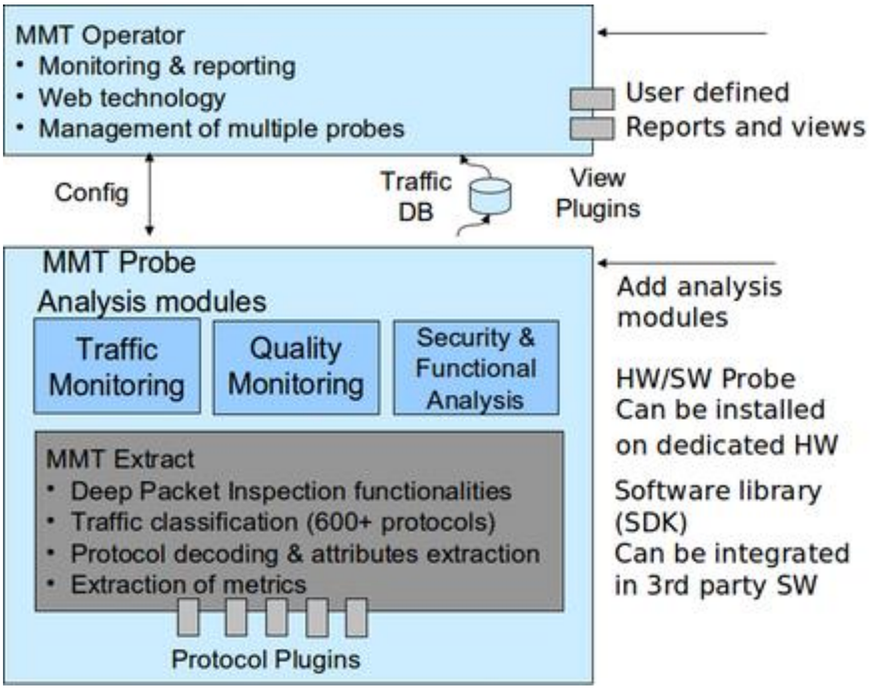
MMT User Guide

Monitoring Tool of MEASURE Platform

Montimage Monitoring Tool (MMT) is a monitoring solution that combines data capture, filtering and storage, events extraction and statistics collection, and traffic analysis and reporting, providing network, application, session, and user-level visibility. Furthermore, it is able to correlate information from different sources to detect complex events, and thanks to an advanced rule-based engine, propose counter-measures to react to detected situations (e.g., performance, security, operational incidents). MMT performs online and offline monitoring of the traces of a running system, and it allows the extraction of complex measurements from individual pieces of data. It is able to operate in a non-obstructive fashion, since the execution traces are observed without interfering with the behaviour of the system.

MMT can be easily integrated with third parties in various ways: structured data produced by other applications or systems can feed the Extract module; extracted data and detected events can be used by other tools; behaviour models, pattern matching rules, etc. can be converted to properties to correlate information; and verdicts and events can be used by external tools. All these functionalities are summarized in the MMT global view presented in Figure below.



MMT-Operator

This document presents Graphical User Interface of MMT-Operator.

MMT-Operator is a Web application. It has typically 2 parts: Client (front end) and Server (back end).

- **The Server** is written in NodeJS running at the server side.
- **The Client** is written in JavaScript and HTML running on Web browsers at the client sides. There may be many users using their Web browsers to connect to the Server to statistics of

MMT. These statistics will be graphically represented in Web browsers of users in forms of chart elements, such as, bar, line, pie, or table. This document presents in detail of the elements.

```
 --------------------                --------------
|                    |               |              |<=====> Database
|       Client       | <==RESTful==> |    Server    |
| (HTML, Javascript) |               |   (NodeJS)   |<===== MMT-Probe(s)
 --------------------                --------------
```

General Structure

The followings are some basic notations being used in MMT:

- **Protocol** is a network protocol such as, IP, HTTP, NDN, etc.
- **Application** such as BitTorrent, Skype, etc. Contact us to get the full list of protocols and applications that have been supported by MMT.
- **Profile** is a group of protocols and/or applications. MMT-Operator has currently 13 profiles: Content Delivery Network, Cloud Storage, Conversational, DataBase, Direct Download Link, File Transfer, Gaming, Mail, Network, Peer to Peer, SocialNetwork, Streaming, Web.
- **Packet** is a term used in MMT to represent a data unit of a protocol. It is not restricted only for protocols at layer 3 of OSI. A packet consists of a **header** part and **payload** part. Header part contains control information that provides data for delivering the payload, for example: source and destination network addresses, error detection codes, and sequencing information. Payload part contains user data that may be a packet of a higher protocol, e.g., payload of IP packet can be a TCP packet.
- **Micro Session** is a set of very small sessions. A session is considered as a micro one if its number of packets and data are less than some thresholds. MMT allows user to change easily these thresholds via a configuration file. Micro session will not be reported separately, rather, aggregated statistics from micro sessions will be reported together. Using micro sessions statistics reduces the report size. However, one will loose microscopic information about these micro sessions.
- Network traffic are represented through 4 metrics:
    - **Data Volume** is size of data, in Bytes or Bits, of packets.
    - **Payload Volume** is size of payload part, in Bytes or Bits, of packets.
    - **Packet Count** is number of packets.
    - **Session Count** is number of TCP/IP sessions. Each session is differed by a 4-tuple (IP source, IP destination, Port source and Port destination).

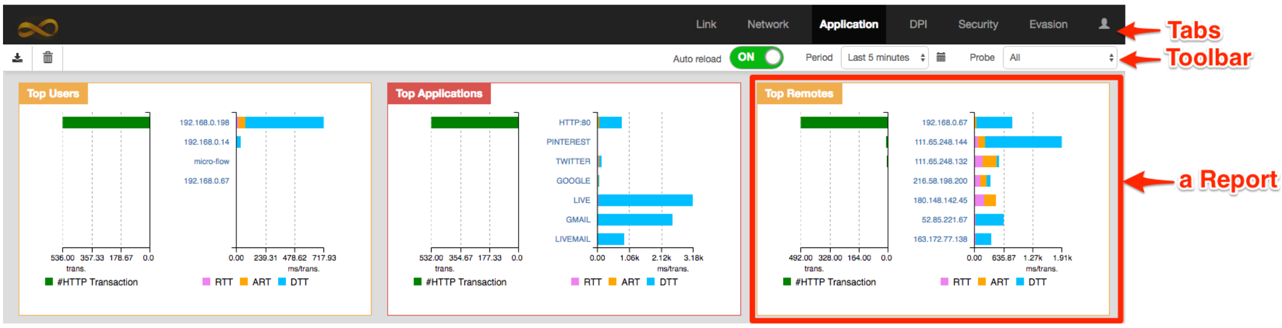
The following things are applied on GUI:

- When a button is available, the cursor will be change to a pointer when moving over the button.
- The changing of display, such as, delete/resize a Report, reorder Report, etc., is only locally. It only effects the current Web browser.

