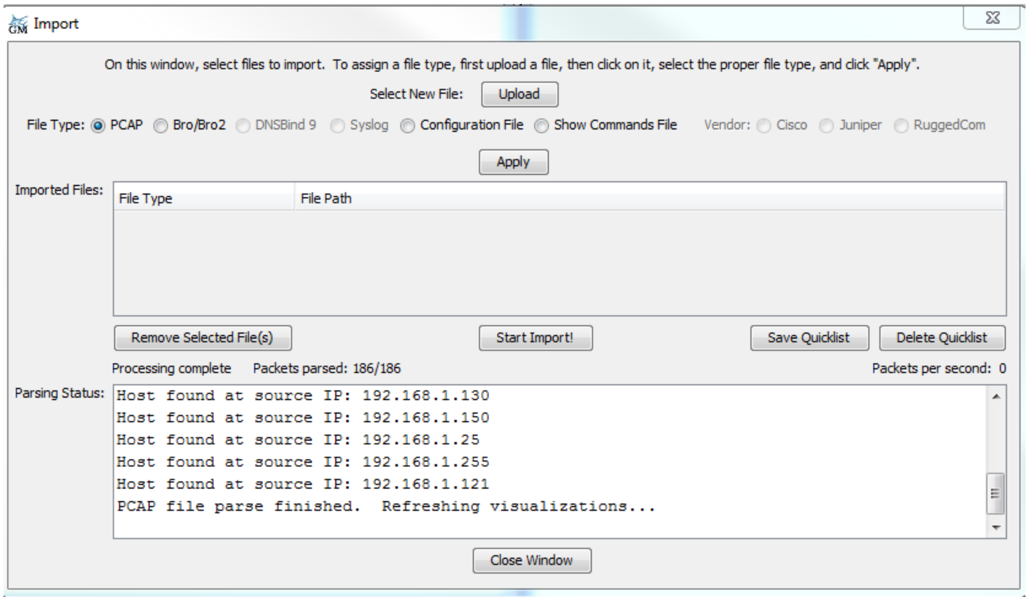
Apply Skip >>

Figure 5: Apply Filetypes

Once the file type is applied, the file will be listed in the Imported Files box. Before the import process starts, the user has the option to change the file type or remove files within the Import Dialog. The user may change the file type by selecting the file, choosing another file type, and selecting **Apply**. Files are removed by selecting the file(s) and clicking the **Remove Selected File(s)** button.

The user also has the option to create a Quicklist. A Quicklist allows the user to save a set of imported files as a list so for future imports the list is already displayed and queued up for quick import. The Quicklist is only available when starting a new session. Quicklists can be saved by selecting **Save Quicklist**, and can be deleted by selecting **Delete Quicklist**.

Once all the desired files are listed in the Imported Files box, the user can then select **Start Import!** The Parsing Status box will update the user with status information as each file is analyzed and read into GRASSMARLIN. Once all the files have been imported, the Import Dialog box will display Processing Complete above the status box (Figure 6). Selecting **Close Window** will close the Import Dialog window and return to the GRASSMARLIN user interface that has been updated with the imported data.



On this window, select files to import. To assign a file type, first upload a file, then click on it, select the proper file type, and click "Apply".

Select New File:

File Type: ● PCAP ○ Bro/Bro2 ○ DNSBind 9 ○ Syslog ○ Configuration File ○ Show Commands File   Vendor: ○ Cisco ○ Juniper ○ RuggedCom

Imported Files:

File Type	File Path

Processing complete   Packets parsed: 186/186   Packets per second: 0

Parsing Status:

```
Host found at source IP: 192.168.1.130
Host found at source IP: 192.168.1.150
Host found at source IP: 192.168.1.25
Host found at source IP: 192.168.1.255
Host found at source IP: 192.168.1.121
PCAP file parse finished.  Refreshing visualizations...
```

Figure 6: Processing Complete

Another option for importing data is to import a previously exported XML file. However, GRASSMARLIN does not allow you to open a saved session from a previous version in a newer version. If you want to bring in data from a saved session from a previous version of GRASSMARLIN, you must open the session and export the data in the older version, then import data in the new version.

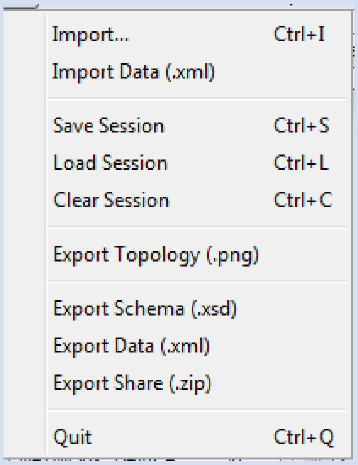
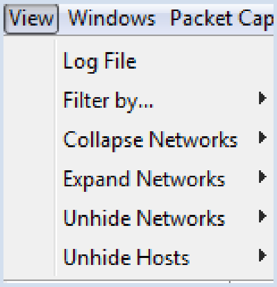
3. The User Interface

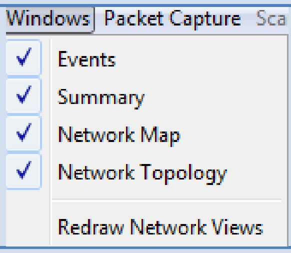
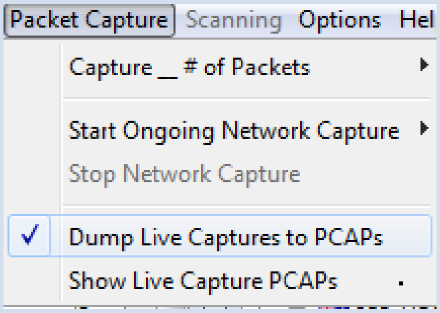
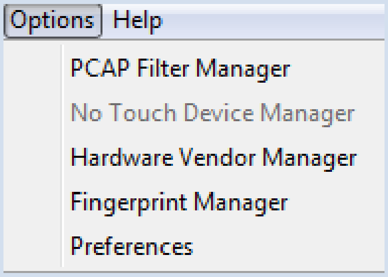
The GRASSMARLIN user interface is comprised of the Home Toolbar, and four internal windows. The Home Toolbar at the top of the screen contains all the necessary options for running various tasks in GRASSMARLIN: File, View, Windows, Packet Capture, Scanning, Options, and Help. Below the Home

Toolbar is the Live Network Capture tool. The four internal windows are titled Events, Summary, Network Tree Map, and Network Topology.

3.1. Home Toolbar

The Home Toolbar contains options for operating and configuring GRASSMARLIN. Each menu item is described below in Table 1.

Home Toolbar Item	*Description*	*Menu*
File Menu	The File menu has options to import/export data, handle sessions, and quit the program. - **Import**: Opens the Import Dialog, which allows for the importing of data - **Import Data:** Allows the user to import an exported data session - **Save Session**: Saves all of the data in memory to disk - **Load Session**: Loads a previously saved session - **Clear Session:** Clears all data in the session and brings the program back to its starting/initial state - **Export Topology**: Allows the user to export both the logical and physical topologies to a PNG file - **Export Schema***:* Allows the user to export a data model schema - **Export Data***:* Allows the user to export all session data to an XML file - **Export Share:** Allows the user to export both the data and the PCAPs into a folder for easy sharing. - **Quit:** Exits GRASSMARLIN	 Import... Ctrl+I Import Data (.xml) Save Session Ctrl+S Load Session Ctrl+L Clear Session Ctrl+C Export Topology (.png) Export Schema (.xsd) Export Data (.xml) Export Share (.zip) Quit Ctrl+Q
View Menu	The View menu allows the user to open the log file, filter the view, and modify the appearance of networks and hosts. - **Log File:** Opens the GRASSMARLIN log file in a separate window - **Filter by:** Allows the user to filter data based on protocol/fingerprint, host type, or country - **Collapse Networks**: Allows the user to select specific networks to collapse. It also allows the user to collapse all networks. - **Expand Networks:** Allows the user to	 View Windows Packet Cap Log File Filter by... Collapse Networks Expand Networks Unhide Networks Unhide Hosts

	either expand all networks or choose specific networks to expand • **Unhide Networks:** Allows the user to unhide networks • **Unhide Hosts:** Allows the user to unhide hosts	
Windows Menu	The Windows menu allows the user to toggle the visibility of the Events, Summary, Network Map, and Network Topology windows. From this menu, the user also has the ability to redraw the network views.	 Windows Packet Capture Sca ✓ Events ✓ Summary ✓ Network Map ✓ Network Topology Redraw Network Views
Packet Capture Menu	The Packet Capture menu contains items associated with live network data capture. To start either type of live capture, the user is required to select a network interface to use for the capture. • **Capture _ # of Packets**: Prompts the user for a specific number of packets to capture on the selected network interface • **Start Ongoing Network Capture**: Starts a live capture on the selected network interface • **Stop Network Capture**: Stops the live capture or prematurely stops *Capture_# of Packets* • **Dump Live Captures to PCAPs**: Automatically saves the captured packets to a file when enabled • **Show Live Capture PCAPs**: Opens the GRASSMARLIN PCAP folder to allow the user to open selected files in Wireshark	 Packet Capture Scanning Options Hel Capture __ # of Packets Start Ongoing Network Capture Stop Network Capture ✓ Dump Live Captures to PCAPs Show Live Capture PCAPs
Options Menu	The Options menu contains items that allow the user to alter the functionality and behavior of GRASSMARLIN. • **PCAP Filter Manager**: Allows the user to filter specific types of network traffic and to create new filters • **No Touch Device Manager**: Allows the user to view and edit the list of no touch devices. (Currently unavailable) • **Hardware Vendor Manager**: Allows the user to view and edit the list of hardware vendors • **Fingerprint Manager**: Allows the user to view, edit, delete, and create new	 Options Help PCAP Filter Manager No Touch Device Manager Hardware Vendor Manager Fingerprint Manager Preferences

