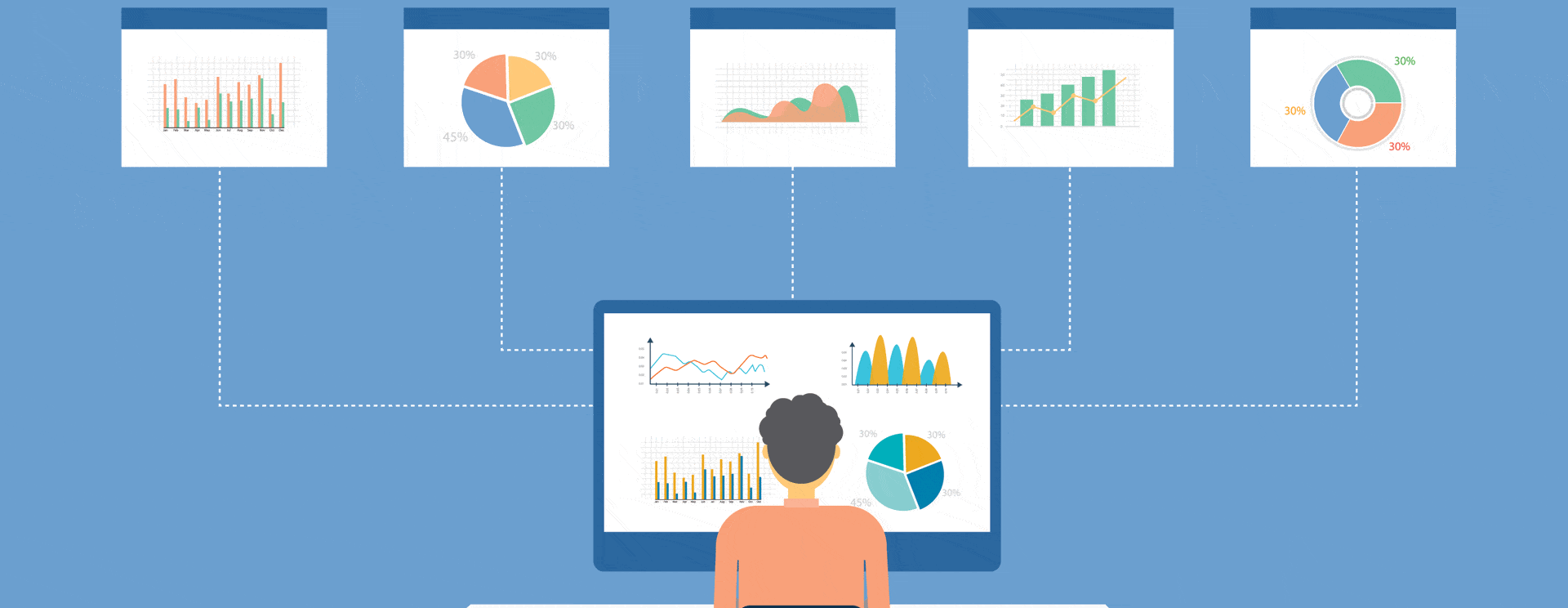
## 



Traffic Classification & Monitoring

Oct 2020

**─**

Gayathri Devi. A (17MCME19) Under:

Leela Srija. A (17MCME18) Dr. Saifullah

Vaishnavi. K (17MCME04) SCIS, UoH

# Contents

[**Introduction**](#_wpxshwnjj982) **3**

[**Tools**](#_3at9u9s4e0vp) **3**

[**ntopng**](#_kpoixu22s5hg) **4**

[Introduction](#_2r88r0oly3mi) 4

[Tech Specifications](#_2r88r0oly3mi) 4

[Main Features](#_qqmnqd5pitg6) 5

[Installation](#_viku726e6edv) 5

[Configuration](#_2r88r0oly3mi) 6

[Startup and Usage](#_2r88r0oly3mi) 6

[Description](#_v6uwjby08b4d) 7

[Traffic Dashboard](#_6rtlyjlrlxrw) 7

[Hosts](#_62bujco6xcbi) 7

[Individual host:](#_wj3eqxynwqng) 8

[Interface section:](#_2fkk6g3x93h1) 9

[Alerts:](#_funf8qxjka60) 10

[Other sections:](#_f56yacmeekdh) 11

[System statistics:](#_5xflb3ocpil) 12

[Snapshots from Professional Version](#_pnw9ybvrzyws) 13

[Conclusions](#_50sgu3g6yeyv)

15

[**Nagios XI**](#_z6aykpyk2gcz) **16**

[Introduction](#_d326s3q49oxq) 16

[Installation](#_rp4g6weul1xh) 17

[Configuration](#_x0ar9yau22da) 18

[Usage](#_629cshrki4ur) 19

[Host Status](#_vmppgjc1f54g) 20

[Service Status](#_ucfaeg6u8nto) 21

[Reports](#_p6sl6kw46hfn) 22

[Graphs](#_hrxqfmhsz09l) 22

[**Colasoft Capsa**](#_vagbks3oucjm) **24**

[Introduction](#_aoo6rj69vu0u) 24

[Tech Specifications](#_hdfu4pi1txga) 24

[Software requirements:](#_vlpdgl7yjlzn) 24

[Hardware Requirements:](#_k54j16en6yjs) 24

[Current System Used:](#_2ylmh0j8ook7) 24

[Installation](#_biosz51mxgdd) 25

[Configuration](#_7qav8sgvy5sr) 25

[Features and Demo](#_1locs0cmeh8j) 26

[Extended Network Analysis:](#_5weza6e7ltkc) 26

[Node Explorer:](#_m64ks9c3lnn) 26

[Capture Default:](#_o371j58oqno) 26

[Protocol Explorer:](#_ngvho1jfbvi3) 28

[TCP Flow Analysis:](#_6xkv474rdh9) 29

[HTTP Analysis:](#_tmetxvai2o36) 29

[MAC Explorer:](#_ruoeq74zcpc) 30

[IP Explorer:](#_2jx1uiqtelze) 30

[VoIP Explorer:](#_pjpfzlrwprmy) 30

[Process Explorer:](#_cqdbbucdi9ac) 31

[Application Explorer:](#_mb9nwr95x0y7) 31

[Notifying Alarms and Emails & Audio:](#_fkexk5tc6grj) 32

[Task Scheduler:](#_b6bfrlvxejti) 33

[Visualized Connections in Matrix:](#_1qhw97vplgq5) 33

[**Comparison**](#_k28iqzo9cewh) **34**

[**Learnings and Challenges**](#_qibtymlmmzum) **35**

[**Contributions**](#_yyrhu7ml5bea) **35**

# 

# Introduction

This project report presents the study and comparison of three Network Classification and Monitoring Tools. The main aim of these tools is to monitor live traffic and classify it based on various parameters. Each tool has its own technical specifications and unique features that stand out in the market.

The vendor, installation, configuration and usage of each tool are briefly stated and described below. And they are compared in terms of

* Cost of ownership
* Version
* Availability of web interface
* Supporting platforms
* Support for various features such as
  + Traffic Analysis
  + Bandwidth Monitoring
  + Application Monitoring
  + Protocol Support
  + Troubleshooting
  + VoIP Analysis
  + Data Storage Method
  + Possibility of Integration with other tools
  + Ease of use and many others

# Tools

Following are the tools we chose.

1. ntopng
2. Nagios XI
3. Colasoft Capsa

# 

# ntopng

## Introduction

ntopng is a high-speed web-based traffic analysis and flow collection tool. It is based on libcap, a portable C/C++ library for network traffic capture.

It comes in four versions: Community, Professional, Enterprise M, Enterprise L.

The community version is **open source** and free to use. We shall use the Community version for this study.

## Tech Specifications

* Platforms
  + Runs on Unix, Linux, MacOSX, Windows x64 and ARM platforms.
* Web UI
  + Its web UI is intuitive, encrypted and available through any HTML5-ready web browser.
* Protocols
  + Ethernet, IPv4/IPv6, TCP/UDP/ICMP, DHCP/DNS/BOOTP, 250+ Layer-7 application protocols supported by nDPI ( its own Deep Packet Inspection toolkit ) and many more protocols.
* Requirements
  + Memory Usage depends on the ntop configuration, number of hosts, and number of active TCP sessions. In general it ranges from a few MB (little LAN) to 100 MB for a WAN.
  + CPU Usage depends on the ntop configuration, and traffic conditions. On a modern PC and large LAN, it is less than 10% of overall CPU load.
* Extensibility
  + LUA scriptability
  + Web interface extensions without having to change the ntopng C++ engine.

## 

## Main Features

* Shows real time network traffic and active hosts.
* Sorts network traffic according to many criteria.
* Identifies Top talkers (senders/receivers).
* Monitors and reports live throughput, network and application latencies, Round Trip Time (RTT), TCP statistics (retransmissions, out of order packets, packets lost), and bytes and packets transmitted.
* Geolocate and overlay hosts in a geographical map.
* Alerts engine to capture anomalous and suspicious hosts.Discovers application protocols (Facebook, YouTube, BitTorrent, etc) by leveraging on nDPI ( its own GPL DPI toolkit ).
* Characterises HTTP traffic by leveraging on characterisation services provided by Google and HTTP Blacklist.
* Continuous monitoring of SNMP devices.
* Interactive historical exploration of monitored data exported to MySQL.
* Identity Management, including correlation of VPN users to traffic.
* Can be integrated with other softwares and tools.

## Installation

A complete detailed description is available at [ntopng Documentation](https://www.ntop.org/guides/ntopng/index.html)

As ntopng Community is an open source tool, code can be found on [Github](https://github.com/ntop/ntopng) and no license is required.

In addition, pre-compiled, binary ntopng packages are available both for Linux and Windows. Download the file or package repository from [Packages](http://packages.ntop.org/) (both development and stable builds are available). All installation instructions can be found after choosing the platform and build type.

For linux system with root privileges (Ubuntu 20.04), we are installing ntopng Community Edition v.4.0.201007

* Install wget (if not present) using

$ apt-get install software-properties-common wget

$ add-apt-repository universe

* Get the ntopng stable build for Ubuntu 20.04 LTS using

$ wget <https://packages.ntop.org/apt-stable/20.04/all/apt-ntop-stable.deb>

$ apt install ./apt-ntop-stable.deb

* Once the ntop repository has been added, run the following commands (as root)

$ apt-get clean all

$ apt-get update

$ apt-get install ntopng

## Configuration

In the Linux system with root privileges,

* Open the configuration file located at /etc/ntopng.conf or /etc/ntopng/ntopng.conf
* Go to the interface section and specify your network interface (This is optional. Ntopng will try to auto detect interfaces in most of the cases.)
* Uncomment and set the http port number. (Default is 3000)

-w=3000

* Save and close the file.

## Startup and Usage

* Run the following command in the terminal and allow it to complete its startup.

$ sudo ntopng

* After the startup, open the web browser (which supports html5) and type any of the following URLs

http://localhost:3000 or http://your-server-ip:3000

(port number given in the configuration file is 3000)

* A login page appears on successful installation and configuration.
* For the first time, login with default username and password ‘admin’ (change your password after first login).
* Every time you login, it provides access to the professional version for 10 minutes and thereafter it comes back to Community version. (Reload the page if needed)

## 

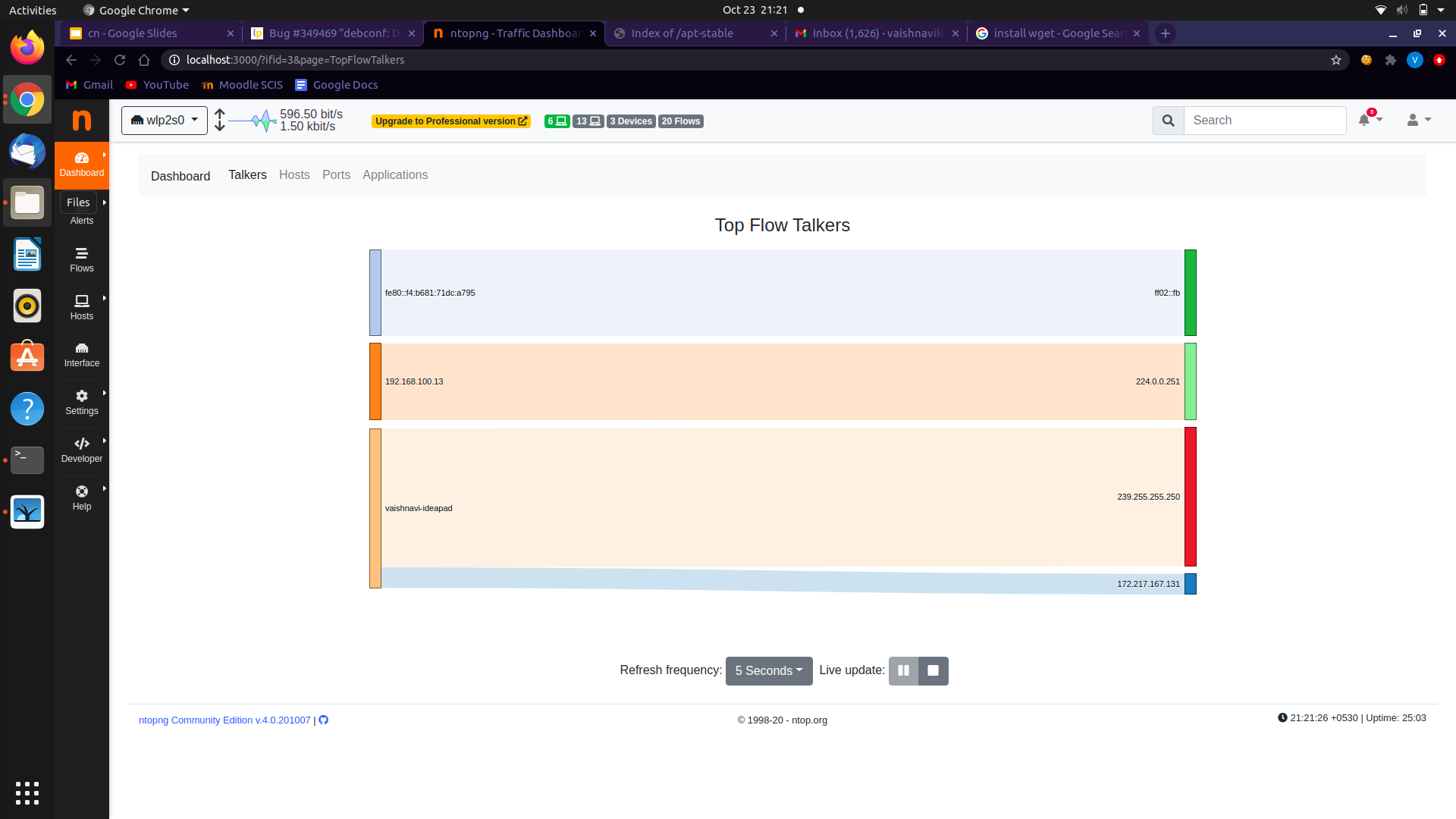
## Description

It consists of an interface drop down through which the interface can be selected. The average traffic/sec sent and received by that interface, number of local, remote and other hosts, number of devices and flows are shown at the top.

#### Traffic Dashboard

It consists of four sections: Talkers, Hosts, Ports, Applications.