Tab

Statistics will be grouped into tabs, e.g., Link, Network, Application, DPI, Security, Evasion and Setting.

Each tab has a Toolbar and a set of Reports. The Figure below represents the Application tab having 3 reports: Top Users, Top Applications and Top Remotes.



Toolbar

The toolbar often shows the following buttons, from left to right:

1. **Export Charts to Images** : When click on this button, all displayed Reports will be exported to .png files. You might allow Google Chrome to download multiple files to download several report pictures.

2. **Delete a Report** : Drag and drop a Report over this button to delete that Report.

3. **Reset View** : Click on this button to reset the view of reports to the initial state.

4. **Auto Reload** : When it is enabling, the current Tab is automatically reloaded periodically.

5. **Period** decides a period of statistic to shown, such as, the statistic of the last 5 minutes. The available periods are: Last 5 minutes, Last hour, Last 6 hours, Last 12 hours, Last 24 hours, Last 7 days, and, Last 30 days.

One might also select a period between two dates by clicking on a small calendar button at the right of combobox.

6. **Probe** lists all running MMT-Probe in the current Period. If there is only one MMT-Probe, this combobox has only one value "All". When more than one MMT-Probe is running, one might select the combobox to see the statistics of one or all MMT-Probes.

Please note that, one of the buttons above can be hidden on some specific Tabs.

Report

A Report graphically represents a statistic of MMT. A Report consist of :

1. **A title** located on the top-left corner

2. **One or many Filters** to filter out unnecessary data. When user changes value of a Filter, the other Filters and Charts will be reloaded.

3. **One or many Charts** is the main part of a Report. A Chart might depend on another, e.g., when an element in a Chart is selected another Chart will be reloaded to show the statistic concerning to the selected element.

One can do the following actions on Report:

1. **Delete a Report**: This action is available when there are more than one Report on a Tab. In such a case, there exists a RecycleBin icon on the left of Toolbar.

To delete a Report, click and hold on the title of the report, then drag and drop it on the RecycleBin icon.

2. **Resize a Report**: To resize a Report, move cursor to an edge of Report, then drag cursor to resize it. Some Reports cannot be resized.

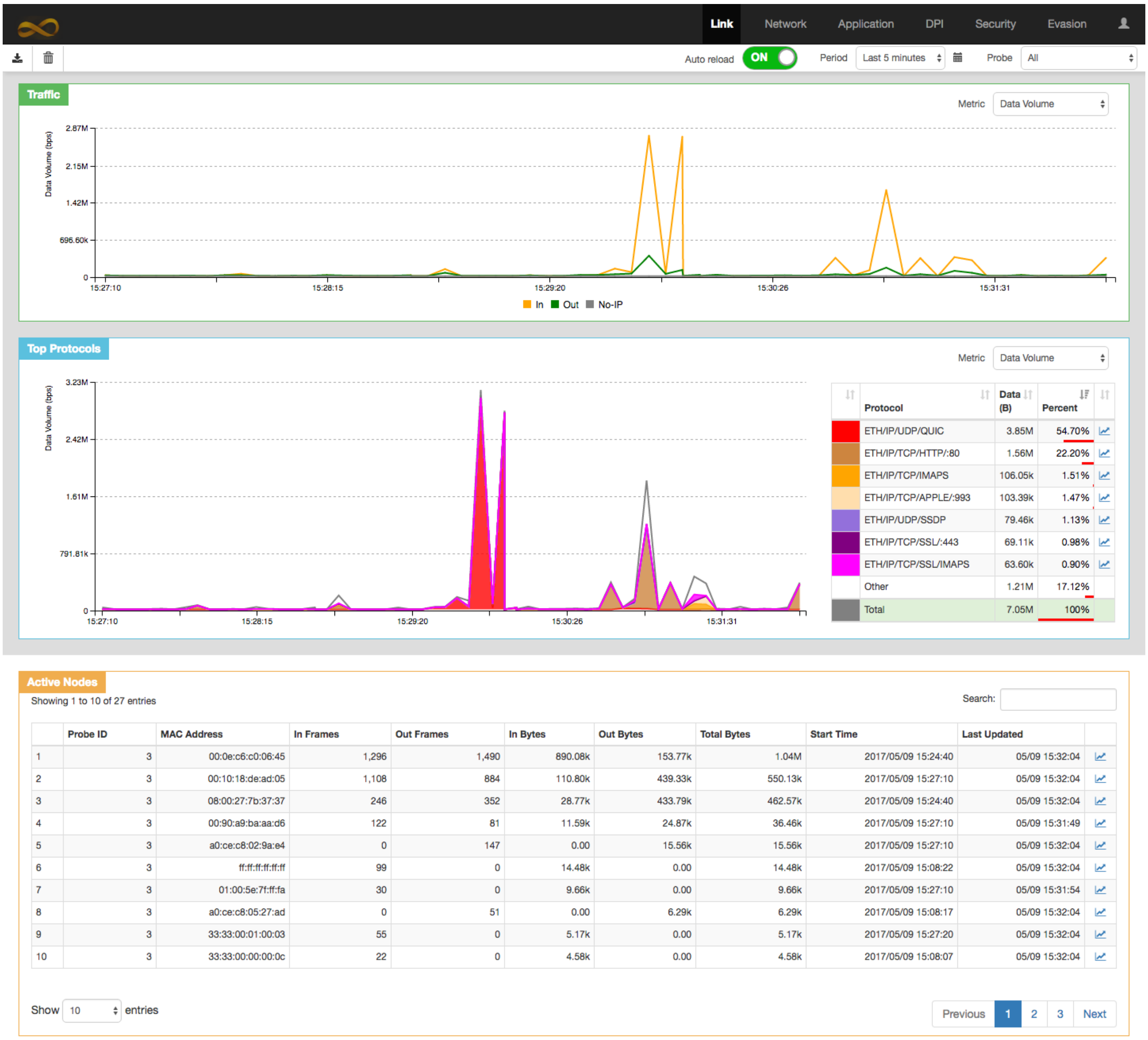
3. **Reorder Reports in a Tab**: To reorder Reports, drag and drop a Report to a position by click and hold on its title.

4. **Save a Report as a Picture**: Click on the left button on the Toolbar.

