MANAJEMEN JARINGAN

ANALISA SNMP

RIZKY SOUFI GUSTIAWAN

09011281520111

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2018

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) adalah spesifikasi manajemen jaringan yang dikembangkan oleh Internet Engineering Task Force (IETF), sebuah bagian dari Internet Activities Board (IAB), pada pertengahan tahun 1980-an sebagai standar manajemen untuk produk-produk jaringan berbasis LAN, seperti bridge, router, dan wiring concentrator. SNMP didesain untuk mengurangi tingkat kompleksitas dari manajemen jaringan dan banyaknya sumber daya yang dibutuhkan untuk mendukung manajemen tersebut. Adanya SNMP memungkinkan manajemen jaringan yang tersentralisasi, kuat, dan kompatibel pada semua platform. Selain itu, SNMP memberikan fleksibilitas untuk manajemen informasi-informasi yang dimiliki oleh vendor produk tertentu. SNMP merupakan spesifikasi komunikasi yang menjelaskan bagaimana informasi manajemen dipertukarkan antara aplikasi manajemen jaringan dengan agen manajemen. Terdapat beberapa versi dari SNMP, tetapi yang populer adalah SNMPv1 dan SNMPv2. Terdapat 3 konsep dasar pada SNMP, yaitu : manager, agent, dan management information based (MIB). Pada beberapa konfigurasi di titik manager menjalankan suatu software management, dimana perangkat yang dapat dimanage seperti bridges, routers, servers dan workstations yang dapat integrasikan dengan sebuah modul software agent.Agent pertanggung jawab untuk menyediakan akses ke lokal MIB dari object resources dan aktivitas node tersebut. Agen tersebut juga akan bereaksi terhadap perintah manager untuk mendapat kembali nilai-nilai dari MIB dan untuk menetapkan nilainilai di dalam MIB. Satu contoh dari suatu obyek didapat kembali dari suatu perhitungan dari banyaknya paket-paket pengirim dan penerima pada sebuah node. Manager dapat memonitor nilai yang diload pada jaringan tersebut. Software Agent berada pada di devices tersebut, beberapa agent menerima pesan yang masuk dari manager, pesan permintaan tersebut di baca atau ditulis pada data device tersebut. Agent akan mengirimkan kembali respon yang diterima, dimana agent tidak harus menunggu untuk bertanya tentang sebuah informasi. Namun pada beberapa kasus tertentu agent akan mengirimkan sebuah pesan notifikasi untuk melakukan trap ke satu atau lebih manager. Software Management pada sebuah station management akan mengirimkan pesan request ke agent dan menerima respon dan trap dari agent. Protocol UDP yang biasa digunakan sebagai pembawa paket tersebut dengan karakteristiknya yang hemat dengan bandwidth, namun protocol pembawa lainnya juga dapat digunakan.

SNMP Versi 1

SNMP versi 1 adalah standar protokol SNMP yang pertama kali dibuat, SNMP dibuat untuk digunakan sebagai alat manajemen jaringan untuk jaringan dan mengoperasikan internetworking TCP/IP. (Stallings, 2007,p761). SNMP sebenarnya digunakan untuk merujuk kepada kumpulan spesifikasi manajemen jaringan yang mencakup protocol itu sendiri, definisi database, dan konsep-konsep yang terkait.

Model manajemen jaringan yang digunakan untuk SNMP mencakup elemen-elemen utama sebagai berikut:

1. Management station atau Manager
2. Agent
3. Management Information Base
4. Network Management Protocol

SNMP Versi 2

SNMPv2 menyediakan framework dimana dapat dibangun aplikasi manajemen jaringan dan menyediakan infrastruktur untuk manajemen jaringan. (Stallings, 2007, p765). Fungsi-fungsi pada SNMP v1 masih sama dengan yang digunakan pada SNMP v2, namun ada fungsi-fungsi yang dikembangkan, seperti pada fungsi trap. SNMP v2 juga memperkenalkan 2 protokol baru yaitu GetBulk dan inform. GetBulk digunakan oleh NMS untuk mendapatkan data yang berukuran besar dengan efisien. Operasi Inform memungkinkan NMS untuk saling mengirimkan informasi trap. Dari segi keamanan SNMP v2 juga dikembangkan sehingga lebih aman dibanding SNMP v1.

SNMP Versi 3

SNMPv3 menyediakan 3 layanan penting yaitu authentication, privacy, dan access control, Authentication dan privacy adalah bagian dari User-Based Security Model (USM) dan access control didefinisikan dalam View-Based Access Control Model (VACM). (Stallings, 2007, p769).

Management Information Base (MIB)

Management information base (MIB) adalah koleksi dari objek-objek atau variable data-data yang merupakan salah satu aspek dari managed agent. (Stallings, 2007, p762). Setiap perangkat memiliki unique object identifier (OID) yang terdiri dari angka – angka yang dipisahkan oleh titik. OID secara alami akam membentuk tree. MIB menghubungkan setiap OID dengan label dan parameter lain yang berhubungan dengan objek yang bersangkutan. MIB kemudian bertindak sebagai kamus atau buku kode ang digunakan untuk menghubungkan dan menerjemahkan SNMP.

Komponen utama dalam proses manajemen jaringan TCP/IP terdiri dari tiga elemen, yaitu:

1. **MIB (Management Information Database)**

MIB Adalah struktur basis data variabel dari elemen jaringan yang dikelola. Pada kelompok interface terdapat variabel objek MIB yang mendefinisikan karakteristik interface diantaranya : *ifInOctets* mendefinisikan jumlah total byte yang diterima, *ifOutOctets* mendefinisikan jumlah total byte yang dikirim, *ifInErrors* mendefinisikan jumlah paket diterima yang dibuang karena rusak, *ifOutErrors* mendefinisikan jumlah paket dikirim yang dibuang karena usak, dan variable objek lainnya yang juga berkaitan dengan paket internet.

2. **Agen**

Merupakan software yang dijalankan di setiap elemen jaringan yang dimonitor. Agen bertugas mengumpulkan seluruh informasi yang telah ditentukan dalam MIB.