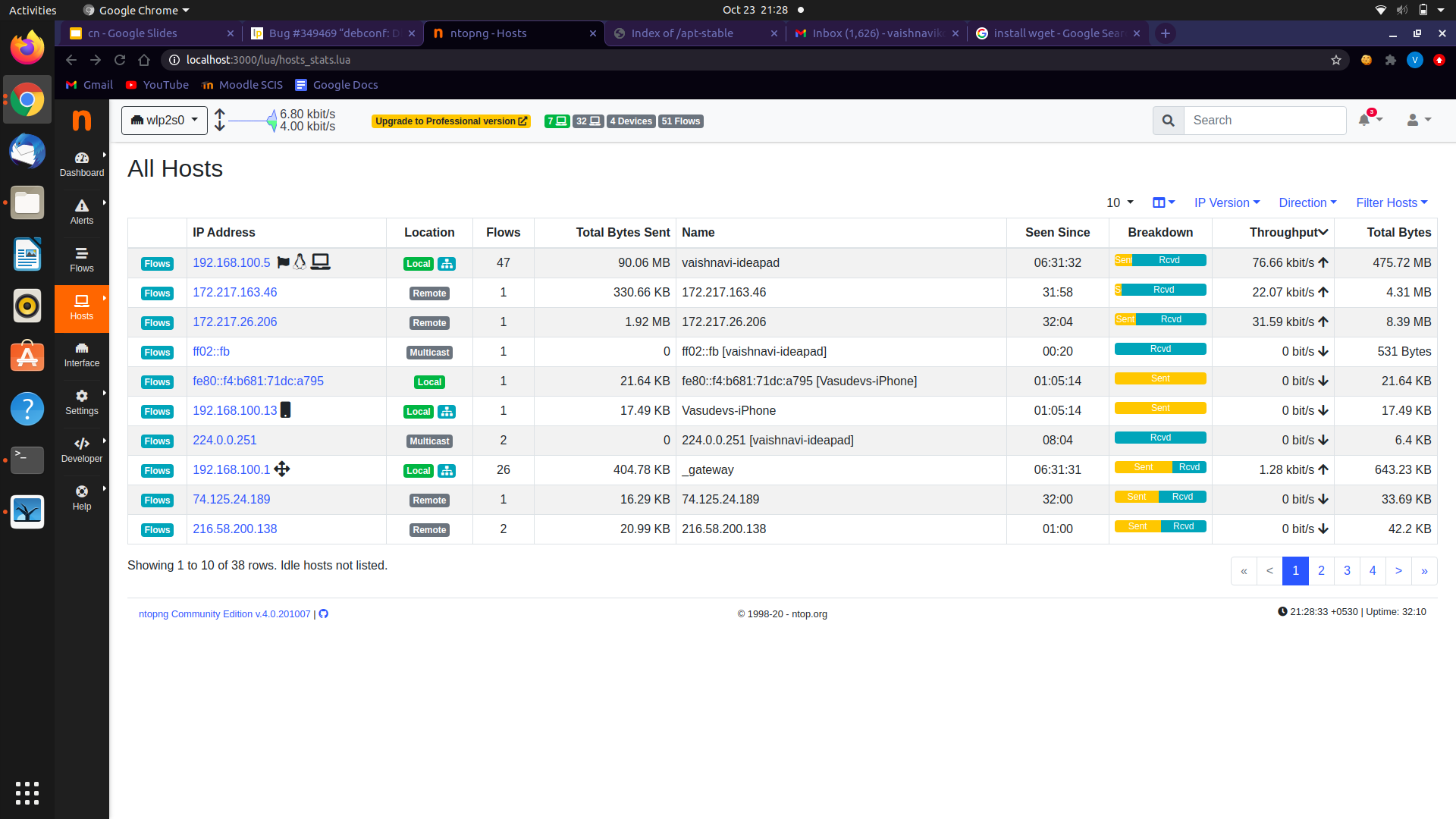
* Talkers sections shows live update of the Top Flow Talkers
* Hosts section shows the Top Hosts (Send + Receive)
* Ports section displays the Top Client Ports and Top Server Ports
* Application sections shows the Top Application Protocols in use

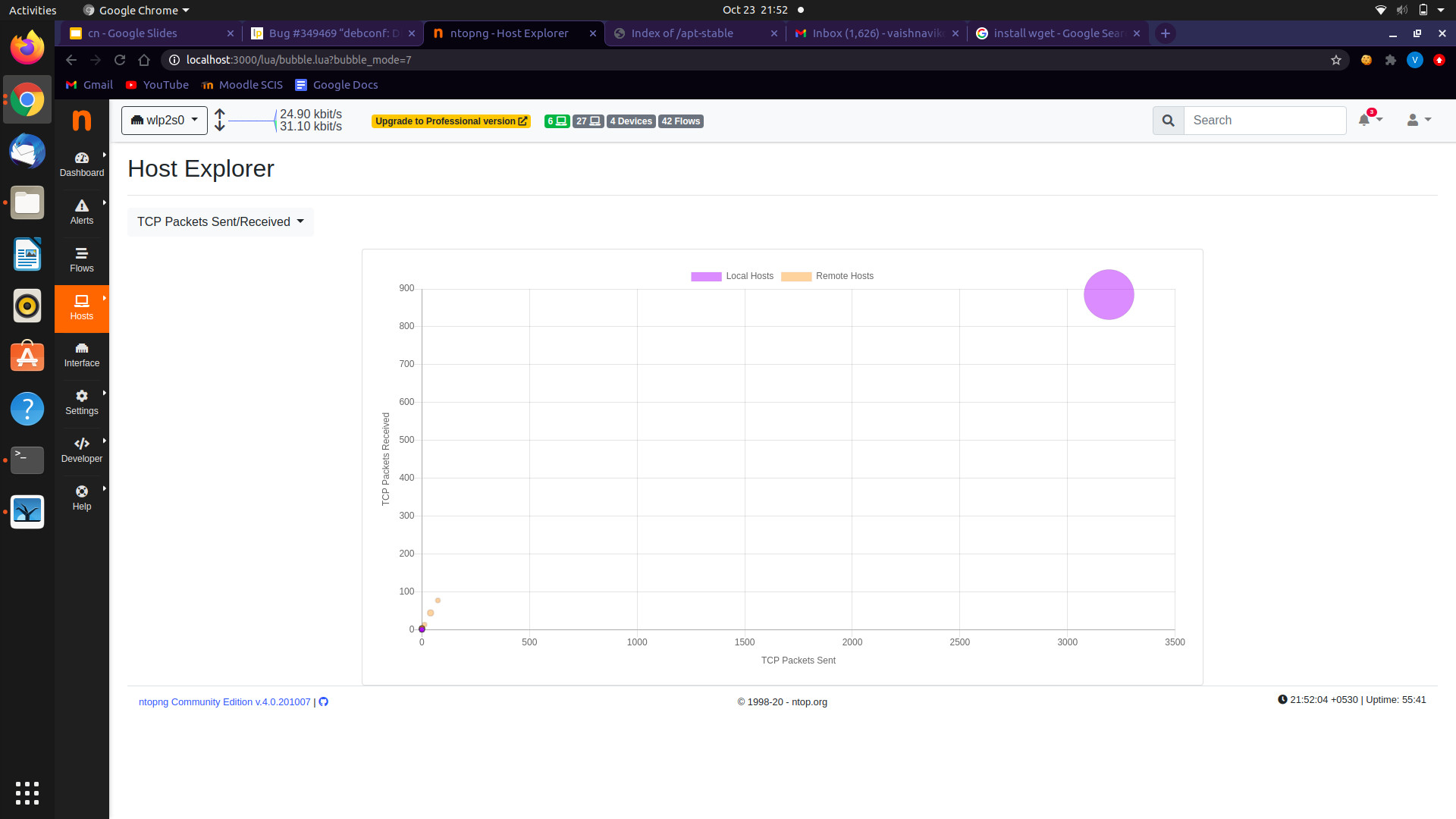


#### Hosts

This sections has the following sub pages

* Hosts - Shows all the hosts present (local hosts, remote hosts, broadcast domain hosts, blacklisted hosts and any other hosts)
* Mac addresses - Shows mac addresses of the recognised devices
* Networks - Shows the details of a particular network through different Time Series
* Host Pools - Lists host pools if any
* Operating systems - Classifies hosts by operating system
* Server HTTP - Local HTTP servers
* Top Hosts - Shows top local hosts
* Host explorer - Contains some graphs for visualisation of hosts according to different parameters

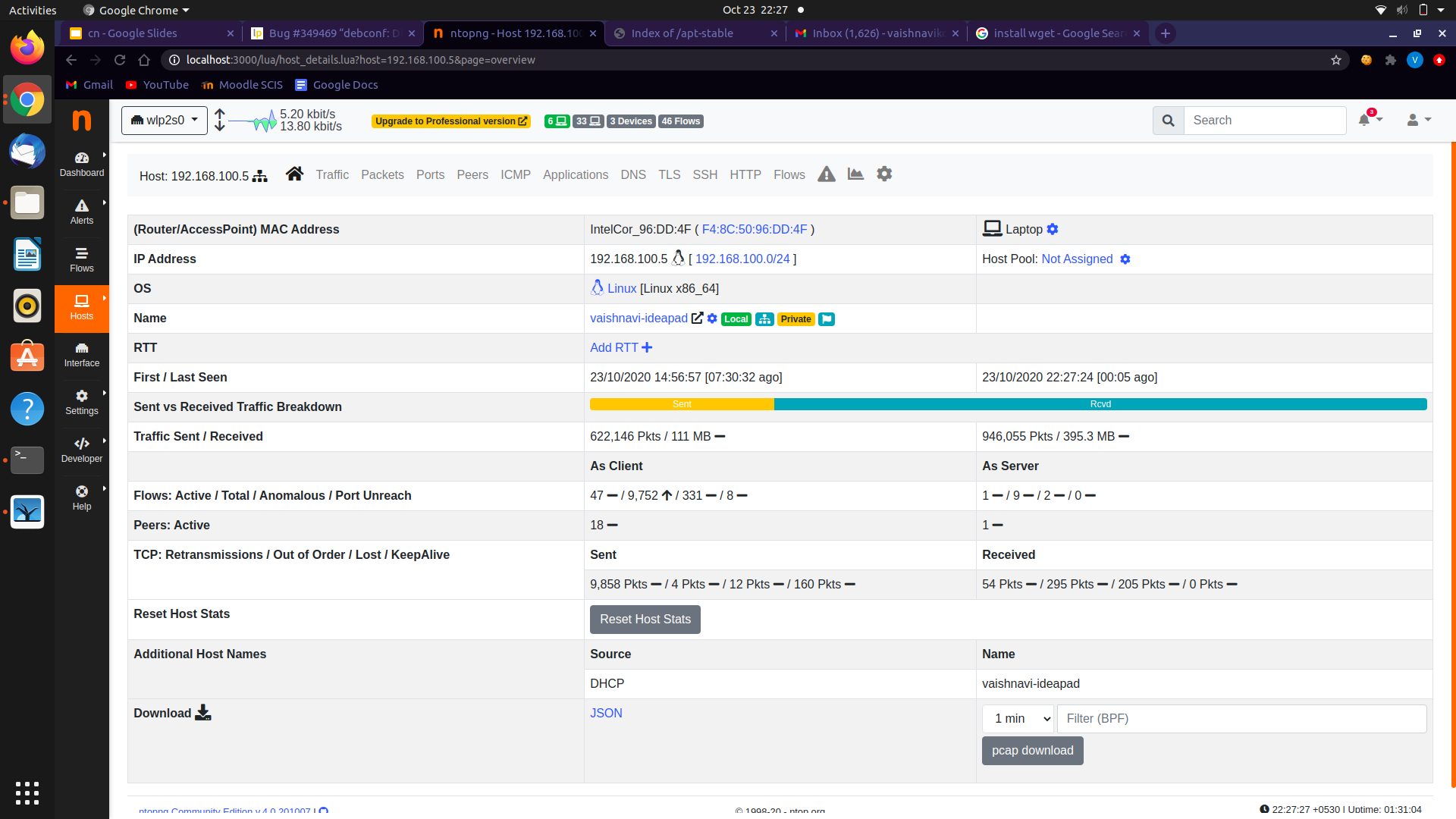


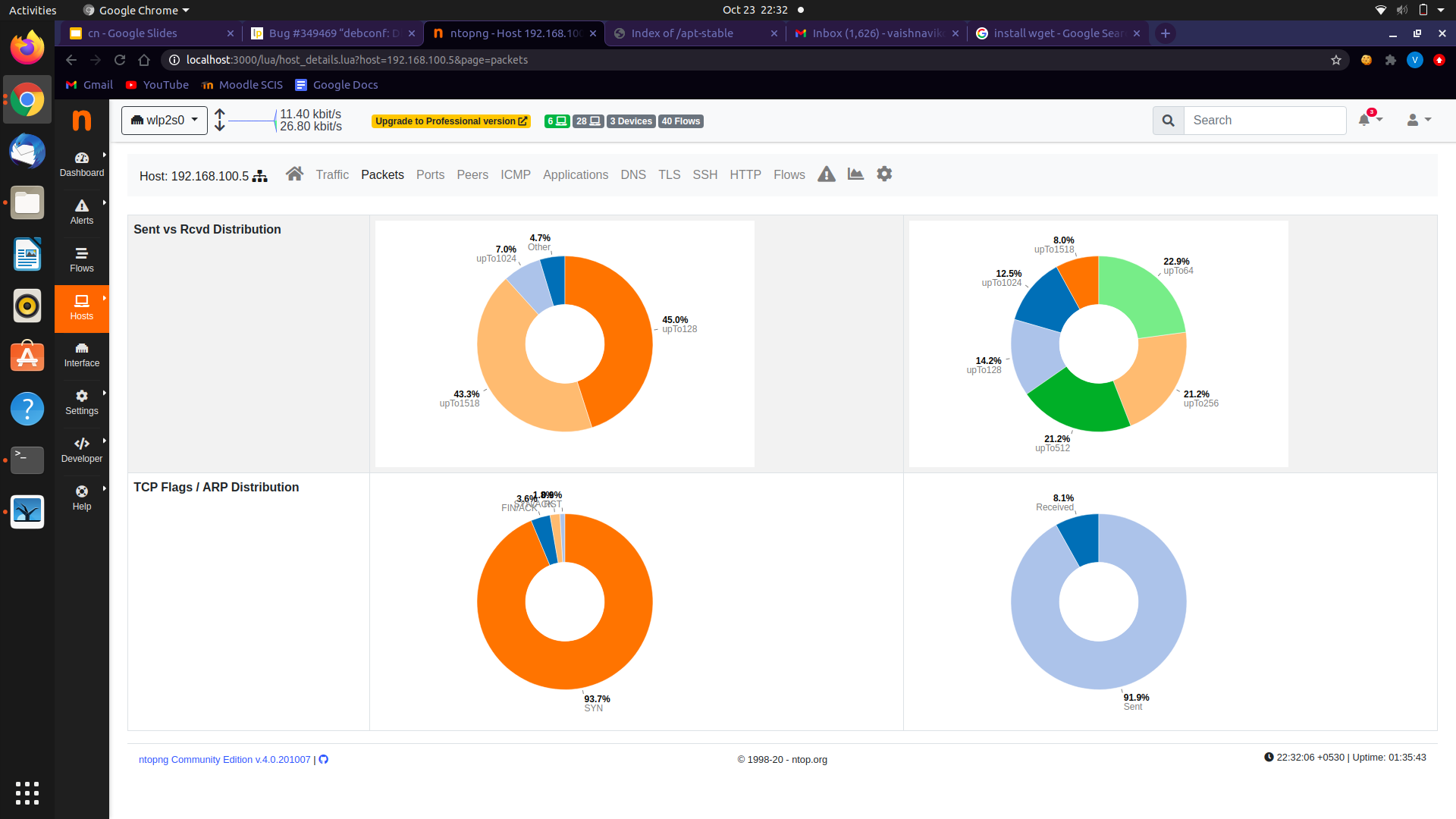


#### 

#### Individual host:

For a particular host, the classification and distribution of Traffic, TCP packets, Ports, Peers, ICMP, Applications, DNS, TLS, SSH, HTTP, Flows, Alerts, Time series charts are shown.

