**Monitoring Simple Network Management Protocol (SNMP) with Wireshark**



Name : Prinita Ayuningtias

NIM : 09011381520061

**Computer Engineering**

**Faculty Of Computer Scince**

**Sriwijaya University**

**2018**

Monitoring Simple Network Management Protocol (SNMP) with Wireshark

Monitoring a network is very necessary at this time. Because by monitoring a network we can monitor the status of a network infrastructure, monitor the network in good condition or not and maintain operational stability. Some protocols that can be monitored one of them is the Simple Network Management Protocol (SNMP).

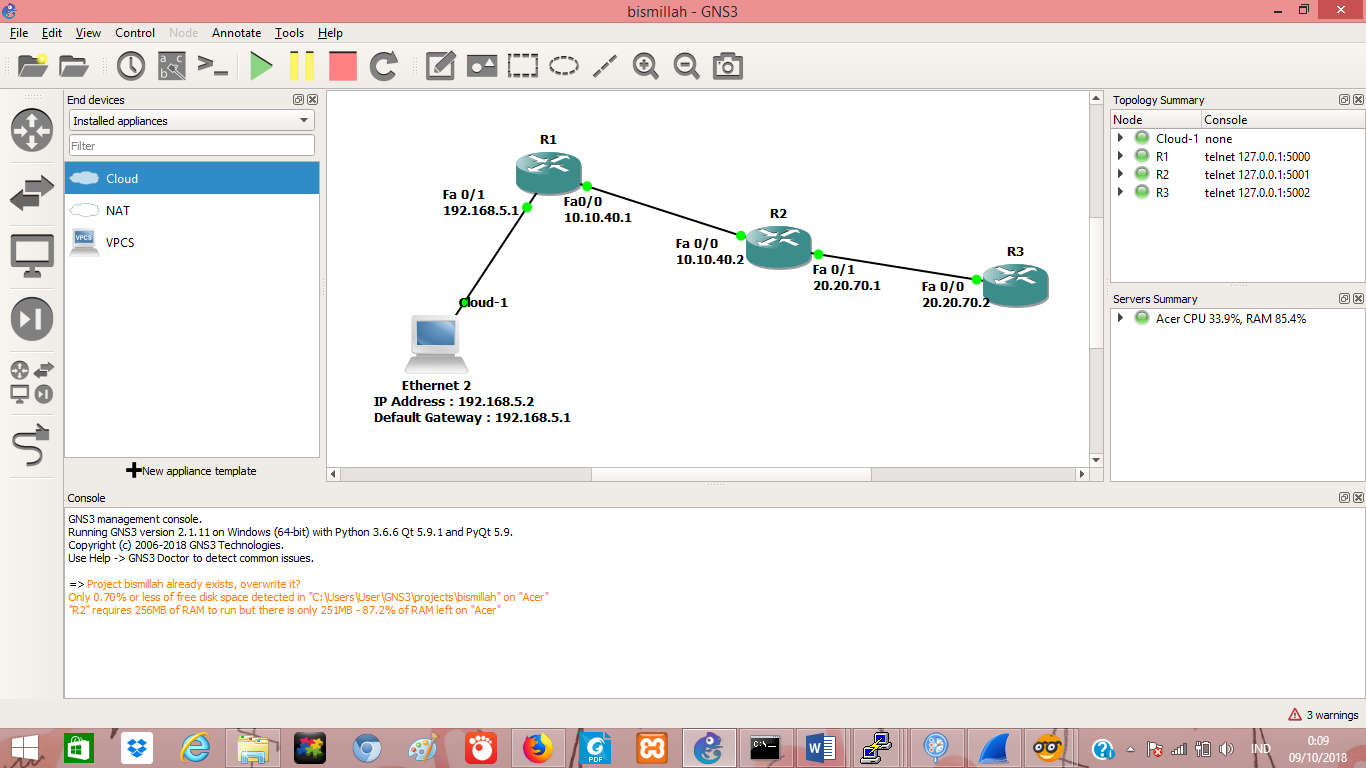
**Simple Network Management Protocol** (**SNMP**) is an [Internet Standard](https://en.wikipedia.org/wiki/Internet_Standard) protocol for collecting and organizing information about managed devices on [IP](https://en.wikipedia.org/wiki/Internet_Protocol) networks and for modifying that information to change device behavior. Devices that typically support SNMP include cable modems, routers, switches, servers, workstations, printers, and more.