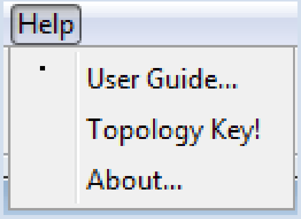
	fingerprints • **Preferences**: Allows the user to customize GRASSMARLIN options	
Help Menu	The Help menu provides information about the GRASSMARLIN tool. • **User Guide:** Opens the user guide in PDF format • **Topology Key:** Identifies the colors and icons used in the logical and physical views • **About:** Displays the version of GRASSMARLIN currently running, as well as additional information	

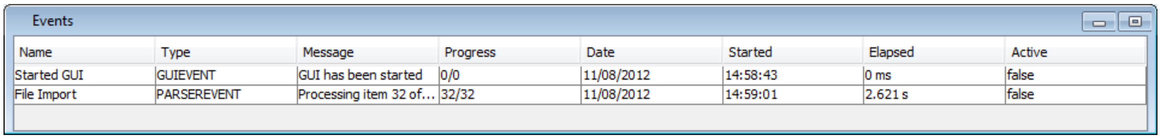
Table 1: GRASSMARLIN Home Toolbar Items

3.2. GRASSMARLIN Internal Windows

The internal windows form the visual portion of GRASSMARLIN. The GRASSMARLIN tool has four primary windows that appear by default: Events, Summary, Network Tree Map, and Network Topology. The user may resize these windows. Alternatively, the user may toggle the visibility of these windows from the **Windows** menu.

3.2.1. Events Window

The Events window lists GRASSMARLIN actions to include file imports, live network captures, session activities, and exporting data. For each event, the window displays the event name, the event type, a status message, a progress count, the date, the start time, and time elapsed (Figure 7). All items in the Events window are updated in real time. For events such as parsing multiple files, the event message will show the individual progress (eg. Processing item 3 of 9). Event progress is also shown in the bottom right of the tool, which displays both a progress bar and message about the event currently in progress.



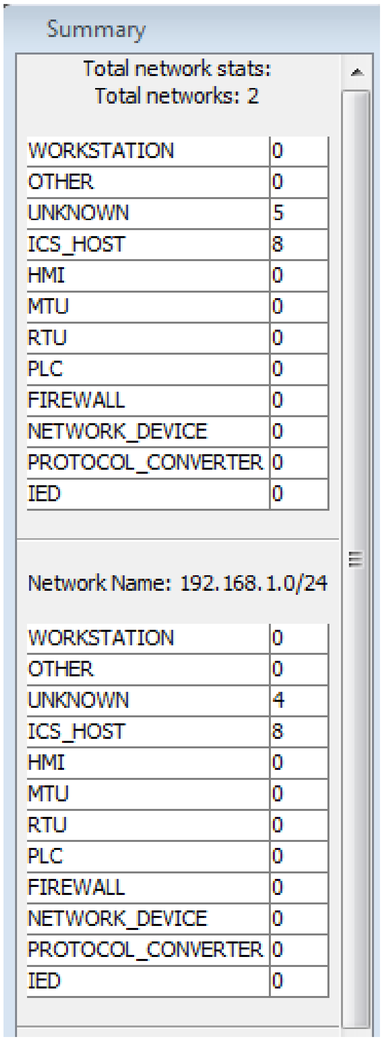
Events

Name	Type	Message	Progress	Date	Started	Elapsed	Active
Started GUI	GUIEVENT	GUI has been started	0/0	11/08/2012	14:58:43	0 ms	false
File Import	PARSEREVENT	Processing item 32 of...	32/32	11/08/2012	14:59:01	2.621 s	false

Figure 7: Events Window

3.2.2. Summary Window

The Summary Window is responsible for displaying statistics about the types of devices present in the network (Figure 8). At the top, GRASSMARLIN shows the number of networks found and the number of each specific host type for the entire session. Just below that, the number of different host types is summarized for each individual network. This is a useful view to get a quick understanding of what types of devices reside on the entire network. The window is updated in real-time as new hosts are found and new information is discovered from the analysis of incoming data.



Total network stats:
Total networks: 2

WORKSTATION	0
OTHER	0
UNKNOWN	5
ICS_HOST	8
HMI	0
MTU	0
RTU	0
PLC	0
FIREWALL	0
NETWORK_DEVICE	0
PROTOCOL_CONVERTER	0
IED	0

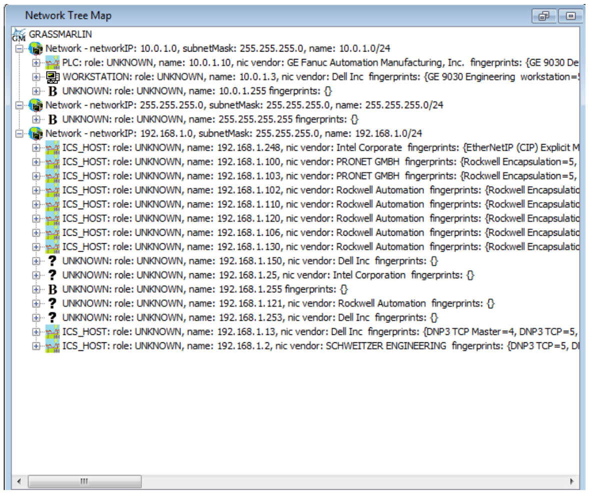
Network Name: 192.168.1.0/24

WORKSTATION	0
OTHER	0
UNKNOWN	4
ICS_HOST	8
HMI	0
MTU	0
RTU	0
PLC	0
FIREWALL	0
NETWORK_DEVICE	0
PROTOCOL_CONVERTER	0
IED	0

Figure 8: Summary Window

3.2.3. Network Tree Map Window

The Network Tree provides a hierarchical view of the network topology (Figure 9). As new networks and hosts are discovered, they are dynamically added to the tree view. These new additions to the tree are temporarily highlighted in green, and updates to existing tree items are temporarily highlighted in blue. Each item contains a short description and may have associated child nodes with additional details.



```
GRASSMARLIN
⊟ Network - networkIP: 10.0.1.0, subnetMask: 255.255.255.0, name: 10.0.1.0/24
    ⊞ PLC: role: UNKNOWN, name: 10.0.1.10, nic vendor: GE Fanuc Automation Manufacturing, Inc.  fingerprints: {GE 9030 De
    ⊞ WORKSTATION: role: UNKNOWN, name: 10.0.1.3, nic vendor: Dell Inc  fingerprints: {GE 9030 Engineering  workstation=
    ⊞ B UNKNOWN: role: UNKNOWN, name: 10.0.1.255 fingerprints: {}
⊟ Network - networkIP: 255.255.255.0, subnetMask: 255.255.255.0, name: 255.255.255.0/24
    ⊞ B UNKNOWN: role: UNKNOWN, name: 255.255.255.255 fingerprints: {}
⊟ Network - networkIP: 192.168.1.0, subnetMask: 255.255.255.0, name: 192.168.1.0/24
    ⊞ ICS_HOST: role: UNKNOWN, name: 192.168.1.248, nic vendor: Intel Corporate  fingerprints: {EtherNetIP (CIP) Explicit M
    ⊞ ICS_HOST: role: UNKNOWN, name: 192.168.1.100, nic vendor: PRONET GMBH  fingerprints: {Rockwell Encapsulation=5,
    ⊞ ICS_HOST: role: UNKNOWN, name: 192.168.1.103, nic vendor: PRONET GMBH  fingerprints: {Rockwell Encapsulation=5,
    ⊞ ICS_HOST: role: UNKNOWN, name: 192.168.1.102, nic vendor: Rockwell Automation  fingerprints: {Rockwell Encapsulatic
    ⊞ ICS_HOST: role: UNKNOWN, name: 192.168.1.110, nic vendor: Rockwell Automation  fingerprints: {Rockwell Encapsulatic
    ⊞ ICS_HOST: role: UNKNOWN, name: 192.168.1.120, nic vendor: Rockwell Automation  fingerprints: {Rockwell Encapsulatic
    ⊞ ICS_HOST: role: UNKNOWN, name: 192.168.1.106, nic vendor: Rockwell Automation  fingerprints: {Rockwell Encapsulatic
    ⊞ ICS_HOST: role: UNKNOWN, name: 192.168.1.130, nic vendor: Rockwell Automation  fingerprints: {Rockwell Encapsulatic
    ⊞ ? UNKNOWN: role: UNKNOWN, name: 192.168.1.150, nic vendor: Dell Inc  fingerprints: {}
    ⊞ ? UNKNOWN: role: UNKNOWN, name: 192.168.1.25, nic vendor: Intel Corporation  fingerprints: {}
    ⊞ B UNKNOWN: role: UNKNOWN, name: 192.168.1.255 fingerprints: {}
    ⊞ ? UNKNOWN: role: UNKNOWN, name: 192.168.1.121, nic vendor: Rockwell Automation  fingerprints: {}
    ⊞ ? UNKNOWN: role: UNKNOWN, name: 192.168.1.253, nic vendor: Dell Inc  fingerprints: {}
    ⊞ ICS_HOST: role: UNKNOWN, name: 192.168.1.13, nic vendor: Dell Inc  fingerprints: {DNP3 TCP Master=4, DNP3 TCP=5,
    ⊞ ICS_HOST: role: UNKNOWN, name: 192.168.1.2, nic vendor: SCHWEITZER ENGINEERING  fingerprints: {DNP3 TCP=5, DI
```

Figure 9: Network Tree Map Window

3.2.4. Network Topology Window: Logical View

The logical network topology is a radial graph of networks, hosts, and host-to-host communications (Figure 10). The topology view groups hosts and devices into their appropriate networks. As hosts are found through PCAP parsing or ingestion of data, nodes are added to represent hosts, ICS hosts, and networks. The Logical View uses the same icons as the Network Tree Map to represent Hosts and Networks. In addition, the Logical View uses colors to represent the different host types. The tolopogy key of colors and icons can be found by going to **Help -> Topology Key**.

