



AirDefense Advanced Forensics How-To Guide

MOTOROLA SOLUTIONS and the Stylized M Logo are registered in the US Patent & Trademark Office. © Motorola Solutions, Inc. 2013. All rights reserved.

Contents

1	Introduction	5
2	Licensing Advanced Forensics	6
3	Advanced Forensic Analysis	7
3.1	Initiating Forensics Analysis	7
3.2	Using Advanced Forensics	8
4	Sensor	10
4.1	Summary.....	11
4.2	Threat Analysis.....	11
4.3	Threat Breakdown	14
4.4	Traffic Analysis.....	14
4.5	Traffic Breakdown	15
4.6	Channel Analysis.....	15
4.7	Device Analysis	15
4.8	Bandwidth Analysis	15
5	BSS and Wireless Client	16
5.1	Summary.....	17
5.2	Device Info	17
5.3	Threat Analysis.....	19
5.4	Association Analysis	20
5.5	Traffic Analysis.....	20
5.6	Signal Analysis	20
5.7	Location Analysis.....	21
6	Access Point	23
6.1	Summary.....	23
6.2	Device Info	24
6.3	Threat Analysis.....	24
6.4	Adoption History.....	24
6.5	Radio Analysis	25
6.6	Radio Info	26

7	Wireless Switch	27
7.1	Summary.....	28
7.2	Device Info	28
7.3	Threat Analysis.....	29
7.4	Adoption History.....	29
7.5	Performance Analysis	29
8	Backing-up Forensic Data	30

1 Introduction

Wireless Local Area Networks are pervasive in enterprises. But, as 802.11 networks operate in unlicensed 2.4GHz and 5GHz ISM bands, network administrators are faced with challenges to manage the performance and reliability of these networks. The mobility of devices, transient interference sources, and unbounded nature of “wireless” networks will have greater impact on network performance and utilization. The Advanced Forensics Module gives you the tools to monitor, investigate and troubleshoot network performance, roaming and connectivity issues.

This module provides forensic data that allows any device activity to be retraced down to the minute. With forensic analysis, investigating an event takes minutes instead of hours and the remote analysis tools eliminate the need for administrators to physically visit site for carrying out the investigation. Administrators can remotely rewind and review minute-by-minute records of connectivity and communication of the devices with the wireless network.

This module provides the following key benefits:

- Accurate record of wireless threats over time for forensic analysis and policy compliance
- Historic data on wireless activity for quick troubleshooting of performance issues
- Allows trend analysis for network performance and capacity planning

By default, the Basic Forensic Analysis is provided in the AirDefense Service Platform. The Advanced Forensic Analysis has all the features of the Basic Forensic Analysis and the following key additional features.

- Scope Based Forensic Analysis - the ability to show forensic data for the entire system or for a single network level
- The ability to analyze the data for more than a 24 hour time period
- The ability to adjust the time window using sliders
- Graphical views provided in all the tabs of forensics analysis window
- Data filters are enabled
- Location Analysis tab is activated

This document provides details on licensing and using the Advanced Forensics module.

2 Licensing Advanced Forensics

Before using Advanced Forensics on a client or network device, one needs to install the appropriate license in the AirDefense Service Platform (ADSP). The Advanced Forensic license unlocks the functionality to provide unrivaled visibility into network activity and threats.

The license is assigned “per Sensor”. Advanced Forensics Analysis can also be used in deployments where there are no dedicated sensors, but only if the RadioShare option is enabled on Motorola APs (WiNG 5.2.6 and above). In that case, Radioshare Advanced Forensics license (AD-FERS-P-1) will be required for each of the APs. With Advanced Forensics, ADSP stores more than 325 per-minute data points for each wireless device and equips organizations to view months of historical data on any wireless device observed in the environment.

In addition, the Advanced Infrastructure Forensics license can be used for WLAN infrastructure devices like APs and wireless switches to retrieve forensics details from the polled data from these devices. With this license, ADSP stores up to 75 per-minute data points per AP and 40 per-minute data points per WLAN switch.

Note that the same “per-Sensor” license can also cover up to 4 APs or wireless switches for each license ordered. A single license covers 1 sensor and 4 WLAN devices (AP or switch) in deployments with sensors. In non-sensor deployments, the AD-FESN-P-1 license should be ordered for every 4 devices (AP or WLAN controller).

The following table provides different licensing options for the Advanced Forensics module.

Part number	Description
<i>AD-FESN-P-1</i>	AirDefense Advanced Forensic Analysis license for one (1) sensor.
<i>AD-FERS-P-1</i>	AirDefense Radio-share Advanced Forensic Analysis license for one (1) AP.
<i>ADB-NARS-P-1</i>	AirDefense Radio-share license, Network Assurance bundle for one (1) AP. Includes: AP Test, Adv. Forensics, Connectivity Troubleshooting, LiveRF and Spectrum Analysis.

Table 1: License Options for Advanced Spectrum Analysis

The license can be applied to a sensor or AP from an ADSP appliance. In ADSP version 9.x, the above licenses can be applied from **Configuration > Appliance Platform > Appliance Licensing** in the ADSP User Interface.

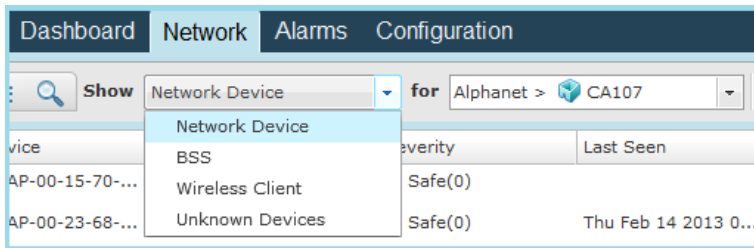
3 Advanced Forensic Analysis

Advanced Forensics allows you to analyze historical information gathered from your WLAN environment. You can rewind and analyze historical data for any wireless devices on your network. The device could be a Sensor, BSS, Wireless Client, Access Point, or a WLAN switch.