3. **Manajer**

Merupakan software yang berjalan di sebuah host di jaringan. Bertugas meminta informasi ke SNMP Agen. Manajer biasanya tidak meminta semua informasi yang dimiliki oleh agen, tetapi hanya meminta informasi tertentu saja yang akan digunakan untuk mengamati unjuk kerja jaringan. Manager biasanya menggunakan komputer yang memiliki tampilan grafis dan berwarna sehingga selain dapat menjalankan fungsinya sebagai Manager, juga untuk melihat grafik unjuk kerja dari suatu elemen jaringan yang dihasilkan oleh proses monitoring.

SNMP terdiri dari dua jenis yakni:

- Network Management Station, yang berfungsi sebagai pusat penyimpanan untuk pengumpulan dan analisa dari data manajemen jaringan.
- Peralatan yang dimanage menjalakan SNMP agent, yaitu proses background yang memonitor peralatan tersebut dan mengkomunikasikannya ke network management station.

4. **PDU SNMPv1**

- *GetRequest*

Adalah jenis PDU yang dikirimkan dari manager kepada agent. PDU ini bertujuan untuk me-request data pada agent.

- *GetNextRequest*

Adalah jenis PDU yang dikirimkan dari manager kepada agent. Operasi ini hampir sama dengan operasi GetRequest, hanya saja, GetNextRequest ini meminta data setelahnya dari OID yang dispesifikasikan dalam paket GetNextRequest.

- *SetRequest*

Adalah jenis PDU yang dikirimkan dari manager kepada agent. PDU ini bertujuan untuk mengubah data pada agent.

- *GetResponse*

Adalah jenis PDU yang dikirimkan dari agent kepada manager. PDU ini bertujuan untuk me-reply data kepada manager sebagai response atas data yang diminta oleh manager melalui operasi GetRequest, GetNextRequest, dan SetRequest.

- *Trap*

Adalah jenis PDU yang dikirimkan dari agent kepada manager. SNMP trap ini adalah sebuah pesan yang diprakarsai oleh suatu elemen dalam jaringan (agent) dan dikirimkan kepada manager untuk memberitahu atau memberikan informasi kepada manager bahwa terjadi suatu event tertentu pada objek yang di-manage (managed device).

5. Struktur MIB ()

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

6. Object Identifier (OID)

- Object Identifier (OID) merupakan sebuah pengenal yang digunakan untuk menamakan sebuah objek yang terdapat dalam MIB.
- OID bersifat unik untuk masing-masing objek.
- Secara struktural, sebuah OID terdiri dari sebuah node dalam namespace yang

  ditetapkan secara hirarki, yang didefinisikan secara formal menggunakan standar ASN.1.

OID dapat didefinisikan dalam dua format, yaitu :

1. Textual OID

Pendefinisian OID berdasarkan nama tiap node mulai dari root, dengan dipisahkan oleh titik (.) .

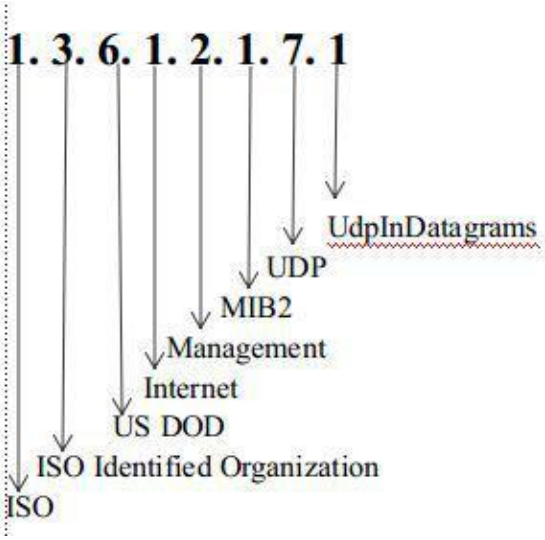
Contoh : .iso.org.dod.internet.mgmt.mib.system.sysDescr

2. Numerical OID

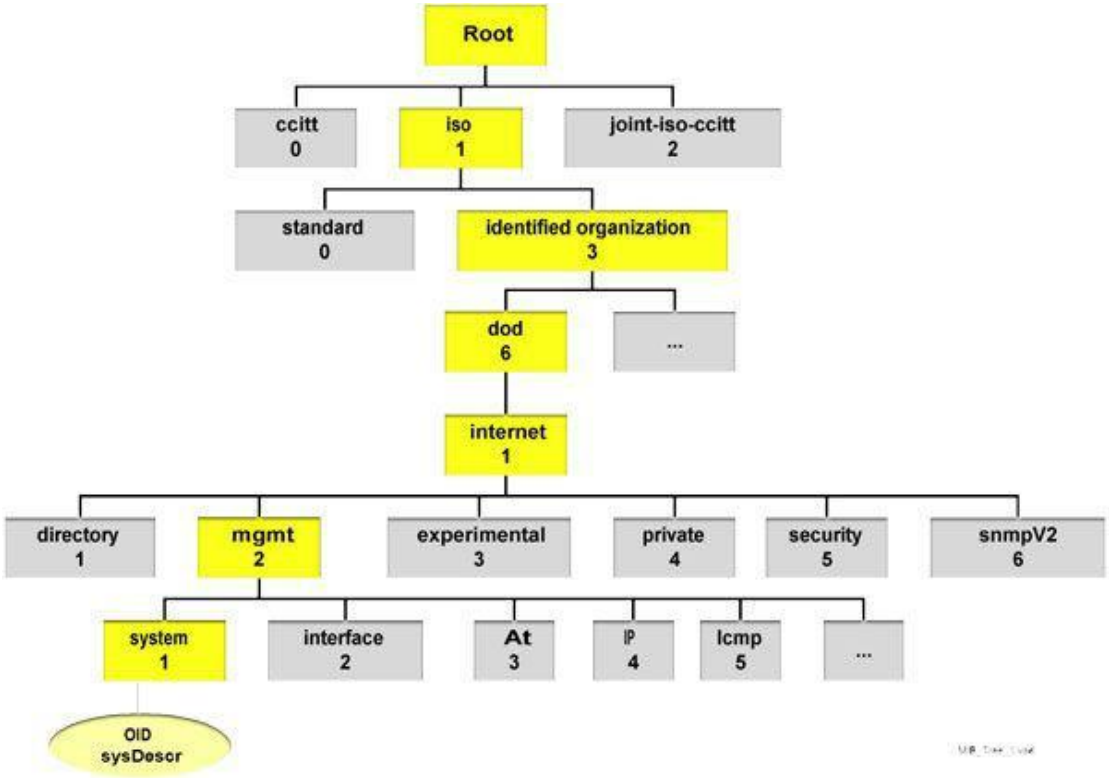
Pendefinisian OID berdasarkan angka integer sebagai pengganti nama, juga dipisahkan dengan titik (.) .

Contoh : .1.3.6.1.2.1.1.1

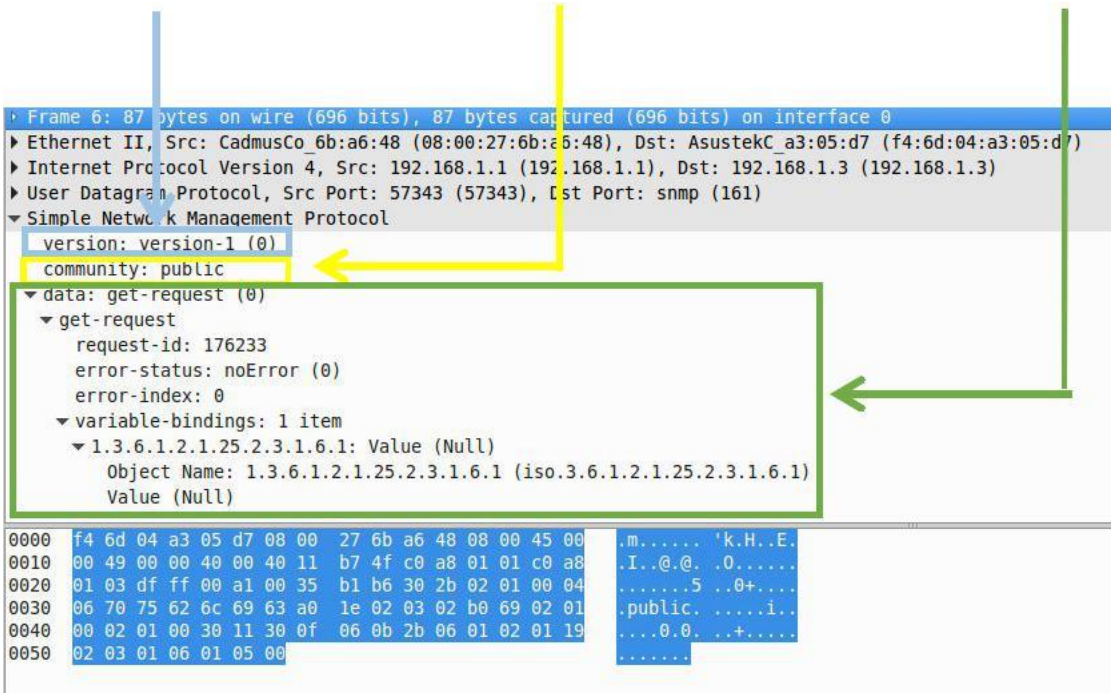
7. ISO Object Identifier (OID) Tree



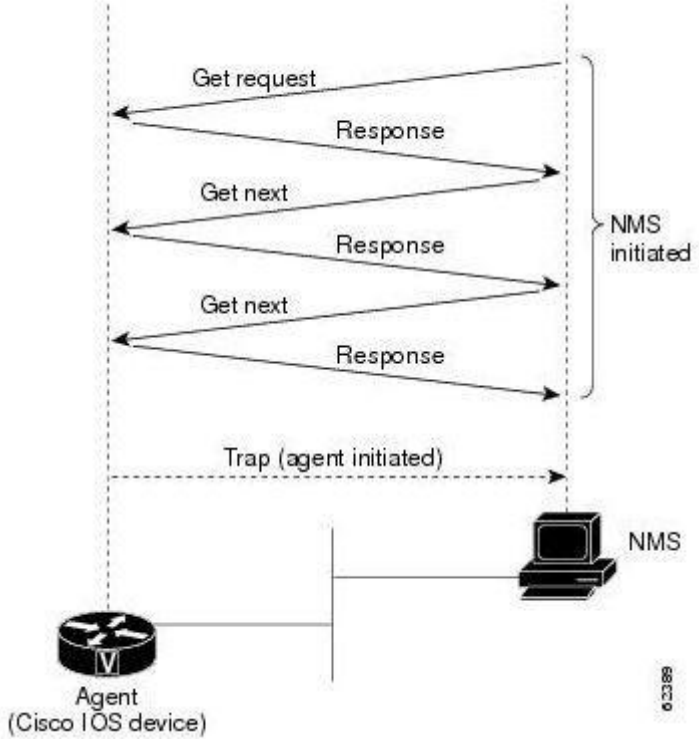
8. MIB (Management Information Base) Tree



9. Format Pesan SNMPv1

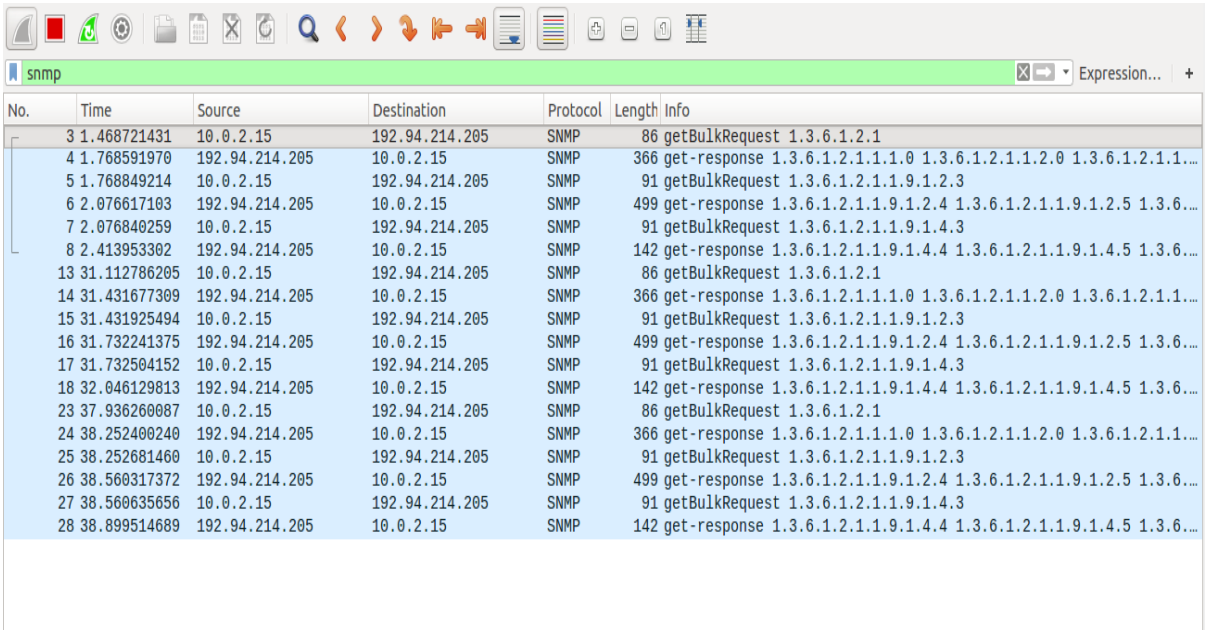


10. SNMP Event Interaction and Timing



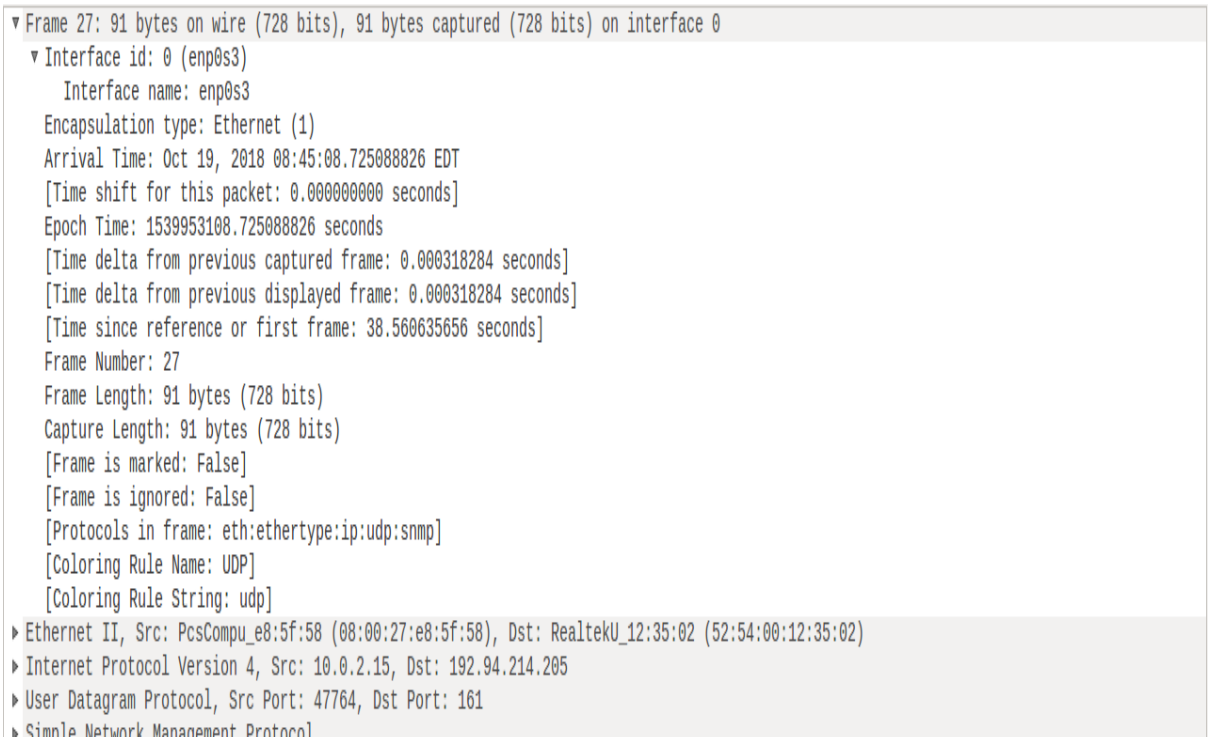
Analisa Packet Capture Pada Wireshark

Hasil capture packet dengan “Wiresharks”



No.	Time	Source	Destination	Protocol	Length	Info
3	1.468721431	10.0.2.15	192.94.214.205	SNMP	86	getBulkRequest 1.3.6.1.2.1
4	1.768591970	192.94.214.205	10.0.2.15	SNMP	366	get-response 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.2.0 1.3.6.1.2.1.1.…
5	1.768849214	10.0.2.15	192.94.214.205	SNMP	91	getBulkRequest 1.3.6.1.2.1.1.9.1.2.3
6	2.076617103	192.94.214.205	10.0.2.15	SNMP	499	get-response 1.3.6.1.2.1.1.9.1.2.4 1.3.6.1.2.1.1.9.1.2.5 1.3.6.…
7	2.076840259	10.0.2.15	192.94.214.205	SNMP	91	getBulkRequest 1.3.6.1.2.1.1.9.1.4.3
8	2.413953302	192.94.214.205	10.0.2.15	SNMP	142	get-response 1.3.6.1.2.1.1.9.1.4.4 1.3.6.1.2.1.1.9.1.4.5 1.3.6.…
13	31.112786205	10.0.2.15	192.94.214.205	SNMP	86	getBulkRequest 1.3.6.1.2.1
14	31.431677309	192.94.214.205	10.0.2.15	SNMP	366	get-response 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.2.0 1.3.6.1.2.1.1.…
15	31.431925494	10.0.2.15	192.94.214.205	SNMP	91	getBulkRequest 1.3.6.1.2.1.1.9.1.2.3
16	31.732241375	192.94.214.205	10.0.2.15	SNMP	499	get-response 1.3.6.1.2.1.1.9.1.2.4 1.3.6.1.2.1.1.9.1.2.5 1.3.6.…
17	31.732504152	10.0.2.15	192.94.214.205	SNMP	91	getBulkRequest 1.3.6.1.2.1.1.9.1.4.3
18	32.046129813	192.94.214.205	10.0.2.15	SNMP	142	get-response 1.3.6.1.2.1.1.9.1.4.4 1.3.6.1.2.1.1.9.1.4.5 1.3.6.…
23	37.936260087	10.0.2.15	192.94.214.205	SNMP	86	getBulkRequest 1.3.6.1.2.1
24	38.252400240	192.94.214.205	10.0.2.15	SNMP	366	get-response 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.2.0 1.3.6.1.2.1.1.…
25	38.252681460	10.0.2.15	192.94.214.205	SNMP	91	getBulkRequest 1.3.6.1.2.1.1.9.1.2.3
26	38.560317372	192.94.214.205	10.0.2.15	SNMP	499	get-response 1.3.6.1.2.1.1.9.1.2.4 1.3.6.1.2.1.1.9.1.2.5 1.3.6.…
27	38.560635656	10.0.2.15	192.94.214.205	SNMP	91	getBulkRequest 1.3.6.1.2.1.1.9.1.4.3
28	38.899514689	192.94.214.205	10.0.2.15	SNMP	142	get-response 1.3.6.1.2.1.1.9.1.4.4 1.3.6.1.2.1.1.9.1.4.5 1.3.6.…

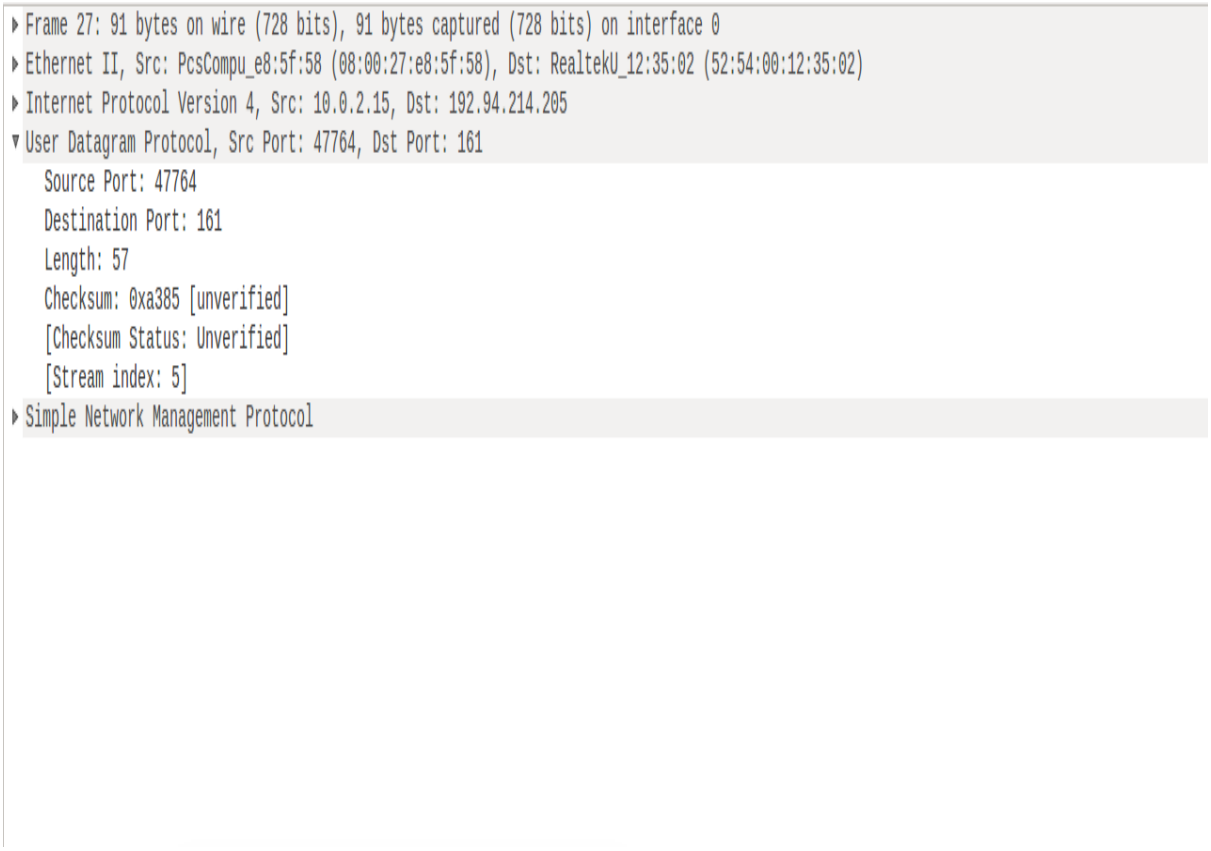
Paket No. 27 digunakan sebagai sample.

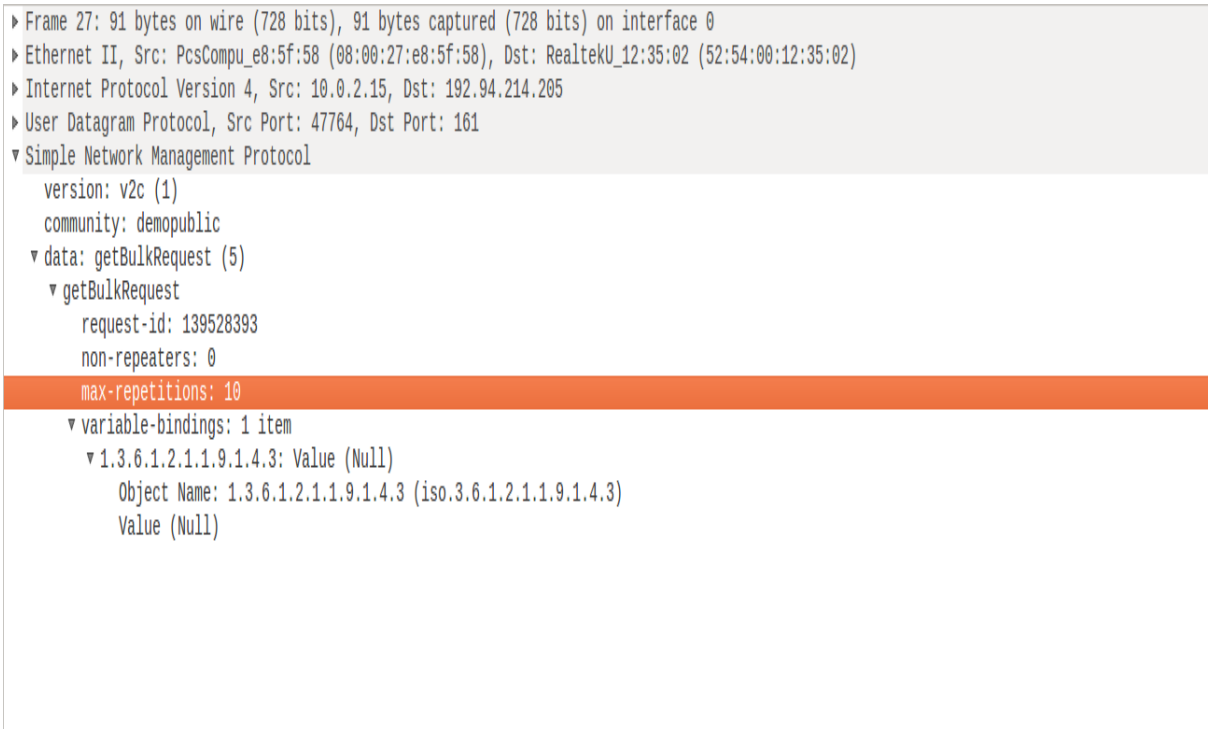


```
▾ Frame 27: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface 0
  ▾ Interface id: 0 (enp0s3)
      Interface name: enp0s3
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 19, 2018 08:45:08.725088826 EDT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1539953108.725088826 seconds
    [Time delta from previous captured frame: 0.000318284 seconds]
    [Time delta from previous displayed frame: 0.000318284 seconds]
    [Time since reference or first frame: 38.560635656 seconds]
    Frame Number: 27
    Frame Length: 91 bytes (728 bits)
    Capture Length: 91 bytes (728 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:snmp]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
▸ Ethernet II, Src: PcsCompu_e8:5f:58 (08:00:27:e8:5f:58), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.94.214.205
▸ User Datagram Protocol, Src Port: 47764, Dst Port: 161
▸ Simple Network Management Protocol
```

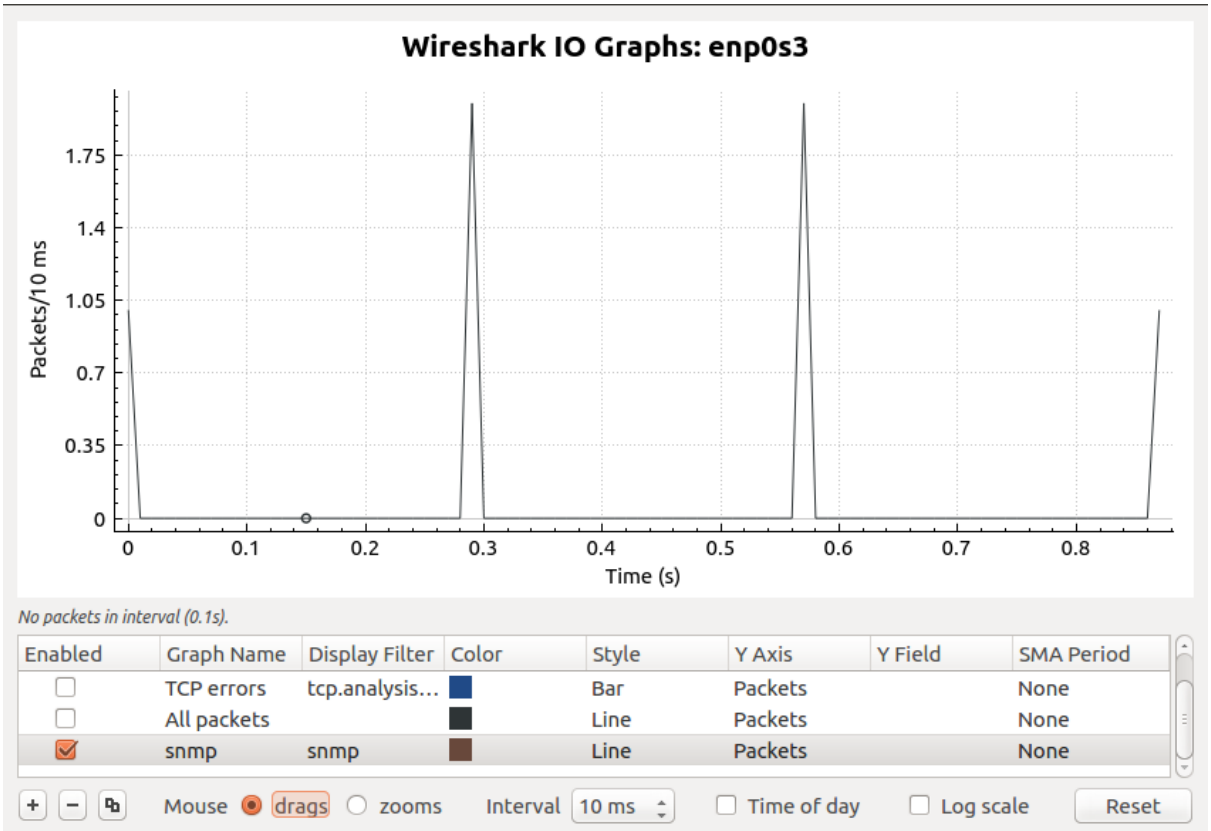
```
▸ Frame 27: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface 0
▾ Ethernet II, Src: PcsCompu_e8:5f:58 (08:00:27:e8:5f:58), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
  ▾ Destination: RealtekU_12:35:02 (52:54:00:12:35:02)
      Address: RealtekU_12:35:02 (52:54:00:12:35:02)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: PcsCompu_e8:5f:58 (08:00:27:e8:5f:58)
      Address: PcsCompu_e8:5f:58 (08:00:27:e8:5f:58)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.94.214.205
▸ User Datagram Protocol, Src Port: 47764, Dst Port: 161
▸ Simple Network Management Protocol
```

```
▸ Ethernet II, Src: PcsCompu_e8:5f:58 (08:00:27:e8:5f:58), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▾ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.94.214.205
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 77
    Identification: 0x8b0f (35599)
  ▾ Flags: 0x4000, Don't fragment
      0... .... .... .... = Reserved bit: Not set
      .1.. .... .... .... = Don't fragment: Set
      ..0. .... .... .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0x0c56 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.15
    Destination: 192.94.214.205
▸ User Datagram Protocol, Src Port: 47764, Dst Port: 161
▸ Simple Network Management Protocol
```

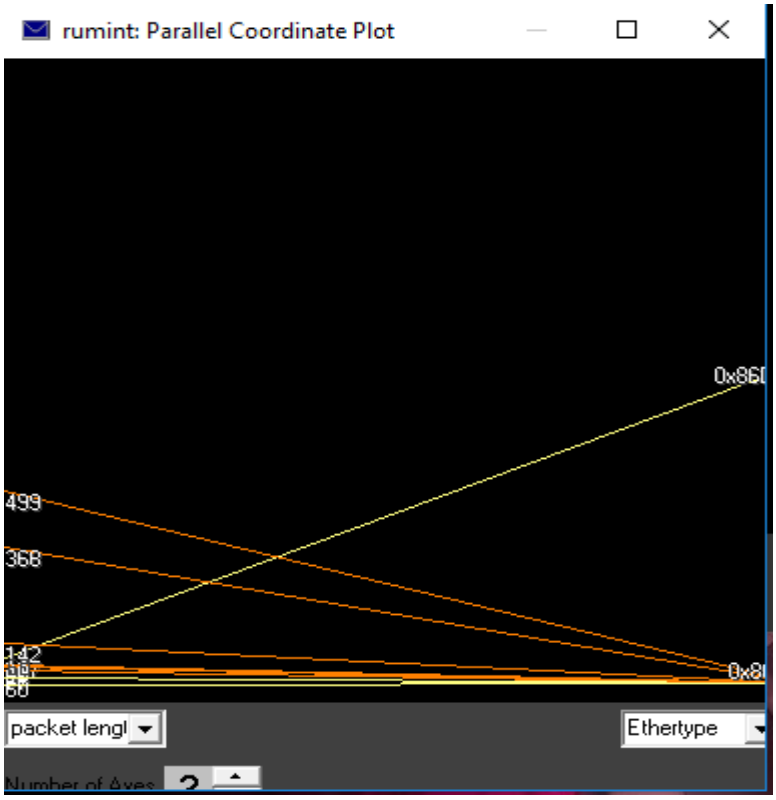

▸ Frame 27: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_e8:5f:58 (08:00:27:e8:5f:58), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.94.214.205
▾ User Datagram Protocol, Src Port: 47764, Dst Port: 161
Source Port: 47764
Destination Port: 161
Length: 57
Checksum: 0xa385 [unverified]
[Checksum Status: Unverified]
[Stream index: 5]
▸ Simple Network Management Protocol

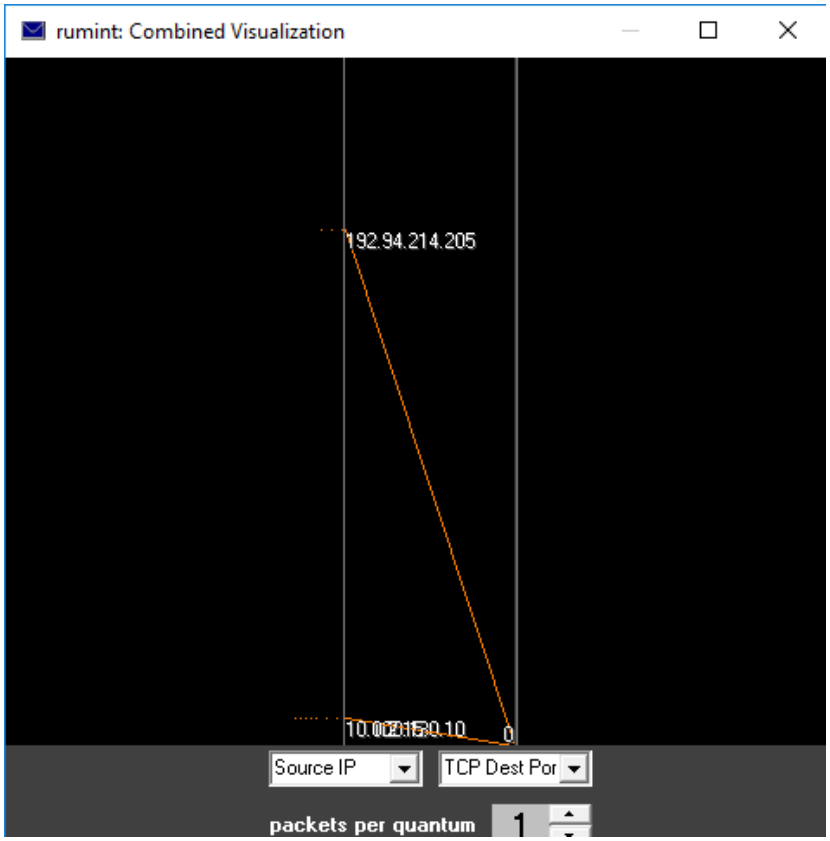

▸ Frame 27: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_e8:5f:58 (08:00:27:e8:5f:58), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.94.214.205
▸ User Datagram Protocol, Src Port: 47764, Dst Port: 161
▾ Simple Network Management Protocol
version: v2c (1)
community: demopublic
▾ data: getBulkRequest (5)
▾ getBulkRequest
request-id: 139528393
non-repeaters: 0
max-repetitions: 10
▾ variable-bindings: 1 item
▾ 1.3.6.1.2.1.1.9.1.4.3: Value (Null)
Object Name: 1.3.6.1.2.1.1.9.1.4.3 (iso.3.6.1.2.1.1.9.1.4.3)
Value (Null)

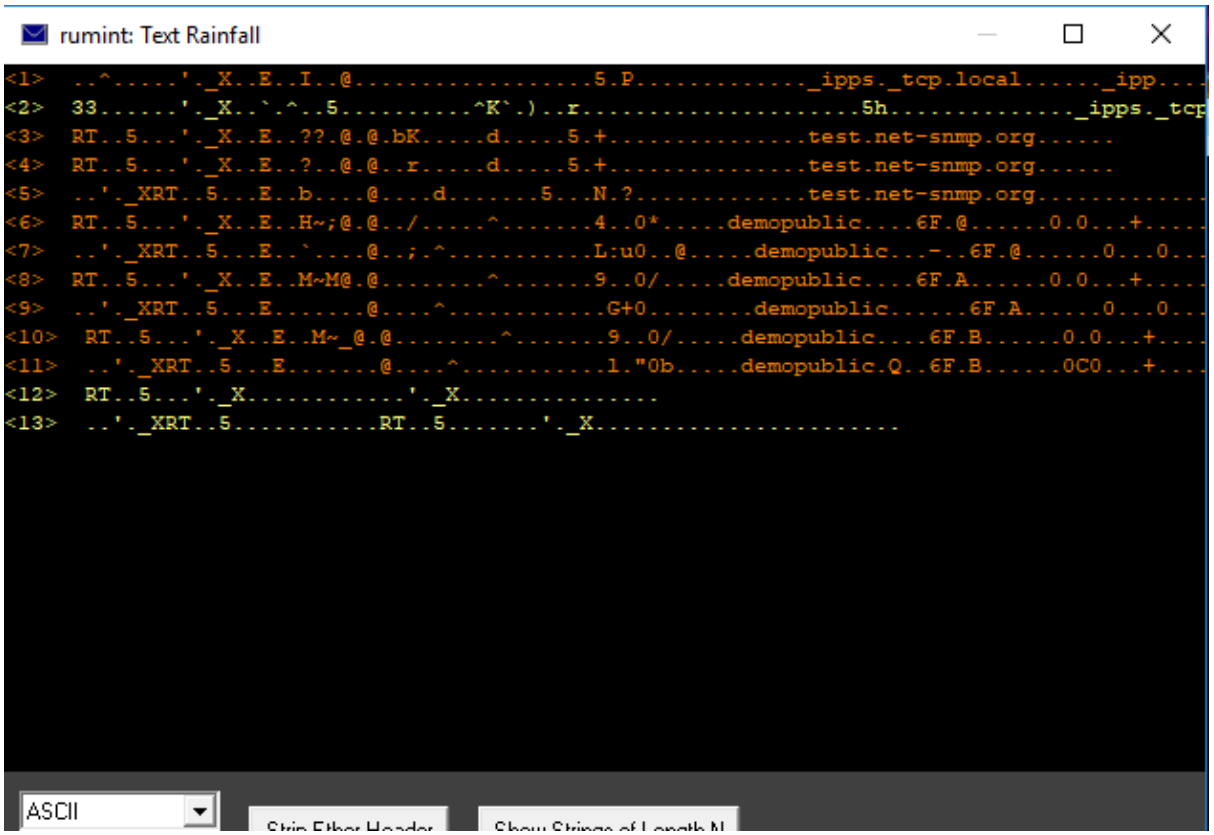
Trafic Percobaan



Visualisasi Pada Rumint




rumint: Combined Visualization
192.94.214.205
Source IP
TCP Dest Por
packets per quantum
1


rumint: Text Rainfall
<1> ..^.....'._X..E..I..@.....5.P.....ipps._tcp.local.....ipp...
<2> 33.....'._X..`.^..5.....^K`.)..r.....5h.....ipps._tcp
<3> RT..5...'._X..E..??.@.@.bK.....d.....5.+.....test.net-snmp.org.....
<4> RT..5...'._X..E..?..@.@..r.....d.....5.+.....test.net-snmp.org.....
<5> ..'._XRT..5...E..b....@....d.....5...N.?.....test.net-snmp.org.....
<6> RT..5...'._X..E..H~;@.@../.....^.....4..0*.....demopublic....6F.@.....0.0...+.....
<7> ..'._XRT..5...E..`....@..;.^.....L:u0..@.....demopublic...-..6F.@.....0...0...
<8> RT..5...'._X..E..M~M@.@.....^.....9..0/.....demopublic....6F.A.....0.0...+.....
<9> ..'._XRT..5...E.....@....^.....G+0.....demopublic.....6F.A.....0...0...
<10> RT..5...'._X..E..M~_@.@.....^.....9..0/.....demopublic....6F.B.....0.0...+....
<11> ..'._XRT..5...E.....@....^.....l."0b.....demopublic.Q..6F.B.....0C0...+....
<12> RT..5...'._X.....'._X.....
<13> ..'._XRT..5.....RT..5.....'._X.....
ASCII