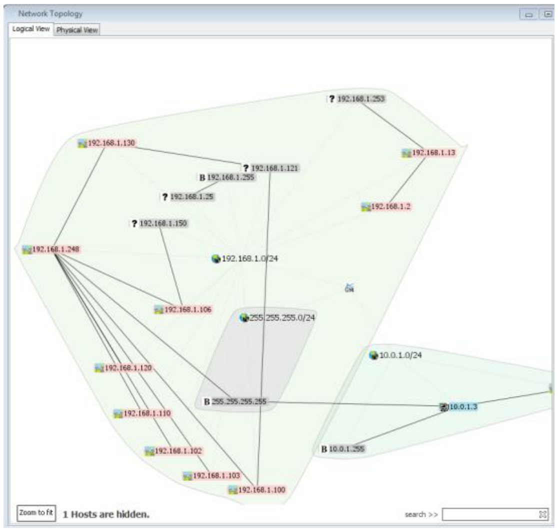


Figure 10: Network Topology - Logical View

3.2.5. Network Topology Window: Physical View

The physical network topology is a line graph of identified network components and the device links between them (Figure 11). The Physical View may not show every host on the network.

In order for the physical view to be rendered, GRASSMARLIN requires the user to import the results of all three of the following commands:

- *show running-configu*ration
- *show ip arp* **OR** *show* mac address-table
- *show interfaces*

After the data has been imported, the physical view will display any detected switches, routers, hosts, and potential unknown devices; VLANs are shown as text between connections. Each device is represented by an icon and corresponding color. GRASSMARLIN combines the data from configuration files, CAM tables, PCAP files or live network captures to determine the physical connections between network devices and hosts. The topology key of colors and icons can be found by going to **Help -> Topology Key**.

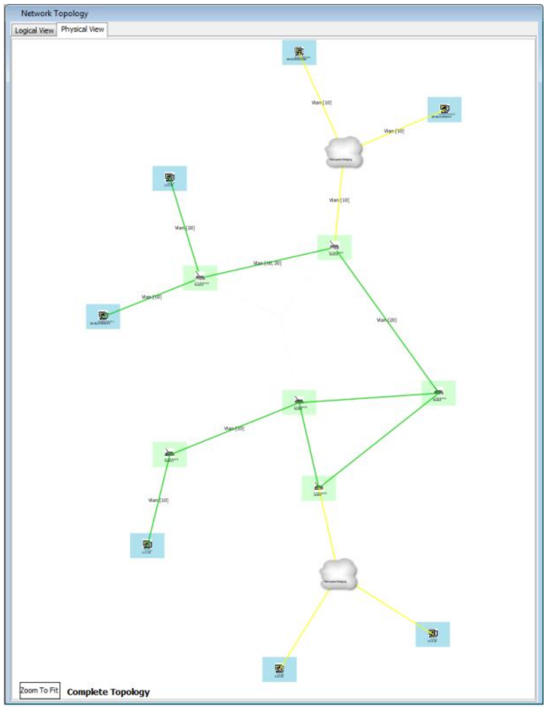


Figure 11: Network Topology - Physical View

3.3. GRASSMARLIN Analysis Capabilities

GRASSMARLIN has a range of analysis capabilities. The home toolbar also has a variety of analysis options to apply to the data.

3.4. Network Map and Topology Icon/Color Key

Icon	*Color*	*Name*	*Description*
GM	None	GRASSMARLIN Session	First item in the tree view. All the data collected are child nodes of the GRASSMARLIN session node.

🌐	Varies	Network	Second item in the tree view. A network node may or may not contain hosts.
🖥	Blue	Generic Host	A generic host type refers to a workstation or other similar host type.
?	Grey	Unknown Host	An unknown host type is used when no information is known about the host other than its IP address.
	Pink	ICS Host	ICS hosts are a special type of host that is used only for ICS devices (RTU, PLC, HMI, etc.)
	Green	Network Device	A network device host type that includes switches and routers.
	Yellow	Server	This host type is used for servers.
	Purple	Other	All other types of hosts.
🇺🇸, *Varies*	Flag	Host	Replaces host icon with a flag if it has a routable IP address, which can be mapped to a country code.
	None	Network Interface	Each host will have at least one network interface. *Only used in the Network Tree Map.*
	None	Address	Each network interface will have at least one address. *Only used in the Network Tree Map.*
	None	Connection	Each address could have zero or more connections. A connection represents communication between this host and another host. *Only used in the Network Tree Map.*
B	Grey	Broadcast Host	This is not an actual host rather a visual representation to display the broadcast traffic.
B	Red	ICS Broadcast Host	This is a host that is broadcasting through a typical ICS protocol such as BACNET.

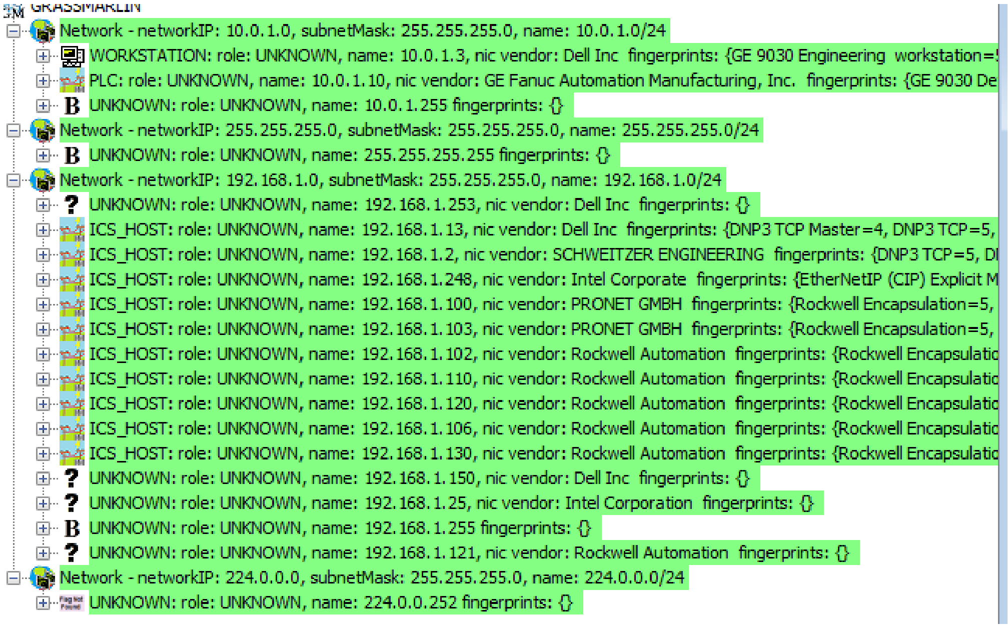
Table 2: GRASSMARLIN Analysis Capabilities

3.5. Network Tree View

The first item in the tree is the GRASSMARLIN session object, which contains all of the data found during the current session. Discovered items are displayed in the following hierarchy:

GRASSMARLIN
- ↳ Networks
  - ↳ Hosts
    - ↳ Network Interfaces
      - ↳ Addresses

- Connections



```
GRASSMARLIN
Network - networkIP: 10.0.1.0, subnetMask: 255.255.255.0, name: 10.0.1.0/24
    WORKSTATION: role: UNKNOWN, name: 10.0.1.3, nic vendor: Dell Inc  fingerprints: {GE 9030 Engineering  workstation=
    PLC: role: UNKNOWN, name: 10.0.1.10, nic vendor: GE Fanuc Automation Manufacturing, Inc.  fingerprints: {GE 9030 De
    UNKNOWN: role: UNKNOWN, name: 10.0.1.255 fingerprints: {}
Network - networkIP: 255.255.255.0, subnetMask: 255.255.255.0, name: 255.255.255.0/24
    UNKNOWN: role: UNKNOWN, name: 255.255.255.255 fingerprints: {}
Network - networkIP: 192.168.1.0, subnetMask: 255.255.255.0, name: 192.168.1.0/24
    UNKNOWN: role: UNKNOWN, name: 192.168.1.253, nic vendor: Dell Inc  fingerprints: {}
    ICS_HOST: role: UNKNOWN, name: 192.168.1.13, nic vendor: Dell Inc  fingerprints: {DNP3 TCP Master=4, DNP3 TCP=5,
    ICS_HOST: role: UNKNOWN, name: 192.168.1.2, nic vendor: SCHWEITZER ENGINEERING  fingerprints: {DNP3 TCP=5, DI
    ICS_HOST: role: UNKNOWN, name: 192.168.1.248, nic vendor: Intel Corporate  fingerprints: {EtherNetIP (CIP) Explicit M
    ICS_HOST: role: UNKNOWN, name: 192.168.1.100, nic vendor: PRONET GMBH  fingerprints: {Rockwell Encapsulation=5,
    ICS_HOST: role: UNKNOWN, name: 192.168.1.103, nic vendor: PRONET GMBH  fingerprints: {Rockwell Encapsulation=5,
    ICS_HOST: role: UNKNOWN, name: 192.168.1.102, nic vendor: Rockwell Automation  fingerprints: {Rockwell Encapsulatic
    ICS_HOST: role: UNKNOWN, name: 192.168.1.110, nic vendor: Rockwell Automation  fingerprints: {Rockwell Encapsulatic
    ICS_HOST: role: UNKNOWN, name: 192.168.1.120, nic vendor: Rockwell Automation  fingerprints: {Rockwell Encapsulatic
    ICS_HOST: role: UNKNOWN, name: 192.168.1.106, nic vendor: Rockwell Automation  fingerprints: {Rockwell Encapsulatic
    ICS_HOST: role: UNKNOWN, name: 192.168.1.130, nic vendor: Rockwell Automation  fingerprints: {Rockwell Encapsulatic
    UNKNOWN: role: UNKNOWN, name: 192.168.1.150, nic vendor: Dell Inc  fingerprints: {}
    UNKNOWN: role: UNKNOWN, name: 192.168.1.25, nic vendor: Intel Corporation  fingerprints: {}
    UNKNOWN: role: UNKNOWN, name: 192.168.1.255 fingerprints: {}
    UNKNOWN: role: UNKNOWN, name: 192.168.1.121, nic vendor: Rockwell Automation  fingerprints: {}
Network - networkIP: 224.0.0.0, subnetMask: 255.255.255.0, name: 224.0.0.0/24
    UNKNOWN: role: UNKNOWN, name: 224.0.0.252 fingerprints: {}
```