SNMP is widely used in [network management](https://en.wikipedia.org/wiki/Network_management) for [network monitoring](https://en.wikipedia.org/wiki/Network_monitoring). SNMP exposes management data in the form of variables on the managed systems organized in a [management information base](https://en.wikipedia.org/wiki/Management_information_base) (MIB) which describe the system status and configuration. These variables can then be remotely queried (and, in some circumstances, manipulated) by managing applications.

Three significant versions of SNMP have been developed and deployed. SNMPv1 is the original version of the protocol. More recent versions, SNMPv2c and SNMPv3, feature improvements in performance, flexibility and security. SNMP is a component of the [Internet Protocol Suite](https://en.wikipedia.org/wiki/Internet_Protocol_Suite) as defined by the [Internet Engineering Task Force](https://en.wikipedia.org/wiki/Internet_Engineering_Task_Force" \o "Internet Engineering Task Force) (IETF). It consists of a set of [standards](https://en.wikipedia.org/wiki/Technical_standard) for network management, including an [application layer](https://en.wikipedia.org/wiki/Application_layer) protocol, a database [schema](https://en.wikipedia.org/wiki/Logical_schema), and a set of [data objects](https://en.wikipedia.org/wiki/Data_object" \o "Data object) [1]

Testing :

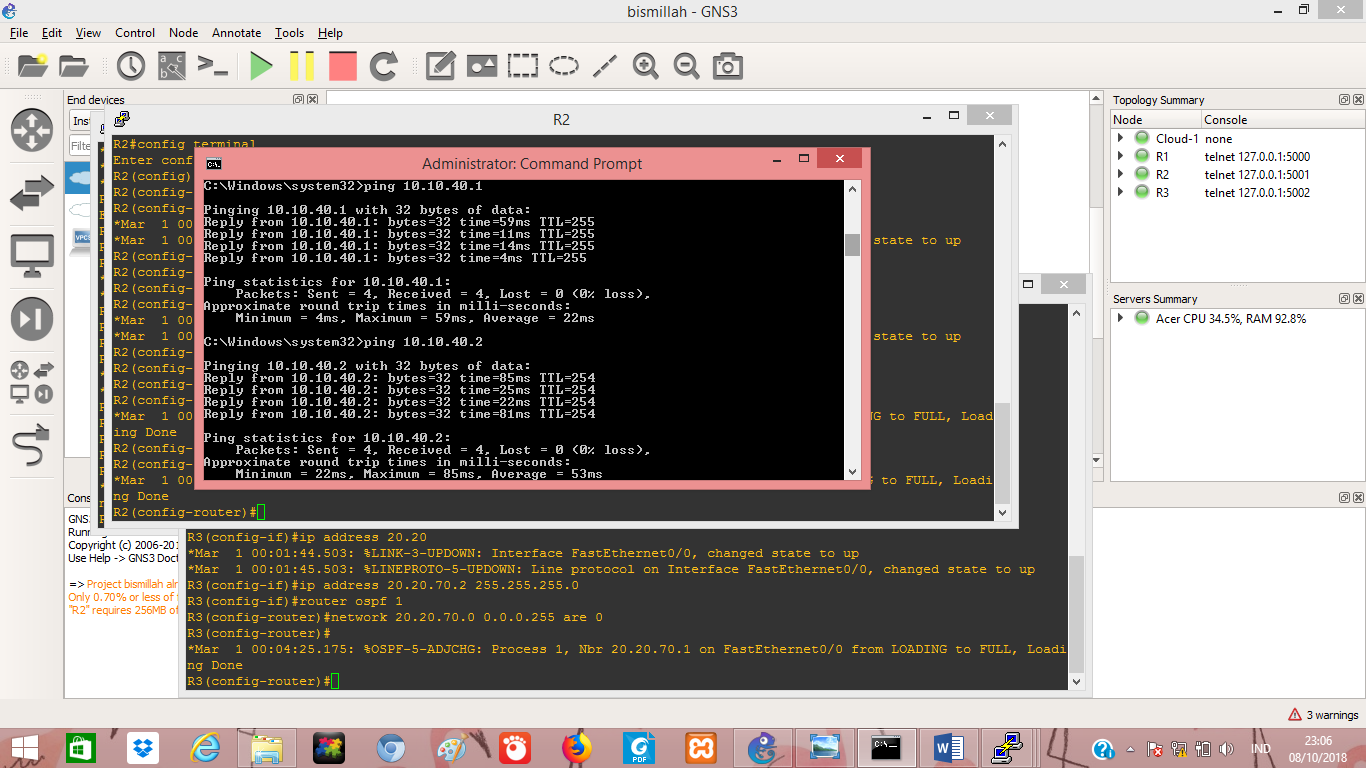
Fo get SNMP-based network traffic results and to find out more about SNMP, the test have been conducted by simulating SNMP. Application used to make SNMP topology using GNS3 application.