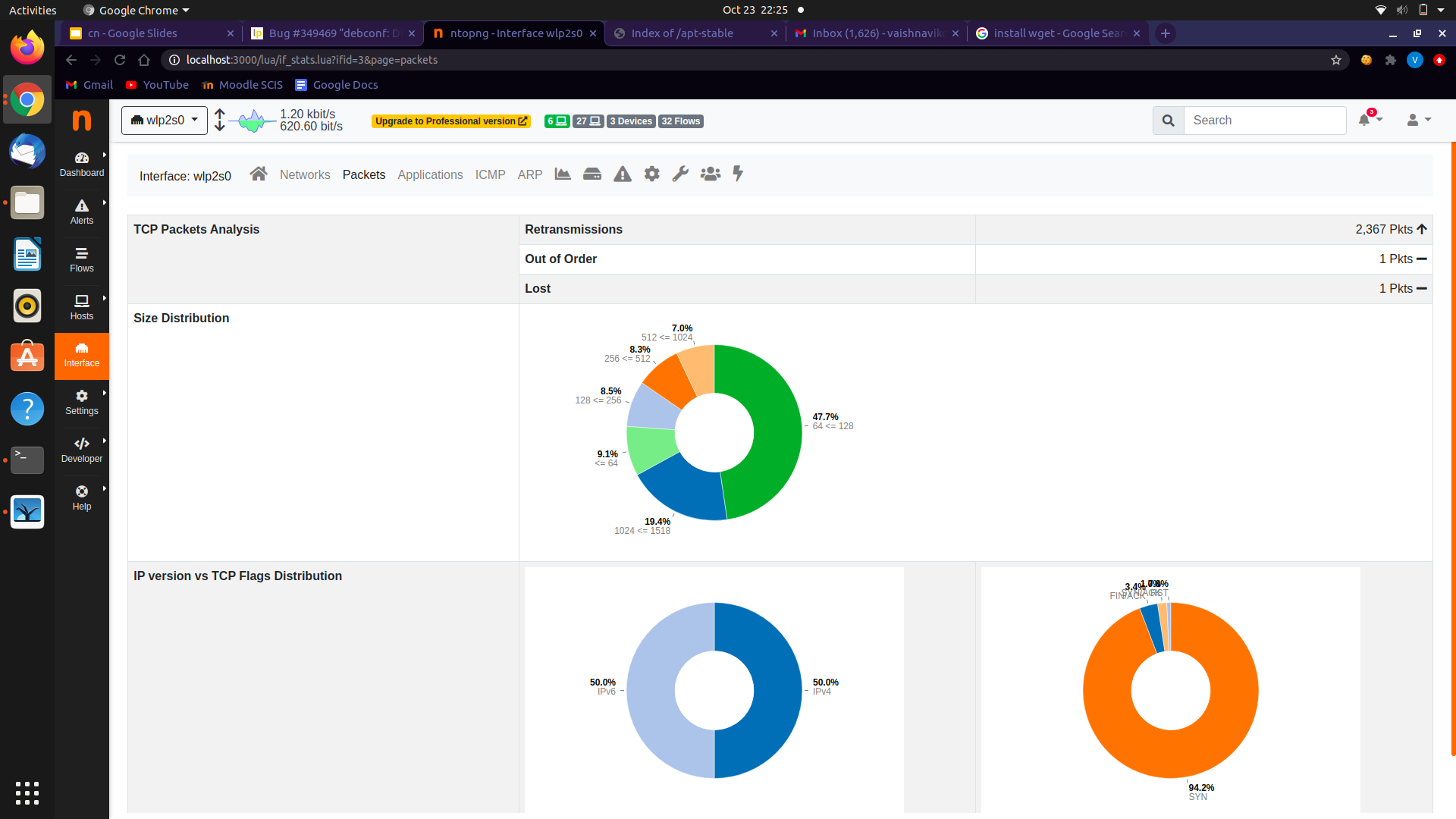




#### Interface section:

This page has the following sections

* Home - Displays complete details of that particular interface (state, speed, traffic breakdown, statistics, etc.). Pcap download is also available.
* Networks - Contains IP addresses read from interface configuration and broadcast domains from ARP traffic.
* Packets - Contains TCP packets analysis, size distribution of packets, distribution based on IP version and TCP flags.
* Applications - Contains application overview, category overview and live flows.
* ICMP - Shows ICMP messages.
* ARP - Shows number of ARP requests and replies.
* Charts - Time series of traffic, hosts, flows, active servers and packets.
* Traffic recording settings
* Alerts - Past and current alerts and alert settings
* Interface settings
* Hash tables
* Pools
* DHCP ranges

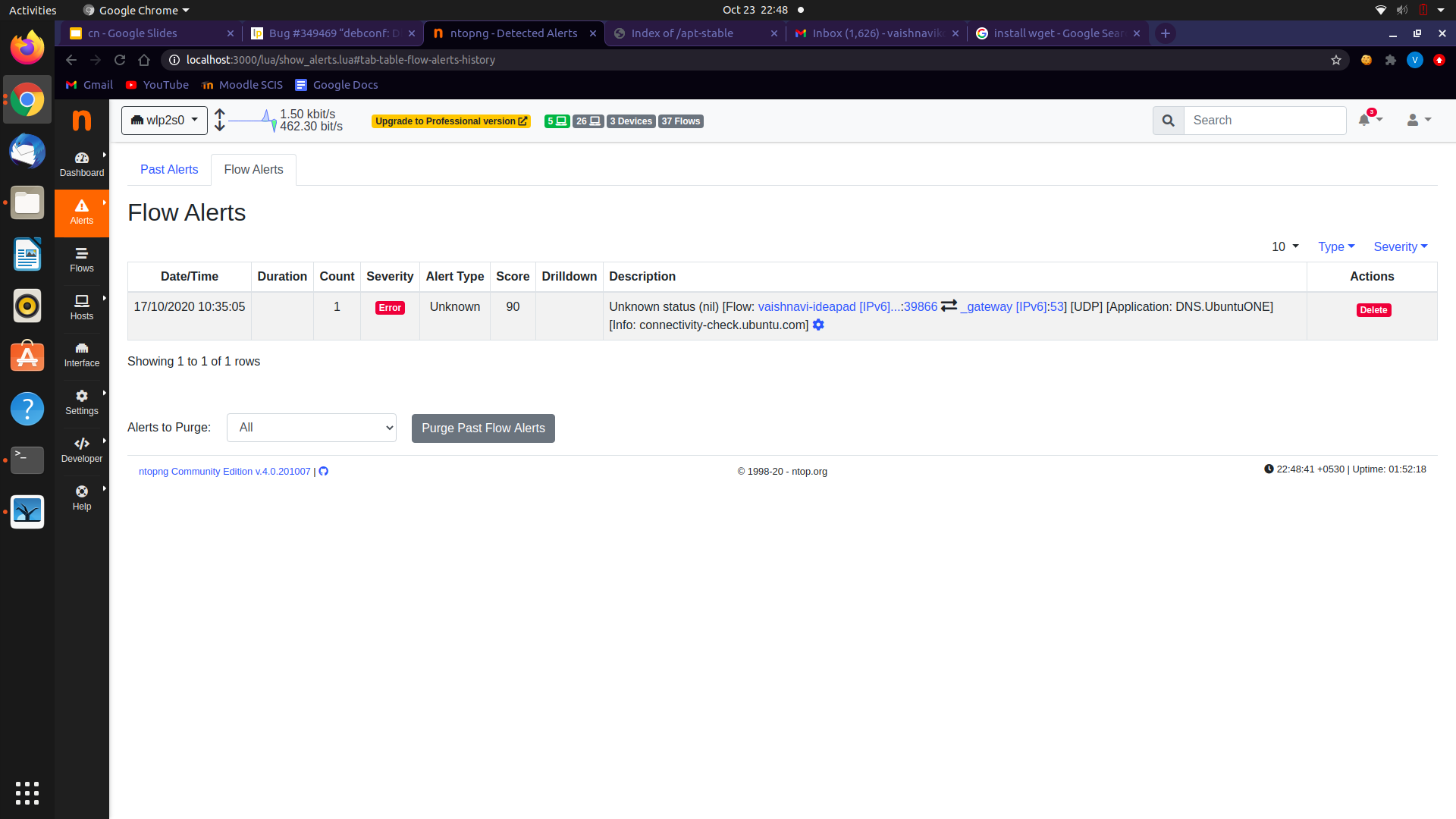


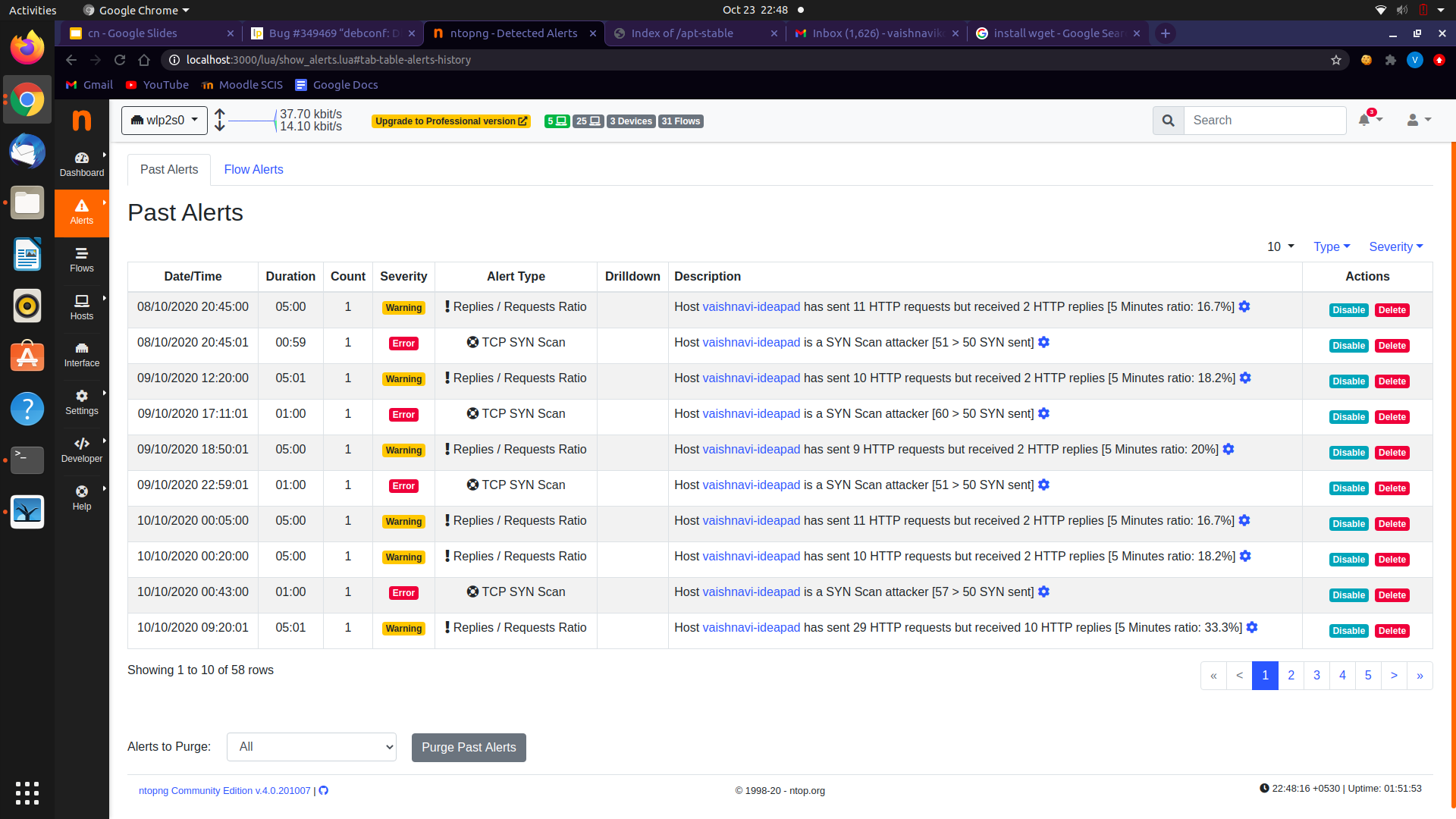
#### Alerts:

This page contains Past alerts and Flow alerts.

For each alert it shows

* Date and Time
* Duration
* Count
* Severity
* Alert type
* Description
* Actions





#### Other sections:

There are various settings available through which we can

* Manage users (ntopng supports multiple users)
* Manage runtime preferences
* Manage data
* Manage applications and categories
* Manage device applications

Developer options include

* Loaded Plugins
* User Scripts
* Alert Definitions
* Directories

#### System statistics:

The health section shows the following details

System status:

* CPU load and CPU states of system
* RAM details of system
* Process ID, RAM used, Alerts count of ntopng
* Storage Utilization and Last Log Trace of ntopng

Interface status:

* Names
* Alerts
* Local hosts
* Remote hosts
* Devices
* Flows
* Total Traffic
* Total Packets

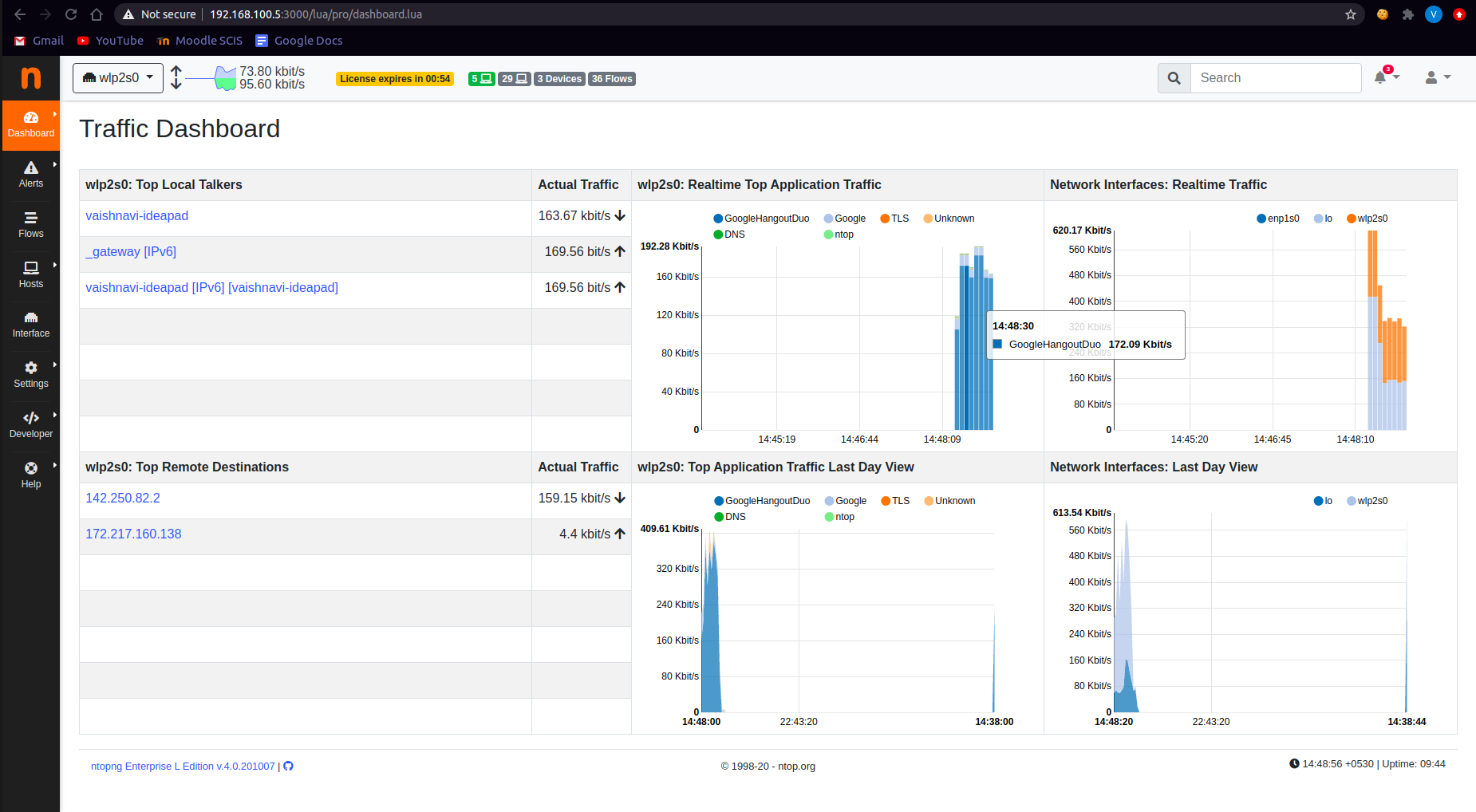
Other sections include

* Redis
* RTT monitor
* ntopng Remote Assistance
* Backup Configuration
* Settings
* Developer Options