Figure 12: New Tree Items Highlighted in Green

Each item in the tree contains an icon representing one of these categories. Host items are further broken down into different host types, with their own unique icons (Table 2). In addition to the icons, a short description about the node (IP address, hostname, and host type, etc.) is also displayed in this view (Figure 12).

3.6. Network Topology: Logical

In this view, GRASSMARLIN only shows which end devices are communicating and not the actual route the packet took to reach its destination. Once a host is seen in the network traffic it will remain in the logical view; hosts do not disappear from the logical view after a set period of time. GRASSMARLIN does map one way connections, as well as bi-directional connections.

3.7. Manipulating the Logical View

The user is able to hide and unhide hosts and networks in the logical view to help with analysis and manage the amount of nodes in view. To hide a host, the user must right click on the host in the logical view and select **Hide Host.** To hide a network the user must right click a network and select **Hide Network.** To unhide a network, the user must go **View -> Unhide host/network**. The topology is interactive; each node and session line can be selected by the user to change the orientation of the view or to show more detail. The user can also right click in the Logical View and select Unhide Host/Network. Right clicking on a node and selecting **Center Item** will center that node and all of its connections on the screen, and reorient the rest of the map accordingly. Left clicking and holding on a host or network container allows the user to drag the item around in the view. When a host or a network is right-clicked, a menu is displayed which presents the user with several options that will be described in Section 3.10. The **Restore Logical View** button can be used to restore the logical view, if for instance it is showing only some connections or showing only a certain network. If you want to hide the network information so you only see the hosts you can check the box **Hide Network Info**. (Figure 13) This does take a couple seconds to refresh though.

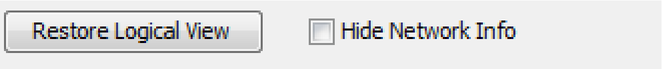


Figure 13: Restore Logical View & Hide Network Info

3.8. Manipulating the Physical View

Importing a network device configuration file into GRASSMARLIN (**File -> Import**) provides valuable details about the physical layout of that device and the devices directly connected to it. While viewing devices in the Physical View, the user can right click on a device and select **View CAM Table**. The CAM table provides details about which hosts are connected to which ports, or if a port is connected to another network device.

In its initial view, the Physical Network view only shows network devices seen on the network so far. Solid green lines identify actual physical connections between the devices and/or hosts, while solid yellow lines identify potential physical connections between the devices and/or hosts. These yellow lines are essentially a guess of physical connectivity between devices, which GRASMARLIN does not have enough information to confirm. If a network device has more than one network interface, a description will be displayed under a minimized network device icon with its number of interfaces (Figure 14).

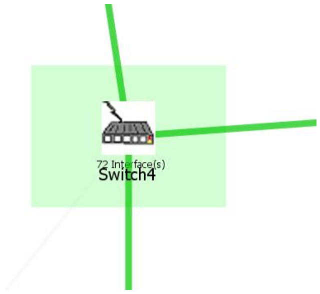


Figure 14: Network Device - Physical View

As more details about the network are found, the graph will continue to be populated with this additional data and the user will see an overview of the physical layout of the network begin to develop. By right-clicking on a device with multiple interfaces and selecting **Show Host Details**, a quick view of the interfaces for that device with additional details is shown. Network devices with multiple interfaces can also be expanded by right-clicking on the icon and selecting **Expand this Network Device**. In the expanded view, all the interfaces and any physical connections to hosts and/or other network devices are shown. The physical connections will link the port to the connected host (Figure 15).

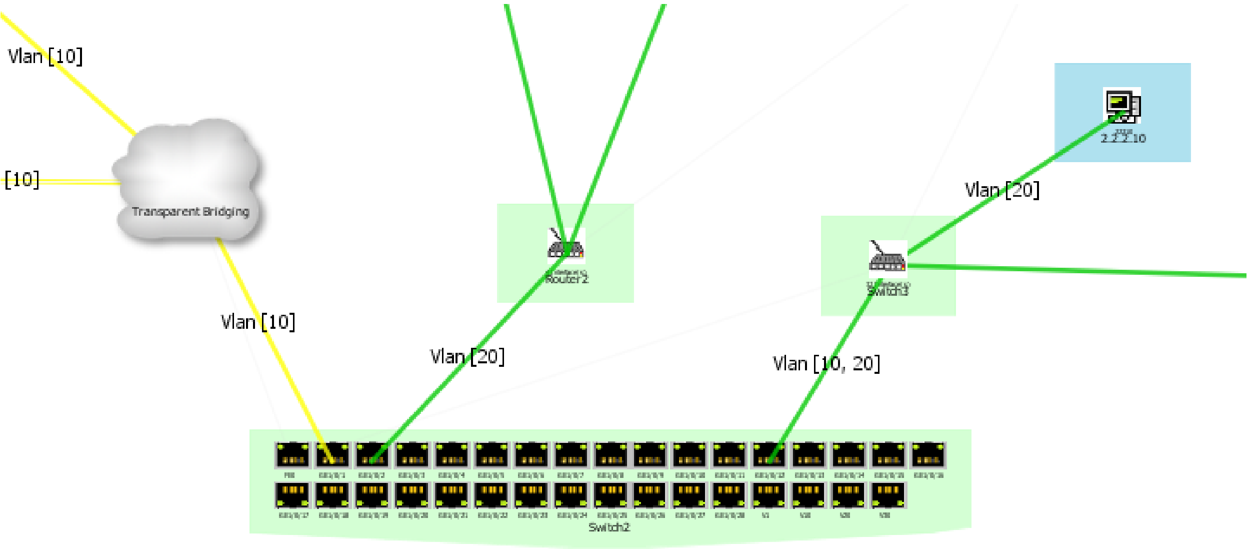


Figure 15: Physical Connections – Physical View

3.9. Searching for Hosts and Networks

The Search Box in the bottom right corner is used to find networks or hosts by entering either the IP address or hostname. GRASSMARLIN will focus on the item, host, or network searched for, and center it in the Logical View window. The user has the ability to hide an item from view by right clicking on the item and selecting **Hide Host or Hide Network** depending on the type of item. When a host is hidden, a message will appear in the left corner of the Logical View informing the user that a network is hidden. Hiding hosts and networks can be useful when there are a large number of hosts/networks, or if the user only needs to focus on a particular section of the network.

3.10. Right Click Options for Network Tree Map and Network Topology

In the Network Tree Map and the Network Topology, the user can right click any item to open a menu with a variety of options. The options vary depending on the window and the item selected. Table 3~~Table 3Table 3~~ summarizes the different right click menu options.

