Analisa File Pcap Protokol SNMP

Saat ini sistem informasi merupakan bagian yang sangat penting untuk setiap organisasi/korporasi [1]. Sistem Informasi adalah kombinasi dari teknologi informasi dan aktivitas orang yang menggunakan teknologi itu untuk mendukung operasi dan manajemen. Dalam pengertian tersebut, istilah ini merujuk tidak hanya pada penggunaan organisasi teknologi informasi dan komunikasi (TIK), tetapi juga untuk cara di mana orang berinteraksi dengan teknologi ini dalam mendukung proses bisnis (https://id.wikipedia.org/wiki/Sistem_informasi)

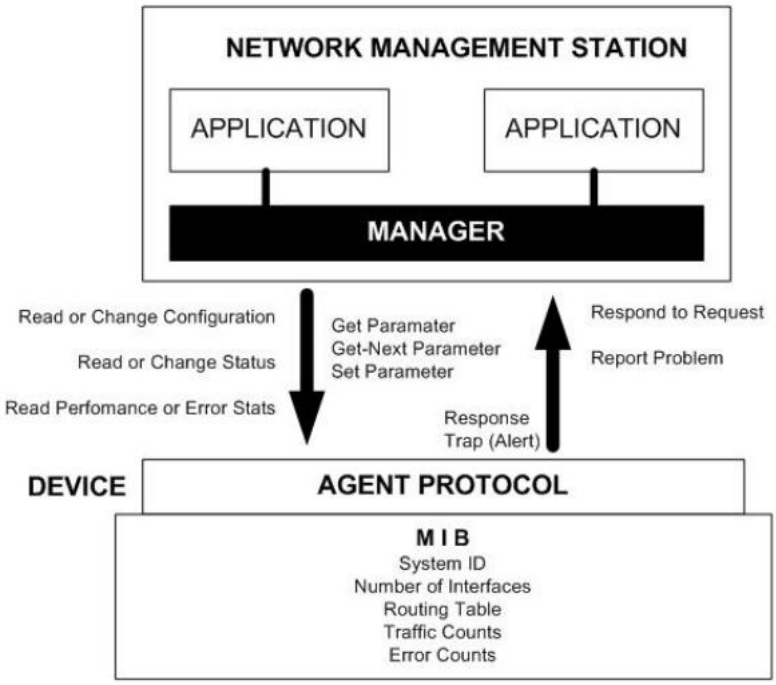
Perkembangan teknologi informasi, khususnya jaringan memungkinkan terjadinya pertukaran informasi yang cepat dan semakin kompleks[1]. Pengaturan jaringan yang baik tentu akan memaksimalkan pemanfaatan informasi tersebut. Oleh sebab itu jaringan harus diatur dan dipantau, sehingga kelancaran pengiriman informasi dapat berjalan baik. Semakin besar dan luas sistem jaringan, maka akan semakin sulit untuk mengatur dan mengawasinya.

Banyaknya *device* yang digunakan dalam infrastruktur jaringan, maka diperlukanlah suatu manajemen jaringan yang baik dan sistem monitoring yang mampu memantau kinerja dari jaringan tersebut, kemudian sistem monitoring yang didesain untuk memantau status infrastuktur LAN/WAN, memastikan *device* tersebut dalam kondisi normal dan aktif, dapat melihat statistik dalam bentuk grafik, pengecekan kondisi sinyal, dapat memprediksi masalah yang akan muncul atau dapat memantau paket data yang lewat di trafik jaringan[2].

Salah satu protokol yang populer digunakan untuk manajemen jaringan adalah Simple Network Management Protocol (SNMP). SNMP merupakan sebuah protokol yang digunakan sebagai standar untuk melakukan pengaturan perangkat-perangkat jaringan[2]. SNMP dapat digunakan untuk mengkonfigurasi device yang jauh, menyediakan sekumpulan operasi yang dapat melakukan pengelolaan beberapa perangkat jaringan secara jarak jauh sehingga monitoring dapat dilakukan tidak hanya pada *Local Area Network* (LAN) tapi juga dapat dioperasikan pada skala jaringan yang lebih luas seperti *Wide Area Network* (WAN), mendeteksi kesalahan jaringan atau akses

yang tidak cocok, dan mengaudit pemakaian jaringan[1,2]. SNMP adalah protocol pada level aplikasi yang merupakan bagian dari protokol TCP/IP, menggunakan model UDP untuk membentuk fungsi transport[4]. Sampai sekarang terdapat versi dari SNMP: versi 1 (SNMPv1) dan versi 2 (SNMPv2), dan versi 3 (SNMPv3). ketiganya mempunyai fungsi dasar yang sama, tetapi semakin mengalami peningkatan versi, kemampuan dan fungsi yang dimiliki bertambah[abstrak].

Elemen-elemen SNMP



(**Gambar 1:** Interaksi Manager dan Agent[2])

1. **Manager**

   Manager adalah pelaksana dan manajemen jaringan. Pada kenyataannya manager ini merupakan komputer biasa yang ada pada jaringan yang mengoperaksikan perangkat lunak untuk manajemen jaringan. Manager ini terdiri atas satu proses atau lebih yang berkomunikasi dengan agen-agennya dan dalam jaringan. Manajer akan mengumpulkan informasi dari agen dari jaringan yang diminta oleh administrator saja bukan semua informasi yang dimiliki agen.

2. **MIB atau Manager Information Base**

   Dapat dikatakan sebagai struktur basis data variabel dari elemen jaringan yang dikelola. Struktrur ini bersifat hierarki dan memiliki aturan sedemikian rupa sehingga informasi setiap variabel dapat dikelola atau ditetapkan dengan mudah. Berikut adalah struktur dari MIB, yaitu:

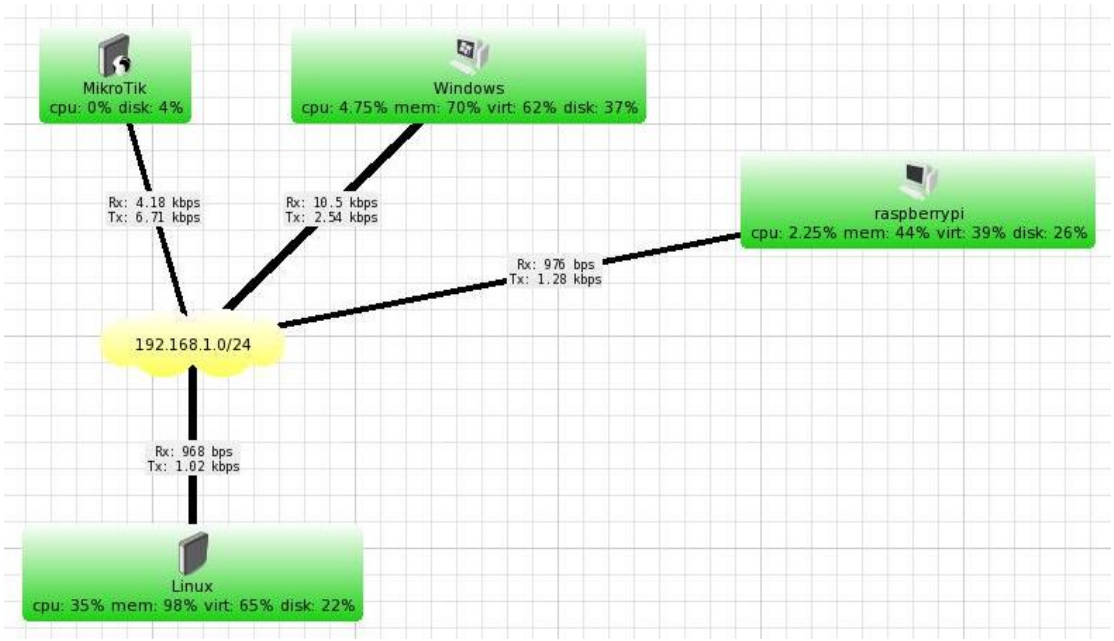
   - Setiap object mempunyai ID unik (OID).
   - MIB mengasosiasikan setiap OID menggunakan label dan parameter lain.
   - MIB bertindak sebagai kamus data digunakan untuk menyusun terjemahan pesan SNMP.

3. **Agent**

   Agent merupakan perangkat lunak yang dijalankan disetiap elemen jaringan yang dikelola. Setiap agen mempunyai basis data variabel yang bersifat lokal yang menerangkan keadaan dan berkas aktivitasnya dan pengaruhnya terhadap operasi.

Untuk mendapatkan hasil pcap traffic jaringan berbasis SNMP dan untuk mengetehaui lebih dalam lagi mengenai SNMP, maka telah dilakukan percobaan di Laboratorium Computer and Networks (Comnets) Fakultas Ilmu Komputer Universitas Sriwijaya pada hari Senin (10 Oktober 2016).

Berikut adalah topologi hasil percobaan menggunakan aplikasi *The Dude. The Dude* adalah aplikasi buatan Mikrotik yang berfungsi untuk memonitor jaringan komputer. *The Dude* akan secara otomatis membaca atau mendeteksi setiap perangat yang terhubung ke jaringan yang satu segment[5].

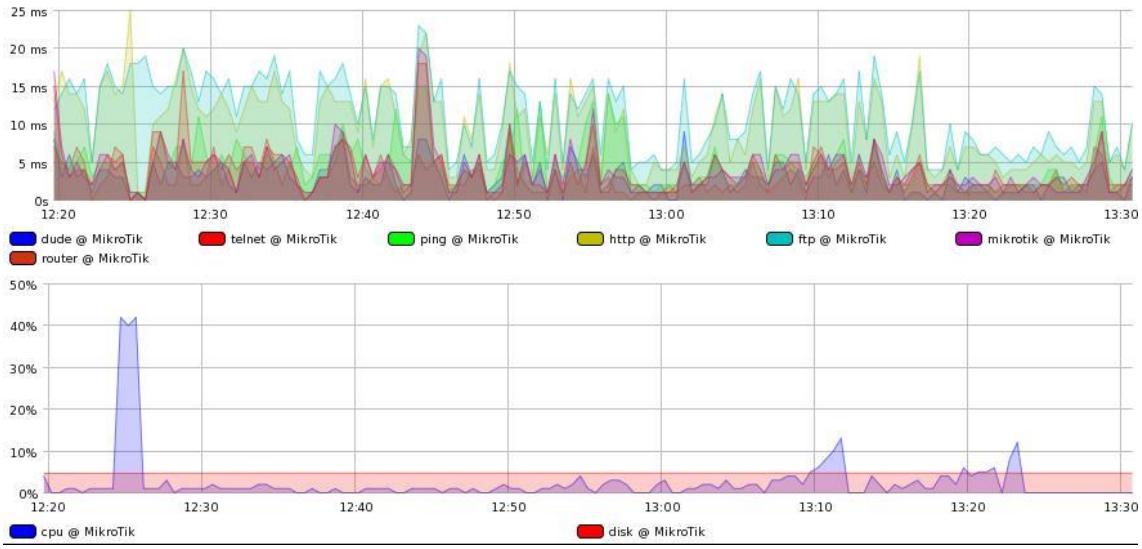


(**Gambar 2:** Topologi Jaringan yang dirancang)

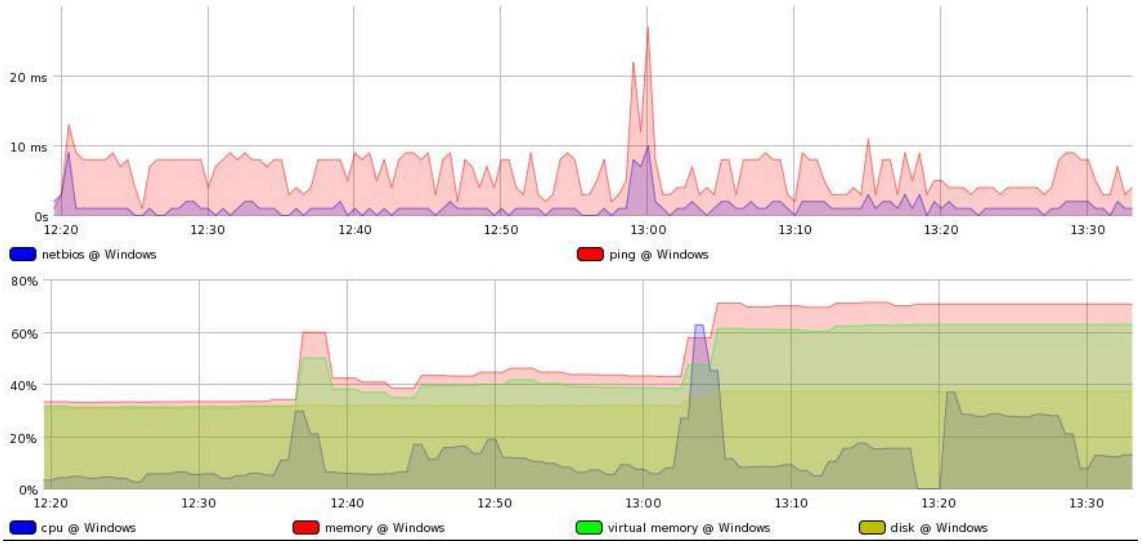
Device	***IP Address***	**Fungsi**
Mikrotik (Server)	192.168.1.1	Manager
Windows (Client)	192.168.1.2	Agent
Linux (Client)	192.168.1.3	Agent
Raspberry Pi (Client)	192.168.1.4	Agent

(**Tabel 1:** informasi device)

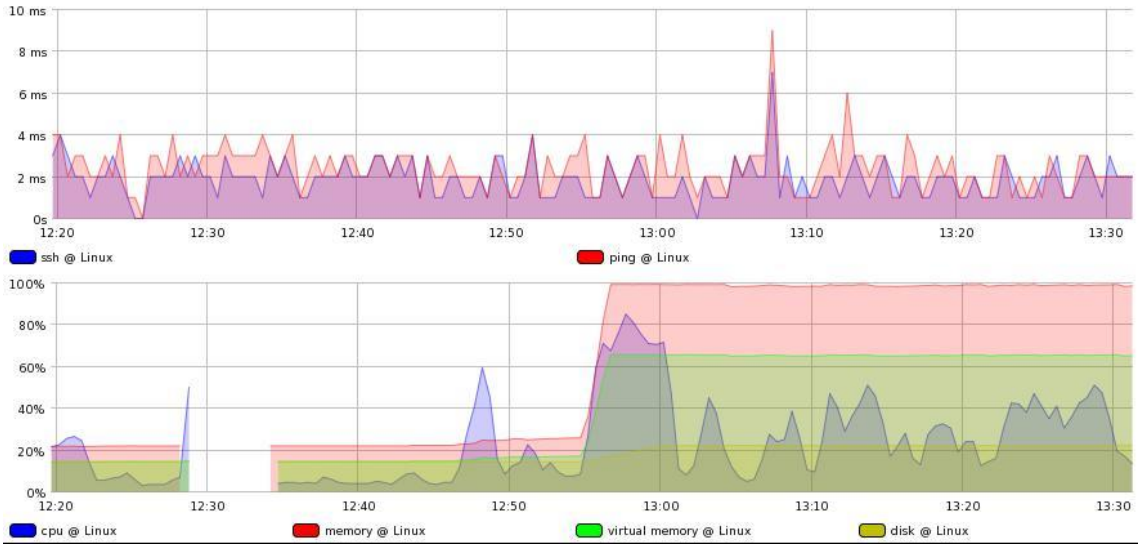
Berikut adalah traffic dari setiap *device* :



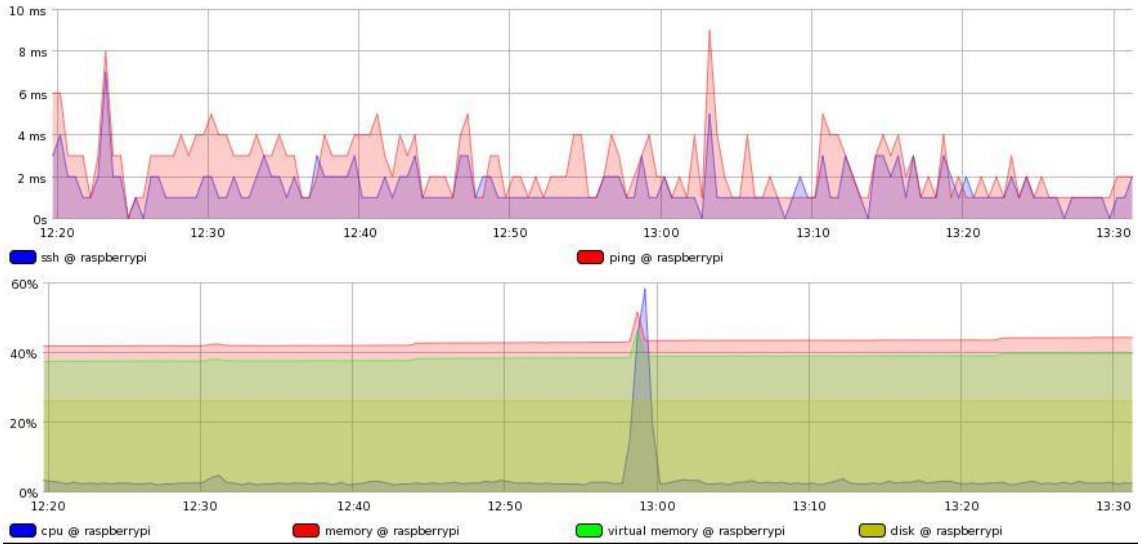
(**Gambar 3:** Traffic Mikrotik)



(**Gambar 4:** Traffic Windows)

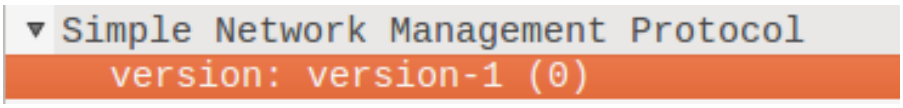


(**Gambar 5:** Traffic Linux)

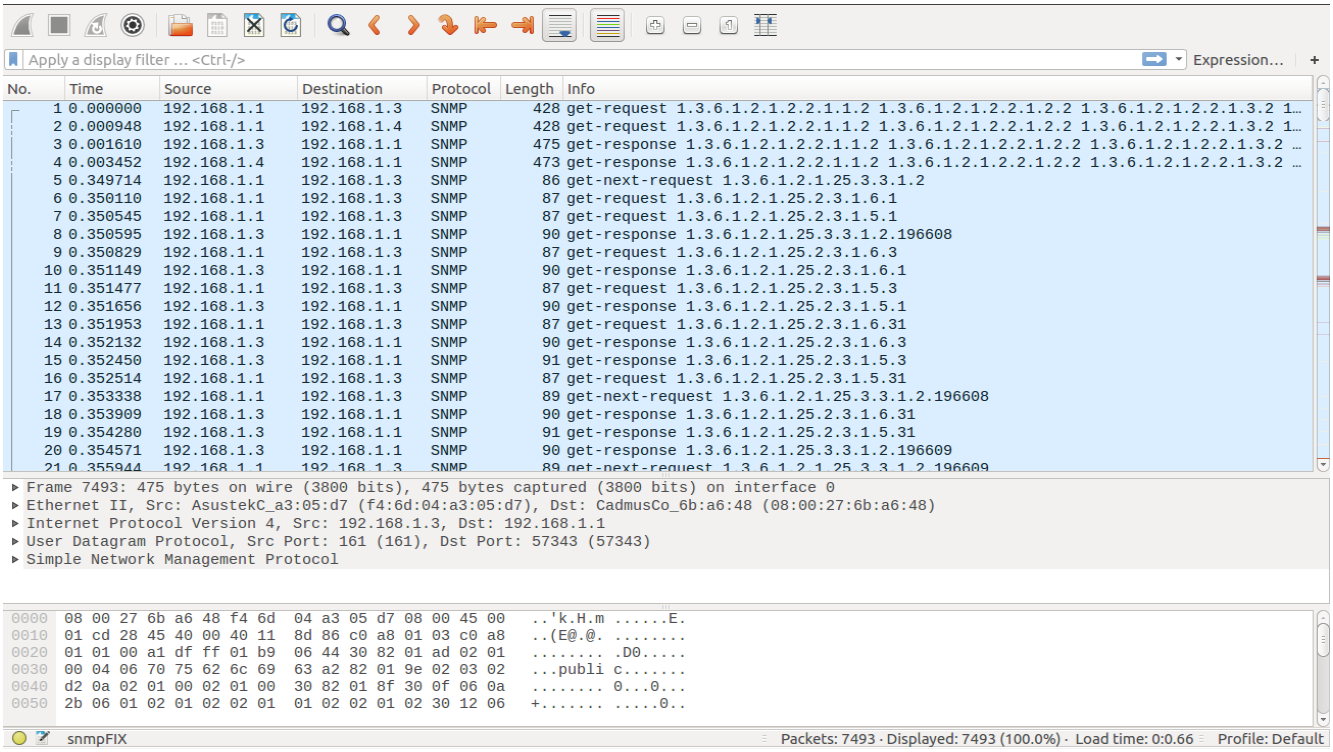


(**Gambar 6:** Traffic Raspberry Pi)

Setelah melakukan percobaan, maka didapatkanlah hasil capture pcap SNMP. Protokol SNMP yang digunakan adalah versi 1 (SNMPv1).



(**Gambar 7:** Versi SNMP)



(**Gambar 8:** Hasil Capture Pcap Wireshark)

Berdasarkan gambar (sekian), dapat kita lihat pada bagian INFO bahwa setiap pesan SNMP terdapat Protocol Data Unit (PDU). PDU merupakan unit data yang terdiri atas sebuah header dan beberapa data yang ditempelkan. SNMP PDU digunakan untuk komunikasi antara manager SNMP dan agent SNMP [4]

Arsitektur SNMP Versi 1 mendefinisikan tipe pesan dari PDU sebagai berikut[4]:

***1. Get-Request PDU* :** dikirim oleh SNMP manager untuk mengambil satu atau lebih variabel MIB yang diminta yang telah ditentukan oleh PDU.

***2. Get-Next-Request PDU* :** dikirim oleh SNMP manager untuk mengambil variabel MIB berikutnya. Anda dapat memiliki beberapa pernintaan di PDU.

***3. Set-Request PDU* :** dikirim oleh SNMP manager untuk mengatur satu atau lebih variabel MIB dengan nilai yang telah ditentukan dalam PDU.

***4. Get-Response PDU* :** dikirim oleh SNMP agent dalam menanggapi *Get-Request PDU, Get-Next-Request PDU* atau *Set-Request PDU*

***5. Trap PDU* :** berisikan pesan yang tidak diinginkan yang dikirim oleh SNMP agent untuk memberitahu SNMP manager tentang peristiwa penting yang terjadi di agent.

Kemudian pada bagian INFO terdapat juga OID dari MIB. OID adalah angka unik yang dipisahkan oleh titik-titik. Setiap OID memiliki arti masing-masing. Untuk mengetahui artinya, lihat tabel dibawah ini:

SNMP OID	Description
.1.3.6.1.4.1.2021.9.1.7.1 UCD-SNMP-MIB::dskAvail.1	*Disk space available in / directory*
.1.3.6.1.4.1.2021.9.1.7.2 UCD-SNMP-MIB::dskAvail.2	*Disk space available in /var directory*
.1.3.6.1.4.1.2021.9.1.8.1 UCD-SNMP-MIB::dskUsed.1	*Disk space used in / directory*
.1.3.6.1.4.1.2021.9.1.8.2 UCD-SNMP-MIB::dskUsed.2	*Disk space used in /var directory*
.1.3.6.1.2.1.25.2.3.1.5.1	*Total memory available*

SNMP OID	Description
HOST-RESOURCES-MIB::hrStorageSize.1	
.1.3.6.1.2.1.25.2.3.1.6.1 HOST-RESOURCES-MIB::hrStorageUsed.1	*Memory in use*
.1.3.6.1.4.1.2021.8.1.101.1 UCD-SNMP-MIB::extOutput.1	*Open monitored session count*
.1.3.6.1.4.1.2021.8.1.101.2 UCD-SNMP-MIB::extOutput.2	*Requests logged by the current sniffer process (set to zero for each restart)*
.1.3.6.1.4.1.2021.8.1.101.3 UCD-SNMP-MIB::extOutput.3	*Last session timestamp*
.1.3.6.1.4.1.2021.8.1.101.4 UCD-SNMP-MIB::extOutput.4	*Last construct timestamp*
.1.3.6.1.4.1.2021.8.1.101.5 UCD-SNMP-MIB::extOutput.5	*Memory used by the sniffer process*
.1.3.6.1.4.1.2021.8.1.101.7 UCD-SNMP-MIB::extOutput.7	*Packets in on ETH1/ out on ETH2; usually only one number (inbound) when a SPAN port or TAP is used*

SNMP OID	Description
.1.3.6.1.4.1.2021.8.1.101.8 UCD-SNMP-MIB::extOutput.8	*Same as above, for ETH3 / ETH4*
.1.3.6.1.4.1.2021.8.1.101.9 UCD-SNMP-MIB::extOutput.9	*Same as above, for ETH5 / ETH6*

(**Tabel 2:** Deskripsi OID)

Object Name	Object Identifier
host	1.3.6.1.2.1.25
hrSystem	1.3.6.1.2.1.25.1
hrSystemUptime	1.3.6.1.2.1.25.1.1
hrSystemDate	1.3.6.1.2.1.25.1.2
hrSystemInitialLoadDevice	1.3.6.1.2.1.25.1.3
hrSystemInitialLoadParameters	1.3.6.1.2.1.25.1.4
hrSystemNumUsers	1.3.6.1.2.1.25.1.5
hrSystemProcesses	1.3.6.1.2.1.25.1.6
hrSystemMaxProcesses	1.3.6.1.2.1.25.1.7
hrStorage	1.3.6.1.2.1.25.2
hrStorageTypes	1.3.6.1.2.1.25.2.1
hrMemorySize	1.3.6.1.2.1.25.2.2
hrStorageTable	1.3.6.1.2.1.25.2.3
hrStorageEntry	1.3.6.1.2.1.25.2.3.1
hrStorageIndex	1.3.6.1.2.1.25.2.3.1.1

hrStorageType	1.3.6.1.2.1.25.2.3.1.2
hrStorageDescr	1.3.6.1.2.1.25.2.3.1.3
hrStorageAllocationUnits	1.3.6.1.2.1.25.2.3.1.4
hrStorageSize	1.3.6.1.2.1.25.2.3.1.5
hrStorageUsed	1.3.6.1.2.1.25.2.3.1.6
hrStorageAllocationFailures	1.3.6.1.2.1.25.2.3.1.7
hrDevice	1.3.6.1.2.1.25.3
hrDeviceTypes	1.3.6.1.2.1.25.3.1
hrDeviceTable	1.3.6.1.2.1.25.3.2
hrDeviceEntry	1.3.6.1.2.1.25.3.2.1
hrDeviceIndex	1.3.6.1.2.1.25.3.2.1.1
hrDeviceType	1.3.6.1.2.1.25.3.2.1.2
hrDeviceDescr	1.3.6.1.2.1.25.3.2.1.3
hrDeviceID	1.3.6.1.2.1.25.3.2.1.4
hrDeviceStatus	1.3.6.1.2.1.25.3.2.1.5
hrDeviceErrors	1.3.6.1.2.1.25.3.2.1.6
hrProcessorTable	1.3.6.1.2.1.25.3.3
hrProcessorEntry	1.3.6.1.2.1.25.3.3.1
hrProcessorFrwID	1.3.6.1.2.1.25.3.3.1.1
hrProcessorLoad	1.3.6.1.2.1.25.3.3.1.2
hrNetworkTable	1.3.6.1.2.1.25.3.4
hrNetworkEntry	1.3.6.1.2.1.25.3.4.1
hrNetworkIfIndex	1.3.6.1.2.1.25.3.4.1.1
hrPrinterTable	1.3.6.1.2.1.25.3.5
hrPrinterEntry	1.3.6.1.2.1.25.3.5.1

hrPrinterStatus	1.3.6.1.2.1.25.3.5.1.1
hrPrinterDetectedErrorState	1.3.6.1.2.1.25.3.5.1.2
hrDiskStorageTable	1.3.6.1.2.1.25.3.6
hrDiskStorageEntry	1.3.6.1.2.1.25.3.6.1
hrDiskStorageAccess	1.3.6.1.2.1.25.3.6.1.1
hrDiskStorageMedia	1.3.6.1.2.1.25.3.6.1.2
hrDiskStorageRemoveble	1.3.6.1.2.1.25.3.6.1.3
hrDiskStorageCapacity	1.3.6.1.2.1.25.3.6.1.4
hrPartitionTable	1.3.6.1.2.1.25.3.7
hrPartitionEntry	1.3.6.1.2.1.25.3.7.1
hrPartitionIndex	1.3.6.1.2.1.25.3.7.1.1
hrPartitionLabel	1.3.6.1.2.1.25.3.7.1.2
hrPartitionID	1.3.6.1.2.1.25.3.7.1.3
hrPartitionSize	1.3.6.1.2.1.25.3.7.1.4
hrPartitionFSIndex	1.3.6.1.2.1.25.3.7.1.5
hrFSTable	1.3.6.1.2.1.25.3.8
hrFSEntry	1.3.6.1.2.1.25.3.8.1
hrFSIndex	1.3.6.1.2.1.25.3.8.1.1
hrFSMountPoint	1.3.6.1.2.1.25.3.8.1.2
hrFSRemoteMountPoint	1.3.6.1.2.1.25.3.8.1.3
hrFSType	1.3.6.1.2.1.25.3.8.1.4
hrFSAccess	1.3.6.1.2.1.25.3.8.1.5
hrFSBootable	1.3.6.1.2.1.25.3.8.1.6
hrFSStorageIndex	1.3.6.1.2.1.25.3.8.1.7
hrFSLastFullBackupDate	1.3.6.1.2.1.25.3.8.1.8

hrFSLastPartialBackupDate	1.3.6.1.2.1.25.3.8.1.9
hrFSTypes	1.3.6.1.2.1.25.3.9
hrSWRun	1.3.6.1.2.1.25.4
hrSWOSIndex	1.3.6.1.2.1.25.4.1
hrSWRunTable	1.3.6.1.2.1.25.4.2
hrSWRunEntry	1.3.6.1.2.1.25.4.2.1
hrSWRunIndex	1.3.6.1.2.1.25.4.2.1.1
hrSWRunName	1.3.6.1.2.1.25.4.2.1.2
hrSWRunID	1.3.6.1.2.1.25.4.2.1.3
hrSWRunPath	1.3.6.1.2.1.25.4.2.1.4
hrSWRunParameters	1.3.6.1.2.1.25.4.2.1.5
hrSWRunType	1.3.6.1.2.1.25.4.2.1.6
hrSWRunStatus	1.3.6.1.2.1.25.4.2.1.7
hrSWRunPerf	1.3.6.1.2.1.25.5
hrSWRunPerfTable	1.3.6.1.2.1.25.5.1
hrSWRunPerfEntry	1.3.6.1.2.1.25.5.1.1
hrSWRunPerfCPU	1.3.6.1.2.1.25.5.1.1.1
hrSWRunPerfMem	1.3.6.1.2.1.25.5.1.1.2
hrSWInstalled	1.3.6.1.2.1.25.6
hrSWInstalledLastChange	1.3.6.1.2.1.25.6.1
hrSWInstalledLastUpdateTime	1.3.6.1.2.1.25.6.2
hrSWInstalledTable	1.3.6.1.2.1.25.6.3
hrSWInstalledEntry	1.3.6.1.2.1.25.6.3.1
hrSWInstalledIndex	1.3.6.1.2.1.25.6.3.1.1
hrSWInstalledName	1.3.6.1.2.1.25.6.3.1.2

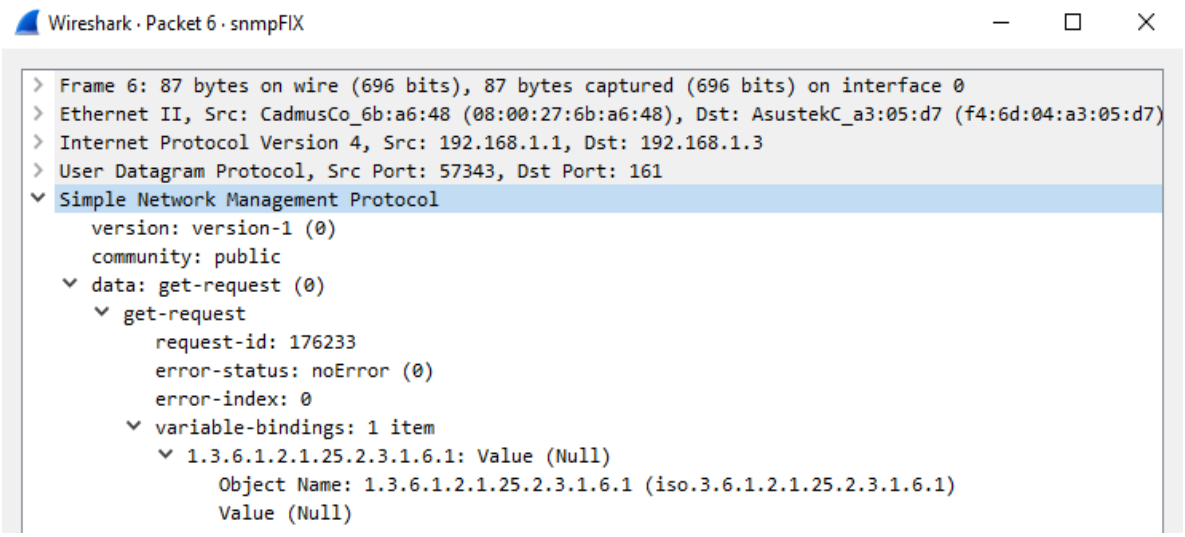
hrSWInstalledID	1.3.6.1.2.1.25.6.3.1.3
hrSWInstalledType	1.3.6.1.2.1.25.6.3.1.4
hrSWInstalledDate	1.3.6.1.2.1.25.6.3.1.5
hrMIBAdminInfo	1.3.6.1.2.1.25.7
hostResourcesMibModule	1.3.6.1.2.1.25.7.1
hrMIBCompliances	1.3.6.1.2.1.25.7.2
hrMIBCompliance	1.3.6.1.2.1.25.7.2.1
hrMIBGroups	1.3.6.1.2.1.25.7.3
hrSystemGroup	1.3.6.1.2.1.25.7.3.1
hrStorageGroup	1.3.6.1.2.1.25.7.3.2
hrDeviceGroup	1.3.6.1.2.1.25.7.3.3
hrSWRunGroup	1.3.6.1.2.1.25.7.3.4
hrSWRunPerfGroup	1.3.6.1.2.1.25.7.3.5
hrSWInstalledGroup	1.3.6.1.2.1.25.7.3.6

(**Tabel 3:** Informasi HOST RESOURCE MIB[6])

Sebagai sampel analisa pcap SNMP, penulis memilih relasi antara manager (IP Address *Souce* 192.168.1.1) dan agent (IP *Address Destination* 192.168.1.3). Pada pcap SNMP kita dapat melihat MAC *Address Source* yaitu 08:00:27:6b:a6:48 dan MAC *Address Destination* yaitu f4:6d:04:a3:05:d7.

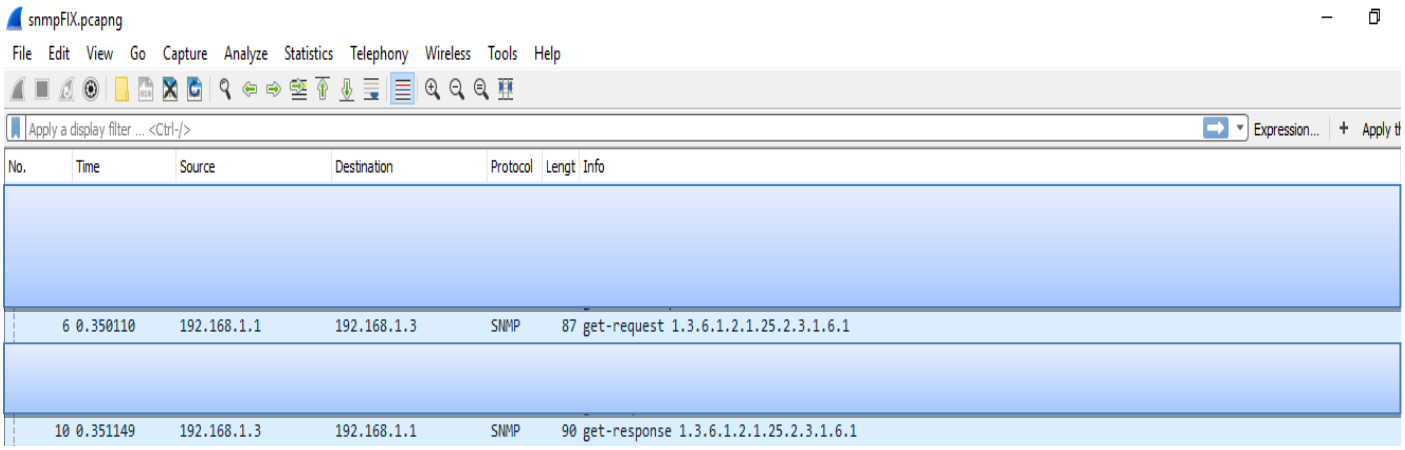
Berikut ini adalah informasi SNMP ***Get-Request PDU*** dari manager ke agent pada Packet 6 yang penulis pilih sebagai sampel analisa. Pada isi pesan tersebut kita dapat mengetahui *request-id* adalah 176233, dengan *variable-bindings* berjumlah 1 item, yaitu: 1.3.6.1.2.1.25.2.3.1.6.1.

Dilihat pada **Tabel 2**, SNMP OID dengan iso 1.3.6.1.2.1.25.2.3.1.6.1 *(HOST-RESOURCES-MIB::hrStorageUsed.1)* berisikan pesan tentang memori yang digunakan.

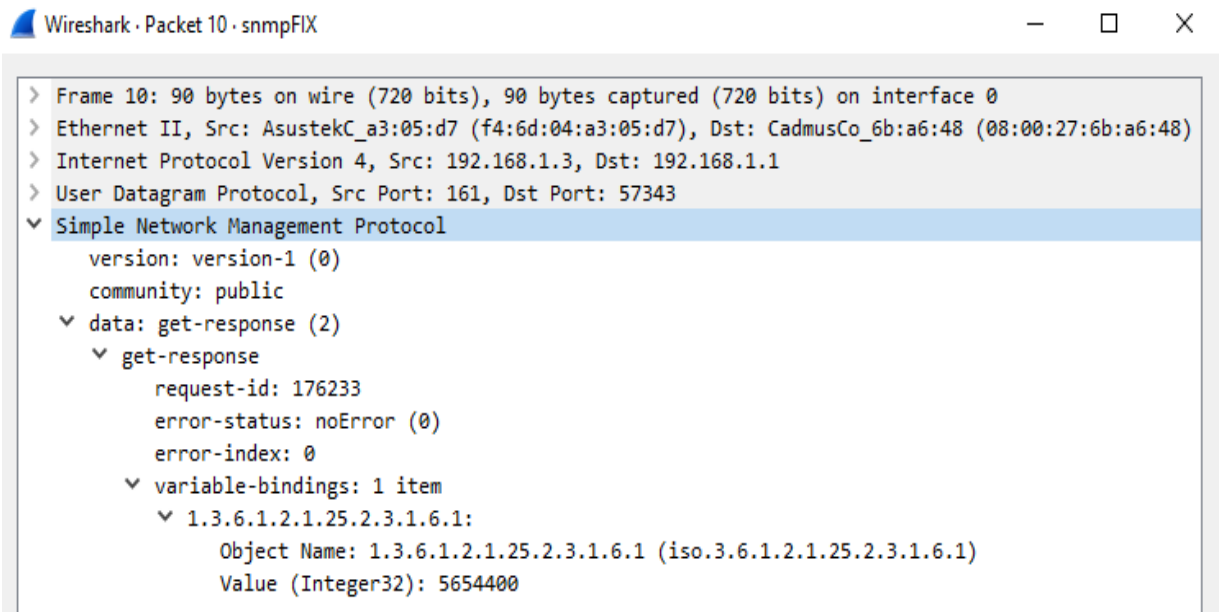


(**Gambar 9:** Isi Informasi Get-Request 1.3.6.1.2.1.25.2.3.1.6.1)

Setelah diperhatikan, ketika manager telah mengirim *Get-Request 1.3.6.1.2.1.25.2.3.1.6.1* kepada agent, maka agent akan mengirim *Get-Respone 1.3.6.1.2.1.25.2.3.1.6.1* (dapat dilihat pada paket 10 file pcap). ***Get-Respone PDU*** dikirim oleh SNMP agent untuk menanggapi *Get-Request PDU, Get-Next-Request PDU* atau *Set-Request PDU.*



(**Gambar 10:** Bukti bahwa agent telah mengirim *Get-Respone* 1.3.6.1.2.1.25.2.3.1.6.1 kepada manager)

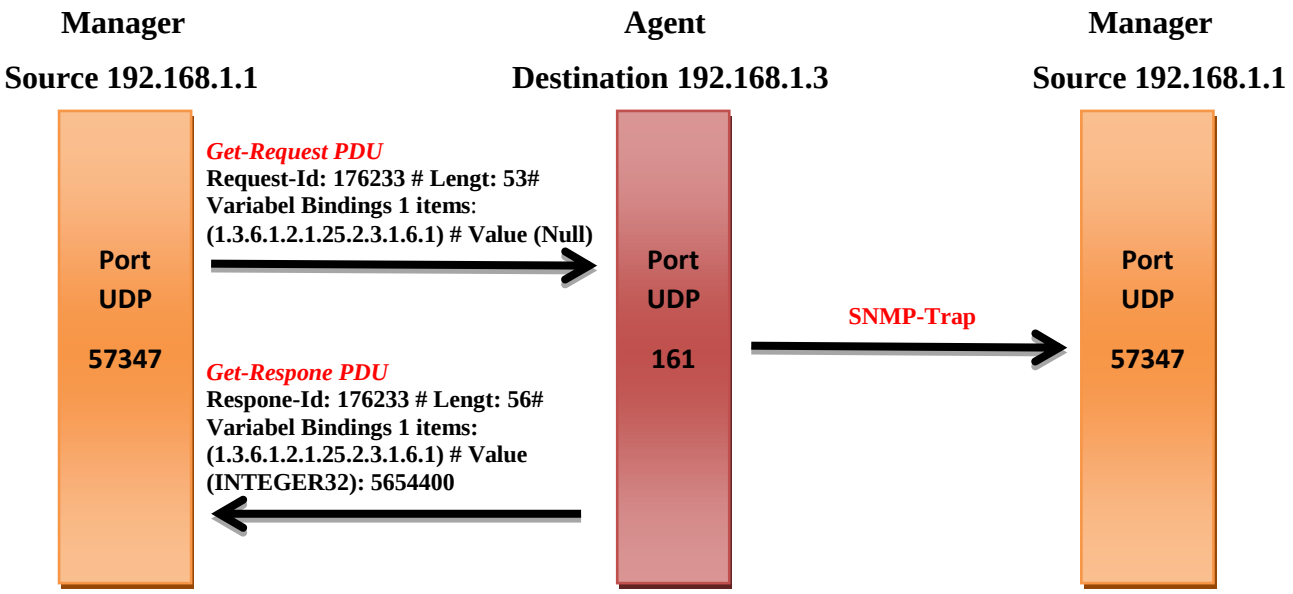


(**Gambar 11:** Isi Informasi *Get-Respone* 1.3.6.1.2.1.25.2.3.1.6.1)

Pada informasi paket 10, dapat dilihat pada sisi *get-response* bahwa *respone-id* adalah 176233 dan iso 1.3.6.1.2.1.25.2.3.1.6.1, nilai-nilai tersebut sama seperti *request-id* dan iso pada *get-request*.

Perbedaan antara ***Get-Request*** dan ***Get-Respone*** terdapat pada nilai *Value*-nya. Pada saat pertama kali manager mengirim *Get-Request* kepada agent, nilai *Value* yaitu Null. Kemudian agent menanggapi permintaan dari manager. maka agent akan mengirimkan *Get-Respone* ke manager. Di detail informasi *get-respone*, kita dapat melihat bahwa nilai Value adalah 5654400 yang bertipe INTEGER32, lalu nilai Value itulah yang akan di kirim kepada manager.

Dibawah ini adalah *three way handshake* SNMP :



(**Gambar 12:** *Three Way Handshake* SNMP)

DAFTAR PUSTAKA

[1] M. Rizky, D. Jurusan, T. Elektro, F. Teknologi, and U. Andalas, "IMPLEMENTASI PROTOKOL SNMP UNTUK JARINGAN Abstrak," vol. 1, no. 1, pp. 15–19, 2013.

[2] D. Stiawan, D. Jurusan, S. Komputer, and F. Unsri, "Network Management : Optimalisasi untuk mencapai High Reliability Sisi Teknis …," no. i.

[3] G. D. Harmawan and U. Gunadarma, "Aplikasi Pemantauan Jaringan Dengan Agen SNMP Menggunakan Pemrograman TCL Dengan Perluasan Scotty."

[4] Admin. "IBM Knowledge Center: Protocol data units (PDUs)" http://www.ibm.com/support/knowledgecenter/SSB23S_1.1.0.13/gtpc1/pdus.html (Diakses pada Selasa, 11 Oktober 2016)

[5] Agung, Ricky. 2014. "Cara Memantau dan Memonitor Jaringan Mikrotik Menggunakan The Dude" https://mikrotikindo.blogspot.co.id/2014/11/cara-memonitor-jaringan-mikrotik-menggunakan-thedude.html (Diakses pada Selasa, 11 Oktober 2016)

[6] OidView. "HOST-RESOURCES-MIB". http://www.oidview.com/mibs/0/HOST-RESOURCES-MIB.html (Diakses pada Selasa, 11 Oktober 2016)