**Figure 1.1** *Topology SNMP with GNS3*

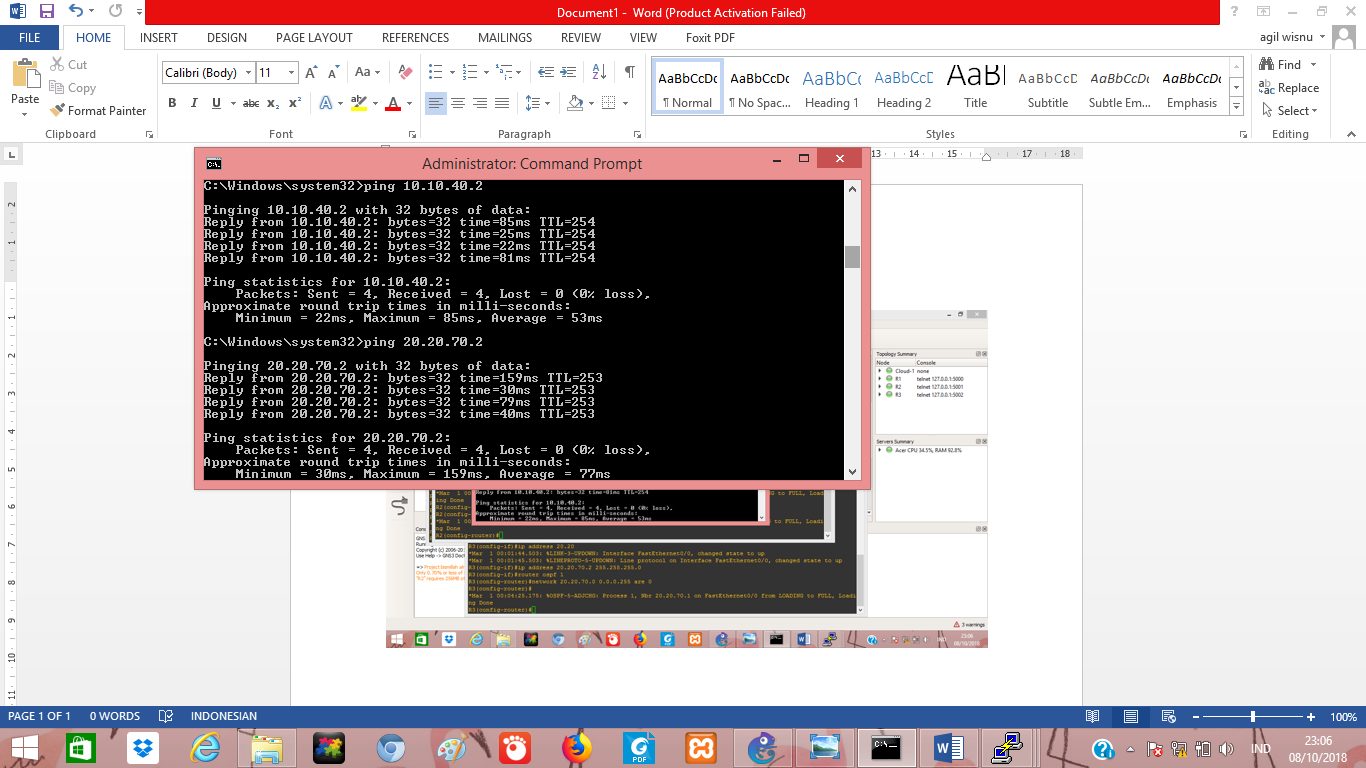
For the test whether the topology that is connected or not, we must do PING on the Command Prompt by using the IP that is connected to each Router as shown below :