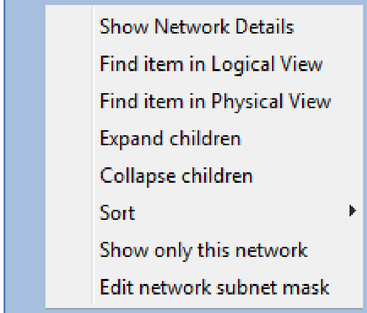
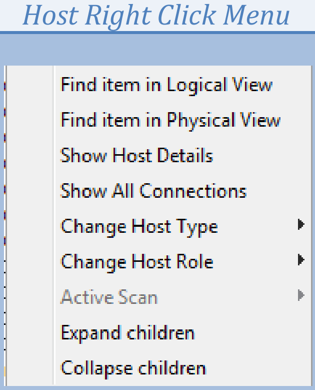
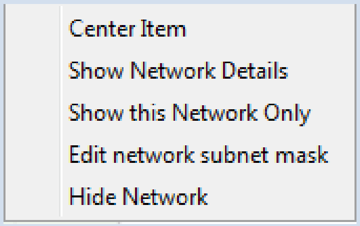
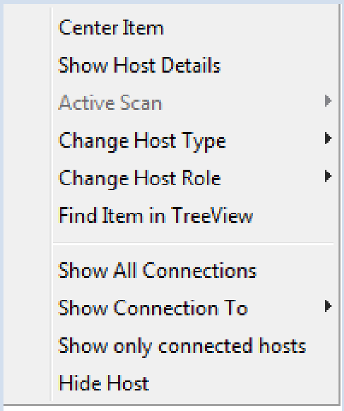
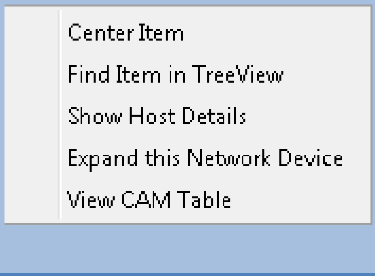
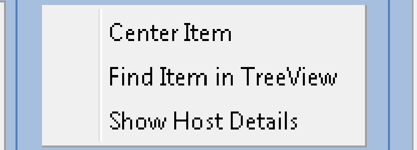
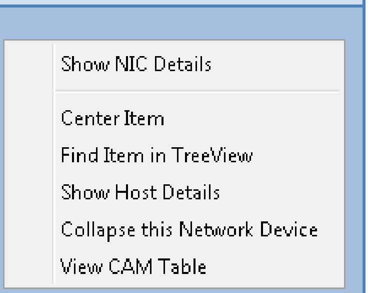
Window	*Network Right Click Menu*	*Host Right Click Menu*	*NIC Right Click Menu*
Tree Map	 Show Network Details Find item in Logical View Find item in Physical View Expand children Collapse children Sort Show only this network Edit network subnet mask	 Find item in Logical View Find item in Physical View Show Host Details Show All Connections Change Host Type Change Host Role Active Scan Expand children Collapse children	**N/A**
Network Topology : Logical View	 Center Item Show Network Details Show this Network Only Edit network subnet mask Hide Network	 Center Item Show Host Details Active Scan Change Host Type Change Host Role Find Item in TreeView Show All Connections Show Connection To Show only connected hosts Hide Host	**N/A**
Network Topology: Physical View	 Center Item Find Item in TreeView Show Host Details Expand this Network Device View CAM Table		 Show NIC Details Center Item Find Item in TreeView Show Host Details Collapse this Network Device View CAM Table

Table 3: Right Click Menus Options

Since the right click commands vary depending on the window and host type, Table 4~~Table 4Table 4~~ summarizes each command based on node type and the associated window.

Right Click Command	*Node Type*	*Window*	*Description*
Find item in logical view	Network, Network Device & Host	Tree Map	Centers and highlights the selected item in the **Logical View**

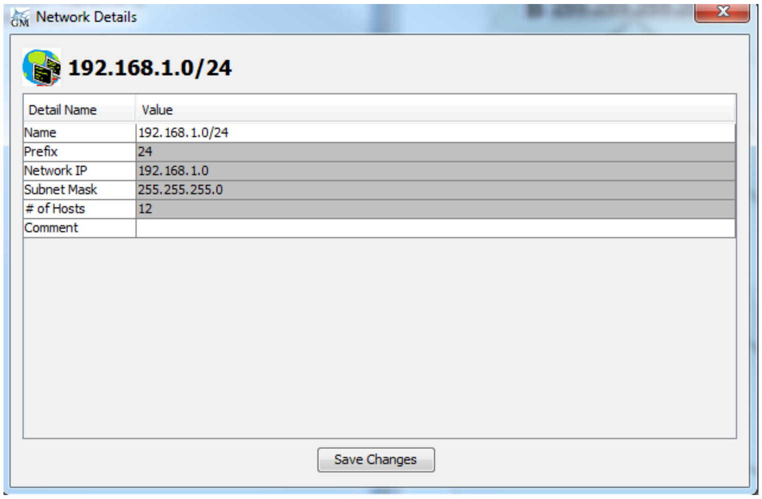
Show Network Details	Network	Tree Map & Logical View	Opens the **Network Details** window (Figure 16) which contains information about the network including the IP address, subnet mask, and number of hosts in the network
Show Host Details	Network Device, Host & NIC	Tree Map, Logical View & Physical View	Opens the **Host Details** window that contains detailed information about that host including IP address, hardware version, interfaces, and host type
Change Host Type	Host	Tree Map & Logical View	Allows the user to change the host type. If the host has already been designated as an ICS Host or Network Device, its type cannot be changed because of special attributes belonging to those particular types. Changing a host to a Network Device or ICS Host is not reversible.
Change Host Role	Host	Tree Map & Logical View	Allows the user to change the host role. Options include: Client, Server, Master, Slave, Operator, Engineer, Unknown (Default) , and Other
Sort	Network	Tree Map	Allows the user to sort the child nodes by their primary IP address or name. At the GRASSMARLIN level, sorting will sort all the networks by their primary IP address or name
Show only this network	Network	Tree Map & Logical View	Displays only the selected network in the **Logical View**
Expand Children	Network, Network Device & Host	Tree Map	Expands all child nodes
Collapse Children	Network, Network Device & Host	Tree Map	Collapses all child nodes
Find Item in TreeView	Host, Network Device & NIC	Logical View & Physical View	Finds the item in the **Network Tree Map** and highlights it
Hide Network	Network	Logical View	Hides an entire network in the **Network Tree Map** & **Logical View**
Hide Host	Network Device & Host	Logical View	Hides the host in the **Network Tree Map** & **Logical View**

Show All Connections	Network Device & Host	Tree Map & Logical View	Opens the **Connections for Host** window showing all detected traffic to and from this host
Show Connection To	Network Device & Host	Logical View	Opens the **Connections for Host** window showing only traffic between the two hosts
Show only connected hosts	Network Device & Host	Logical View & Tree Map	Shows only the hosts connected to the selected host. Everything else is hidden in the **Logical View**.
Edit network subnet mask	Network	Tree Map & Logical View	Allows the subnet mask for the network to be modified.
Center Item	All Items	Logical View & Physical View	This centers the focus around the selected host or device
Expand this Network Device	Network Device	Physical View	Expands the selected network device to show connections to each individual NIC/port.
Collapse this Network Device	NIC	Physical View	Collapses the selected network device to display as a single connection point, without showing individual ports/NICs.
View CAM Table	Network Device & NIC	Physical View	Displays the IP ARP table information for the selected device.
Show NIC Details	NIC	Physical View	Opens the NIC Details window which displays information about the NIC such as name, type, MAC, vendor, IP, subnet, and VLANs.

Table 4: Network/Host Right-Click Menu Options

3.11. Show Network Details

The **Show Network Details** command is accessible by right clicking on a network node in either the Network Tree Map or the Logical View. This command opens the **Network Details** window (Figure 16), which contains details that GRASSMARLIN collects about the network. The user is able to edit any of the information in this window and save the changes. Each of the fields is described in Table 5 below.



192.168.1.0/24

Detail Name	Value
Name	192.168.1.0/24
Prefix	24
Network IP	192.168.1.0
Subnet Mask	255.255.255.0
# of Hosts	12
Comment	

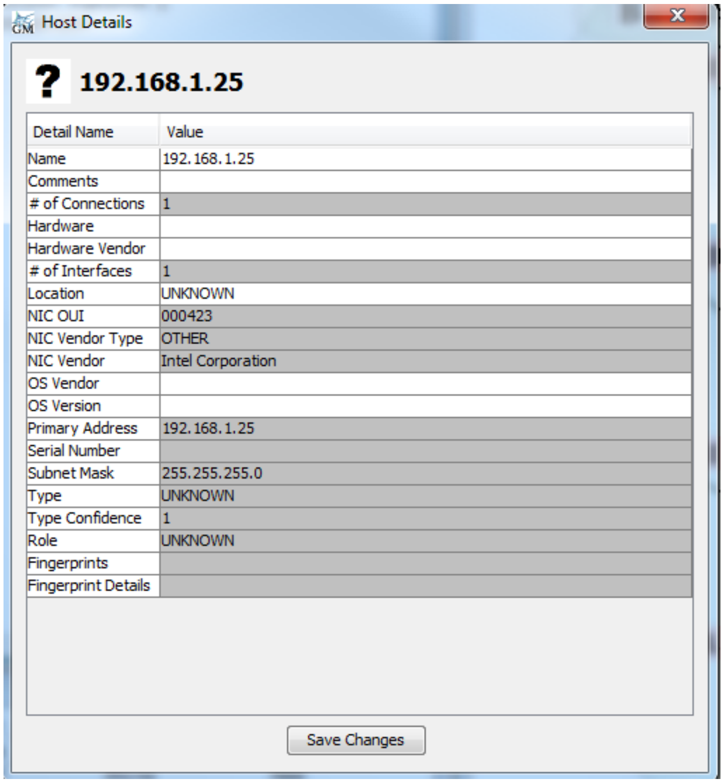
Figure 16: Network Details Window

Detail Name	*Value*
Name	Identifies the IP network range
Prefix	The prefix of the subnet
Network IP	The network IP
Subnet Mask	The subnet mask
Subnetwork Count	N/A
# of Hosts	The number of hosts within the network
Comment	Allows the user to insert any comments about the network

Table 5: Network Details

3.12. **Show Host Details**

Similar to network details, the user has the ability to edit the host details here. As seen in Figure 17, the capabilities allow the user to see an extensive list of host details.