Chart

Tab Link

This tab gives an overview of the network being monitored by MMT-Probes, such as, Input/output traffic, the top 7 protocols having highest traffic, list of active nodes since the last 5 minutes. On each report, one can click on detail button 📈 to view bandwidth of an individual such as a protocol or a node.



Auto reload ON Period Last 5 minutes Probe All

Metric Data Volume

Metric Data Volume

	Protocol	Data (B)	Percent	
🟥	ETH/IP/UDP/QUIC	3.85M	54.70%	📈
🟫	ETH/IP/TCP/HTTP/:80	1.56M	22.20%	📈
🟧	ETH/IP/TCP/IMAPS	106.05k	1.51%	📈
🟨	ETH/IP/TCP/APPLE/:993	103.39k	1.47%	📈
🟪	ETH/IP/UDP/SSDP	79.46k	1.13%	📈
🟪	ETH/IP/TCP/SSL/:443	69.11k	0.98%	📈
🟪	ETH/IP/TCP/SSL/IMAPS	63.60k	0.90%	📈
	Other	1.21M	17.12%	
⬛	Total	7.05M	100%	

Showing 1 to 10 of 27 entries

Search:

	Probe ID	MAC Address	In Frames	Out Frames	In Bytes	Out Bytes	Total Bytes	Start Time	Last Updated	
1	3	00:0e:c6:c0:06:45	1,296	1,490	890.08k	153.77k	1.04M	2017/05/09 15:24:40	05/09 15:32:04	📈
2	3	00:10:18:de:ad:05	1,108	884	110.80k	439.33k	550.13k	2017/05/09 15:27:10	05/09 15:32:04	📈
3	3	08:00:27:7b:37:37	246	352	28.77k	433.79k	462.57k	2017/05/09 15:24:40	05/09 15:32:04	📈
4	3	00:90:a9:ba:aa:d6	122	81	11.59k	24.87k	36.46k	2017/05/09 15:27:10	05/09 15:31:49	📈
5	3	a0:ce:c8:02:9a:e4	0	147	0.00	15.56k	15.56k	2017/05/09 15:27:10	05/09 15:32:04	📈
6	3	ff:ff:ff:ff:ff:ff	99	0	14.48k	0.00	14.48k	2017/05/09 15:08:22	05/09 15:32:04	📈
7	3	01:00:5e:7f:ff:fa	30	0	9.66k	0.00	9.66k	2017/05/09 15:27:10	05/09 15:31:54	📈
8	3	a0:ce:c8:05:27:ad	0	51	0.00	6.29k	6.29k	2017/05/09 15:08:17	05/09 15:32:04	📈
9	3	33:33:00:01:00:03	55	0	5.17k	0.00	5.17k	2017/05/09 15:27:20	05/09 15:32:04	📈
10	3	33:33:00:00:00:0c	22	0	4.58k	0.00	4.58k	2017/05/09 15:08:07	05/09 15:32:04	📈

Show 10 entries

Tab link consists of 3 reports:

1. **Traffic** represents the total bandwidth of the network representing via 3 lines: in-bound and out-bound of IP traffic, along with the total bandwidth of other traffic that are non-IP based protocols such as ARP.

One can click on a legend item to hide/unhide the line corresponding.

2. **Top Protocols** contains the top 7 protocols. This report consists of 2 charts: the left one represents historical bandwidth, in bit per second, of the top protocols; the right one is the list of these protocols along with their total data and percentage.

One can click on one item of the list to hide/unhide the line corresponding on the left side.

3. **Active Nodes** contains the information about the nodes in the network that are being active since the last 5 minutes. A node in a network is identified by its unique media access control address (MAC address).

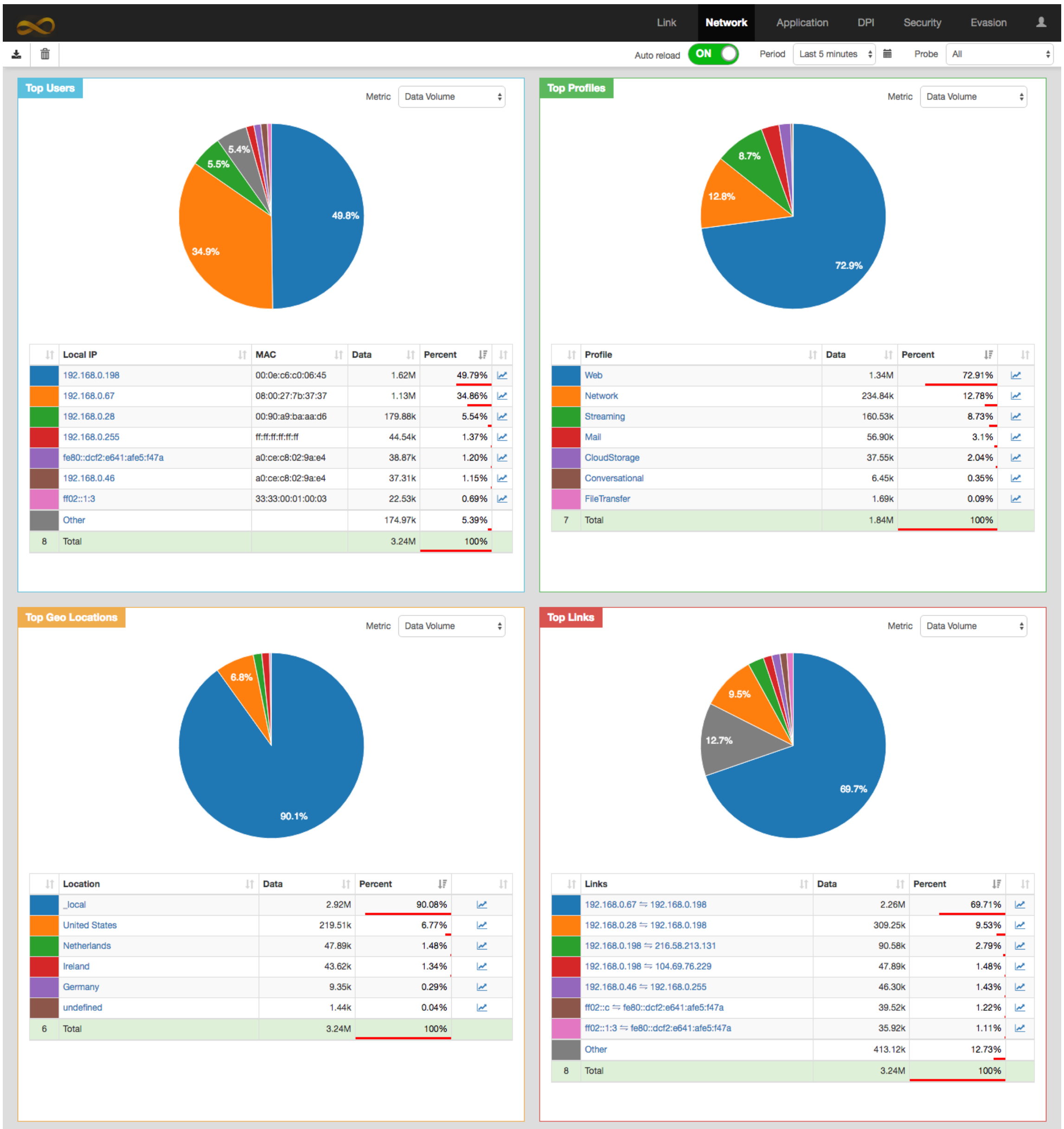
This report is not influenced by the Period filter on the toolbar. It always shows the active nodes since the last 5 minutes or the moment started MMT if MMT has been started less than 5 minutes.