1. Test PING Router 1



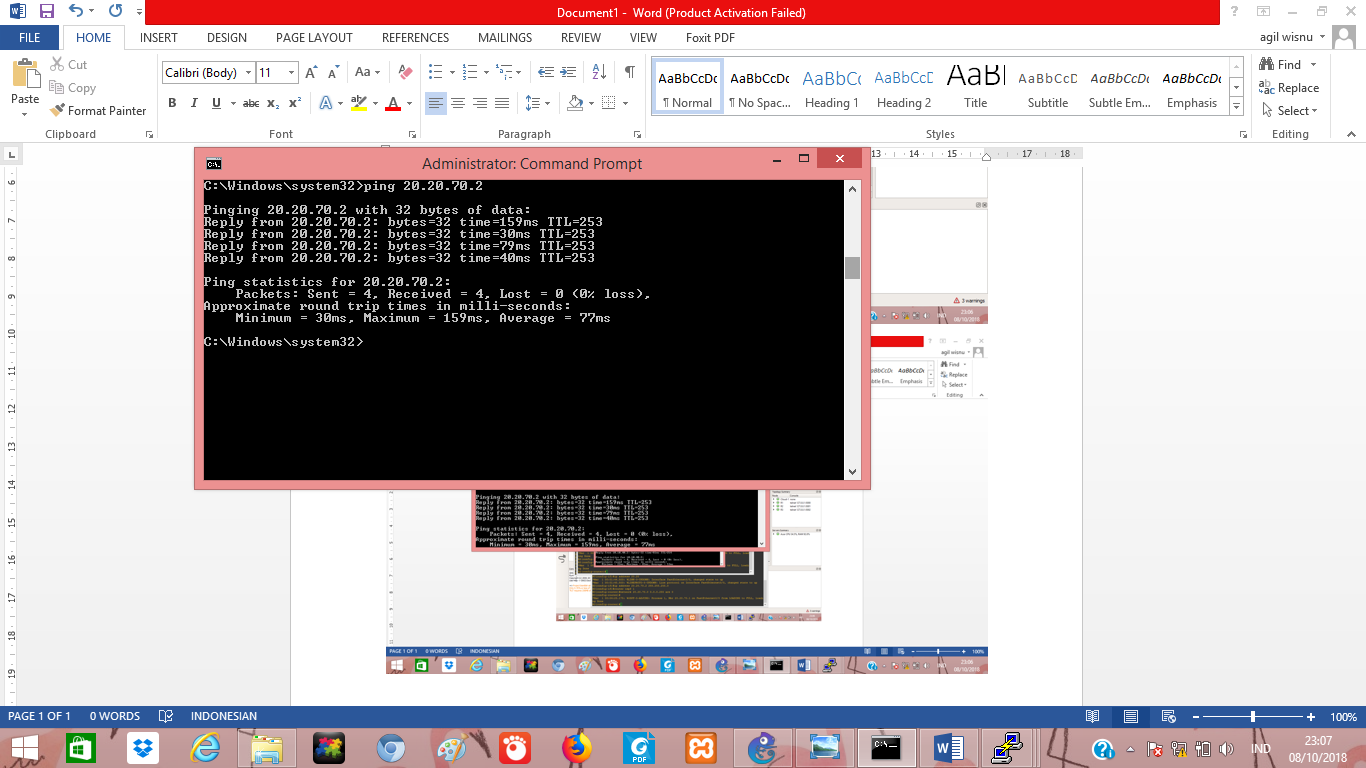
**Figure 1.2** *Test PING Router 1*

1. Test PING Router 2



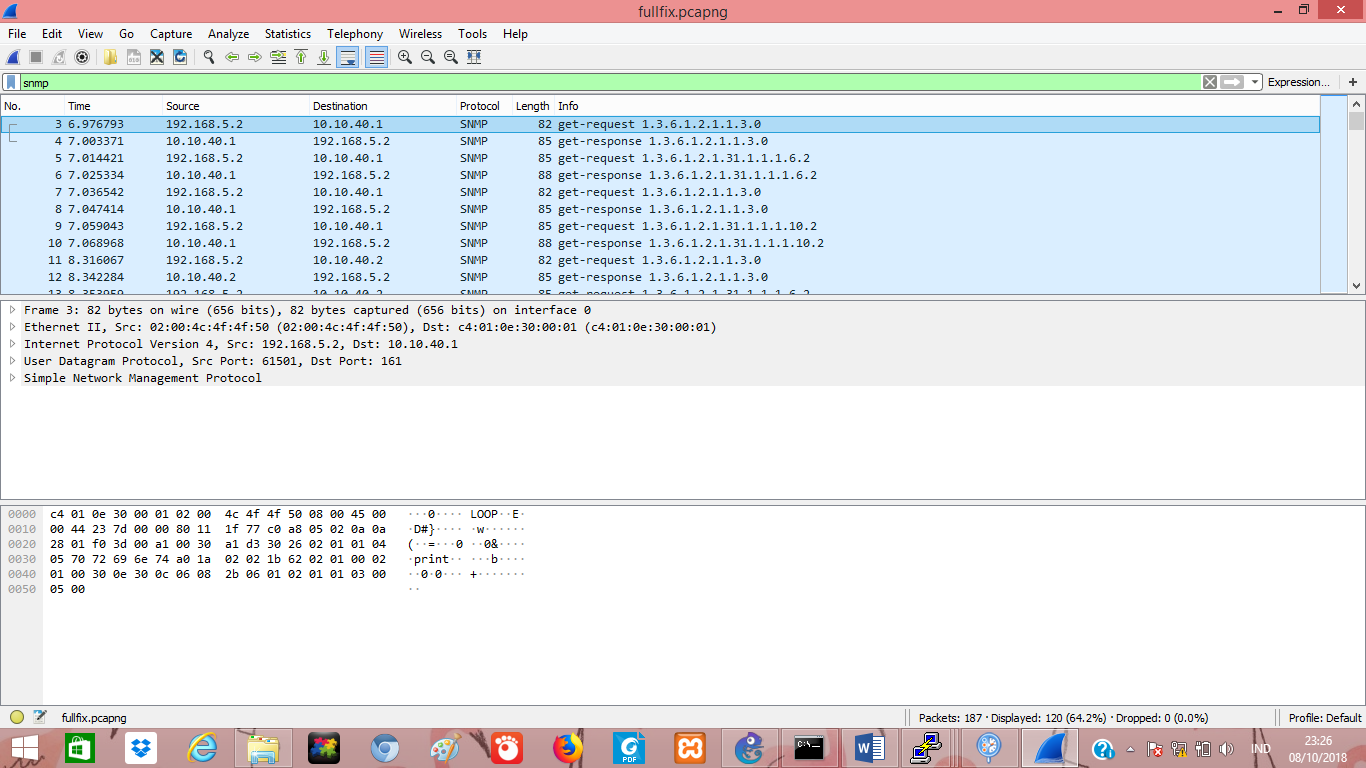