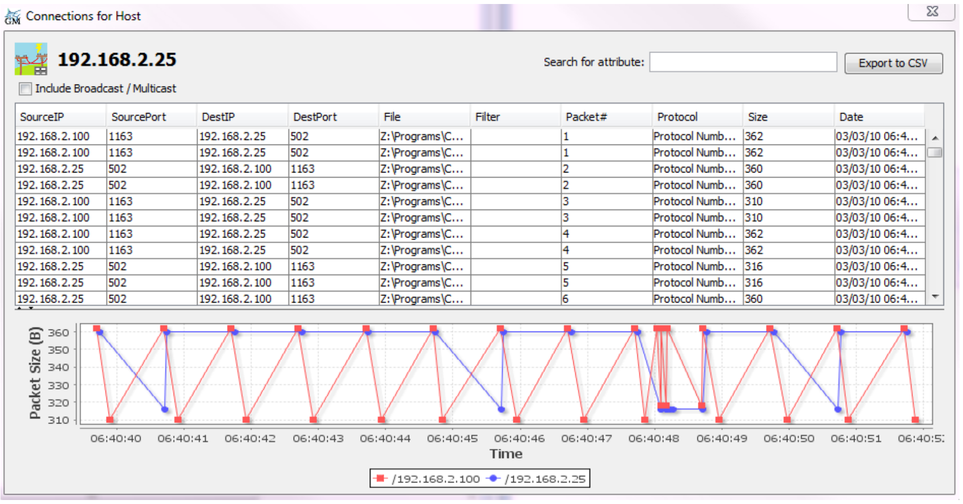
? 192.168.1.25

Detail Name	Value
Name	192.168.1.25
Comments	
# of Connections	1
Hardware	
Hardware Vendor	
# of Interfaces	1
Location	UNKNOWN
NIC OUI	000423
NIC Vendor Type	OTHER
NIC Vendor	Intel Corporation
OS Vendor	
OS Version	
Primary Address	192.168.1.25
Serial Number	
Subnet Mask	255.255.255.0
Type	UNKNOWN
Type Confidence	1
Role	UNKNOWN
Fingerprints	
Fingerprint Details	

Figure 17: Host Details Window

3.13. Show Connections

The Host Connections window (Figure 18) is accessible by right clicking a host in either the Network Tree or the Logical View (Table 4~~Table 4Table 4~~). This window shows all connections found during a packet capture, either live or imported. GRASSMARLIN stores the essential information including a reference to the file it came from, the packet number, and the filter used during the capture. This information allows the user to analyze the data further in Wireshark or another network protocol analyzer. GRASSMARLIN can send a packet directly to Wireshark by right-clicking on a table row and selecting ***Analyze Packet in Wireshark***. In addition to the reference information, the window includes sortable columns for source IP, source port, destination IP, destination port, protocol, packet size, date, and time. There is also the ability to include Broadcast/Multicast traffic, which will be highlighted in yellow. The top right corner of the window has a Search for attribute feature, which allows the user to search for a specific IP address, as well as the ability to export the data currently displayed in the window to a CSV file.



192.168.2.25

Search for attribute:

□ Include Broadcast / Multicast

SourceIP	SourcePort	DestIP	DestPort	File	Filter	Packet#	Protocol	Size	Date
192.168.2.100	1163	192.168.2.25	502	Z:\Programs\C...		1	Protocol Numb...	362	03/03/10 06:4...
192.168.2.100	1163	192.168.2.25	502	Z:\Programs\C...		1	Protocol Numb...	362	03/03/10 06:4...
192.168.2.25	502	192.168.2.100	1163	Z:\Programs\C...		2	Protocol Numb...	360	03/03/10 06:4...
192.168.2.25	502	192.168.2.100	1163	Z:\Programs\C...		2	Protocol Numb...	360	03/03/10 06:4...
192.168.2.100	1163	192.168.2.25	502	Z:\Programs\C...		3	Protocol Numb...	310	03/03/10 06:4...
192.168.2.100	1163	192.168.2.25	502	Z:\Programs\C...		3	Protocol Numb...	310	03/03/10 06:4...
192.168.2.100	1163	192.168.2.25	502	Z:\Programs\C...		4	Protocol Numb...	362	03/03/10 06:4...
192.168.2.100	1163	192.168.2.25	502	Z:\Programs\C...		4	Protocol Numb...	362	03/03/10 06:4...
192.168.2.25	502	192.168.2.100	1163	Z:\Programs\C...		5	Protocol Numb...	316	03/03/10 06:4...
192.168.2.25	502	192.168.2.100	1163	Z:\Programs\C...		5	Protocol Numb...	316	03/03/10 06:4...
192.168.2.25	502	192.168.2.100	1163	Z:\Programs\C...		6	Protocol Numb...	360	03/03/10 06:4...

Figure 18: Host Connections Window

At the bottom of the Host Connections window is the packet visualization chart, which plots packet size versus time for that host. Each point on the graph represents a connection established between this host and another host. The position on the graph is determined by the time sent and the packet size in bytes. Each communication between unique hosts is assigned a different color and shape. Lines represent consecutive communications with the same host. The user can zoom in on a section of the chart by simply left-clicking and dragging the mouse cursor to highlight a particular region. To zoom you start at the upper left-hand corner of the desired section and drag to the lower right hand corner. After selecting the bounded region, the graph will redraw, zoomed-in on this selection. The user also has the option to right click in the graph, which provides the ability to save the graph as a .png file, copy the graph to the clipboard, or print the graph.

3.14. Show Connection to: Host

This will open up a "Connections for Host" window showing the connection selected.

* Right click connect does not work with collapsed networks

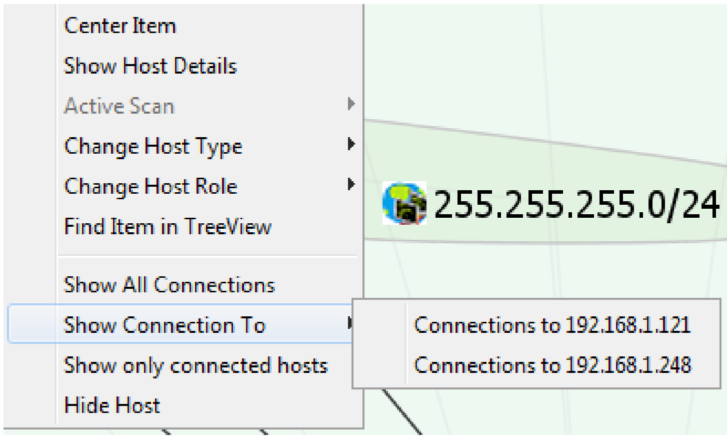


Figure 19: Show Connections to Host

3.15. Show only connected host

This will hide all hosts except the connected hosts (Figure 20). To unhide the hidden hosts/networks the user can right click the logical view, and choose the **Restore Logical View** option.

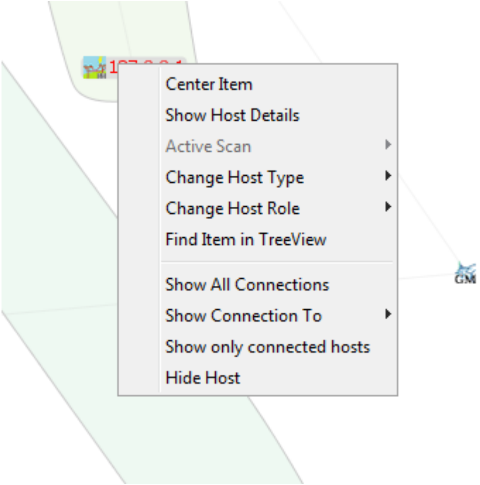


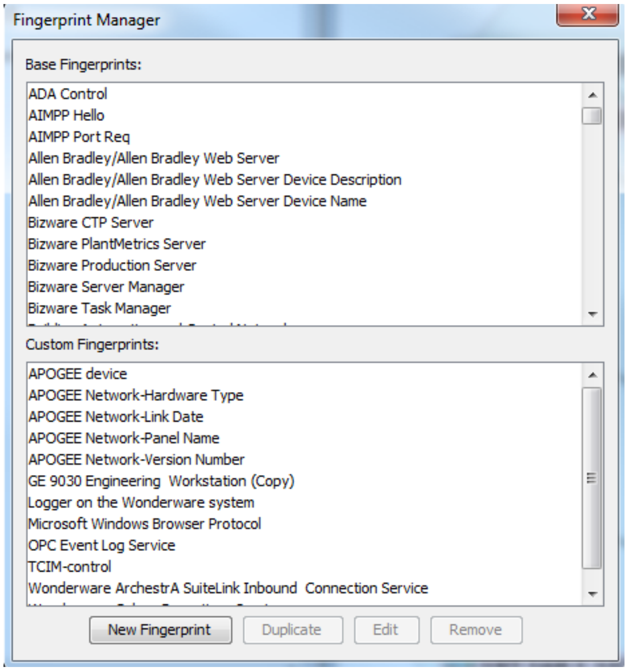
Figure 20: Show Only Connected Hosts

3.16. Fingerprints

Fingerprints are an essential part of GRASSMARLIN; they provide the information needed for GRASSMARLIN to identify traffic on a SCADA/ICS network. GRASSMARLIN contains a number of well-known fingerprints built in to identify common protocols. The tool is built with a robust framework to enable the quick customization of fingerprints. To view, edit, or add fingerprints, go to **Options -> Fingerprint Manager** from the home toolbar.

3.17. Fingerprint Manager

The Fingerprint Manager helps users organize, modify, create, or delete fingerprints (Figure 21). The manager will display a list of all the current fingerprints and give the user the option to create a new fingerprint, duplicate a fingerprint, edit a fingerprint, or remove a fingerprint. To create a new fingerprint, select **New Fingerprint.** The Edit Fingerprint Option window will then appear, containing four tabs: Basic, Additional, Payload, and Return Values. The more information that is provided when creating a fingerprint, the better defined and more precise it will be in identifying traffic.