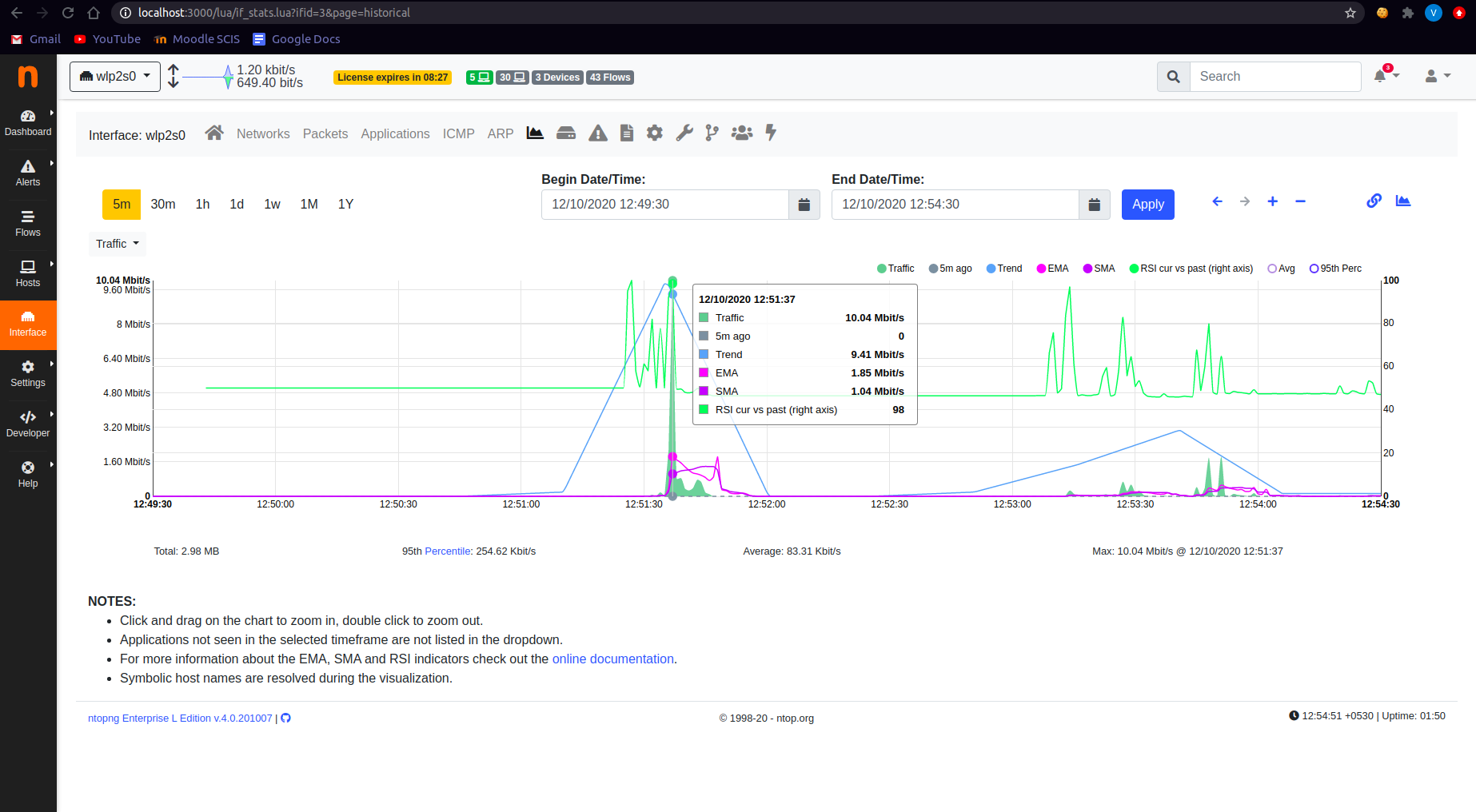
## 

## Snapshots from Professional Version

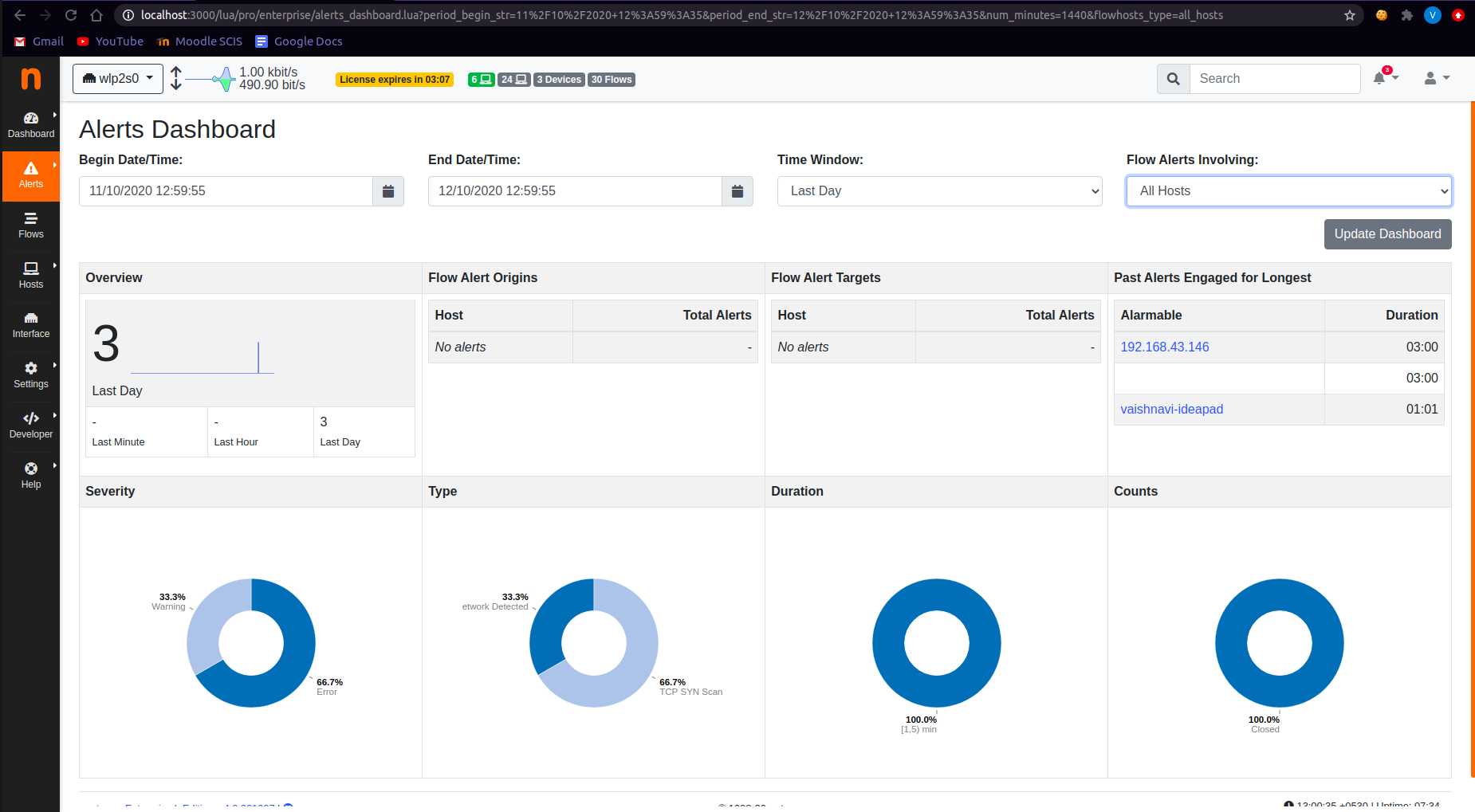
Dashboard:



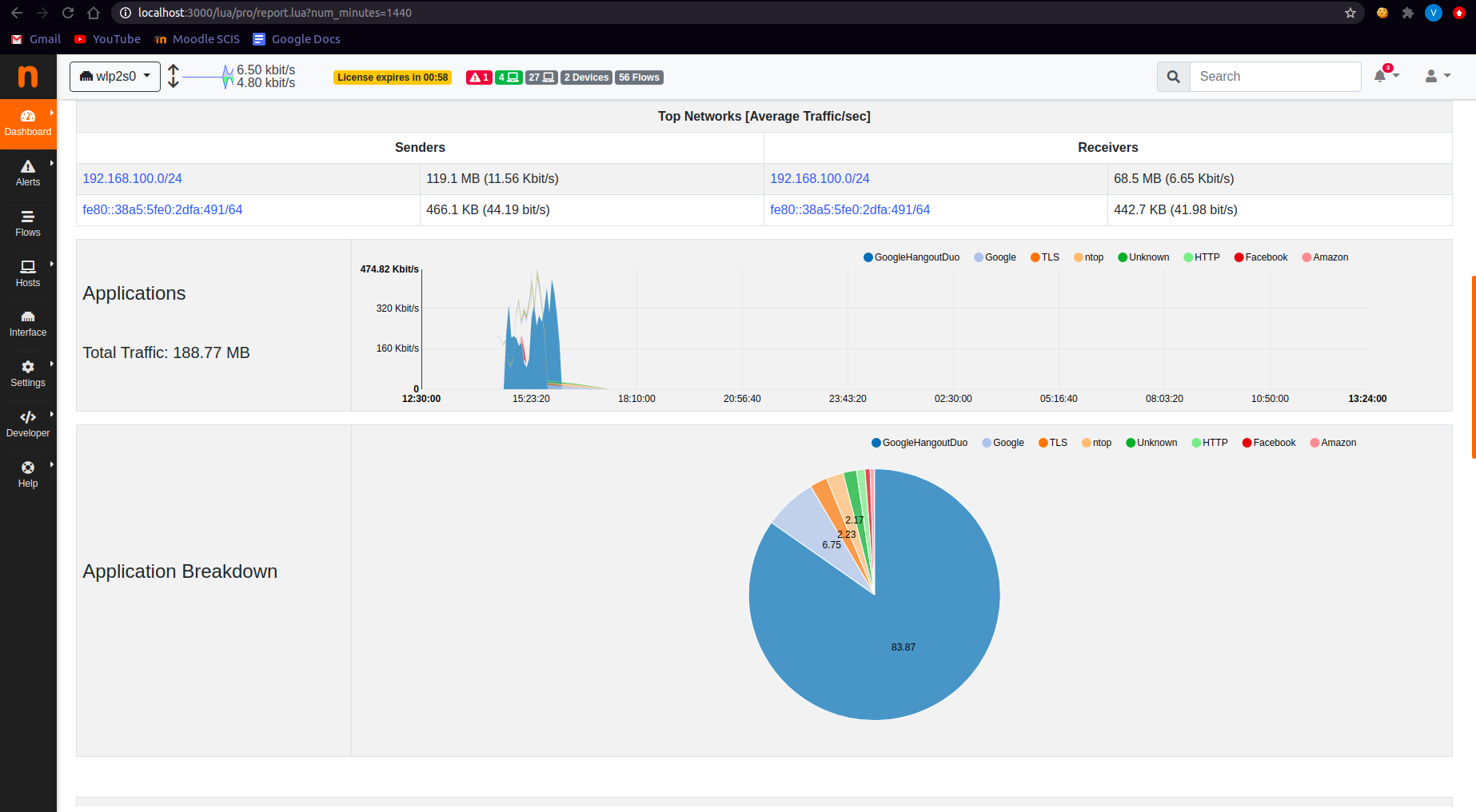
Interface charts:



Alerts:



Application Breakdown:



## 

## Conclusions

* Ntopng is easy to install and configure
* Its web UI is simple and highly interactive
* It provides classifications of several parameters
  + Traffic distributions
  + TCP packet distributions based on size and type
  + Application protocol distribution
  + Live flow distribution
* Alerts are generated when suspicious activities happen.

# Nagios XI

## Introduction

Nagios is an **open-source** network monitoring application designed to run on a Linux operating system that monitors systems, networks on devices running Linux, Windows, and Unix operating systems which was initially designed by Ethan Galstad as part of the NetSaint. A network flow data analysis solution for providing organizations with a view into all network traffic.It marks the hosts and services specified, alerting critical parameters of applications, network and server resources. Nagios also monitors services like SMTP, POP3, HTTP, NNTP, PING, etc.

Nagios Network Analyzer is a NetFlow analysis, monitoring software along with a bandwidth utilization measuring tool, where bandwidth is a key metric in measuring traffic on a particular interface. Analyzer with a flow enable network device gives all about the traffic source, destination port, and what is it being used for.

Nagios Architecture

Nagios is a client-server architecture where the Nagios server runs on a host, and plugins are running on all the remote hosts to be monitored. Nagios Core serves as the basic event scheduler, event processor, and alert manager for elements that are monitored. It features several APIs that are used to extend its capabilities to perform additional tasks, is implemented as a daemon written in C for performance reasons, & is designed to run natively on Linux systems.

* Nagios
* Plugins
* Status

Products

* Nagios XI
* Nagios Log Server
* Nagios Network Analyzer
* Nagios Fusion

## 

## Installation

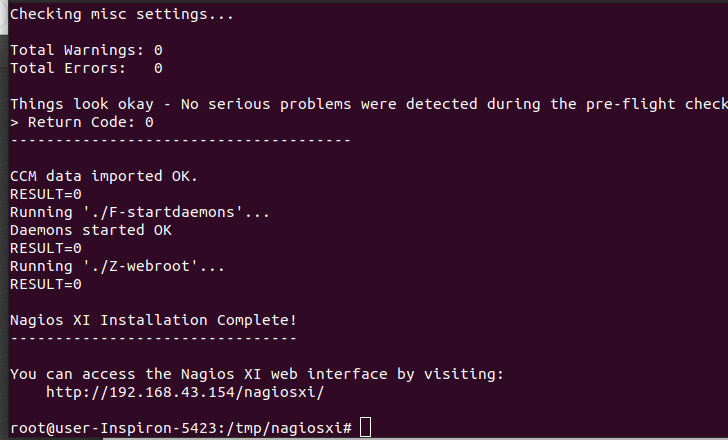
Installation process of Nagios XI in the [link](https://www.nagios.com/downloads/nagios-xi/). The installation guide gives a digest of prerequisites and the hardware requirements for smooth installation for supported systems.