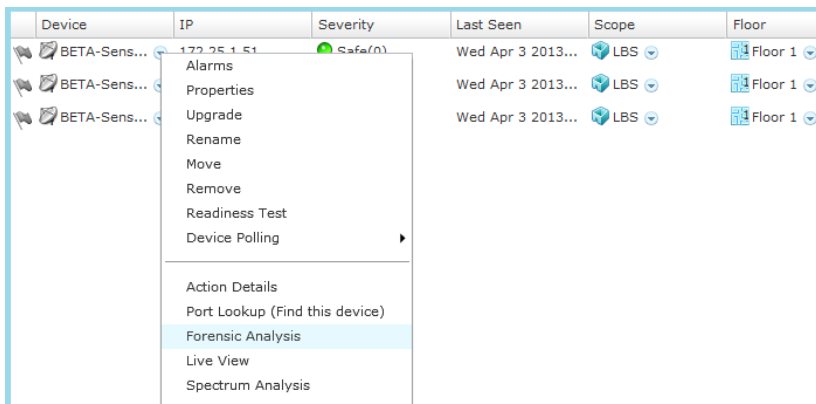
3.1 Initiating Forensics Analysis

The Forensic Analysis can be run in two ways — directly on the device, or from main **Menu**

If you want to run the forensics on the device directly, go to **Network** tab and list the appropriate device category in the target network scope as shown below.

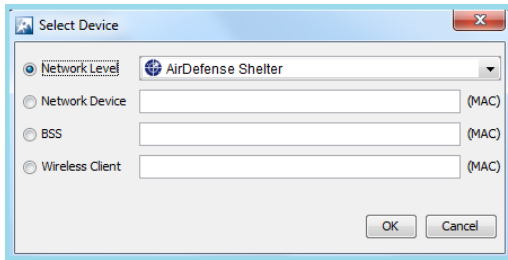


Right-click on the target device in **Device** column. Select **Forensic Analysis** option as mentioned below to launch the **Forensic Analysis** on that device.



Alternatively, to initiate forensic analysis, select **Menu > Forensic Analysis**.

The **Select Device** window displays. Select one of the following device options.



Network Level — to run forensic analysis on a particular scope. Note, there must be at least one sensor in that scope with forensics license installed for using this option. Otherwise you will get an error message.

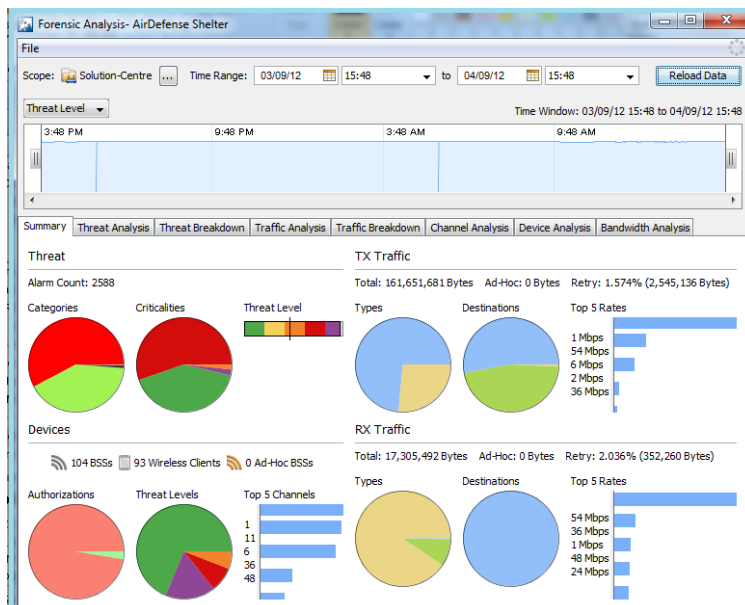
Network Device — to run forensic analysis on a desired network device like Sensor, AP or WLAN switch. Enter a valid MAC address of the device.

BSS or Wireless Client — to run forensic analysis on a BSS or a wireless client. Enter a valid MAC address of the BSS or client device.

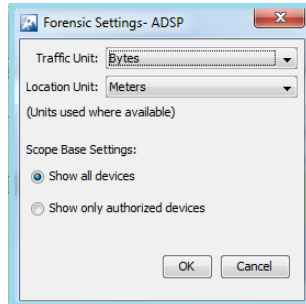
Press **OK** to launch the **Forensic Analysis** window.

3.2 Using Advanced Forensics

Depending on the device type being analyzed — sensor, AP, switch, BSS, or wireless client, a different Forensic Analysis window will be displayed. The different windows are discussed in detail from section 4 to section 7 of this document. An example Forensics Analysis Window for a sensor device is shown in below.



The following fields are common to all device types. The **File** menu provides an option to change forensic settings. Click **File** menu and select the **Settings** option. The following window will be displayed.



The forensic settings are used to set the traffic and location units for traffic and location Analysis respectively. You can also select whether to show forensic information for all devices or only for authorized devices.

Scope — the Scope field displays the device name or network scope that is being analyzed. By right clicking on the device, a device's MAC address can be copied for later use.

Switching Devices — the forensic analysis can be switched to another device using the device's MAC Address. To switch devices, click the “...” button and select appropriate option.

Time Range — by default, the time period is set 24 hours prior to when the Forensic Analysis is first accessed. The 24 hour period can be changed by selecting the desired range for the date and time of day. Press the **Reload Data** button to load the data for the chosen period.

Time Window — the Time window has one or more graphical views based on the target device type on which forensic analysis is carried out. You can narrow the forensic data to a specific time period by using the slider buttons on the left and right hand side of this window. The following table lists different graphical views available for different device types.