Base Fingerprints:

- ADA Control
- AIMPP Hello
- AIMPP Port Req
- Allen Bradley/Allen Bradley Web Server
- Allen Bradley/Allen Bradley Web Server Device Description
- Allen Bradley/Allen Bradley Web Server Device Name
- Bizware CTP Server
- Bizware PlantMetrics Server
- Bizware Production Server
- Bizware Server Manager
- Bizware Task Manager

Custom Fingerprints:

- APOGEE device
- APOGEE Network-Hardware Type
- APOGEE Network-Link Date
- APOGEE Network-Panel Name
- APOGEE Network-Version Number
- GE 9030 Engineering Workstation (Copy)
- Logger on the Wonderware system
- Microsoft Windows Browser Protocol
- OPC Event Log Service
- TCIM-control
- Wonderware ArchestrA SuiteLink Inbound Connection Service

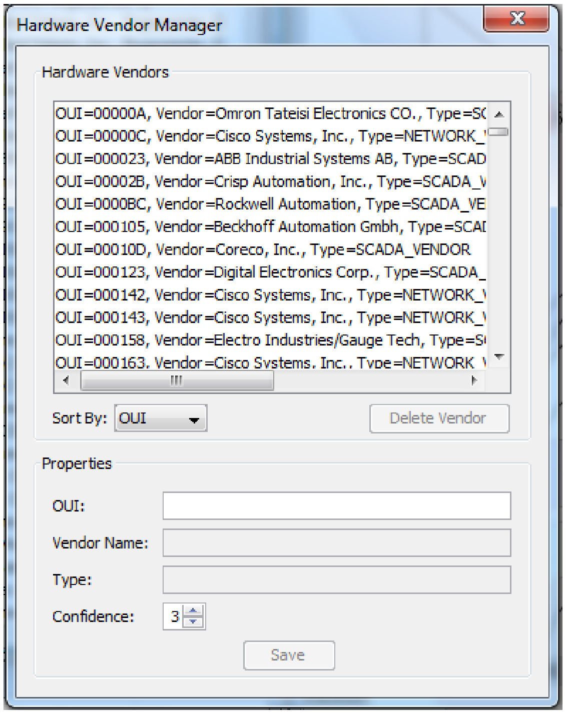
Figure 21: Fingerprint Manager Window

These values are standard IP and TCP/UDP fields which can easily be extracted from packets during a live-capture or an offline capture. All of these fields are treated as AND, so when multiple fields are used, their combined filter will characterize the device. This means that all the elements must exactly match the information found in the packet for the fingerprint identification to be successful. If an element could have multiple values for identification, a fingerprint will need to be created for each possibility.

Fingerprints can be created or edited outside of GRASSMARLIN. The fingerprint files are just XML files and can be easily edited. The format of a fingerprint is defined by the schema, *fingerprints.xsd*, located in the GRASSMARLIN specific files under the fingerprints directory. Changes to an existing fingerprint or creation of a new fingerprint in a text editor will be available the next time GRASSMARLIN starts. For further explanation on how to create a fingerprint, please see the dedicated Fingerprint How-To Guide.

3.18. Hardware Vendors

GRASSMARLIN maintains a list of hardware vendors and their associated OUIs. Some OUIs are identified as belonging to known SCADA vendors and their devices are tagged as SCADA devices. For each packet, GRASSMARLIN will look for MAC addresses and compare the OUI portion of that address to this list to find SCADA devices. This is how GRASSMARLIN populates the NIC Vendor detail in the host details. The user can edit this list by selecting **Options → Hardware Vendor Manager**. From the manager window, the user can delete existing entries (Figure 22). The user also has the ability to set the confidence level for each vendor. The list is a CSV file that can be edited outside of GRASSMARLIN.



```
OUI=00000A, Vendor=Omron Tateisi Electronics CO., Type=SC
OUI=00000C, Vendor=Cisco Systems, Inc., Type=NETWORK_
OUI=000023, Vendor=ABB Industrial Systems AB, Type=SCAD
OUI=00002B, Vendor=Crisp Automation, Inc., Type=SCADA_V
OUI=0000BC, Vendor=Rockwell Automation, Type=SCADA_VE
OUI=000105, Vendor=Beckhoff Automation Gmbh, Type=SCAI
OUI=00010D, Vendor=Coreco, Inc., Type=SCADA_VENDOR
OUI=000123, Vendor=Digital Electronics Corp., Type=SCADA_
OUI=000142, Vendor=Cisco Systems, Inc., Type=NETWORK_V
OUI=000143, Vendor=Cisco Systems, Inc., Type=NETWORK_V
OUI=000158, Vendor=Electro Industries/Gauge Tech, Type=S
OUI=000163, Vendor=Cisco Systems, Inc., Type=NETWORK_V
```

Sort By: OUI

OUI:

Vendor Name:

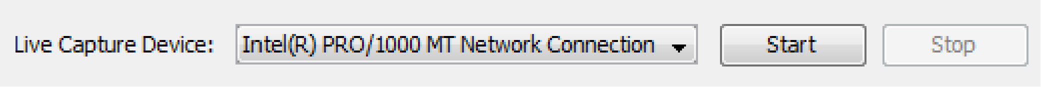
Type:

Confidence: 3

Figure 22: Hardware Vendor Manager Window

3.19. Run a Live Capture

GRASSMARLIN has the capability to passively listen on a network. As packets are captured, GM analyzes, fingerprints, and then displays the data in both the network tree view and the network topology view.



Live Capture Device: Intel(R) PRO/1000 MT Network Connection

Figure 23: Live Capture Device

4. File Storage & Data Management

GRASSMARLIN places all its temporary files in the ${USERHOME}/GRASSMARLIN directory. On Windows systems, this is typically:

[C:\Users\[current_user]\GRASSMARLIN\]

On Linux systems this is typically:

[/home/[current_user]/GRASSMARLIN].

The GRASSMARLIN directories contain a number of files and folders:

- fingerprints/ - Folder for all default fingerprint XML files included with GRASSMARLIN
- custom fingerprints/ - Folder for all user created fingerprints
- livecaptures/ - Folder containing all of the PCAP files generated by GRASSMARLIN during live captures

- logs/ - Folder containing all log entries generated by GRASSMARLIN
- offline captures/- Folder containing PCAPs brought in for storage to use when saving to share
- screenshots/ - Folder containing Topology exports
- sessions/ - Folder for all of the GRASSMARLIN *(.gmses)* saved session files
- shares/- Folder containing zip files to share with partners or collaborators
- filters.txt – Text file containing all of the PCAP filters for live captures
- hardwareVendors.txt – Text files containing all of the Hardware Vendors and associated OUIs
- noTouchDevices.txt – Text file containing all of the No Touch Devices
- userprefs.txt - Text file containing all of the user settings for GRASSMARLIN
- filters.txt – Text file containing the user's custom filters

4.1. Fingerprints

Fingerprints are a component of the GRASSMARLIN Knowledge Base and are used to analyze network traffic, either live or from a PCAP file. Each fingerprint is an XML file stored locally in the *fingerprints* folder. If it is a default fingerprint (included with GRASSMARLIN) it will be stored in the fingerprint folder, if it is a custom fingerprint (user created) it will be stored in the *custom fingerprints* folder.

4.2. Live Captures

When GRASSMARLIN captures live network traffic, a PCAP file will be generated to store all of the data from the live capture. These files are stored in the *livecaptures* folder in the GRASSMARLIN directory. The PCAP file is created for either type of live capture (Ongoing Capture or Preset Number of Packets). This PCAP file can be reopened in GRASSMARLIN or opened with Wireshark. This feature is enabled by default and the user can change this behavior in the **Packet Capture** menu. Checking the **Dump Live Captures to PCAP** menu item will save the captures.

4.3. Offline Captures

When GRASSMARLIN imports PCAP files it stores them in the offline capture folder for future use and for use when exporting data to share.

4.4. Logs

GRASSMARLIN records all activity to a log file, such as loading the knowledge base files, importing a PCAP file for parsing, or starting a live capture. Each log file corresponds to all of the events that occurred from the time the GRASSMARLIN application was opened until it was closed. All of the log files are stored in the GRASSMARLIN directory within the *logs/* folder. The file name contains the date on which the data was recorded. Since it is possible to have multiple files per date, each additional log file after the first for a particular date has a number appended to the filename. A log entry provides details down to the second that an event occurred and information about that event. Each event is assigned a log type:

- INFO: Information regarding normal GRASSMARLIN operations
- WARNING: Semi-important warning about an issue in the program
- SEVERE: Possibly fatal error with the program that should be addressed

Below is an example of some log entries generated by GRASSMARLIN (Figure 24).

```
Feb 06, 2012 10:09:07 AM com.grassmarlin.knowledgebase.KnowledgeBase loadKnowledgeBase
INFO: Started parsing of OUIs
Feb 06, 2012 10:09:07 AM com.grassmarlin.knowledgebase.KnowledgeBase loadKnowledgeBase
INFO: Finished parsing of OUIs
Feb 06, 2012 10:09:07 AM com.grassmarlin.knowledgebase.KnowledgeBase loadKnowledgeBase
INFO: Started parsing of ICS Vendors
Feb 06, 2012 10:09:07 AM com.grassmarlin.knowledgebase.KnowledgeBase
loadHardwareVendors
INFO: An Unknown Exception Occurred in Loading the Hardware Vendors.
```

Figure 24: Example Log Entries

Looking at the entries above, the logs can be used to determine when and where an event or error occurred. The format of the log entries is shown below (Figure 25).