**Figure 1.2** *Test PING Router 2*

1. Test PING Router 3



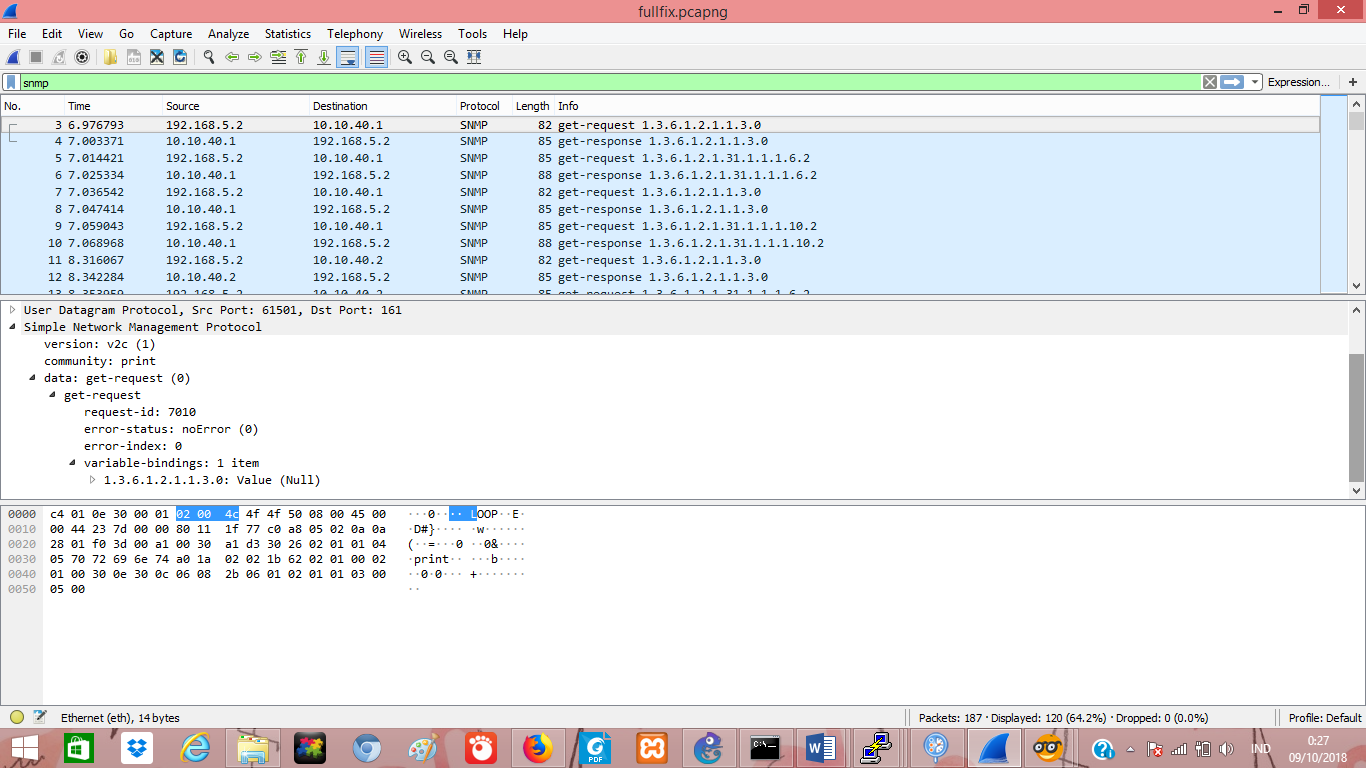
**Figure 1.2** *Test PING Router 3*

After we test, we will get the