Quick Manual for Linux system

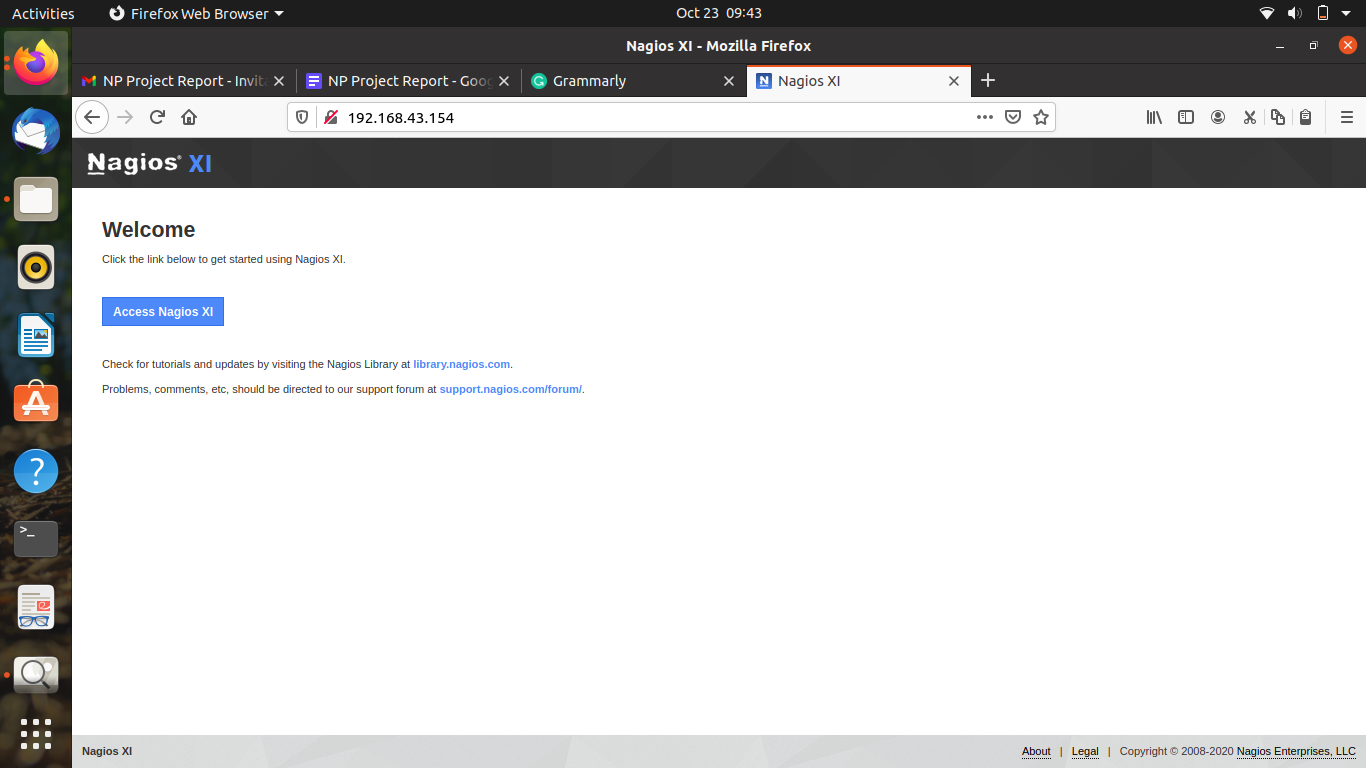
Execute the following commands on the terminal session:

* curl https://assets.nagios.com/downloads/nagiosxi/install.sh | sh
* cd /tmp
* wget <https://assets.nagios.com/downloads/nagiosxi/xi-latest.tar.gz>
* tar xzf xi-latest.tar.gz
* cd nagiosxi
* ./fullinstall

Once the installation is completed you see a message as following:

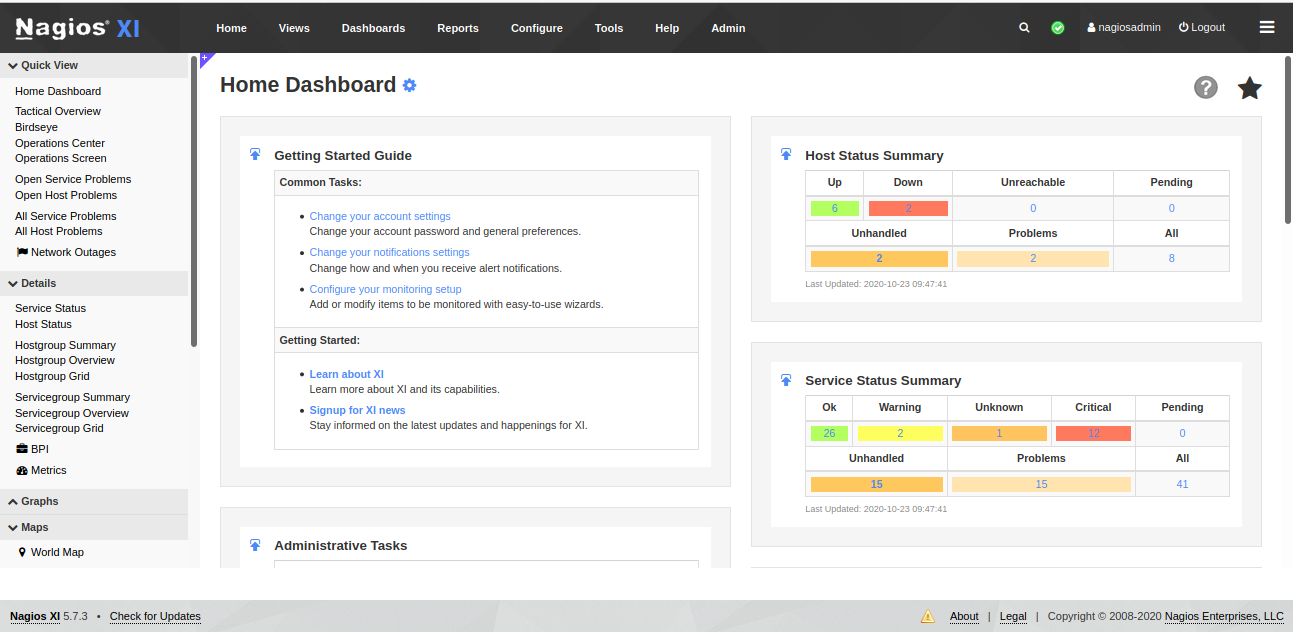


The access link directs you to the web interface which asks for login credentials and gets to the home page.



Click the access Nagios Xi to begin where you redirect for the Admin Account for the administration password and finish the installation.

Click on Login to enter the home screen where the main dashboard is presented.

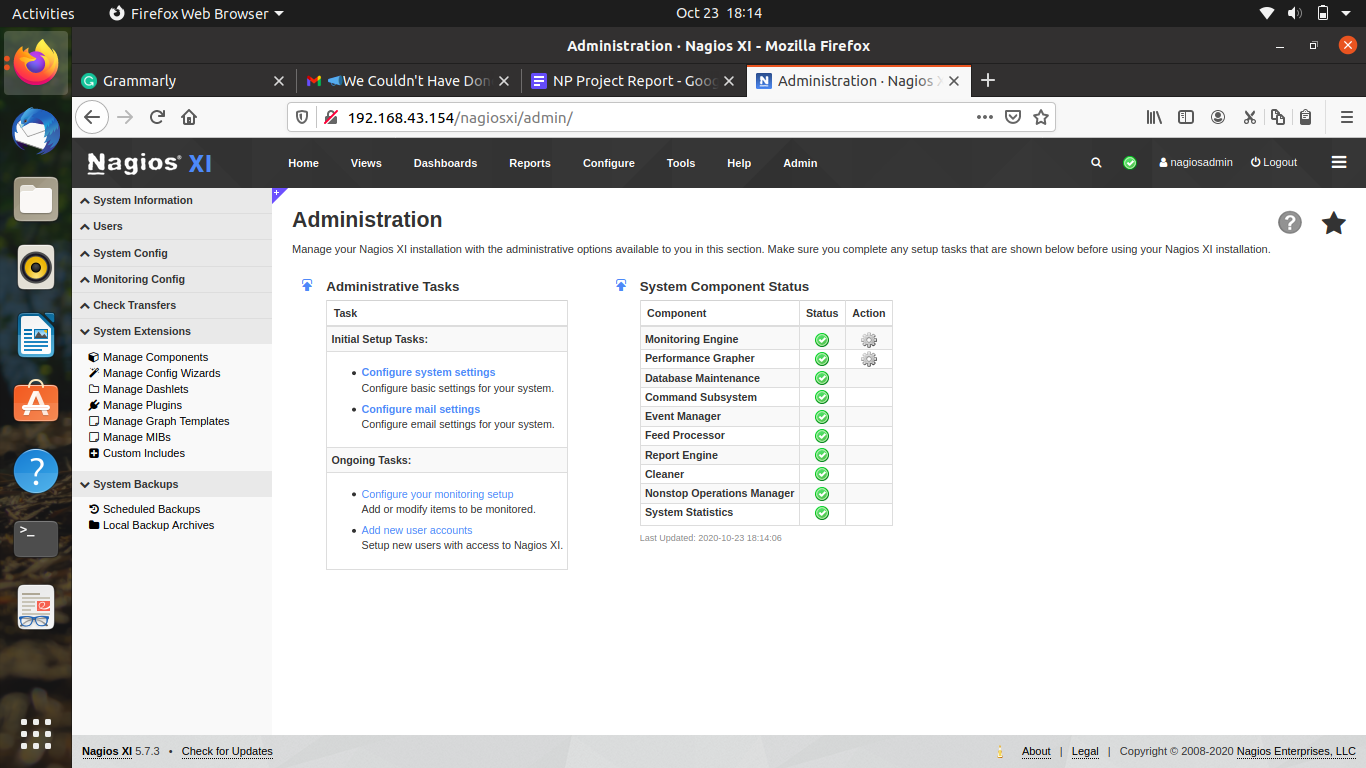


## Configuration

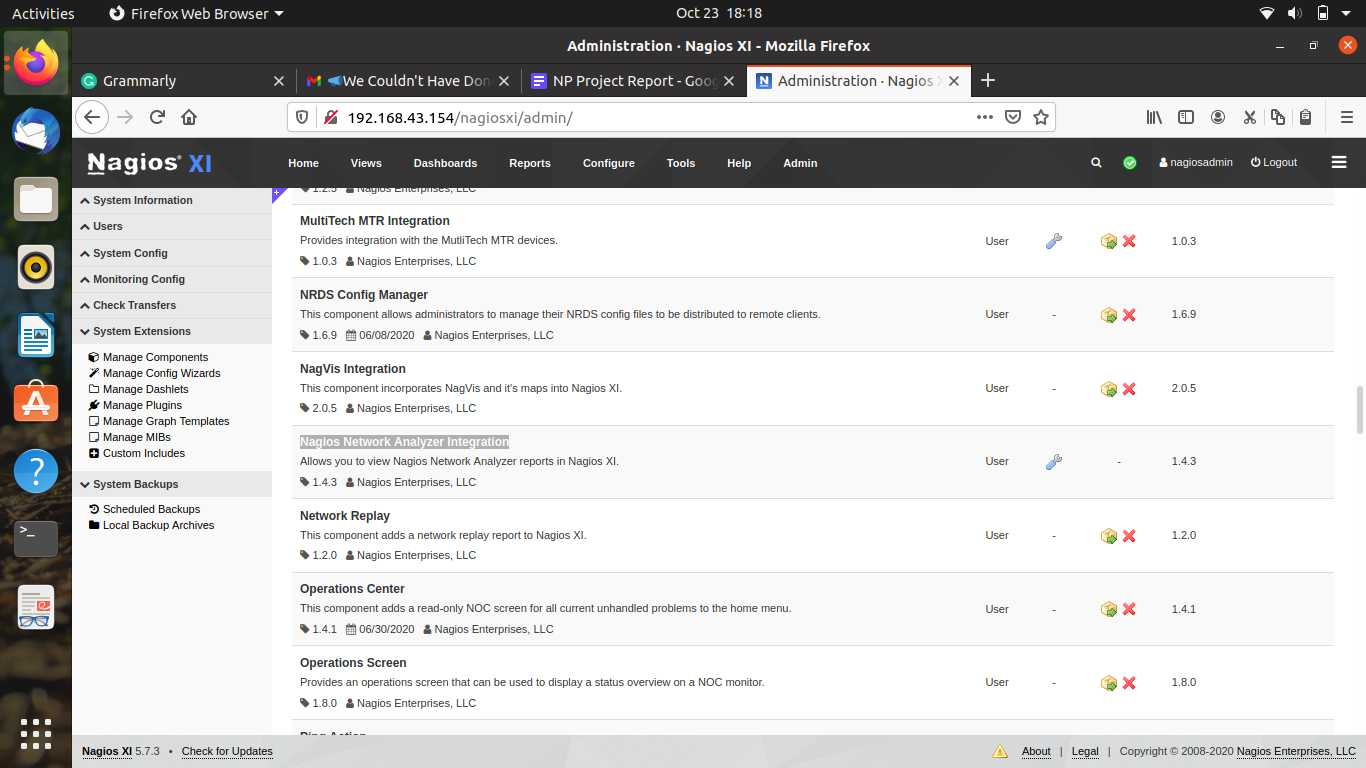
Nagios Network Analyzer is integrated with Nagios XI or Nagios Core, extending the capabilities of the network analyzer.

The integration process is as follows:

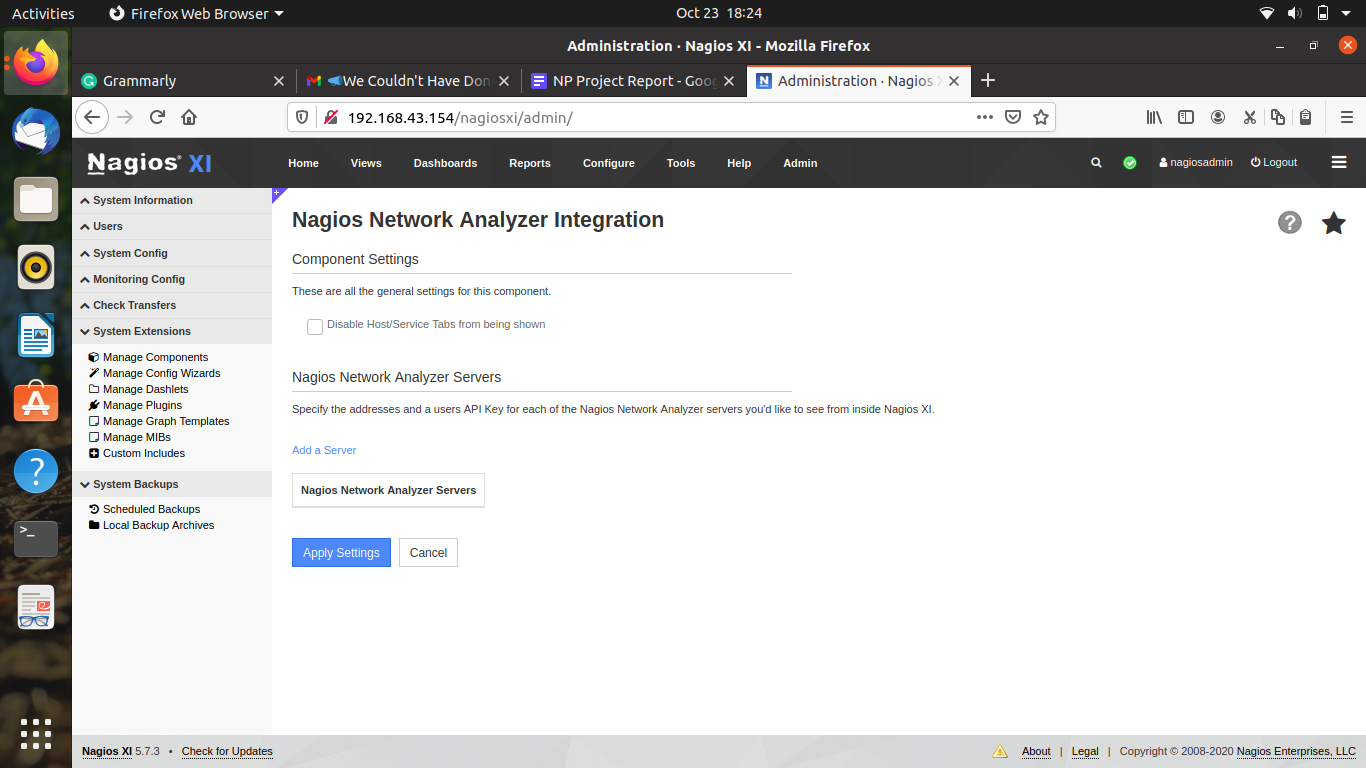
* Login as admin user and navigate to **Administration → System Extensions → Manage Components**

****

* Search for **Nagios Network Analyzer Integration**

****

* Edit settings  **→** Add servers



## Usage

Nagios are limited to monitoring up to seven (7) hosts (nodes) and up to 100 total host and service checks.

Configuration of Websites

* Click on Configure → Configuration Wizards → Website
* Add on the website to be monitored in the text box
* Add on all the website services to be monitored
* Limit the monitoring time and frequency

Home screen includes many options on the left where Details give a brief of host status and service status. These are performed by the Nagios daemon.