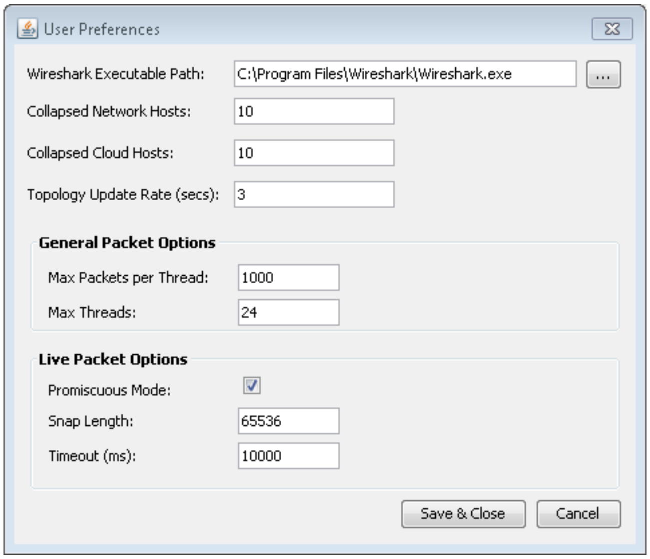
```
<Date> <Time> com.grassmarlin.<Package>.<Class> <Method>
<Severity>: <Message>
```

Figure 25: Log Entry Format

GRASSMARLIN allows the user to save all of the information collected to a binary Session file. These files can be opened by GRASSMARLIN at a later time. By default, GRASSMARLIN saves Session files to the *Sessions* folder within the GRASSMARLIN Directory. Selecting **File → Save Session** will present the user with the option to save the files to an alternate location.

4.6. User Preferences

User Preferences can be accessed within the GRASSMARLIN application by selecting **Options → Preferences** from the home toolbar (Figure 26). Within the window, the user can enter the executable path for Wireshark, if installed. By providing the path, GRASSMARLIN can send packets to Wireshark for in depth analysis. The user can set whether the NIC operates in Promiscuous Mode or not. The other options are for the processing of packets and allow the user to specify the CPU utilization parameters. Any changes will be implemented during program execution after clicking Save & Close. Alternatively, user preferences can be edited within a text editor by opening the file *userprefs.txt* in the GRASSMARLIN directory.



Wireshark Executable Path: C:\Program Files\Wireshark\Wireshark.exe

Collapsed Network Hosts: 10

Collapsed Cloud Hosts: 10

Topology Update Rate (secs): 3

General Packet Options

Max Packets per Thread: 1000

Max Threads: 24

Live Packet Options

Promiscuous Mode: ☑

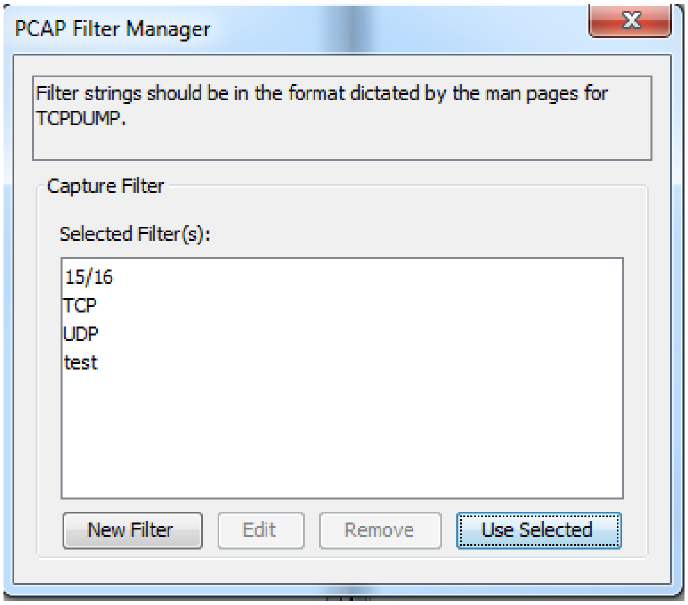
Snap Length: 65536

Timeout (ms): 10000

Figure 26: User Preferences Window

4.7. PCAP Filters

The PCAP filters in GRASSMARLIN are similar to the filters in Wireshark, but the format of the filter string is based on that used for expressions with TCPDUMP (See the TCPDUMP man page for more details). The PCAP Filter Manager allows the user to view, create or modify filters. Within GRASSMARLIN, the PCAP Filter Manager can be accessed from the home toolbar by selecting **Options →PCAP Filter Manager** (Figure 27). As with the user preferences, the *filters.txt* file contains all the filters used by GRASSMARLIN for PCAP filtering. This file can also be edited externally to GRASSMARLIN via a text editor and is located in the GRASSMARLIN directory. Filters can be applied to live captures, as well as imported files.



Filter strings should be in the format dictated by the man pages for TCPDUMP.

15/16
TCP
UDP
test

Figure 27: PCAP Filter Manager

4.7.1. Creating a New PCAP Filter

Clicking the **New Filter** button will open a window as shown in Figure 28. This allows the user to create a new PCAP filter using TCPDUMP syntax for the filter string. Some examples of possible filters are shown in Table 6 below.

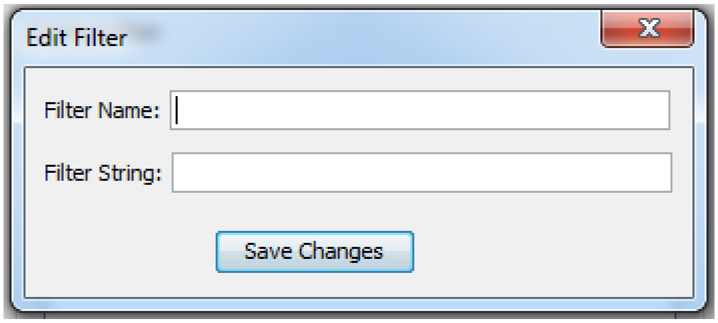


Figure 28: New PCAP Filter Window

Filter String	Description of Packets Filtered
dst host	Destination field of the packet is *host*
src host *host*	Source field of the packet is *host*
host *host*	Either source or destination field of the packet is *host*
dst port *port*	The packet is TCP/IP or UDP/IP and has a destination port value of *port*
src port *port*	The packet is TCP/IP or UDP/IP and has a source port value of *port*
port *port*	The packet is TCP/IP or UDP/IP and has either a source or destination port value of *port*

tcp src port *port*	The packet is TCP/IP and has a source port value of *port*
tcp dst port *port*	The packet is TCP/IP and has a destination port value of *port*
udp src port *port*	The packet is UDP/IP and has a source port value of *port*
udp dst port *port*	The packet is UDP/IP and has a destination port value of *port*

Table 6: PCAP Filter Examples

5. Saving and Exporting

5.1. Save Session

To save a GRASSMARLIN session, go to: **File → Save Session**. A save session window will pop up prompting the user to either use the default session filename, or to change the filename and save location. The session is saved as a .gmses file. Sessions from previous versions of GRASSMARLIN are not compatible with newer versions.

5.2. Export Topology

To export the network topology view, go to: **File → Export Topology**. GRASSMARLIN will export only the view that the user currently has displayed, whether it be logical or physical. The file is saved as a .png in the GRASSMARLIN/ Screenshots folder.

5.3. Export Schema

To export the schema, go to: **File → Export Schema**. GRASSMARLIN will prompt the user to select a file name and save location. The file is saved as an .xsd file.

5.4. Export Data

To export data, go to: **File → Export Data**. A window will pop up prompting the user to select a file name and save location. The file is saved as an .xml file.

5.5. Export Share

To export share, go to: **File -> Export Share**. GRASSMARLIN will save the currently loaded PCAPs and the XML for the current session into a zip file for easy collaboration.

5.6. Quit

Exit the GRASSMARLIN program.

6. Troubleshooting Guide

1) My old session will not open up in the new version of GRASSMARLIN.

Saved sessions from older versions are currently not compatible with newer versions of GM.

2) I am getting the error: “Exception in thread “AWT-EVENTQueue-0” java.lang.UnsatisfiedLinkError. U:\Private\ProgramFiles\grassmarlin1-2-3\ExternalLibs\jnetpcap-1.3.0-1.win32\jnetpcap.d”.

This is caused by jnetpcap not being able to find libpcap. Make sure Packet.dll and wpcap.dll are present in C:\Windows\System32. If they aren’t there, they may be in C:\Windows\SysWOW64.

3) I am getting an error about fingerprints when starting GRASSMARLIN.

The format of the fingerprints has changed: old fingerprints had a classification element that is now unexpected. To resolve this issue, you can do one of the following:

1. Delete C:\Users\<user>\GRASSMARLIN (if you have no saved sessions or custom fingerprints you need from the old version)
2. Rename C:\Users\<user>\GRASSMARLIN to something else such as OLDGRASSMARLIN (if you want to preserve your saved sessions and/or custom fingerprints from the old version)
3. Manually remove all the <classification> lines from the fingerprint files

7. Acronym List

Acronym	Definition
ARP	Address Resolution Protocol
CAM	Content Addressable Memory
CSV	Comma Separated Values
DNP3	Distributed Network Protocol
GUI	Graphical User Interface
HMI	Human Machine Interface
ICS	Industrial Control System
IED	Intelligent Electronic Device
IP	Internet Protocol
MAC	Media Access Control address
MTU	Maximum Transmission Unit
NIC	Network Interface Card
OS	Operating System
OUI	Organizationally Unique Identifier
PCAP	Packet Capture
PLC	Programmable Logic Controller
PNG	Portable Network Graphics
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
TCP	Transmission Control Protocol
TTL	Time-To-Live
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
XML	eXtensible Markup Language

Table 7: List of Acronyms