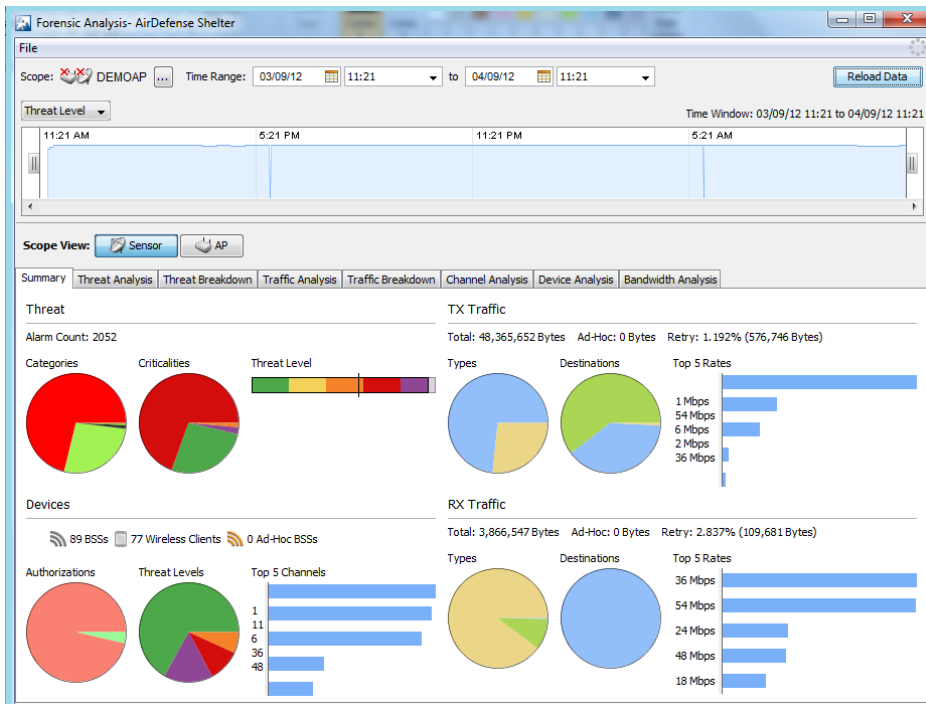
Device Type	Available Views
Sensor or BSS or Wireless Client	<ul style="list-style-type: none"> • Threat Level (default) • Total Traffic • Association Count • <i>Note:- in case of a wireless client, the associated count indicates the number of BSSes that the client was associated within the observed period.</i>
Access Point or Controller	<ul style="list-style-type: none"> • Threat Level • Status Polling Times • Data Polling Times

4 Sensor

When Forensic Analysis is run on a Sensor device, the following eight tabs are available in Forensic Analysis Window. The details for each of these tabs are provided in the following sections.

- Summary
- Threat Analysis
- Threat Breakdown
- Traffic Analysis
- Traffic Breakdown
- Channel Analysis
- Device Analysis
- Bandwidth Analysis.

Refer to section 3.2 for details on the usage of common fields on the Forensic Analysis window.



4.1 Summary

The **Summary** tab shows high-level information about the threat level, device counts and traffic for the entire scope over the selected time range.

It has four main sections — Threat, Devices, TX traffic and RX traffic, as described below.

Threat — this section provides the total alarm count, threat level, and color coded break down of alarms by categories and severity, as seen by the sensor.

Hover the mouse over the different colors in the **Categories** and **Criticalities** pie charts to reveal the tool tip with information on the security threats by threat category and severity respectively.

Devices — this section provides a summary of the total infrastructure networks (BSSes), wireless clients and peer-to-peer or ad-hoc wireless networks observed by the sensor.

It also summarizes devices by authorization, threat level and channel.

TX Traffic — this section provides a summary of the total transmitted traffic and the contribution of traffic from P2P/Ad-hoc wireless networks. It also displays the percentage of re-transmitted packets and top five data rates used for packet transmission to provide an indication of the quality of the RF environment.

- **Types** — pie chart indicates the transmitted frames by frame type, i.e., data or management.
- **Destinations** — pie chart indicates the transmitted frames by frame destination, i.e., broadcast, multi-cast or unicast.

RX Traffic — this section provides summary of the total received traffic by the sensor and traffic from P2P/Ad-hoc wireless networks. It also displays the percentage of received traffic that was retransmitted along with the top five received data rates.

- **Types** — pie chart indicates the received frames by frame type, i.e., data or management.
- **Destinations** — pie chart indicates the received frames by frame destination, i.e., broadcast, multi-cast or unicast.

4.2 Threat Analysis

The **Threat Analysis** tab displays list of alarms generated by the device being analyzed. The following fields are shown in both Graphical and Tabular formats.

Criticality — indicates color coded bubble and name for the threat level, as mentioned below.

- **Severe** — serious alarms that may have catastrophic effects on your WLAN.
- **High/Critical** — serious alarms on devices that require immediate attention.
- **Elevated/Major** — potentially serious alarms on devices that require priority attention.

- *Guarded/Minor* — Potential problem alarms on devices that may develop into worse issues if left unresolved.
- *Safe/Low* — Devices that pose no immediate threat to your WLAN network

Category — the type of category that the alarm falls under.

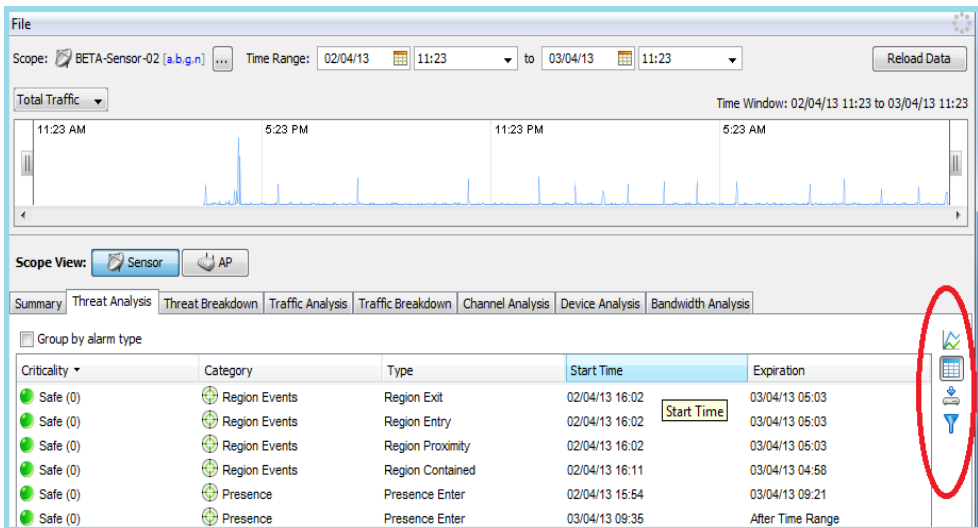
Type — the specific type of alarm, providing detailed information as to what generated the alarm in the first place. Right click on the alarm name to find more details on this alarm.

Start Time — the date and time of when the alarm first occurred.

Expiration — the date and time of when the alarm will expire. The alarm can be an ongoing alarm which never expires.

The data can be displayed in a graphical or tabular format by selecting the **Data Chart** and **Data Table** buttons respectively, which are located on the right hand side of the window as shown below.