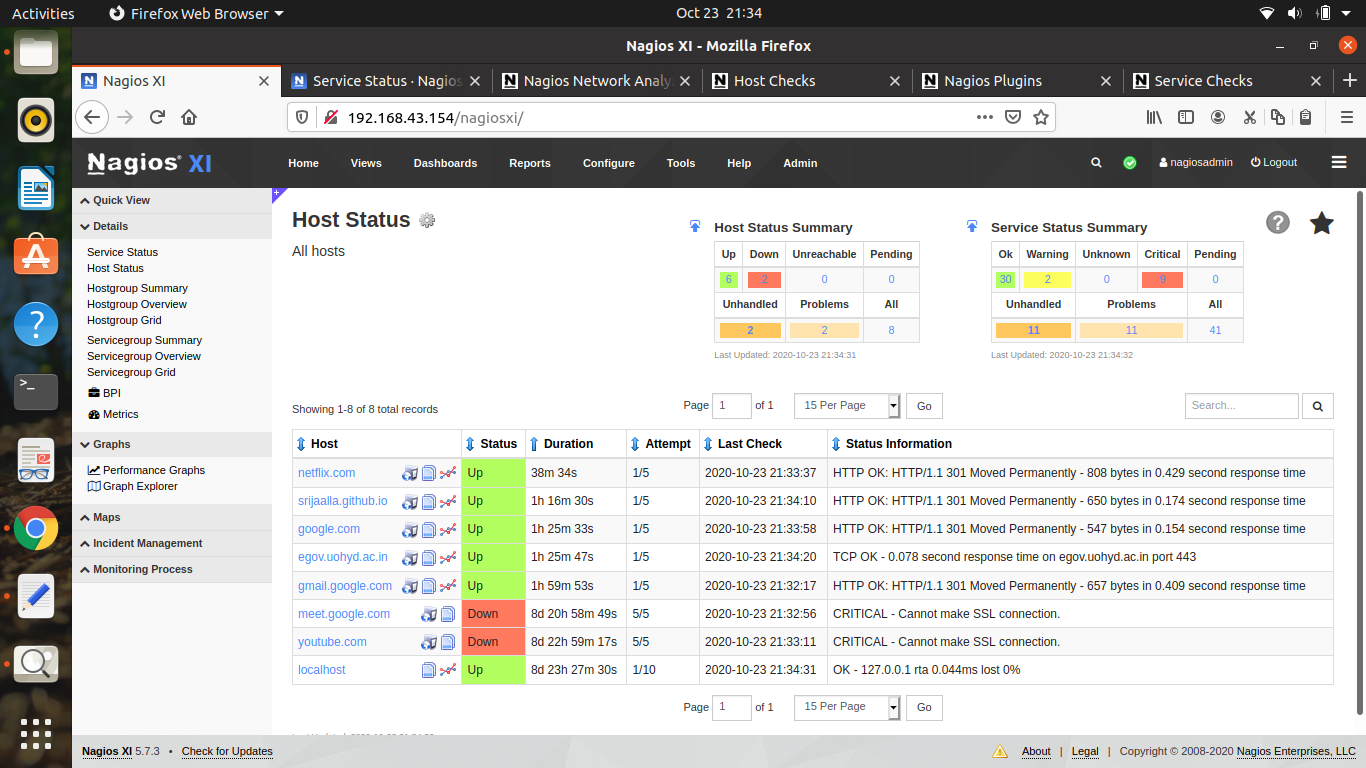
#### Host Status

Hosts are periodically checked by Nagios daemon, where a service associated with the host changes state. The host reachability is distinguished as up, down or unreachable state.

Host checks performed by plugins return the state of ok, warning, or critical which are translated from the states of host reachability the mapping.

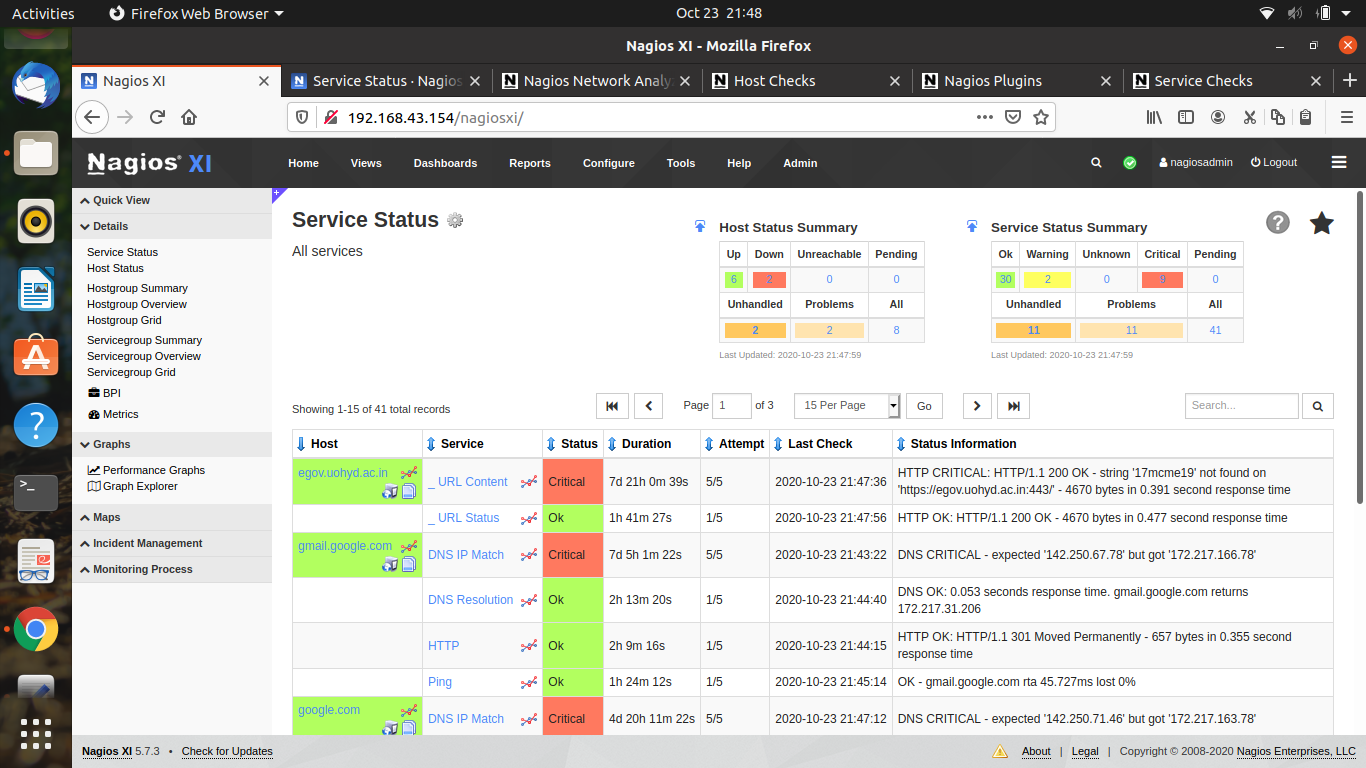
|  |  |
| --- | --- |
| **Plugin** | **Host Status** |
| OK | UP |
| WARNING | UP or DOWN left right |
| UNKNOWN | DOWN |
| CRITICAL | DOWN |

Cached checks improve the performance, which allow Nagios to forgo executing checks to the most recent check result. The states and the changes in states trigger event handlers that notify the user.



#### Service Status

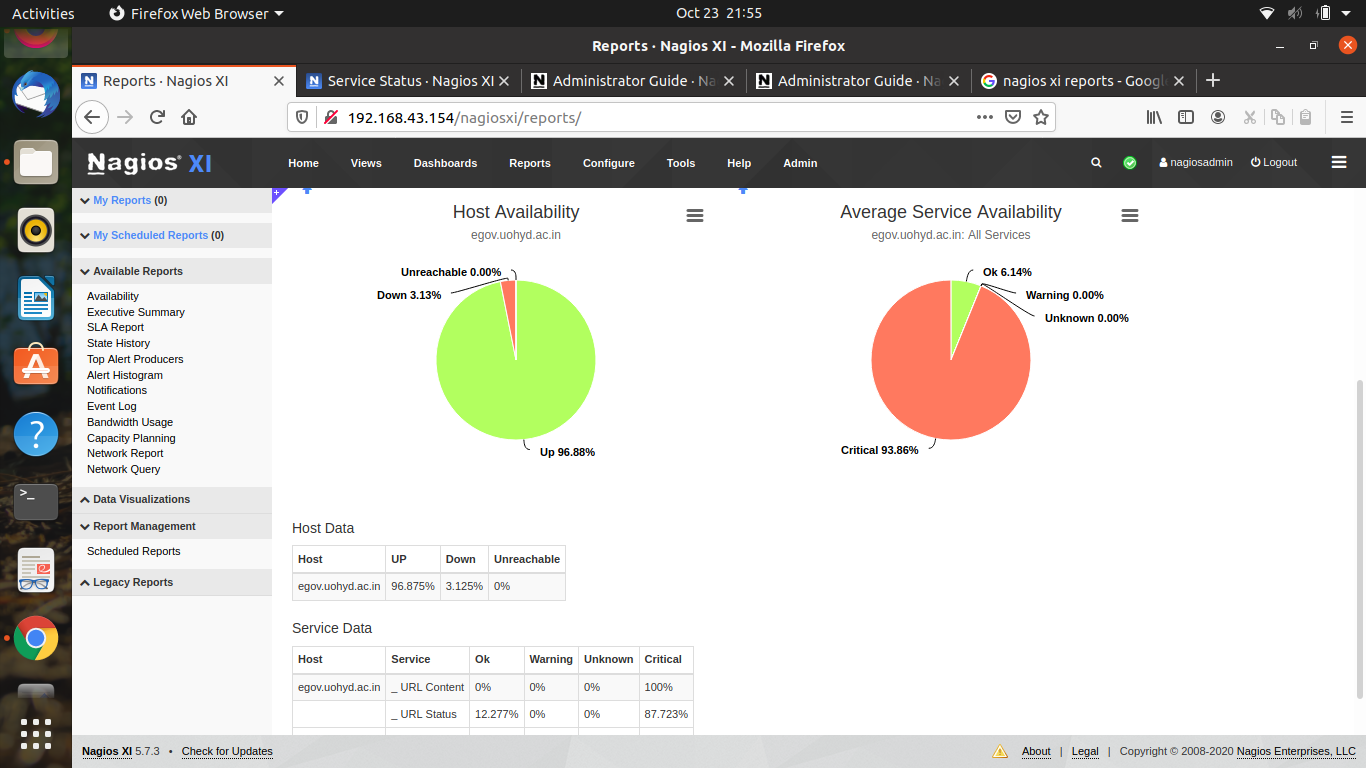
The service checks are performed as part of the predictive service dependency check logic that elaborates the status of a particular service as an example of a website. As in host status the translation of plugins and status inputs are done.



#### Reports

Reports can be accessed by selecting Reports on top which lists the performance graphs of host and services which can be generated with user specific inputs like time period, host limits, hostgroup, and servicegroup.

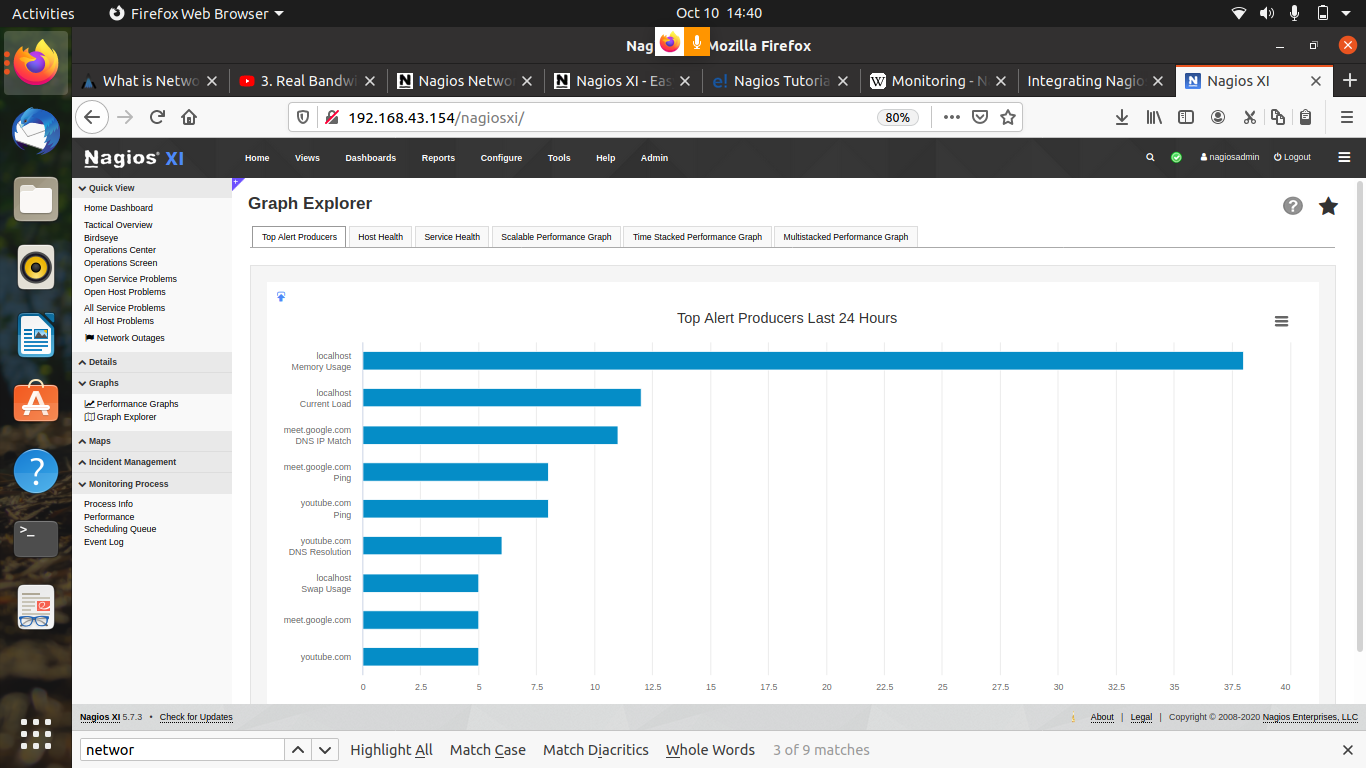
The schedule new report option notifies a new report periodically.



#### Graphs

Highcharts is the module for designing the performance graphs in Nagios XI where the performance in each type of the graph is designed to concentrate a particular metric of the host.

Alerts of hosts availability is shown by Graph Explorer→Top Alert Producers



Performance of the host with respect to time is shown by Graph Explorer→Time Stacked Performance Graph



# Colasoft Capsa

## Introduction

Colasoft Capsa is a **commercial, windows** based tool. Capsa is the name of a packet analyzer developed by colasoft. It’s portable Network performance analysis and diagnostics tool, provides a powerful and comprehensive packet capture and analysis solution with an easy user interface. It performs real-time packet capturing and monitoring. It has 3 editions available.

1. Capsa Standard Edition - Ethernet Packet Analyzer, Network Monitoring and troubleshooting.
2. Capsa Enterprise Edition -Ethernet and WLAN Analyzer, Real- time packet capturing and monitoring.
3. Capsa Free Edition - Freeware Ethernet packet analyzer. Used for geeks to learn protocols , packets and network related knowledge.

The enterprise edition is the flagship of the colasoft family, supports both Ethernet and WLAN. We shall use the Enterprise Edition.

## Tech Specifications

### Software requirements:

* Windows Server 2008, 2012 64 bit Edition
* Windows 7/8/8.1, 64 bit Edition
* Windows Vista, 64 bit Edition
* Windows 10 Professional, 64 bit Edition

### Hardware Requirements:

* CPU: P4 2.8GHz or higher
* RAM: 4GB or higher
* Web Browser - Internet Explorer 8.0 or Higher

#### Current System Used:

* CPU: Intel Core i5 3.2GHz
* RAM: 8GB
* Web Browser - Internet Explorer 8.0

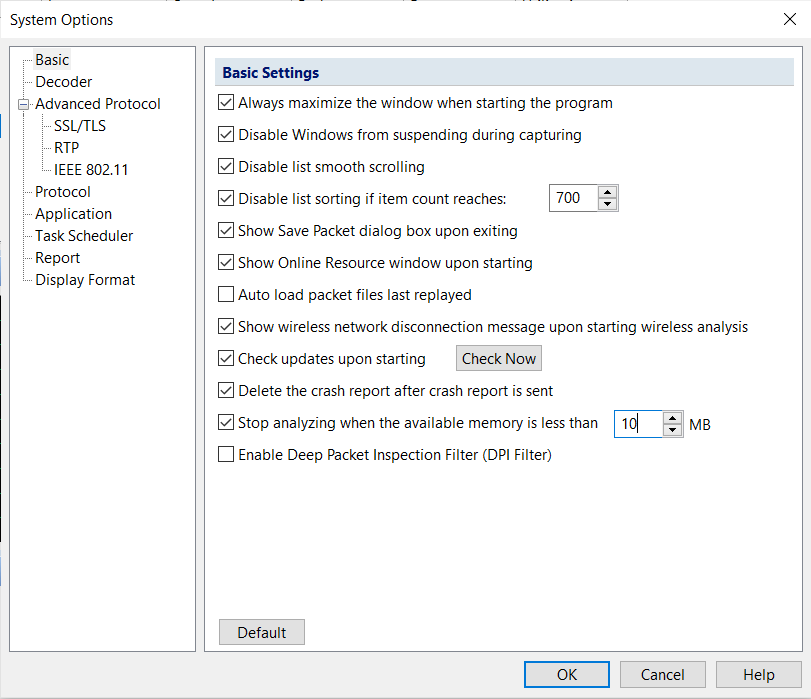
There is no web interface provided for colasoft capsa. It runs as an independent application.

## Installation

* To install Capsa, open the [link](https://www.colasoft.com/download/products/download_capsa.php).
* Fill the details with an enterprise email and click Download.
* Users will then receive a mail with the unique license key and an exe file id downloaded.
* Execute the downloaded exe file and an installation wizard pops up.
* Follow the instructions provided by the wizard.

## Configuration

* Once we install and start the application, it asks permission to make hard drive changes for which users need to click YES to proceed.
* Capsa identifies available Ethernet and WLAN network adapters. Select the network we need to monitor and click **Start.**
* An pop-up shows where we need to set when the packet capturing can stop, it defines the maximum limit.By default it is set to 100MB when first installed which must be changed because the remaining space is easily filled. We change it by clicking SET.
* On clicking set the below box is shown where we can change how the packets are captured. Here we need to set it to stop analyzing when available memory is less than 10MB and click OK
* One can also customize list sorting limits which in this case is set to 700.



* DPI filter in the above snapshot provides users with a separate option to filter packets. Example: filter packets with a particular IP address or protocol.

## Features and Demo

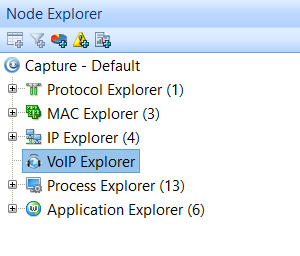
### Extended Network Analysis:

The Capsa Network Analyser performs traffic Analysis as well as Security analysis. Security Analysis detects the following anomalies

* **ARP attack** - The malicious source machine can be found by the MAC address
* **Worm activity** - Worms are identified by their network activity and are located with their IP addresses
* **Dos attack** - Capsa detects both compromised machine and machine under Dos attack
* **TCP port Scanning**
* **Suspicious conversation** - Suppose MSN is blocked in our network and HTTP port 80 is open for web browsing. A malicious user could change MSN port to 80 to chat with others.

### Node Explorer:

This is found on the top left corner after capturing is started. It is to access everything we need through a node connected for an easy understanding.



#### Capture Default:

* Capture default has the similar functioning as a menubar. Here we can see the Dashboard which shows all the **top talkers of the network** in real-time based on packets, Domain, TCP, port, IP, Process, application, SIP, H.323 and MOS\_distribution(count)

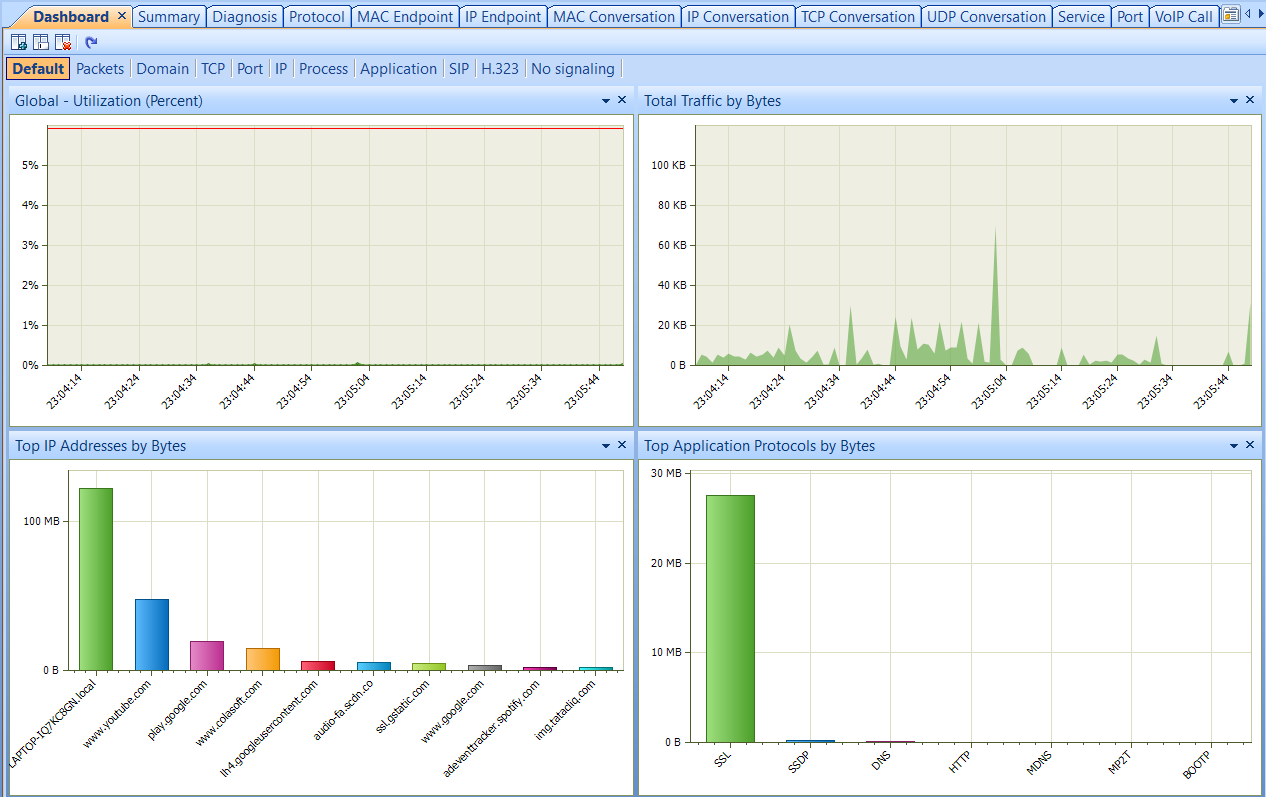


Fig: **Dashboard** - Global utilization (percent) *vs* real-time, Total traffic (bytes) *vs* Real-time, Top IP addresses (bytes) *vs* domains, Top Application protocols (bytes) *vs* protocols

* **Multiple Networks can be monitored in real-time** - *Capture Default -> Log* Monitors HTTP, Emails, DNS, FTP, MSN, SSL and VoIP call signaling.
* **Advanced Protocol Analysi**s - *Capture Default -> Protocol*
* **Packet Decoding**  *- Capture default -> Packet* - captures all network packets transmitted on the network and displays a detailed packet decoding information in HEX, ASCII and EBCDIC.

Packet list: Table offers the list of packets captured from the node selected in node explorer.

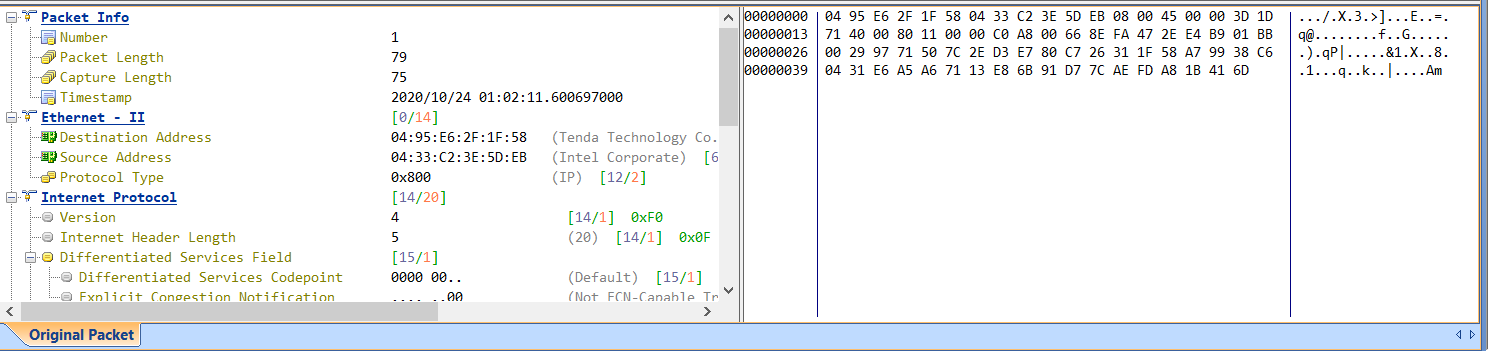


Fig : Example of Packet decoding

* Versatile Network and Bandwidth Monitoring - Capsa provides a unique user interface unlike any other tool. The below figure is found on the top of the measuring and capturing bar. It is common for all the nodes provided under Node Explorer with options changing according to the respective node.



Fig : Filters and options

Important options include:

* Matrix
* Log
* Protocol
* MAC and IP endpoint
* MAC, IP, TCP and UDP conversation
* Application
* Process
* Port
* Service

Opening each option provided above gives information of all packets that are captured in the network according to their respective fields.

#### Protocol Explorer:

The 1 beside protocol explorer represents the no.of protocols that are available. In this case it is Ethernet II

|  |  |
| --- | --- |
| The branching says it all   * IP, IPv6 and ARP are the protocols available. * Under IP there are TCP, UDP and ICMP analysis * Under IPv6 there are UDP, HOPOPT and ICMPv6 analysis * Under ARP there are analysis of request and response ARP packets. |  |

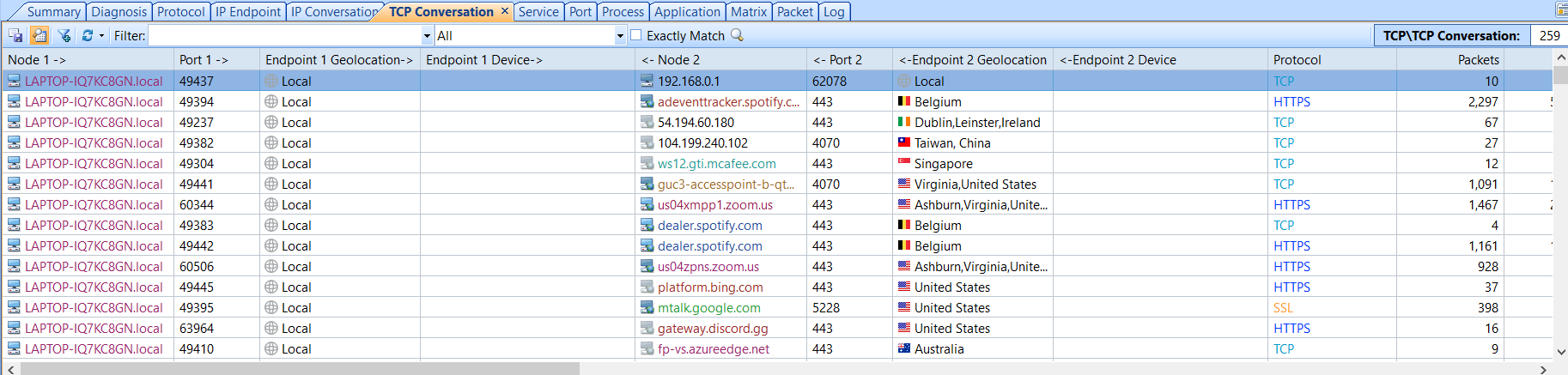
For every protocol the following details are provided along with a summary if it's relevant.

For Example: When we select UDP protocol, TCP conversation is not provided.

##### 

##### TCP Flow Analysis:

* TCP packets give information to help us troubleshoot the network. Capsa detects slow networks, CRM transactions and downloading based on this information



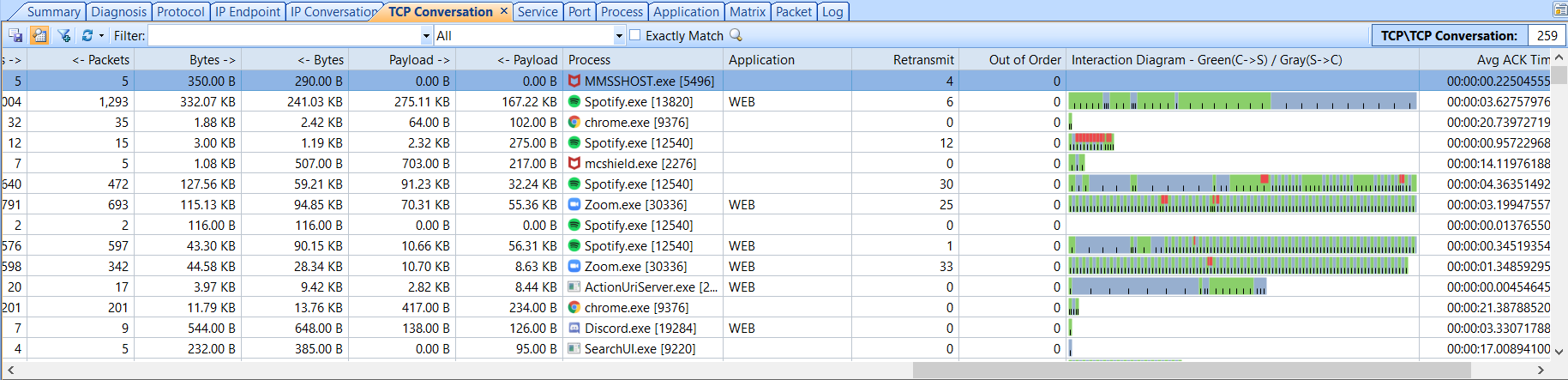


Fig : Information of all TCP packets captured

##### HTTP Analysis:

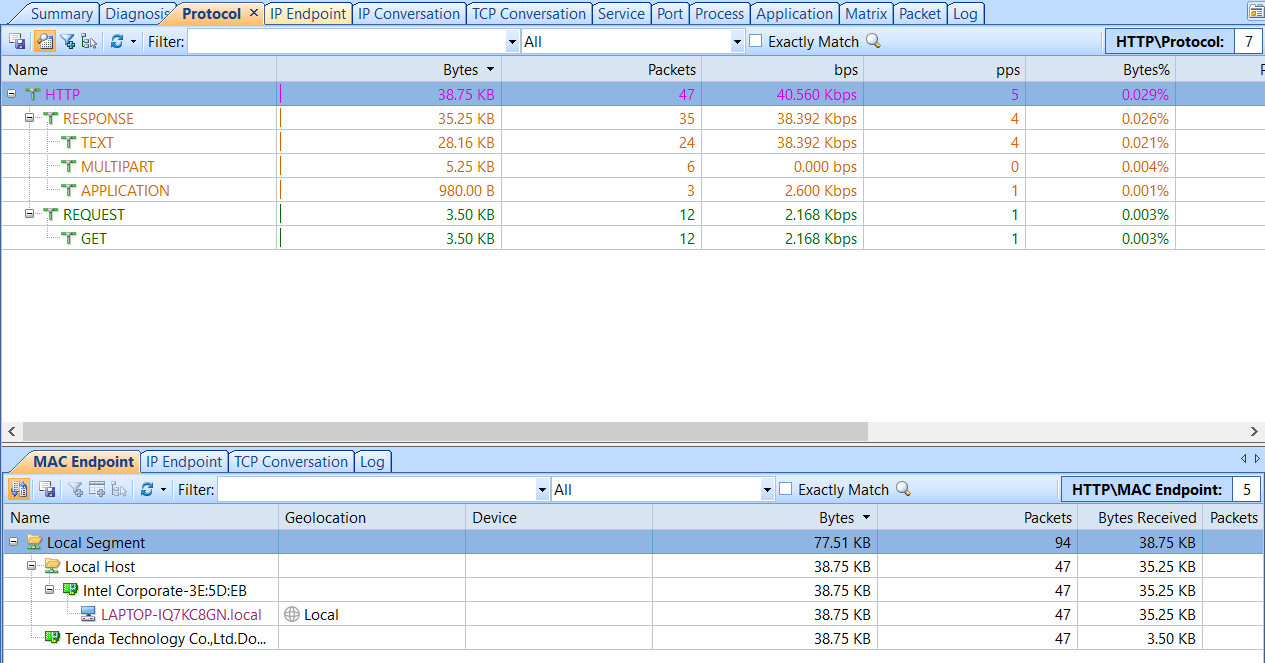
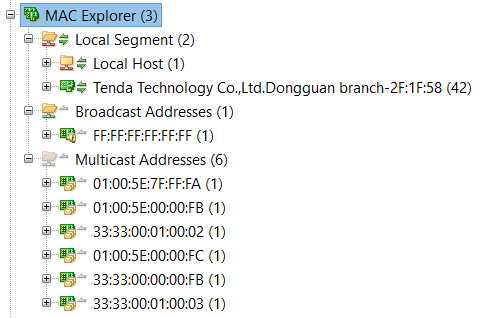


Fig : HTTP analysis

#### MAC Explorer:

Analysis based on MAC addresses of the devices.



#### IP Explorer:

|  |  |
| --- | --- |
| * It has 4 categories Local links, Private-use Networks, Multicast Addresses, Internet Addresses. * Under Internet addresses we can see a list of all the countries the packets are transferred to or received from. * Under Multicast Addresses we see the list of all multicast addresses involved. * Under Private-use Networks we see the private networks. In this case it shows the subnet of the Wi-Fi. * Under Link Local we see the local LAN. |  |

#### VoIP Explorer:

Capsa has a VoIP analysis module to capture and analyse VoIP calls, graphically display VoIP call details.

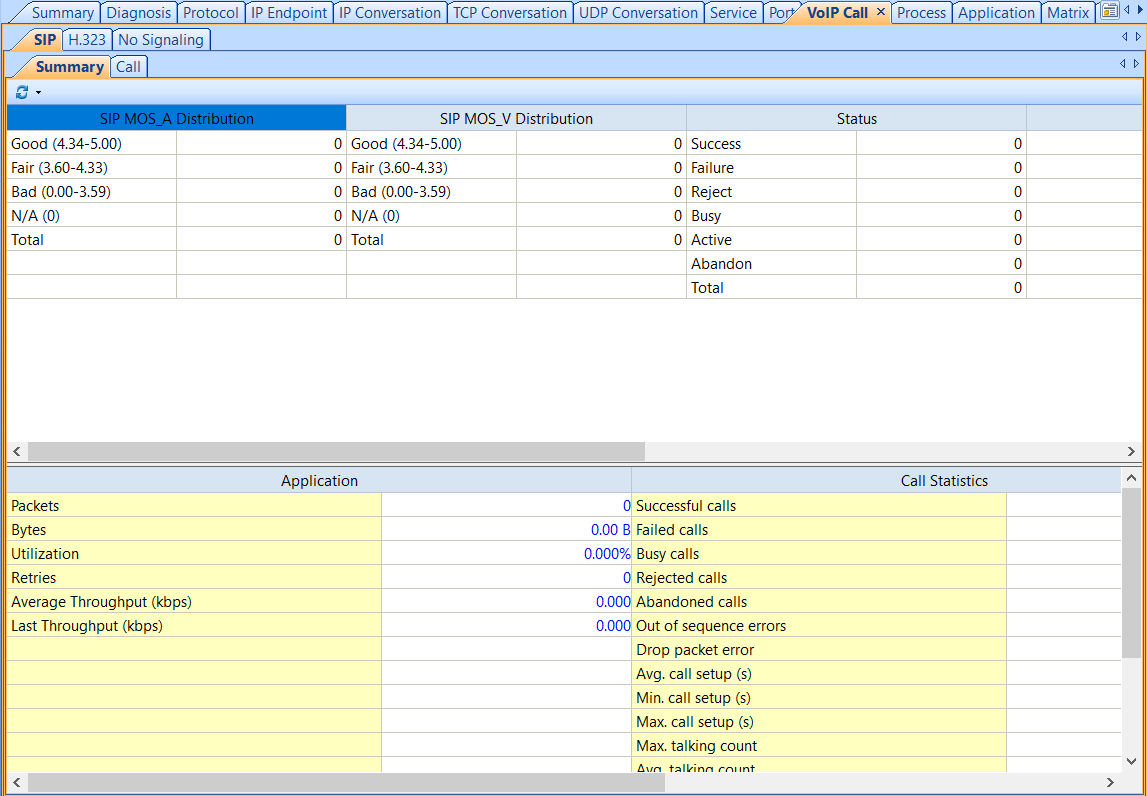


Fig: VoIP analysis

#### Process Explorer:

|  |  |
| --- | --- |
| * List and analysis of all the programs or processes that are currently running in the background are seen under this node.       Fig: Statistics of Process Spotify (3396 and 26692 representing PIDs) |  |

#### Application Explorer:

Lists all the applications running in the background while capturing. It provides analysis of each application in terms of Protocols and Endpoints and conversations.

|  |  |
| --- | --- |
| Fig: Snapshots of two of the reports of an application | Fig : List of Application |

### Notifying Alarms and Emails & Audio:

We can create alarm rules to watch network anomalies, in case of excessive traffic throughput, excessive broadcast packets, etc.

To set an alarm we can either go to the alarm option under node explorer or select alarm from the top in the menu under Analysis.

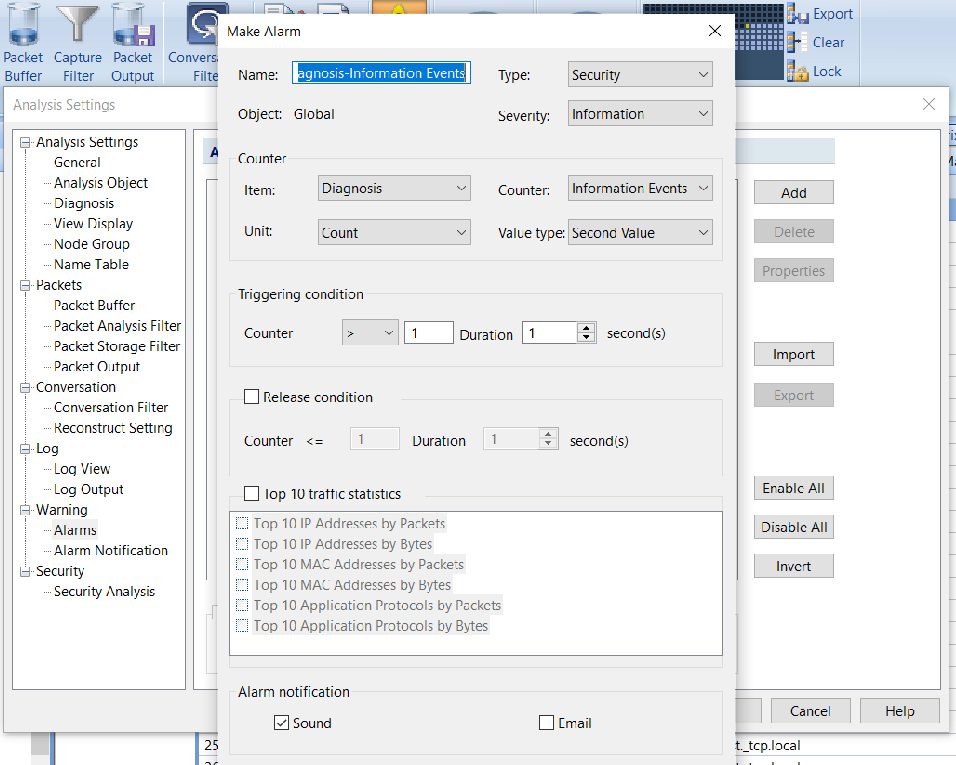


Fig: Alarm

### Task Scheduler:

Task scheduler provides the ability to run packet capture and analysis at a predefined time automatically.

Task Scheduler is found in the menu under System -> Task Scheduler

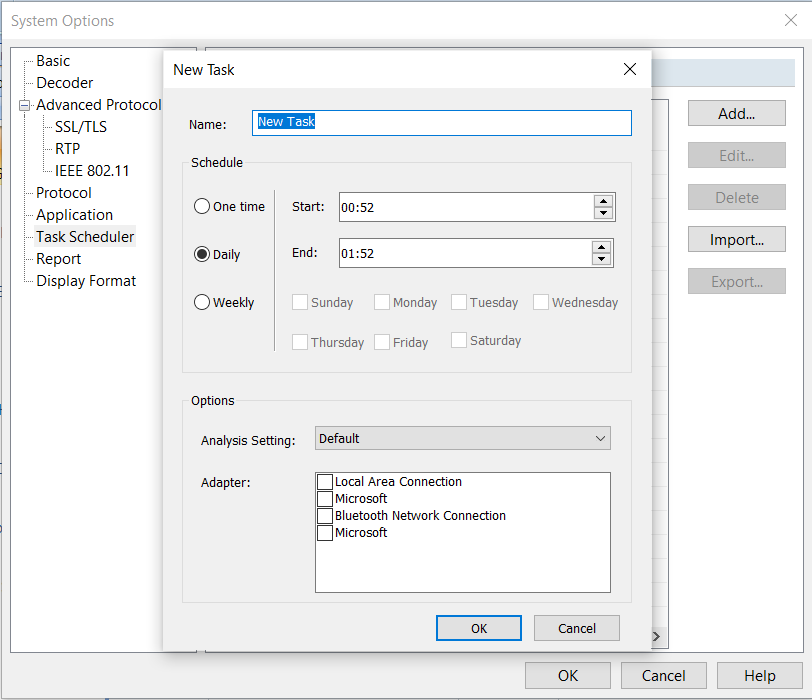


Fig: Task Scheduler

### Visualized Connections in Matrix:

The matrix tab visualizes all the network connections and traffic details in a single graph. The nodes around the elongated ellipse display the hosts in the network; the weight of the line between nodes indicates the traffic, and the color indicates status.

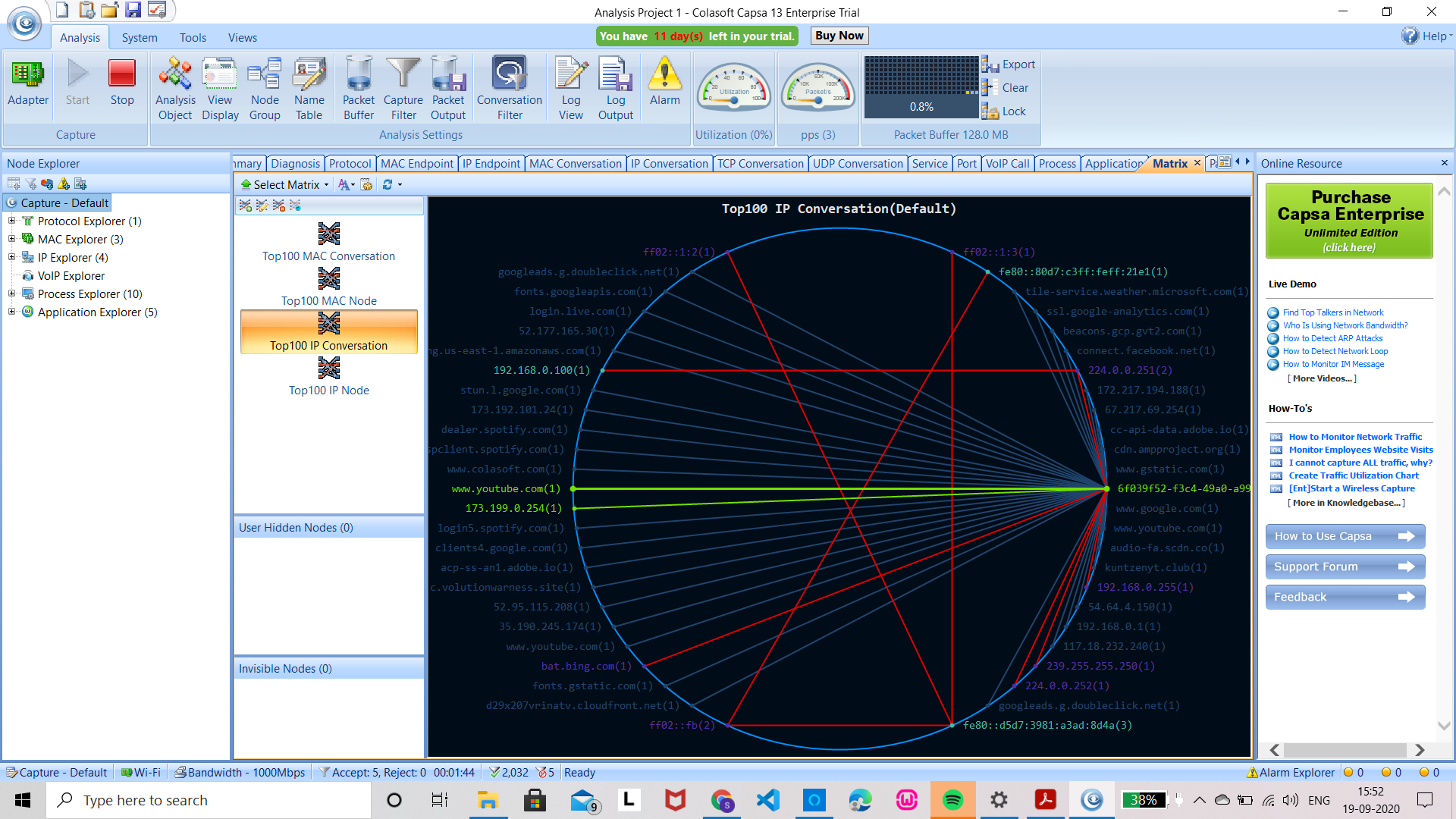


Fig: Matrix with each node representing an address and lines representing the flow

# Comparison

|  |  |  |  |
| --- | --- | --- | --- |
| **Tool / Feature** | **Colasoft Capsa** | **ntopng (community version)** | **Nagios** |
| Type | Packet Analyzer | Network Analyzer | Network Monitoring |
| Open source | No | Yes | Yes |
| Web interface | Yes | Yes | Yes |
| Supporting platforms | Windows | Windows, Debian, MacOS, Raspberry Raspbian. | Windows with VM or Hyper-V,Linux |
| Traffic analysis & Bandwidth monitoring | Yes | Yes | Yes |
| Application monitoring & Network protocol analysis | Yes | Yes | No |
| Triggers / Alerts | Yes | Yes | Yes |
| VoIP analysis | Yes | No | No |
| Data Storage Method | Oracle | MySQL, ElasticSearch and LogStash | MySQL |
| Protocol Support | IP, TCP, HTTP,UDP, ICMP and many more | Ethernet, IPv4/IPv6, TCP, UDP, DHCP and many more | HTTP, FTP, SMTP, SNMP, POP3, SSH and MySQL |
| Network Troubleshooting | Yes | Yes | Yes |
| Integration | Possible | Possible | Possible |
| Latest release version & date | Capsa edition 13, Feb 26, 2020 | ntopng Community Edition v.4.0.201007  Mar 24, 2020 | Nagios Core 4.4. 6 2020-04-28. |

# Learnings and Challenges

During the course of this project, we tried and experimented on various tools on different platforms. Each tool has its own unique features. Zabbix, Colasoft Capsa, Nagios, ntopng, OpUtils are some of the tools we considered. Some of them are easy to install and configure. Some have user-friendly web interfaces. As our project focuses on Traffic Classification, we decided on these three tools - ntopng, Nagios and Capsa.

# Contributions

|  |  |
| --- | --- |
| **Team Member** | **Contribution** |
| Gayathri. A | Worked on Nagios |
| Vaishnavi. K | Worked on ntopng |
| Leela Srija. A | Worked on Capsa |