SNMP Protocol capture results on the Wireshark application as below:



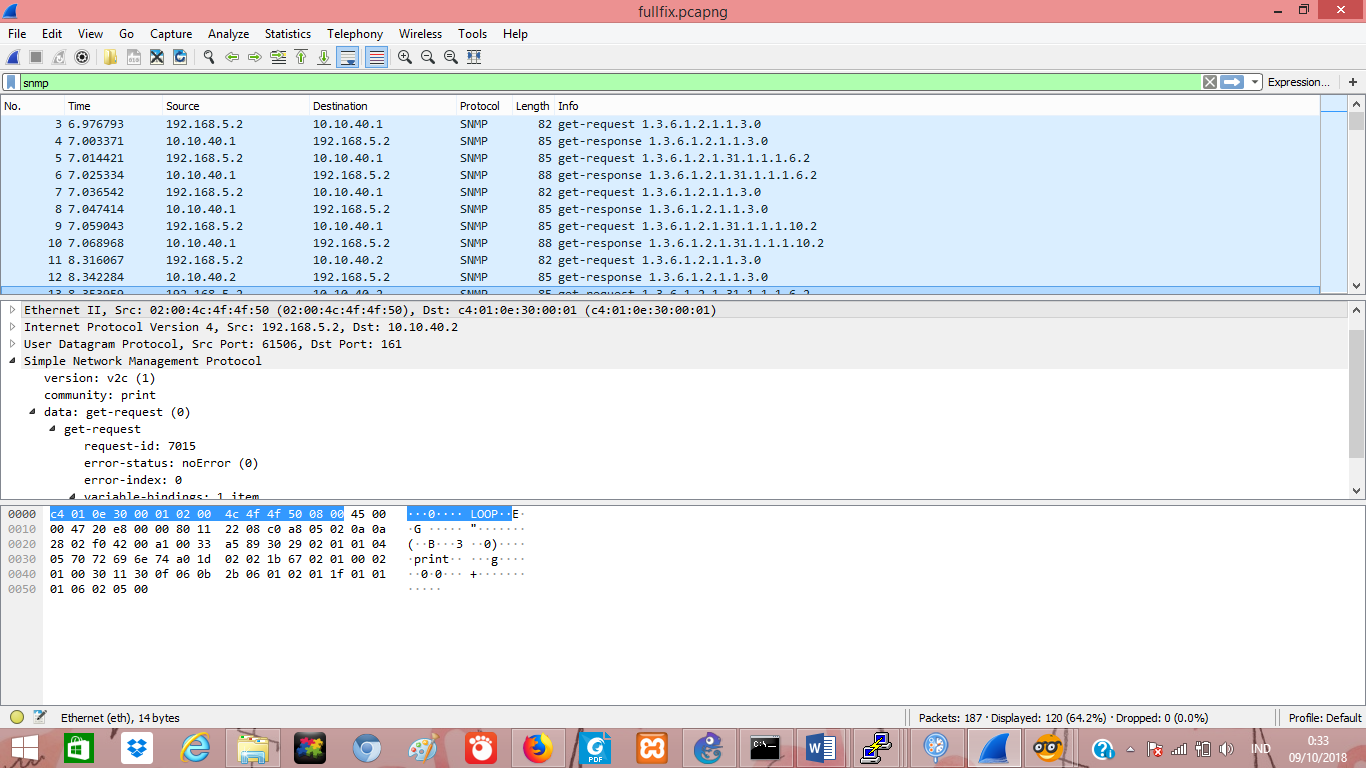
**Figure 1.4** *Capture SNMP Protocol with Wireshark*