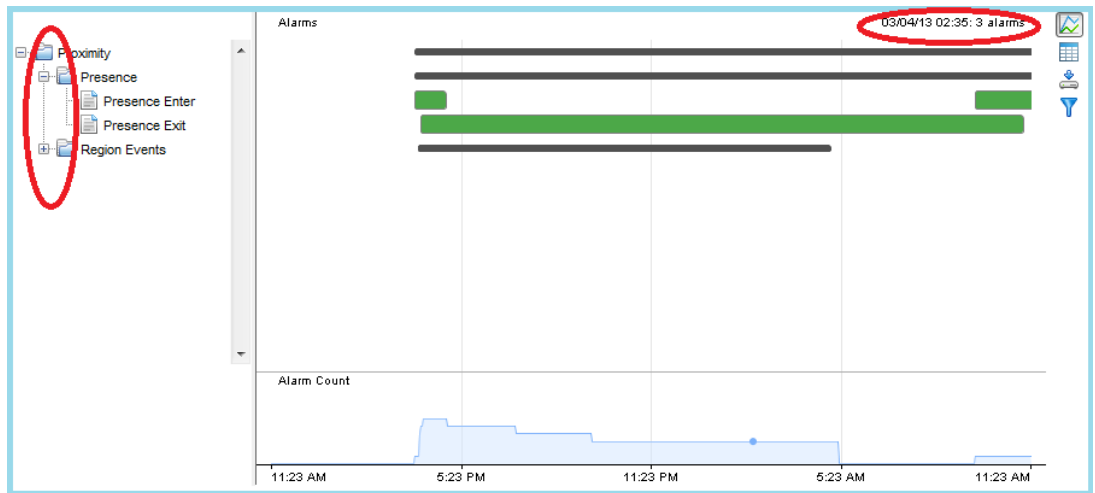
You can export the table data to a CSV file by clicking the **Export Data** button. An Export Table window will display where you can name and save the file to a location on your hard drive. You can filter the alarms by using **Filter Data** button. The columns can be arranged by clicking on the column name and dragging.



In the Tabular view, you can customize columns of your interest in the Forensic Analysis window. A column can be hidden by right-clicking in the column heading area and un-checking the checkbox for a particular column, as shown below.

Criticality	Category		Type	Start Time	Expiration
Safe (0)	Presence	<input checked="" type="checkbox"/> Criticality	Presence Enter	02/04/13 15:54	03/04/13 09:21
Safe (0)	Presence	<input checked="" type="checkbox"/> Category	Presence Enter	03/04/13 09:35	After Time Range
Safe (0)	Presence	<input checked="" type="checkbox"/> Type	Presence Exit	02/04/13 16:05	03/04/13 11:08
Safe (0)	Region Events	<input checked="" type="checkbox"/> Start Time	Region Exit	02/04/13 16:02	03/04/13 05:03
Safe (0)	Region Events	<input checked="" type="checkbox"/> Expiration	Region Entry	02/04/13 16:02	03/04/13 05:03
Safe (0)	Region Events		Region Proximity	02/04/13 16:02	03/04/13 05:03
Safe (0)	Region Events		Region Contained	02/04/13 16:11	03/04/13 04:58

In the Graphical view, you can click on the plus (+) or minus (-) sign on the left side of the window to expand or collapse a category. If you expand it, it will show any changes in the category. If you position your cursor over any part of the graphical data, the exact reading for that moment is displayed in the top, right side the tab. An example is shown in below diagram.



4.3 Threat Breakdown

The **Threat Breakdown** tab displays information on the threat level for all devices within the selected scope.

Time — the date and time stamp, minute-by-minute.

Device Threat Level — a column for each device considered a threat, displaying a numerical value of the threat level.

The information is displayed both in Tabular and Graphical Views. Refer to section 4.2 for details on the usage of Tabular and Graphical Views in general.

4.4 Traffic Analysis

The **Traffic Analysis** tab displays details on the traffic transmitted and received by all devices in the selected scope. The **Traffic Category** field determines the type of data displayed in the table. The traffic category can be changed by selecting one of the following values from the **Traffic Category** dropdown menu:

- Ad-Hoc
- Control Details
- Data Details
- Destinations
- EAP Details
- Encryption Details
- Management Details
- Rates
- Retry
- Types

The **Traffic Type** field determines whether transmitting data (**TX**), receiving data (**RX**), or both TX and RX data (**All**) types is displayed. The traffic type can be changed by selecting the appropriate radio button.

The **Time** column is included in every traffic category. The other columns vary according to selected traffic category.

The traffic details are displayed both in Tabular and Graphical Views. Refer to section 4.2 for details on the usage of Tabular and Graphical Views in general.

4.5 Traffic Breakdown

The **Traffic Breakdown** tab displays breakdown of the traffic generated by individual devices within the selected scope.

The **Time column** is included in every traffic category. The first 8 items are shown in the other columns by default. Column display and arrangement can be customized as mentioned in section 4.2.

The traffic breakdown is displayed both in Tabular and Graphical Views. Refer to section 4.2 for details on the usage of Tabular and Graphical Views in general.

4.6 Channel Analysis

The **Channel Analysis** tab provides information on the total devices observed in each channel over time.

The **Device Type** field determines whether the device listing is displayed per channel for Wireless Clients, BSSs, or all devices in the table. The device type can be changed by selecting the appropriate value.

The **Time** column is included in every device category. The other columns list device count for the individual channels.

The channel analysis information is displayed both in Tabular and Graphical Views. Refer to section 4.2 for details on the usage of Tabular and Graphical Views in general.

4.7 Device Analysis

The **Device Analysis** tab provides total devices observed for various device categories along with information on total online or offline Sensors for the chosen period.

The **Display Category** field determines whether the device count is displayed for *Devices* or *Sensors*. Devices may be Wireless Clients, BSSs, or Ad-Hoc BSSs. Sensors may be Online or Offline Sensors. You can change the display category by selecting the appropriate option in the list box.

The **Time** column is included in every display category. The other columns vary according to the selected display category.

The device analysis information is displayed both in Tabular and Graphical Views. Refer to section 4.2 for details on the usage of Tabular and Graphical Views in general.

4.8 Bandwidth Analysis

The **Bandwidth Analysis** tab provides details of the wired bandwidth usage of the Sensor and related network scopes.

A **Time** category is included in the table along with a column for each of the network levels and the Sensor being analyzed.

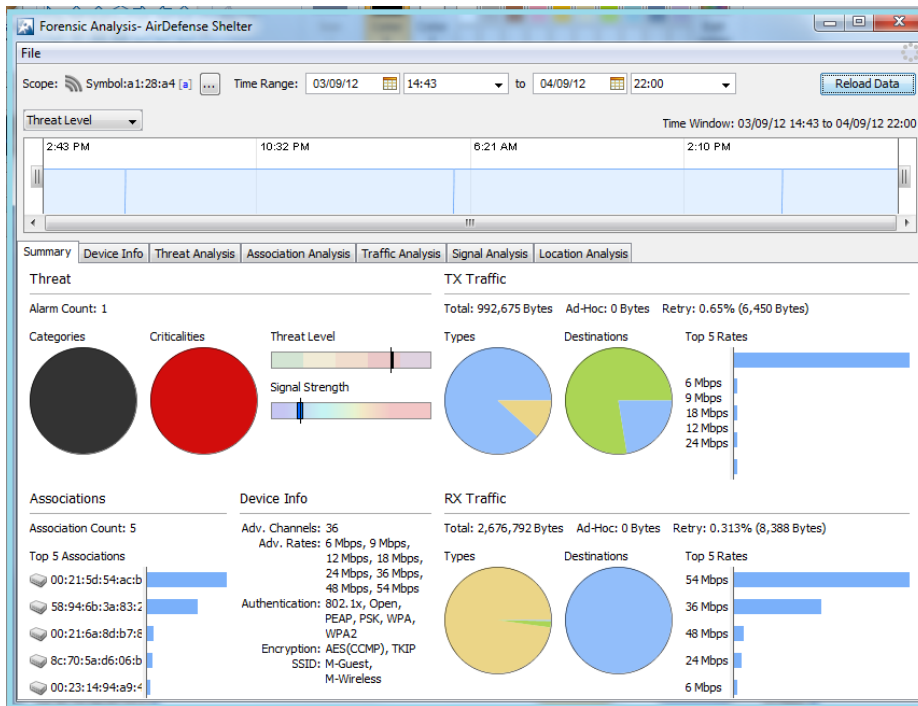
The bandwidth analysis is displayed both in Tabular and Graphical Views. Refer to section 4.2 for details on the usage of Tabular and Graphical Views in general.

5 BSS and Wireless Client

When Forensic Analysis is run on a BSS or a Wireless Client device, the following six tabs are available in the Forensic Analysis Window. The details for each of these are provided in the following sections.

- Summary
- Device Info
- Threat Analysis
- Association Analysis
- Traffic Analysis
- Signal Analysis

Refer to section 3.2 for details on the usage of common fields on the following Forensic Analysis Window.



5.1 Summary

The **Summary** tab provides a summary of forensic data broken down into categories that roughly match contents of the other tabs.

The following fields are present in the **Summary** tab:

Threat:

- *Alarm Count* - Total alarm count
- *Categories and Criticalities* - Alarm pie charts grouped by categories and criticalities
- *Threat Level* - Minimum, maximum, and average threat level
- *Signal Strength* - Minimum, maximum, and average signal strength

Associations:

- *Association Count* - Total number of unique associated devices
- *Top 5 Associations* - Top 5 associated devices based on traffic by associated client

Device Info — the device information contains channel, rates, authentication protocol and encryption type and SSID used by the device.

TX Traffic and RX Traffic — these sections are similar to those found in **Summary** tab of Forensics Analysis on a Sensor device. For details refer to section 4.2.

5.2 Device Info

The **Device Info** tab displays the current settings for the device being analyzed. The following table provides description of each field along with an indication ('x') on whether it is applicable for BSS and Wireless Client.

Column	Description	BSS	Wireless Client
<i>Time</i>	The date and time of day when the device was seen.	X	X
<i>Advanced Capabilities</i>	An abbreviated description indicating the advanced capabilities of a BSS.	X	
<i>Advertised Channels</i>	The WLAN broadcast channel for the device.	X	X

<i>Advertised Rates</i>	The advertised data rates of the BSS in mbps.	X	
<i>Authentication</i>	The type of authentication protocol supported by the BSS.	X	X
<i>Capabilities</i>	Device capabilities including: <ul style="list-style-type: none"> • ESS network • Data confidentiality required • Short slot time enabled • APSD implemented • DSSS-OFDM not in use • RTS/CTS or CTS-to-self protection • Barker Preamble mode • DCF. 	X	X
<i>Channels Used</i>	The WLAN broadcast channel for the device.	X	
<i>Encryption</i>	Encryption type being used.	X	X
<i>IP Address</i>	A Wireless Client's Internet Protocol address.		X
<i>IP-SEC</i>	Internet Protocol Security method being used.	X	X
<i>LEAP User Name</i>	The user name used during LEAP authentication (if used).		X
<i>Rates Used</i>	The data rates used during association.	X	X
<i>Reason Codes</i>	A code representing the reason that a device did not associate or authenticate, or lost association or authentication.	X	X
<i>SSID</i>	The Service Set Identifier, a 32-character unique identifier that represents the name	X	X

	of the network.		
<i>SSID Broadcast</i>	An indication (Yes/No) of whether the SSID is being broadcasted.	X	X
<i>Status Codes</i>	A code representing the status of authentication or association of a device.	X	X

The Tabular View may be shown with **One row per minute** or **One row for every change** in the value of a particular column or category. Select one of these radio buttons in the top, left side of the **Device Info** tab for the appropriate view.

5.3 Threat Analysis

The **Threat Analysis** tab displays a list of alarms generated by the device being analyzed. The following fields are shown both in Graphical and Tabular format.

Criticality — indicates color coded bubble and name for the threat level, as mentioned below.

- *Severe* — Serious alarms that may have catastrophic effects on your WLAN.
- *High/Critical* — serious alarms on devices that require immediate attention.
- *Elevated/Major* — potentially serious alarms on devices that require priority attention.
- *Guarded/Minor* — Potential problem alarms on devices that may develop into worse issues if left alone.
- *Safe/Low* — Devices that pose no immediate threat to your WLAN network

Category — the type of category that the alarm falls under.

Type — the specific type of alarm, providing detailed information as to what generated the alarm in the first place. Right click on the alarm name to find more details on the alarm.

Start Time — the date and time group of when the alarm first occurred.

Expiration — the date and time group of when the alarm will expire. The alarm can be an ongoing alarm which never expires.

SSID — the Service Set Identifier, a 32-character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the BSS.

Channel — the WLAN broadcast channel for the device.

Signal Strength — the signal strength (in dBm) of the device.

Sensor — the name of the Sensor that sees the device.

BSS — The Basic Service Set, a term used to describe the collection of Wireless Clients which may communicate with each other within a WLAN.

The **Group by alarm type** field allows you to group all alarms of the same type together. Only the alarm type is displayed in the table.

Right-clicking on an alarm and selecting **Alarm Details** displays the **Alarm Details** window where you can find detailed information about an alarm.

Refer to section 4.2 for details on the usage of Tabular and Graphical Views in general.

5.4 Association Analysis

The **Association Analysis** tab lists the associations between the device being analyzed and other wireless devices.

Device — MAC address of the device.

SSID — Service Set Identifier of the associated AP.

Start — Time when the association first started.

End — Time when the association ended.

Duration — Total amount of time the association lasted.

RX Traffic — Number of bytes received during the association.

TX Traffic — Number of bytes transmitted during the association.

An option is included to group by associated device. When selected, there will be only one row for each unique device. Click the **Group by associated device** checkbox to select the option.

Right-clicking on a device displays a menu of options that allows you to conduct additional functions on the chosen device. The association information is displayed both in Tabular and Graphical Views. Refer to section 4.2 for details on the usage of Tabular and Graphical Views in general.

5.5 Traffic Analysis

The **Traffic Analysis** tab displays traffic transmitted and received by the device being analyzed. This is similar to the corresponding tab found when you run Forensic Analysis on a sensor device. So, refer to section 4.4 for more details on this tab.

5.6 Signal Analysis

The **Signal Analysis** tab displays a device's signal strength (in dBm) as measured by various Sensors at different point of times. The device's average signal strength (in dBm) is displayed under the **Totals** row.

The table view will have a **Time** column and a column for each Sensor that has seen the device being analyzed.

An option is included to remove empty rows. When selected, any row with no data is removed from the table. Click the **Remove empty rows** checkbox to select the option.

The Signal Analysis is displayed both in Tabular and Graphical Views. Refer to section 4.2 for details on the usage of Tabular and Graphical Views in general.

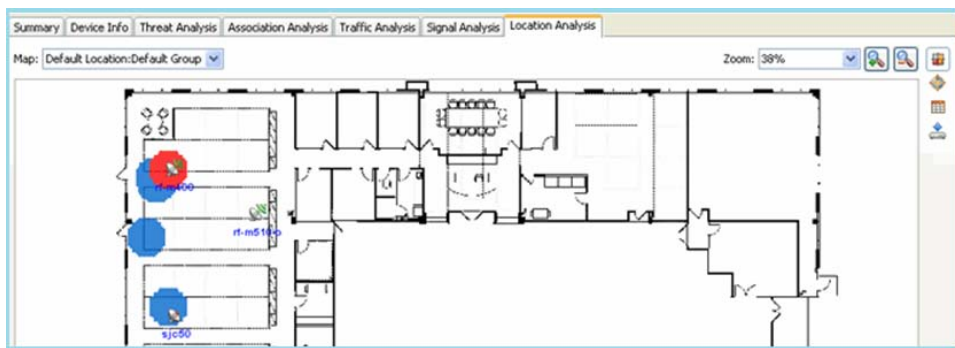
5.7 Location Analysis

The **Location Analysis** tab provides a graphical and tabular view of the device location.

Following three views are available:

- Heat Map
- Location Map
- Table View.

Heat MAP— The first time when the Location Analysis tab is accessed, the **Heat Map** view is displayed, as shown below. This view uses a heat map to show where the device was located during the entire forensic period. Note that, the floor design must be setup in ADSP for using this feature. Higher intensity of the color indicates that the device was at a particular location for a longer period of time. You may select any floor map in the system for display as a heat map. Use the **Map** dropdown menu to select another map.



You may zoom in or out while viewing a map using the controls on the right hand side.

Location MAP—The location map can be switched by clicking the **Location Map** button on the right most corner of the window. This view displays a device's location at a specific point in time. You can use the slider on the top-left to adjust the time to a specific minute during the forensic analysis period. As the slider is moved the device's location is adjusted on the location map. In addition, the map is automatically switched if the device moves between maps during the time period.

The zoom controls and buttons work the same as they do in the Heat Map.

Data Table — Alternatively, you can switch to the table view by clicking the **Data Table** button, as shown below.

Time	Map	X Offset Left (meters)	Y Offset from Top (meters)	Probability
9/12/07 10:00 AM	Default Location:Default Group	16.112 Meters	16.869 Meters	73%
9/12/07 10:01 AM	Default Location:Default Group	16.112 Meters	16.869 Meters	73%
9/12/07 10:02 AM	Default Location:Default Group	16.112 Meters	16.869 Meters	73%
9/12/07 10:03 AM	Default Location:Default Group	16.112 Meters	16.869 Meters	73%
9/12/07 10:04 AM	Default Location:Default Group	16.112 Meters	16.869 Meters	73%
9/12/07 10:05 AM	Default Location:Default Group	16.112 Meters	16.869 Meters	73%
9/12/07 10:06 AM	Default Location:Default Group	16.112 Meters	16.869 Meters	73%
9/12/07 10:12 AM	Default Location:Default Group	16.112 Meters	16.869 Meters	75%
9/12/07 10:13 AM	Default Location:Default Group	16.112 Meters	16.869 Meters	75%
9/12/07 10:14 AM	Default Location:Default Group	16.112 Meters	16.869 Meters	75%

Table view displays the device location over a period of time in a tabular form. Location data is given in the following columns:

Time — Time stamp in 1-minute increments.

Map — Name of floor/location map.

X Offset Left — Distance from the left (in meters).

Y Offset from Top — Distance from the top (in meters).

Probability — a percentage representing the probability that the device will be presented in the location mentioned.

6 Access Point

When Forensic Analysis is run on an Access Point device, the following six tabs are available in the Forensic Analysis Window. The details for each of these are provided in the following sections.

- Summary
- Device Info
- Threat Analysis
- Adoption History
- Radio Analysis
- Radio Info

Refer to section 3.2 for details on the usage of common fields on this Forensic Analysis Window.

6.1 Summary

The **Summary** tab for the AP provides summary of device information about the AP as well as the MAC address of each radio and the 802.11 standard that is being used.

The screenshot shows the 'Forensic Analysis - AirDefense Shelter' window. The 'File' menu is open, and the 'Scope' is set to 'ap300-D5DB18'. The 'Time Range' is from '18/02/13 13:57' to '19/02/13 13:57'. The 'Threat Level' is set to 'Low', and 'Status Polling Times' and 'Data Polling Times' are checked. The 'Time Window' is '18/02/13 13:57 to 19/02/13 13:57'. The timeline shows a series of vertical bars representing data points. The 'Summary' tab is selected, and the 'Device Info' section is expanded. The 'Radios' section shows a diagram of the AP with two radio antennas. The first radio has MAC address '00:15:70:d0:1f:64 [a]' and is identified as 'Symbol d0:1f:64 - AM-Wireless'. The second radio has MAC address '00:15:70:d0:25:98 [b,g]' and is identified as 'Symbol d0:25:98 - AM-Wireless'.

Device Info

Total Uptime: **00d:21h:36m:00s**
First Seen: **Mon Jul 09 23:14:40 BST 2012**
Last Seen: **Tue Feb 19 13:55:16 GMT 2013**
Polled IP: **0.0.0.0**
Audit Status: **N/A**
DNS Name:
Sys Description: **Unknown**
Sys Name: **ap300-D5DB18**
Sys Location: **Unknown**
Manufacturer: **Motorola**
Model: **AP300**
Firmware Version: **01.00-2354r**
Serial Number: **001570D5DB18**
Name:
Polled Name: **Unknown**

Radios

- 00:15:70:d0:1f:64 [a]
Symbol d0:1f:64 - AM-Wireless
- 00:15:70:d0:25:98 [b,g]
Symbol d0:25:98 - AM-Wireless

6.2 Device Info

The **Device Info** tab provides a graphical and tabular view of the current settings of the following fields on the AP being analyzed, which are self explanatory.

- Audit Status
- DNS Name
- Firmware Version
- IP Address
- Name
- Online Status
- Polled Hostname
- Polled IP Address
- Polled Name
- Sys Description
- Sys Location
- Sys Name.

The table may be shown with one row per minute or one row for every change in the value of a particular column. Click the appropriate radio button in the top, left side of the **Device Info** tab.

Refer to section 4.2 for details on the usage of common fields on this Forensic Analysis Window.

6.3 Threat Analysis

The **Threat Analysis** tab displays all alarms generated by the device being analyzed in tabular or graphical view. This is similar to the corresponding tab found when Forensic Analysis is run on a sensor device. So, refer to section 4.24.4 for more details on this tab

6.4 Adoption History

The **Adoption History** tab provides a graphical and tabular view of the devices that have adopted to the device being analyzed. An example screenshot of the tabular view of this tab is shown below.

Group by associated device

Device	Start	End	Duration
RFS4000-C Collier	Ongoing Adoption	4/12/11 11:10 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 11:13 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 11:18 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 11:23 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 11:28 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 11:33 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 11:38 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 11:43 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 11:48 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 11:53 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 11:58 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 12:03 PM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 12:08 PM	11.5 days

The following fields are presented in this tab.

Device — the name of the device that adopted to the AP.

Start — the date and time when the adoption first occurred. This can be an ongoing adoption.

End — the date and time when the adoption last occurred.

Duration — the amount of time the adoption lasted.

The **Group by associated device** field allows you to group devices of the same type together. Refer to section 4.2 for details on the usage of Tabular and Graphical Views in general.

6.5 Radio Analysis

The **Radio Analysis** tab provides historic radio information that can be used to analyze the radios of the AP being investigated. The information is displayed both in tabular and graphical views.

In the **Tabular View**, the **Radio Category** field determines what columns are displayed in the table. The following categories are present.

Noise—displays the average noise seen on each radio in dBm.

Power—displays the average power used by each radio over time.

Retry—displays the total number of retries that has occurred from data being retransmitted.

Traffic—displays the total traffic seen on each radio in bytes.

Traffic Type — determines whether you see above information for transmitting data, receiving data, or all data types. The traffic type can be changed by selecting the appropriate radio buttons – **TX**, **RX**, and **All**.

The **Time** column is included in every radio category while the other columns reflect the MAC address of the radios:

The **Graphical View** presents the same information in graphical chart. The left side of the graphical view has two columns.

Data Series—Acts as a filter to determine how the graphs are displayed. The Radio Category field determines what is shown in this column. Anything with a checkmark in its checkbox will be seen in the graphs. If there is no checkmark, it is filtered out of the graph. Click on the checkbox to change the state.

Highlighted Value—If you position your cursor over any part of the graph, the values for that moment is displayed in this column.

6.6 Radio Info

The **Radio Info** tab provides information on the radio modes and operating channels of the AP for the chosen period of time. The following fields are displayed in the tab.

Time — the date and time of day when the information was recorded.

Channel — the WLAN broadcast channel for the device.

Channel Extension —the channel extension being used if any.

Mode —the mode the AP radio is operating in (Infrastructure or Sensor).

Protocols —the 802.11 standards being used by the AP radio (a, b, g, and n).

Status —the status of the AP radio (enabled or disabled).

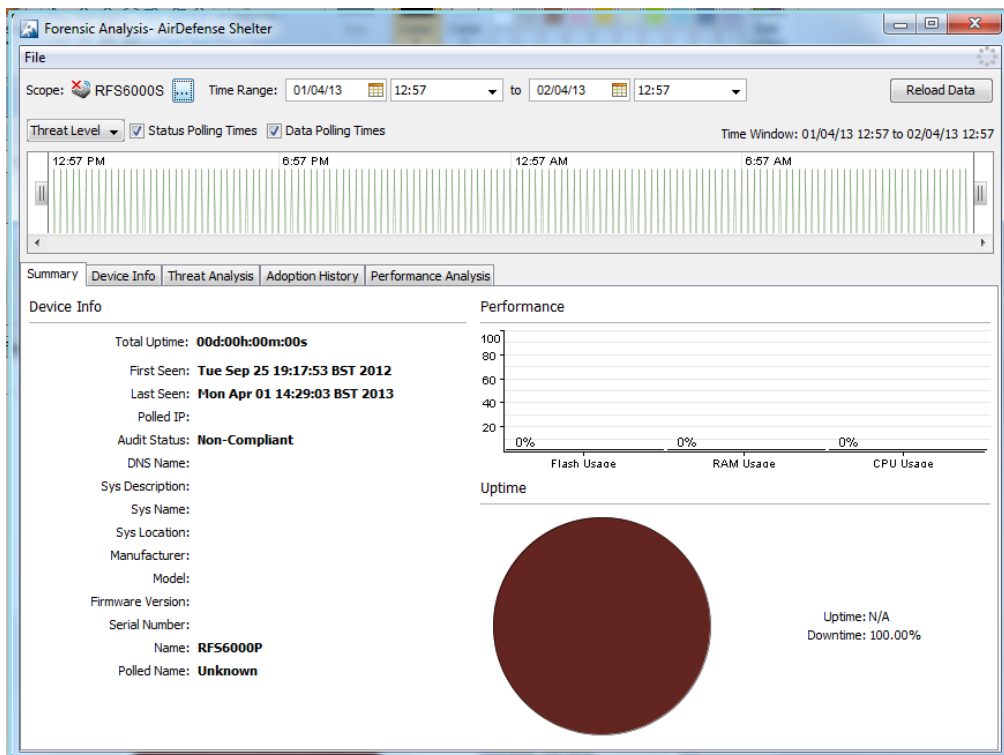
The information is displayed both in tabular and graphical views. Refer to section 4.2 for details on the usage of Tabular and Graphical Views in general.

7 Wireless Switch

When Forensic Analysis is run on a Wireless Switch, the following six tabs are available in the Forensic Analysis Window. The details for each of these are provided in the following sections.

- Summary
- Device Info
- Threat Analysis
- Adoption History
- Radio Analysis
- Radio Info

Refer to section 3.2 for details on the usage of common fields on this Forensic Analysis Window.



7.1 Summary

The **Summary** tab provides device summary, performance details like Flash, RAM and CPU usage, and the uptime and downtime of the wireless switch.

7.2 Device Info

The **Device Info** tab displays the current settings of the following fields of the switch being analyzed.

Total Uptime — the up-time duration of the switch.

First Seen — the date and time when the switch is first discovered by ADSP

Last Seen — the date and time when the switch was last seen by ADSP

Audit Status — the status of the last audit (compliant or non-compliant).

DNS Name — the DNS name assigned to the switch.

Firmware Version — the current firmware version installed on the switch.

IP Address — the Switch's Internet Protocol address.

Name — the name of the Switch. The name is specified by a user through the switch's properties.

Online Status — the online/offline status of the switch.

Polled Hostname — the hostname that is pulled from the switch by ADSP either upon import/discovery of the switch or when ADSP does a data poll.

Polled IP Address — the IP address that is pulled from the switch by ADSP either upon import/discovery of the switch or when ADSP does a data poll.

Polled Name —the device name that is pulled from the switch by ADSP either upon import/discovery of the switch or when ADSP does a data poll.

Sys Description —A description of the switch. This information is obtain from an import/discovery of the switch or when ADSP does a data poll.

Sys Location —the location of the switch. This information is obtain from an import/discovery of the switch or when ADSP does a data poll.

Sys Name —the name of the switch. This information is obtain from an import/discovery of the switch or when ADSP does a data poll.

The information is displayed both in tabular and graphical views. Refer to section 4.2 for details on the usage of Tabular and Graphical Views in general.

7.3 Threat Analysis

The **Threat Analysis** tab displays all alarms generated by the device being analyzed in tabular or graphical view. This is similar to the corresponding tab found when you run Forensic Analysis on a sensor device. So, refer to section 4.2 for more details on using this tab.

7.4 Adoption History

The **Adoption History** tab provides details to determine which devices have been adapted to the switch.

The following fields are presented in this tab.

Device — the name of the device that is (was) adapted to the switch

Start — the date and time when the adoption first occurred. This can be an ongoing adoption.

End — the date and time when the adoption last occurred.

Duration — the amount of time that the adoption has lasted.

The **Group by associated device** field allows you to group devices of the same type together.

The information is displayed both in Tabular and Graphical Views. Refer to section 4.2 for details on the usage of Tabular and Graphical Views in general.

7.5 Performance Analysis

The **Performance Analysis** tab provides performance data of CPU, Flash and RAM over a period of time for the switch being analyzed.

The **Performance Category** field determines what information is displayed in the table. The performance category can be changed by making one of the following selections from the dropdown menu:

Raw Data — this option displays absolute usage of the Flash and RAM at various time periods

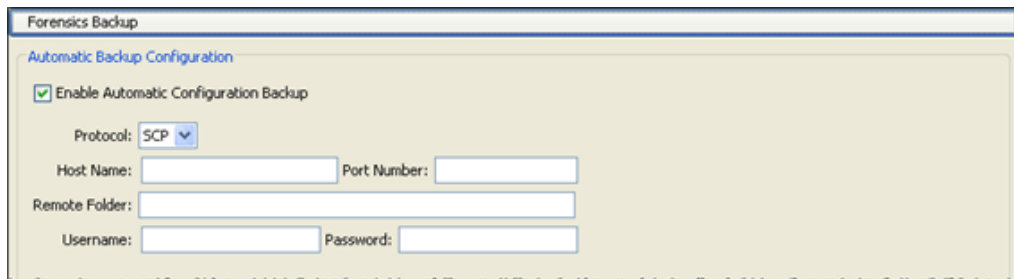
Percentage — this option displays percentage of the utilization of Flash, RAM and CPU at various time periods.

The information is displayed both in Tabular and Graphical Views. Refer to section 4.2 for details on the usage of Tabular and Graphical Views in general

8 Backing-up Forensic Data

It is a good practice to configure an ADSP system to perform the back-up of forensics data automatically, so that in the event that the ADSP appliance needs to be replaced, it can be done so without any loss of forensic data during the transition.

To do this, from the ADSP dashboard interface, select **Menu -> Appliance Manager**. From the launched window, select **Backups -> Forensics Backup**. Select and enable the checkbox named **Enable Automatic Forensics Backup** as shown below.



Then, you need to fill the following fields described.

Protocol — the file transfer protocol to use for backing up forensics.

Host Name — the name of the server where you want to back up forensics. This can be an IP address or a DNS name defined by your DNS server.

Port Number — the port number to use during the backup.

Remote Folder — the directory (folder) where to place the backup on the destination server.

Username — the username used to log in on the destination server.

Password — the password used to log in on the destination server

Now, whenever a forensics data file is created, it is automatically backed up on the host configured above.



NOTE When you first turn on automatic Forensics backup, only new forensic files are backed up. Existing forensic files will not be backed up. You will have to save old files if you want to copy them to another server.



Motorola Solutions, Inc.
1301 E. Algonquin Rd.
Schaumburg, IL 60196-1078, U.S.A.
<http://www.motorolasolutions.com>

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.
© 2012 Motorola Solutions, Inc. All Rights Reserved.