Each row in the table represents a unique. Only the active nodes since the last minutes have statistical data. The statistic of the nodes, that were active since the last 5 minutes and inactive since the last minutes, are set to zero.

The start time and the last updated time are respectively the first and latest moment MMT saw a packet coming/outgoing to this node

Tab Network

This tab gives at the glance the top factors in the networks, such as, top users, top profiles, top locations, top links. These factors consume the most traffic. One can also inspect deeply one session.



Auto reload ON Period Last 5 minutes Probe All

Top Users

Metric Data Volume

	Local IP	MAC	Data	Percent	
■	192.168.0.198	00:0e:c6:c0:06:45	1.62M	49.79%	📈
■	192.168.0.67	08:00:27:7b:37:37	1.13M	34.86%	📈
■	192.168.0.28	00:90:a9:ba:aa:d6	179.88k	5.54%	📈
■	192.168.0.255	ff:ff:ff:ff:ff:ff	44.54k	1.37%	📈
■	fe80::dcf2:e641:afe5:f47a	a0:ce:c8:02:9a:e4	38.87k	1.20%	📈
■	192.168.0.46	a0:ce:c8:02:9a:e4	37.31k	1.15%	📈
■	ff02::1:3	33:33:00:01:00:03	22.53k	0.69%	📈
■	Other		174.97k	5.39%	
8	Total		3.24M	100%	

Top Profiles

Metric Data Volume

	Profile	Data	Percent	
■	Web	1.34M	72.91%	📈
■	Network	234.84k	12.78%	📈
■	Streaming	160.53k	8.73%	📈
■	Mail	56.90k	3.1%	📈
■	CloudStorage	37.55k	2.04%	📈
■	Conversational	6.45k	0.35%	📈
■	FileTransfer	1.69k	0.09%	📈
7	Total	1.84M	100%	

Top Geo Locations

Metric Data Volume

	Location	Data	Percent	
■	_local	2.92M	90.08%	📈
■	United States	219.51k	6.77%	📈
■	Netherlands	47.89k	1.48%	📈
■	Ireland	43.62k	1.34%	📈
■	Germany	9.35k	0.29%	📈
■	undefined	1.44k	0.04%	📈
6	Total	3.24M	100%	

Top Links

Metric Data Volume

	Links	Data	Percent	
■	192.168.0.67 ⇋ 192.168.0.198	2.26M	69.71%	📈
■	192.168.0.28 ⇋ 192.168.0.198	309.25k	9.53%	📈
■	192.168.0.198 ⇋ 216.58.213.131	90.58k	2.79%	📈
■	192.168.0.198 ⇋ 104.69.76.229	47.89k	1.48%	📈
■	192.168.0.46 ⇋ 192.168.0.255	46.30k	1.43%	📈
■	ff02::c ⇋ fe80::dcf2:e641:afe5:f47a	39.52k	1.22%	📈
■	ff02::1:3 ⇋ fe80::dcf2:e641:afe5:f47a	35.92k	1.11%	📈
■	Other	413.12k	12.73%	
8	Total	3.24M	100%	

Tab Network consists of first 4 reports. Each report contains the top 7 factors being represented in 2 charts:

- The pie chart represents the percentages of each factor.

- The table gives the detailed list of factors.

For each row of the table,

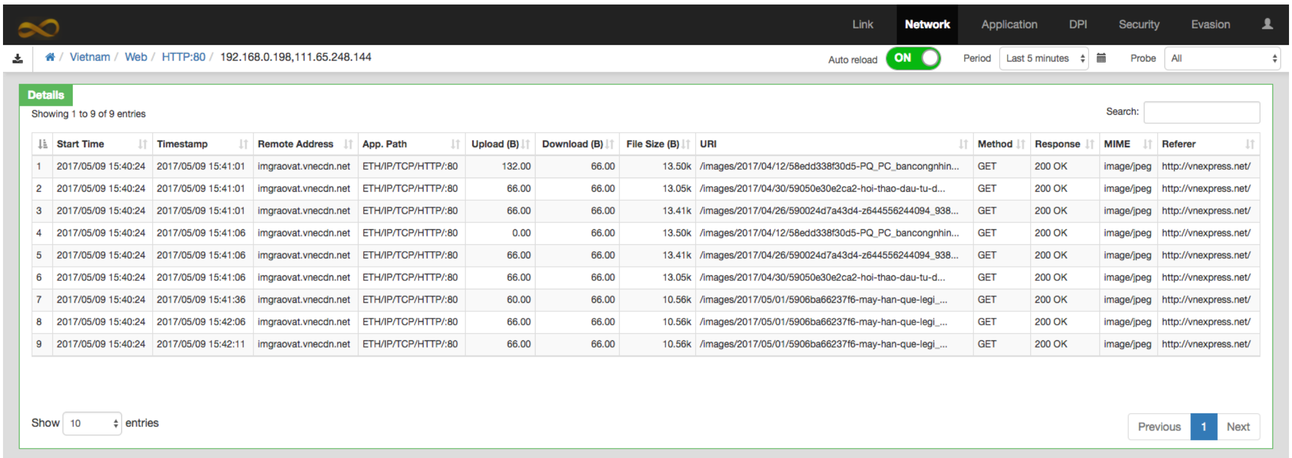
  - Click on one color item, on the left, to hide/unhide the pie corresponding
  - Click on link name to inspect the detail of its factor
  - Click on 📈 to show bandwidth used by its factor

1. **Top Users** is the top 7 users in the network. Each user is identified by a unique IP address.
2. **Top Profiles** is the top 7 Profiles in the network. When click on one profile name, one will get the top 7 applications or protocols of the profile.
3. **Top Geo Locations** is the top 7 destination countries. _local represents the traffic of 2 users in the network.
4. **Top Links** is the top 7 links. One link represents the traffic between 2 users in the network or one user with another from outside the network.

To inspect in detail of one session, one can click on name of each factor. For example, on can:

1. click on Vietnam in the Top Geo Location,
2. then Web on the Profiles,
3. then HTTP:80
4. then 192.168.0.198 <-> 111.65.248.144,

then one obtains the following list:



Vietnam / Web / HTTP:80 / 192.168.0.198,111.65.248.144

Auto reload ON   Period Last 5 minutes   Probe All

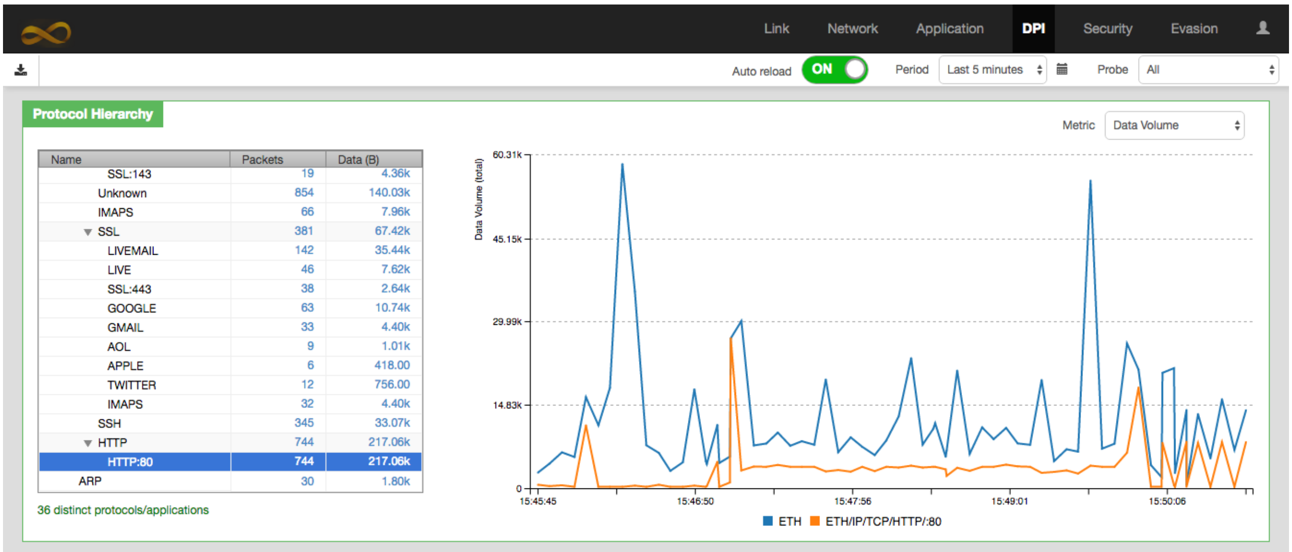
Showing 1 to 9 of 9 entries

	Start Time	Timestamp	Remote Address	App. Path	Upload (B)	Download (B)	File Size (B)	URI	Method	Response	MIME	Referer
1	2017/05/09 15:40:24	2017/05/09 15:41:01	imgraovat.vnecdn.net	ETH/IP/TCP/HTTP/:80	132.00	66.00	13.50k	/images/2017/04/12/58edd338f30d5-PQ_PC_bancongnhin...	GET	200 OK	image/jpeg	http://vnexpress.net/
2	2017/05/09 15:40:24	2017/05/09 15:41:01	imgraovat.vnecdn.net	ETH/IP/TCP/HTTP/:80	66.00	66.00	13.05k	/images/2017/04/30/59050e30e2ca2-hoi-thao-dau-tu-d...	GET	200 OK	image/jpeg	http://vnexpress.net/
3	2017/05/09 15:40:24	2017/05/09 15:41:01	imgraovat.vnecdn.net	ETH/IP/TCP/HTTP/:80	66.00	66.00	13.41k	/images/2017/04/26/590024d7a43d4-z644556244094_938...	GET	200 OK	image/jpeg	http://vnexpress.net/
4	2017/05/09 15:40:24	2017/05/09 15:41:06	imgraovat.vnecdn.net	ETH/IP/TCP/HTTP/:80	0.00	66.00	13.50k	/images/2017/04/12/58edd338f30d5-PQ_PC_bancongnhin...	GET	200 OK	image/jpeg	http://vnexpress.net/
5	2017/05/09 15:40:24	2017/05/09 15:41:06	imgraovat.vnecdn.net	ETH/IP/TCP/HTTP/:80	66.00	66.00	13.41k	/images/2017/04/26/590024d7a43d4-z644556244094_938...	GET	200 OK	image/jpeg	http://vnexpress.net/
6	2017/05/09 15:40:24	2017/05/09 15:41:06	imgraovat.vnecdn.net	ETH/IP/TCP/HTTP/:80	66.00	66.00	13.05k	/images/2017/04/30/59050e30e2ca2-hoi-thao-dau-tu-d...	GET	200 OK	image/jpeg	http://vnexpress.net/
7	2017/05/09 15:40:24	2017/05/09 15:41:36	imgraovat.vnecdn.net	ETH/IP/TCP/HTTP/:80	60.00	66.00	10.56k	/images/2017/05/01/5906ba66237f6-may-han-que-legi_...	GET	200 OK	image/jpeg	http://vnexpress.net/
8	2017/05/09 15:40:24	2017/05/09 15:42:06	imgraovat.vnecdn.net	ETH/IP/TCP/HTTP/:80	66.00	66.00	10.56k	/images/2017/05/01/5906ba66237f6-may-han-que-legi_...	GET	200 OK	image/jpeg	http://vnexpress.net/
9	2017/05/09 15:40:24	2017/05/09 15:42:11	imgraovat.vnecdn.net	ETH/IP/TCP/HTTP/:80	66.00	66.00	10.56k	/images/2017/05/01/5906ba66237f6-may-han-que-legi_...	GET	200 OK	image/jpeg	http://vnexpress.net/

Show 10 entries

Tab DPI

Tab DPI gives information about hierarchy of protocols/applications. It consists of 1 Report: Protocol Hierarchy.



Auto reload ON

Period Last 5 minutes

Probe All

Protocol Hierarchy

Metric Data Volume

Name	Packets	Data (B)
SSL:143	19	4.36k
Unknown	854	140.03k
IMAPS	66	7.96k
▼ SSL	381	67.42k
LIVEMAIL	142	35.44k
LIVE	46	7.62k
SSL:443	38	2.64k
GOOGLE	63	10.74k
GMAIL	33	4.40k
AOL	9	1.01k
APPLE	6	418.00
TWITTER	12	756.00
IMAPS	32	4.40k
SSH	345	33.07k
▼ HTTP	744	217.06k
HTTP:80	744	217.06k
ARP	30	1.80k

36 distinct protocols/applications

The Protocol Hierarchy report has 2 charts: a tree chart on the left and a line chart on the right.

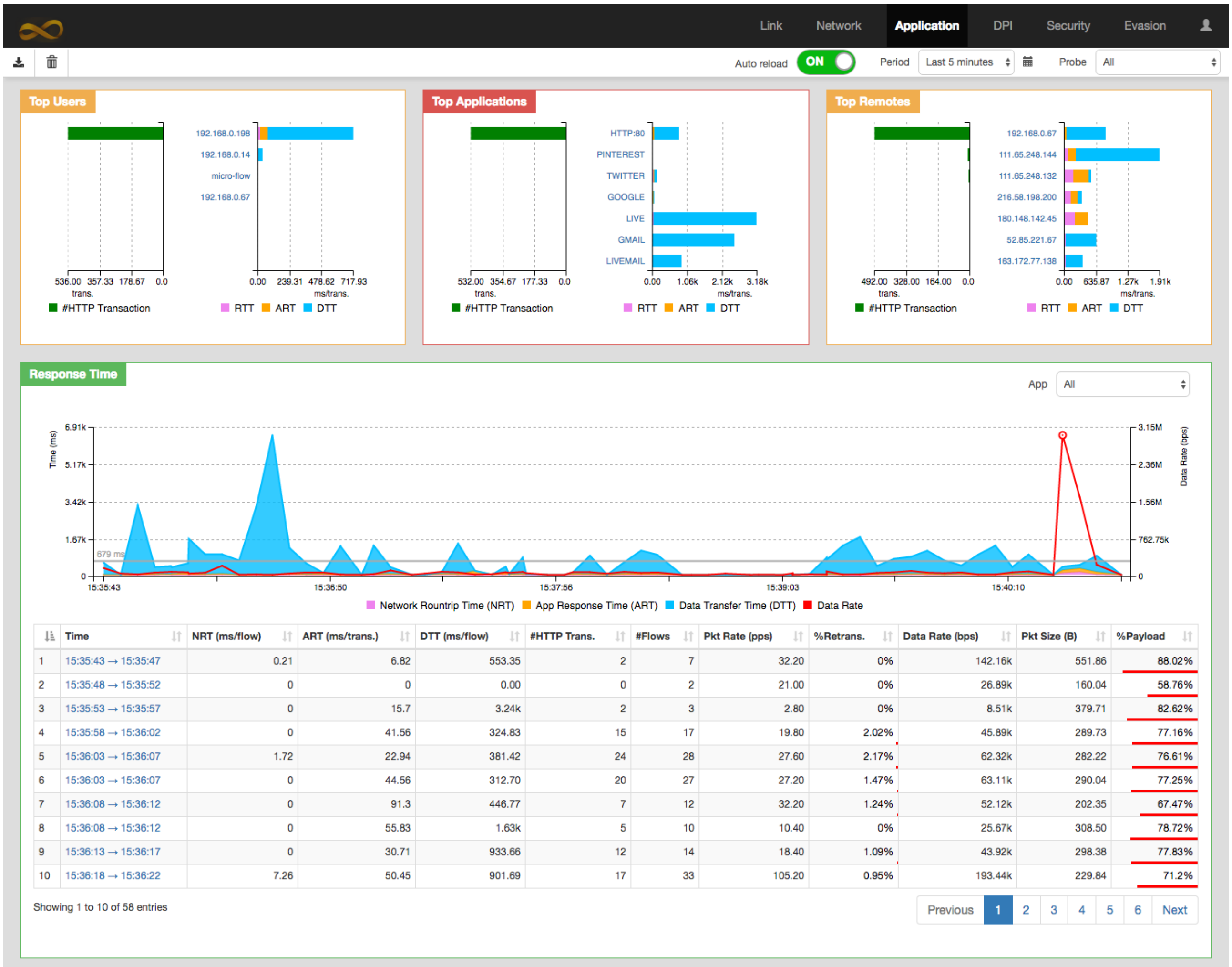
- The tree chart represents the hierarchy of protocols, e.g., there are 36 distinct protocols/application in the figure above.
  - Click on ▼ to collapse/expand the tree.
  - Click on a hyper-link to select/deselect its protocol. When a protocol is selected, its traffic will be shown on the right chart
- The line chart represents the traffic of the selected protocols of the tree chart. These lines do not represent the bandwidth of the protocols but their total traffic during a sample period that is 5 seconds by default.

Through this chart, one can easily see a consistency between protocols. For example, in the figure above, we found that the HTTP traffic vs the total traffic that is represented by ethernet.

Tab Application

Tab Application shows the information about the network's round-trip time, data transfer time, application response time and data rate for the selected application type from the App tab. Moreover, the detailed information is provided in the tables for each application every 5 seconds, that are application response time, data transfer time, server data transfer time, client transfer time, network round-trip time, Number of HTTP transaction, number of active flows, packet rate, data rate, packet size and percentage of payload.

This Tab currently supports only protocols/applications on the top of HTTP and FTP.



	Time	NRT (ms/flow)	ART (ms/trans.)	DTT (ms/flow)	#HTTP Trans.	#Flows	Pkt Rate (pps)	%Retrans.	Data Rate (bps)	Pkt Size (B)	%Payload
1	15:35:43 → 15:35:47	0.21	6.82	553.35	2	7	32.20	0%	142.16k	551.86	88.02%
2	15:35:48 → 15:35:52	0	0	0.00	0	2	21.00	0%	26.89k	160.04	58.76%
3	15:35:53 → 15:35:57	0	15.7	3.24k	2	3	2.80	0%	8.51k	379.71	82.62%
4	15:35:58 → 15:36:02	0	41.56	324.83	15	17	19.80	2.02%	45.89k	289.73	77.16%
5	15:36:03 → 15:36:07	1.72	22.94	381.42	24	28	27.60	2.17%	62.32k	282.22	76.61%
6	15:36:03 → 15:36:07	0	44.56	312.70	20	27	27.20	1.47%	63.11k	290.04	77.25%
7	15:36:08 → 15:36:12	0	91.3	446.77	7	12	32.20	1.24%	52.12k	202.35	67.47%
8	15:36:08 → 15:36:12	0	55.83	1.63k	5	10	10.40	0%	25.67k	308.50	78.72%
9	15:36:13 → 15:36:17	0	30.71	933.66	12	14	18.40	1.09%	43.92k	298.38	77.83%
10	15:36:18 → 15:36:22	7.26	50.45	901.69	17	33	105.20	0.95%	193.44k	229.84	71.2%

Showing 1 to 10 of 58 entries

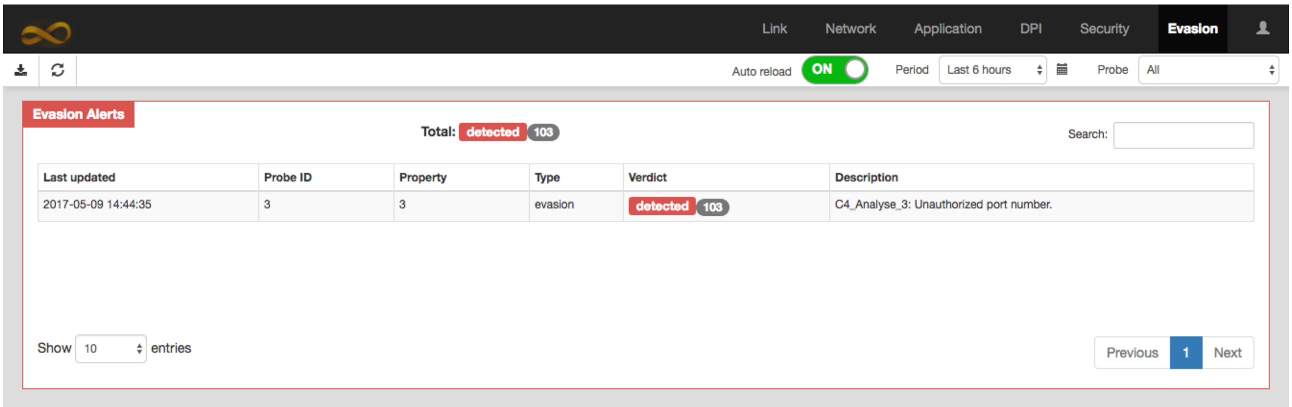
- **FTP Response Time** is the time elapsed between a client sending a request to a FTP server and receiving the response packet. The response time includes the 3 ways TCP handshake.
- **HTTP response Time** is the time elapsed between a client application sending a request (GET) to a HTTP server and receiving the response packet.

Initial TCP RTT (Handshake): Initial RTT of an application is determined by looking at the TCP Three Way Handshake. It is the time elapsed between TCP-SYN and TCP-ACK in the TCP Three Way Handshake.

- **NRT**, Network Response Time, is measured by a TCP handshake.
- **ART**, Application Response Time,
- **DTT**, Data Transfer Time,
- **#HTTP Trans** is the number of HTTP transitions. An HTTP transition is counted from starting a request to receiving completely its response. Different HTTP transitions can perform through only one TCP/IP session.
- **#Flows** indicates the number of TCP/IP sessions.
- **Pkt rate (pps)** indicates the average number of packets received per second
- **%Retrans.** is the percentage of number of packets being retransmitted
- **Data rate (bps)** indicates the average number of bits received per second
- **Packet size (B)** indicates an average packet size, in Bytes
- **%Payload** indicates the percentage of payload on the total data. When this percentage closes to 100%,

Tab Security and Evasion

Tab Security and Tab Evasion list all security alerts. The alerts are grouped by property and probe ID. These tabs list only the latest 5000 alerts.

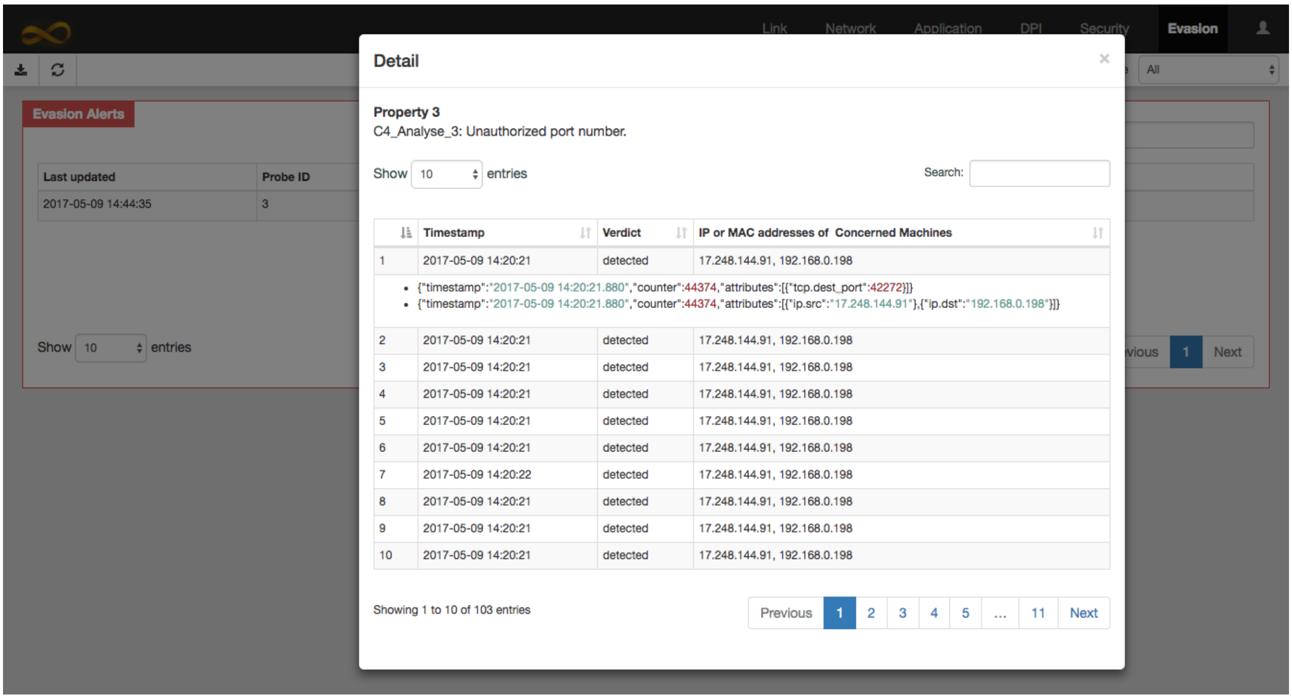


Total: detected 103

Last updated	Probe ID	Property	Type	Verdict	Description
2017-05-09 14:44:35	3	3	evasion	detected 103	C4_Analyse_3: Unauthorized port number.

Show 10 entries

Each tab has only one report consisting of one table. Each row of the table represents the alerts of one property. One can click on one row to see the alerts as in the figure below.



Property 3
C4_Analyse_3: Unauthorized port number.

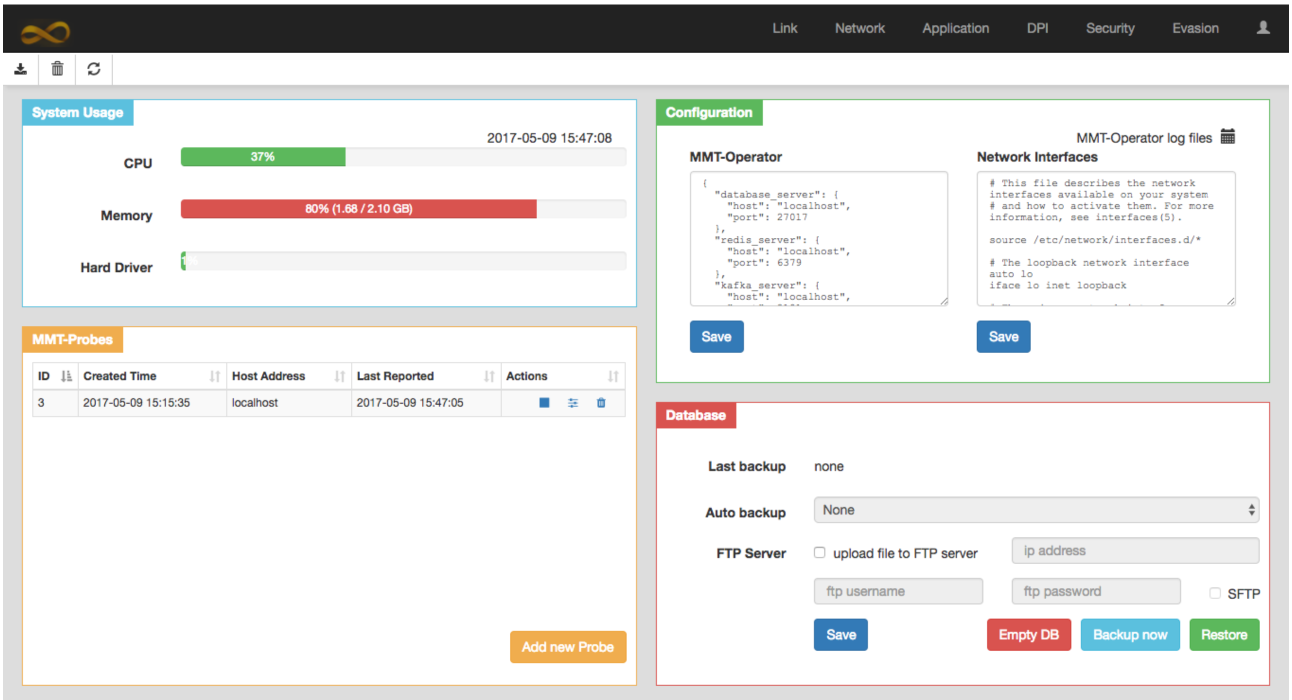
Show 10 entries

	Timestamp	Verdict	IP or MAC addresses of Concerned Machines
1	2017-05-09 14:20:21	detected	17.248.144.91, 192.168.0.198
	• {"timestamp":"2017-05-09 14:20:21.880","counter":44374,"attributes":[{"tcp.dest_port":42272}]} • {"timestamp":"2017-05-09 14:20:21.880","counter":44374,"attributes":[{"ip.src":"17.248.144.91"},{"ip.dst":"192.168.0.198"}]}		
2	2017-05-09 14:20:21	detected	17.248.144.91, 192.168.0.198
3	2017-05-09 14:20:21	detected	17.248.144.91, 192.168.0.198
4	2017-05-09 14:20:21	detected	17.248.144.91, 192.168.0.198
5	2017-05-09 14:20:21	detected	17.248.144.91, 192.168.0.198
6	2017-05-09 14:20:21	detected	17.248.144.91, 192.168.0.198
7	2017-05-09 14:20:22	detected	17.248.144.91, 192.168.0.198
8	2017-05-09 14:20:21	detected	17.248.144.91, 192.168.0.198
9	2017-05-09 14:20:21	detected	17.248.144.91, 192.168.0.198
10	2017-05-09 14:20:21	detected	17.248.144.91, 192.168.0.198

Showing 1 to 10 of 103 entries

Tab Setting

Tab setting gives some statistic of server hosting MMT-Operator such as CPU usage, memory and hard driver free space. It also allows user to update setting of MMT-Operator, backup database.



2017-05-09 15:47:08

CPU 37%

Memory 80% (1.68 / 2.10 GB)

Hard Driver

MMT-Operator log files

MMT-Operator

```
{
  "database_server": {
    "host": "localhost",
    "port": 27017
  },
  "redis_server": {
    "host": "localhost",
    "port": 6379
  },
  "kafka_server": {
    "host": "localhost",
```

Network Interfaces

```
# This file describes the network
interfaces available on your system
# and how to activate them. For more
information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback
```

ID	Created Time	Host Address	Last Reported	Actions
3	2017-05-09 15:15:35	localhost	2017-05-09 15:47:05	■ ☰ 🗑

Last backup none

Auto backup None

FTP Server □ upload file to FTP server ip address

ftp username ftp password □ SFTP

Tab Setting consists of 4 reports.

1. **System Usage** gives a statistic of usage of the server on that MMT-Operator is running.
2. **Configuration** allows to:
   - update file config.json of MMT-Operator
   - update file /etc/network/interfaces of the server
   - view execution logs of MMT-Operator
3. **MMT-Probes** allows to manager MMT-Probe. One can install MMT-Probe on a remote server by giving permission to MMT-Operator to log on that server via SSH.

When clicking on **Add new Probe** button, one is led to another window to enter SSH information of the remote server. After entering successfully, MMT-Operator will install a new MMT-Probe on the server and add it to the list of management.

For the existing MMT-Probe, one can:

- stop/start a probe
- update config file of a probe
- uninstall a probe

4. **DataBase**
   - **Save** button saves information in the form: Auto backup, FTP Server
   - **Empty DB** button empties database that contains MMT statistic. This does not change user information such as password, license, and information in this tab.

After clicking on the button, one need to confirm in another windows before MMT-Operator can empty its database.

- **Backup now** button backups immediately database using the current setting. After clicking on the button, one need to confirm the action.
- **Restore** button leads user to another window to select a backup image from a list of available ones to restore.

Others

1. **Login**: Default login information are admin/ mmt2nm for username/password respectively.

2. **Change Password**: One can change the current password by clicking on 👤 button, then "Change password".

Update Licence: One can update the licence by clicking on 👤 button, then "Profile".