Based on capture, the analysis that we can do one of them is that we can see information grouped in Time, Source, Destination, Protocol, etc. Info And to analyze it further then choose the sample with the manager (*Source IP Address* 192.168.5.2) and agent (*IP Address Destination* 10.10.40.1) and *MAC Address* Source (02: 00: 4c: 4f: 4f: 50), *MAC Address Destination* (c4: 01: 0e30: 00: 01). Below is information about *Get Request*.



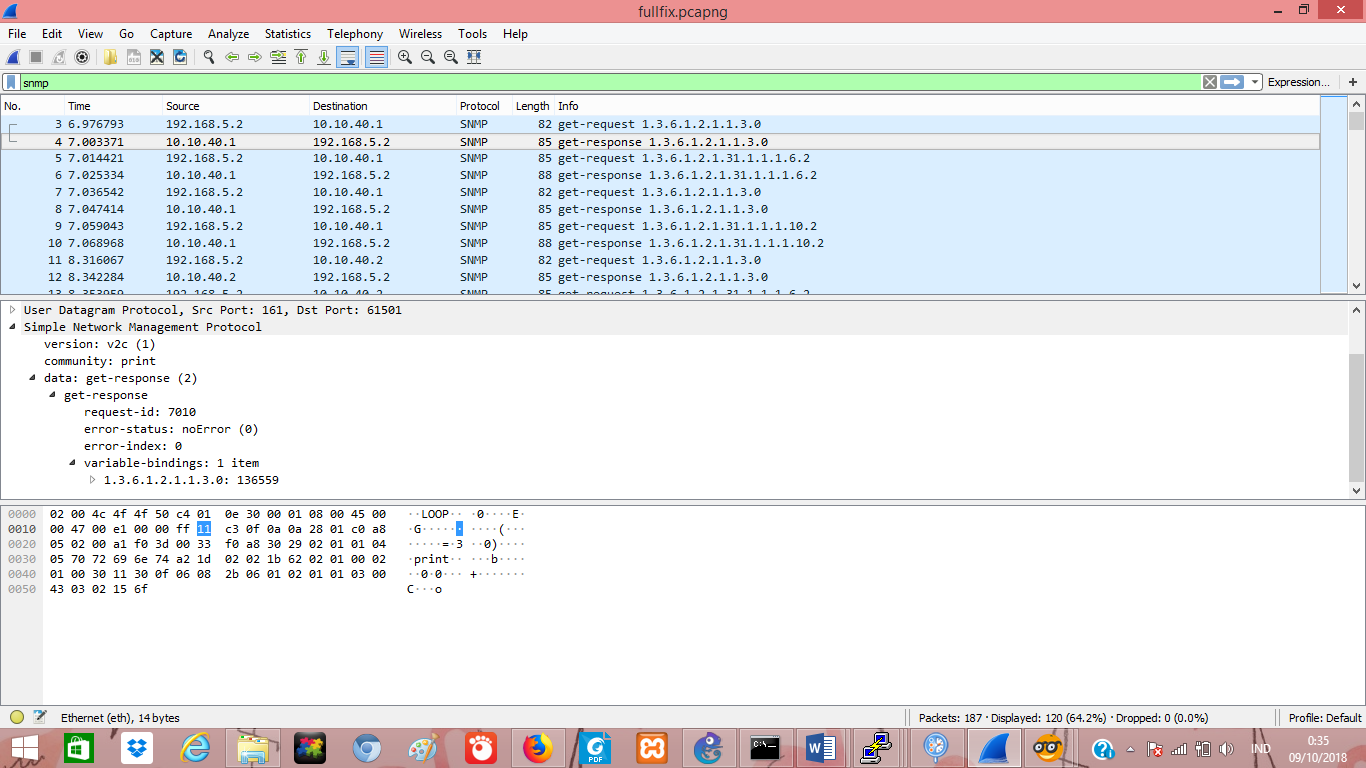
**Figure 1.5** *Get-Request Information*

In this capture we can also find SNMP *Get-Request PDU* information from the manager agent. In the contents of the message we can know the request-id is 7010 with the bindings numbering 1 item, namely: 1.3.6.1.2.1.1.3.0. After being analyzed when the manager has sent *Get-Request* 1.3.6.1.2.1.1.3.0. to the agent, the agent will send Get-respone 1.3.6.1.2.1.1.3.0. *Get-Response* PDU is sent by SNMP agent in reply to a shipment from *Get-Request* PDU.



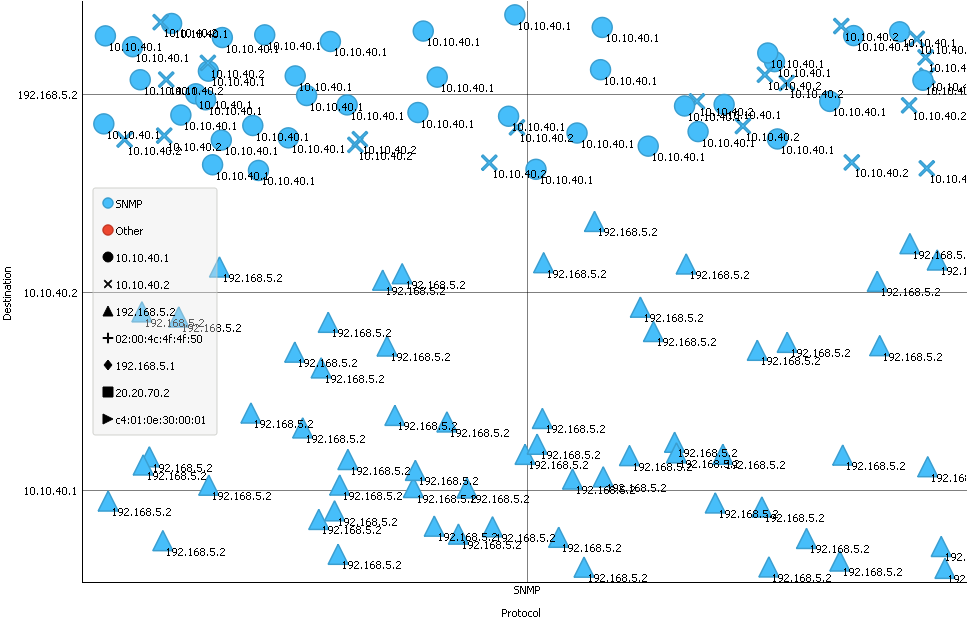
**Figure 1.6** *Sample of agent sent Get-Response to manager*

The next analysis is the information from *Get-Response*, the information obtained is not much different from *Get-Request* as we can know respone-id, etc. Like the picture below :



**Figure 1.7** *Get-Response Information*

After getting data capture by monitoring using Wireshark, then the data obtained can be visualized using the Orange Data mining application. The data that has been obtained in the format (.csv) can be made as data input in the application and we can visualize it as the example below



**Figure 1.8** *Visualization with Orange*

In there visualization was described by using *Protocol* and *Destination* as (x, y) and *Shape* which are used to differentiate each Source for easier to understand data and we can differentiate *Source* that is connected to *Destination*.

Daftar Pustaka

[1] <https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol>