

**ANALISIS KEAMANAN JARINGAN DENGAN ENDEKATAN  
PROTOKOL *AUTHENTICATION HEADER* (AH) DAN *ENCAPSULATING  
SECURITY PAYLOAD* (ESP) *TUNNELING* STUDI KASUS  
UNIVERSITAS MUHAMMADIYAH PALEMBANG**

**Ahmad Rinaldi Albar<sup>1</sup>, Alex Wijaya<sup>2</sup>, Hutrianto<sup>3</sup>**

Fakultas Ilmu Komputer, Universitas Bina Darma

e-mail: <sup>1</sup>rinaldi141420037@gmail.com, <sup>2</sup>allecc\_wj@yao.com, <sup>3</sup>hutrianto@binadarma.ac.id

**ABSTRAK**

Dalam sebuah jaringan computer, keamanan didalam pengiriman serta penerimaan data sangat penting untuk menjamin bahwa data yang dikirim tidak jatuh ke pihak ketiga, terutama jika data tersebut bersifat rahasia. Untuk itu di perlukan implementasi metode-metode pengamanan data pada jaringan. Salah satu solusi pemecahan masalah keamanan dalam sebuah jaringan public adalah menggunakan Protocol Authentication Header (AH) dan Encapsulating Security Payload (ESP) Tunneling. Protocol AH dan ESP Termasuk Protocol di dalam Internet Protocol Security (IPSec). IP Security adalah protocol yang digunakan untuk mengamankan transmisi datagram dalam sebuah internetwork berbasis TCP/IP, IPSec Melakukan enkripsi terhadap data pada lapisan yang sama dengan Protokol IP dan menggunakan teknik tunneling untuk mengirimkan informasi melalui jaringan internet atau Dalam jaringan intranet secara aman. IPSec mendukung dua buah sesi komunikasi keamanan yaitu Protokol Authentication Header (AH) yang berfungsi menawarkan autentikasi penggunaan dan perlindungan dari beberapa serangan, hasil analisis menunjukkan bahwa serangan sniffing tidak bisa melakukan penyadapan karena data teracak dalam dalam peyadapan menggunakan Wireshark.

**Kata kunci:** Analisis keamanan jaringan, AH, ESP Tunneling

**ABSTRACT**

*In a computer network, security in sending and receiving data is very important to ensure that the data sent does not fall to third parties, especially if the data is confidential. For this reason, implementation of methods for securing data on the network is needed. One solution to solving security problems in a public network is to use Protocol Authentication Header (AH) and Encapsulating Security Payload (ESP) tunneling. Protocol AH and ESP Include Protocol in the Internet Protocol Security (IPSec). IP Security is a protocol used to secure the transmission of datagrams in a TCP / IP-based internetwork, IPSec Encrypts data in the same layer as the IP Protocol and uses tunneling techniques to transmit information over the internet or in intranet networks safely. IPSec supports two security communication sessions, namely the Authentication Header (AH) Protocol which serves to offer user authentication and protection from several attacks, the analysis shows that sniffing attacks cannot intercept because the data is encrypted in the view using Wireshark.*

**Keywords :** Network security analysis, AH, ESP Tunneling

## 1. PENDAHULUAN

Perkembangan Teknologi saat ini sangat pesat, dalam kegiatan sehari-hari kita menggunakan teknologi, contohnya jaringan *internet*, jaringan *internet* saat ini sangat diperlukan apalagi dalam hal komunikasi. Seiring dengan meningkatnya pengguna jaringan *internet*, permasalahan keamanan masih menjadi faktor utama dalam sebuah jaringan komputer, keamanan didalam pengiriman serta penerimaan data sangat penting untuk menjamin bahwa data yang dikirim aman tidak jatuh ke pihak ketiga, terutama jika data tersebut bersifat rahasia. Untuk itu perlu dilakukan implementasi metode-metode pengamanan data pada jaringan. Banyak metode yang dapat diimplementasikan, seperti *tunneling*.

Universitas Muhammadiyah Palembang merupakan sebuah instansi yang bergerak dibidang pendidikan. Universitas Muhammadiyah Palembang memiliki beberapa kampus dalam melakukan kegiatan pengolahan data menggunakan jaringan *internet*. Sistem jaringan di Universitas Muhammadiyah Palembang memiliki 3 router terpusat di satu gedung yaitu gedung KPA ( Kantor Pusat Administrasi ) yang menghubungkan antara kampus, setiap router memiliki *switch* masing-masing, router A sebagai *router backbone* terletak di Gedung KPA, Router B terletak di Kampus B yang berjarak 250 meter ke Kampus A, Kampus B terhubung 4 buah *switch* dengan rincian Fakultas Teknik, Perpustakaan, Fakultas Agama Islam, dan Fakultas Kedokteran. Sedangkan Router C terletak di Kampus A berdekatan dengan Gedung KPA yang terhubung oleh 4 *switch* dengan rincian Fakultas Pertanian, Fakultas Ekonomi Bisnis, Fakultas Hukum, dan FKIP.

Jaringan *Internet* Universitas Muhammadiyah Palembang bisa di akses oleh mahasiswa dan dosen dengan bebas, Pada kasus Kampus B, terdapat Fakultas Kedokteran dan Fakultas Agama Islam yang memiliki kecepatan akses 25 MBps dan 15 MBps. Universitas Muhammadiyah Palembang memiliki kerja sama Jaringan Internet yaitu dengan Universitas Muhammadiyah Yogyakarta. Sistem jaringan *internet* Universitas Muhammadiyah Palembang bisa diakses oleh Jaringan *Internet* Universitas Muhammadiyah Yogyakarta. Keamanan Jaringan *Internet* Universitas Muhammadiyah Palembang masih menerapkan sistem *Virtual private Network (VPN) default* yang artinya keamanan yang biasa diterapkan dalam router mikrotik. Walaupun Keamanan Jaringan Universitas Muhammadiyah Palembang sekarang hanya menerapkan *Virtual Private Network (VPN)*, adapun kelebihan nya yaitu dapat mencegah penyusup dari luar, namun juga terdapat kelemahan tidak dapat mencegah jika data disadap oleh orang yang berada dalam jaringan itu sendiri. maka dari itu perlu keamanan dengan metode enkripsi dan deskripsi terhadap Internet Protokol (IP), Dengan menerapkan Protokol Authentication Header (AH) dan Encapsulating Security Payload (ESP) tunneling.

Salah satu solusi pemecahan masalah keamanan jaringan di Universitas Muhammadiyah Palembang adalah berbasis *Internet Protocol Security (IPSec)*. Menurut Wijaya [1], IPSec (singkatan dari IP Security) adalah sebuah perangkat lunak berbasis protokol *Authentication Header (AH)* dan *Encapsulating Security Payload (ESP)* untuk mengamankan transmisi *datagram* dalam sebuah *internetwork* berbasis TCP/IP. *IPSec* mendefinisikan beberapa standar untuk melakukan enkripsi data dan juga integritas data pada lapisan kedua dalam DARPA *Reference Model (internetwork layer)*. IPSec melakukan enkripsi terhadap data pada lapisan yang sama dengan protokol IP dan menggunakan teknik *tunneling* untuk mengirimkan informasi melalui jaringan *Internet* atau dalam jaringan *intranet* secara aman. IPSec didefinisikan oleh badan *Internet Engineering Task Force (IETF)* dan diimplementasikan di dalam banyak sistem operasi. *Windows 2000* adalah sistem operasi pertama dari *Microsoft* yang mendukung IPSec.

## 2. METODOLOGI PENELITIAN

Metode penelitian yang digunakan adalah *Action Research*, Menurut Kock [2], Metode *Action Research* merupakan penelitian tindakan. Pendekatan ini dilakukan sendiri oleh peneliti yang bertujuan untuk mengembangkan metode kerja yang paling efisien. Metode *Action research* dibagi dalam beberapa tahapan, yaitu [3] :

### 1) Melakukan diagnosa (*diagnosing*)

Permasalahan yang sering terjadi pada *Local area network* dikarenakan sering terjadi *Backdoor, Port Scan, Virus dan Malware, Hacker/Cracker, Denial Of Service (Dos/DDos)*. Akibat dari kelemahan sistem keamanan yang ada pada jaringan. Hal ini bukan hanya merugikan satu bidang, bahkan semua bidang yang terhubung pada *Local area network*. Untuk melindungi dari serangan tersebut solusinya adalah mengimplementasikan *protocol authentication header (AH)* dan *Encapsulating Security Payload (ESP)* pada mikrotik.

### 2) Membuat rencana tindakan (*action planning*)

Peneliti memahami pokok masalah yang ada kemudian dilanjutkan dengan menyusun rencana tindakan yang tepat untuk menyelesaikan masalah yang ada, pada tahap ini penulis memasuki tahapan persiapan kebutuhan perangkat lunak (*software*), perangkat keras (*hardware*), dan perancangan topologi jaringan komputer.

### 3) Melakukan tindakan (*action taking*)

Peneliti mengimplementasikan rencana tindakan dengan melakukan implementasi dan pengujian keamanan jaringan. Implementasi dilakukan dengan menggunakan 2 buah server berbasis router Mikrotik *server* dengan pengujian masing-masing menggunakan *client windows* pada masing-masing *server*. Pengujian berupa proses *sniffing* data menggunakan *wireshark* dengan sampel data berupa *http, tcp, udp* dan menguji dengan beberapa serangan yaitu *Attack Dos* dengan *pinglood* dan *TCPdump*.

### 4) Melakukan evaluasi (*evaluating*)

Setelah mendapatkan data analisis hasil pengujian, maka selanjutnya akan dijadikan sebagai bahan evaluasi hasil penelitian yang didapat.

### 5) Pembelajaran (*learning*)

Setelah semuanya selesai, maka tahap akhir adalah peneliti melaksanakan *review* tahap demi tahap kemudian penelitian ini dapat berakhir. Hasilnya juga mempertimbangkan untuk tindakan kedepan.

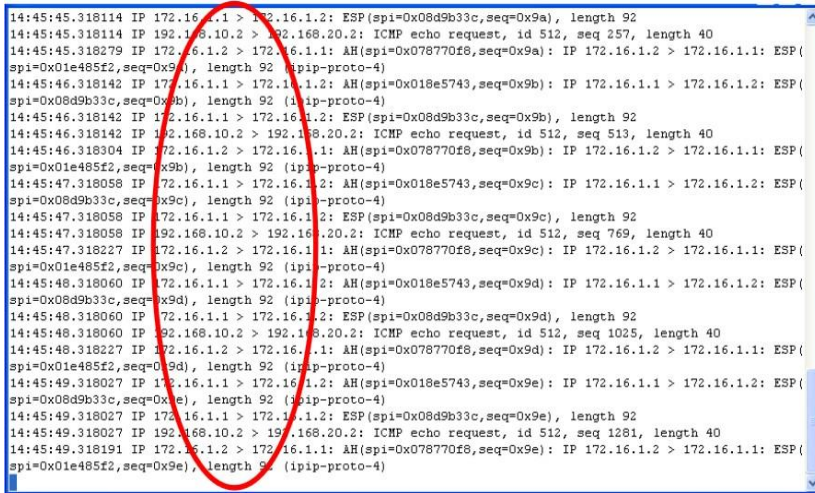
## 3. HASIL DAN PEMBAHASAN

### 3.1 HASIL

Hasil dari Proses *sniffing* menggunakan *Wireshark* pada kedua pengujian yaitu sebelum dan sesudah diimplementasikan *protocol AH* dan *ESP Ipsec*. Diperoleh hasil yang berbeda diantara keduanya. *Sniffing* yang dilakukan pada *VPN Jari ngan Universitas Muhammadiyah Palembang* hanya menunjukkan aktivitas *tunnel VPN* hal itu ditunjukkan pada kolom *info* yaitu tidak dapat menunjukkan tahap selanjutnya yaitu “*follow tcp stream*”. Hasil penangkapan kedua menggunakan *protocol AH* dan *protocol ESP* menunjukkan bahwa paket data yang dikirim telah dienkapsulasi melalui *tunnel VPN* dan hal ini membuktikan bahwa enkripsi telah berjalan dengan baik dan aman untuk digunakan di jalur internet public.

#### 3.1.1 Test Ping *TCPDump* menggunakan *Ipsec*

Hasil tes ping *TCPDump* yang sudah di implementasi *protocol authentication header (AH)* dan *Encapsulating Security Payload (ESP) ipsec Tunneling* dapat dilihat pada gambar 1 dibawah ini.



```
14:45:45.318114 IP 172.16.1.1 > 172.16.1.2: ESP spi=0x08d9b33c,seq=0x9a), length 92
14:45:45.318114 IP 192.168.10.2 > 192.168.20.2: ICMP echo request, id 512, seq 257, length 40
14:45:45.318279 IP 172.16.1.2 > 172.16.1.1: AH spi=0x078770f8,seq=0x9a): IP 172.16.1.2 > 172.16.1.1: ESP (
spi=0x01e485f2,seq=0x9a), length 92 (ipip-proto-4)
14:45:46.318142 IP 172.16.1.1 > 172.16.1.2: AH spi=0x018e5743,seq=0x9b): IP 172.16.1.1 > 172.16.1.2: ESP (
spi=0x08d9b33c,seq=0x9b), length 92 (ipip-proto-4)
14:45:46.318142 IP 172.16.1.1 > 172.16.1.2: ESP spi=0x08d9b33c,seq=0x9b), length 92
14:45:46.318142 IP 192.168.10.2 > 192.168.20.2: ICMP echo request, id 512, seq 513, length 40
14:45:46.318304 IP 172.16.1.2 > 172.16.1.1: AH spi=0x078770f8,seq=0x9b): IP 172.16.1.2 > 172.16.1.1: ESP (
spi=0x01e485f2,seq=0x9b), length 92 (ipip-proto-4)
14:45:47.318058 IP 172.16.1.1 > 172.16.1.2: AH spi=0x018e5743,seq=0x9c): IP 172.16.1.1 > 172.16.1.2: ESP (
spi=0x08d9b33c,seq=0x9c), length 92 (ipip-proto-4)
14:45:47.318058 IP 172.16.1.1 > 172.16.1.2: ESP spi=0x08d9b33c,seq=0x9c), length 92
14:45:47.318058 IP 192.168.10.2 > 192.168.20.2: ICMP echo request, id 512, seq 769, length 40
14:45:47.318227 IP 172.16.1.2 > 172.16.1.1: AH spi=0x078770f8,seq=0x9c): IP 172.16.1.2 > 172.16.1.1: ESP (
spi=0x01e485f2,seq=0x9c), length 92 (ipip-proto-4)
14:45:48.318060 IP 172.16.1.1 > 172.16.1.2: AH spi=0x018e5743,seq=0x9d): IP 172.16.1.1 > 172.16.1.2: ESP (
spi=0x08d9b33c,seq=0x9d), length 92 (ipip-proto-4)
14:45:48.318060 IP 172.16.1.1 > 172.16.1.2: ESP spi=0x08d9b33c,seq=0x9d), length 92
14:45:48.318060 IP 192.168.10.2 > 192.168.20.2: ICMP echo request, id 512, seq 1025, length 40
14:45:48.318227 IP 172.16.1.2 > 172.16.1.1: AH spi=0x078770f8,seq=0x9d): IP 172.16.1.2 > 172.16.1.1: ESP (
spi=0x01e485f2,seq=0x9d), length 92 (ipip-proto-4)
14:45:49.318027 IP 172.16.1.1 > 172.16.1.2: AH spi=0x018e5743,seq=0x9e): IP 172.16.1.1 > 172.16.1.2: ESP (
spi=0x08d9b33c,seq=0x9e), length 92 (ipip-proto-4)
14:45:49.318027 IP 172.16.1.1 > 172.16.1.2: ESP spi=0x08d9b33c,seq=0x9e), length 92
14:45:49.318027 IP 192.168.10.2 > 192.168.20.2: ICMP echo request, id 512, seq 1281, length 40
14:45:49.318191 IP 172.16.1.2 > 172.16.1.1: AH spi=0x078770f8,seq=0x9e): IP 172.16.1.2 > 172.16.1.1: ESP (
spi=0x01e485f2,seq=0x9e), length 92 (ipip-proto-4)
```

Gambar 1. Test Ping client site to site dengan TCPdump

Hasil pengujian ping test dengan menggunakan ip security berbasis *site to site*, dimana saat pengujian *ping test* dari client dengan ip address 192.168.10.2 yang berada di belakang server1 ke client dengan ip address 192.168.20.2 yang dibelakang server2 dengan melewati *ip remote address server1* yaitu 172.16.1.1 menuju ke *ip remote address server2* yaitu 172.16.1.2, pada proses tersebut muncul 2 buah protocol ip security yang mendukung dua buah sesi komunikasi keamanan yaitu protokol *Authentication Header* (AH) yang berfungsi menawarkan *otentikasi* pengguna dan perlindungan dari serangan dan juga menyediakan fungsi *otentikasi* terhadap data serta *integritas* terhadap data. Sedangkan protokol *Encapsulating Security Payload* (ESP) berfungsi untuk melakukan *enkapsulasi* serta *enkripsi* terhadap data pengguna untuk meningkatkan kerahasiaan data.

### 3.1.2 Sharing Data menggunakan IPsecurity

Hasil pengujian sharing data dengan menggunakan ip security berbasis *site to site*, dimana saat pengujian test sharing data dimana client yang berada dibelakang server1 mengakses data yang di sharing oleh client yang berada dibelakang server2 begitu juga sebaliknya.



```
14:48:34.349145 IP 172.16.1.1 > 172.16.1.2: AH spi=0x018e5743,seq=0x214): IP 172.16.1.1 > 172.16.1.2: ESP (
spi=0x08d9b33c,seq=0x214), length 116 (ipip-proto-4)
14:48:34.349145 IP 172.16.1.1 > 172.16.1.2: ESP spi=0x08d9b33c,seq=0x214), length 116
14:48:34.349145 IP 192.168.10.2.xr1 > 192.168.20.2.microsoft-ds: P 32195:32238(43) ack 32261 win 65131
14:48:34.349344 IP 172.16.1.2 > 172.16.1.1: AH spi=0x078770f8,seq=0x20b): IP 172.16.1.2 > 172.16.1.1: ESP (
spi=0x01e485f2,seq=0x20b), length 116 (ipip-proto-4)
14:48:34.349742 IP 172.16.1.1 > 172.16.1.2: AH spi=0x018e5743,seq=0x215): IP 172.16.1.1 > 172.16.1.2: ESP (
spi=0x08d9b33c,seq=0x215), length 116 (ipip-proto-4)
14:48:34.349742 IP 172.16.1.1 > 172.16.1.2: ESP spi=0x08d9b33c,seq=0x215), length 116
14:48:34.349742 IP 192.168.10.2.xr1 > 192.168.20.2.microsoft-ds: P 32238:32277(39) ack 32304 win 65088
14:48:34.349905 IP 172.16.1.2 > 172.16.1.1: AH spi=0x078770f8,seq=0x20c): IP 172.16.1.2 > 172.16.1.1: ESP (
spi=0x01e485f2,seq=0x20c), length 116 (ipip-proto-4)
14:48:34.350415 IP 172.16.1.1 > 172.16.1.2: AH spi=0x018e5743,seq=0x216): IP 172.16.1.1 > 172.16.1.2: ESP (
spi=0x08d9b33c,seq=0x216), length 116 (ipip-proto-4)
14:48:34.350415 IP 172.16.1.1 > 172.16.1.2: ESP spi=0x08d9b33c,seq=0x216), length 116
14:48:34.350415 IP 192.168.10.2.xr1 > 192.168.20.2.microsoft-ds: P 32277:32322(45) ack 32343 win 65049
14:48:34.350604 IP 172.16.1.2 > 172.16.1.1: AH spi=0x078770f8,seq=0x20d): IP 172.16.1.2 > 172.16.1.1: ESP (
spi=0x01e485f2,seq=0x20d), length 116 (ipip-proto-4)
14:48:34.351152 IP 172.16.1.1 > 172.16.1.2: AH spi=0x018e5743,seq=0x217): IP 172.16.1.1 > 172.16.1.2: ESP (
spi=0x08d9b33c,seq=0x217), length 116 (ipip-proto-4)
14:48:34.351152 IP 172.16.1.1 > 172.16.1.2: ESP spi=0x08d9b33c,seq=0x217), length 116
14:48:34.351152 IP 192.168.10.2.xr1 > 192.168.20.2.microsoft-ds: P 32322:32367(45) ack 32382 win 65010
14:48:34.351323 IP 172.16.1.2 > 172.16.1.1: AH spi=0x078770f8,seq=0x20e): IP 172.16.1.2 > 172.16.1.1: ESP (
spi=0x01e485f2,seq=0x20e), length 116 (ipip-proto-4)
14:48:34.485729 IP 172.16.1.1 > 172.16.1.2: AH spi=0x018e5743,seq=0x218): IP 172.16.1.1 > 172.16.1.2: ESP (
spi=0x08d9b33c,seq=0x218), length 76 (ipip-proto-4)
14:48:34.485729 IP 172.16.1.1 > 172.16.1.2: ESP spi=0x08d9b33c,seq=0x218), length 76
14:48:34.485729 IP 192.168.10.2.xr1 > 192.168.20.2.microsoft-ds: . ack 32421 win 64971
```

Gambar 2. Test Sharing Data antar Client Site to Site dgn Tcpdump

Pada Gambar 2 diatas menunjukkan pada saat proses koneksi berlangsung terjadi 2 buah protocol ip security yang mendukung dua buah sesi komunikasi keamanan yaitu protokol Authentication Header (AH) yang berfungsi menawarkan autentikasi pengguna dan perlindungan dari beberapa serangan, dan juga menyediakan fungsi autentikasi terhadap data serta integritas terhadap data. Sedangkan protokol Encapsulating Security Payload (ESP) berfungsi untuk melakukan enkapsulasi serta enkripsi terhadap data pengguna untuk meningkatkan kerahasiaan data.

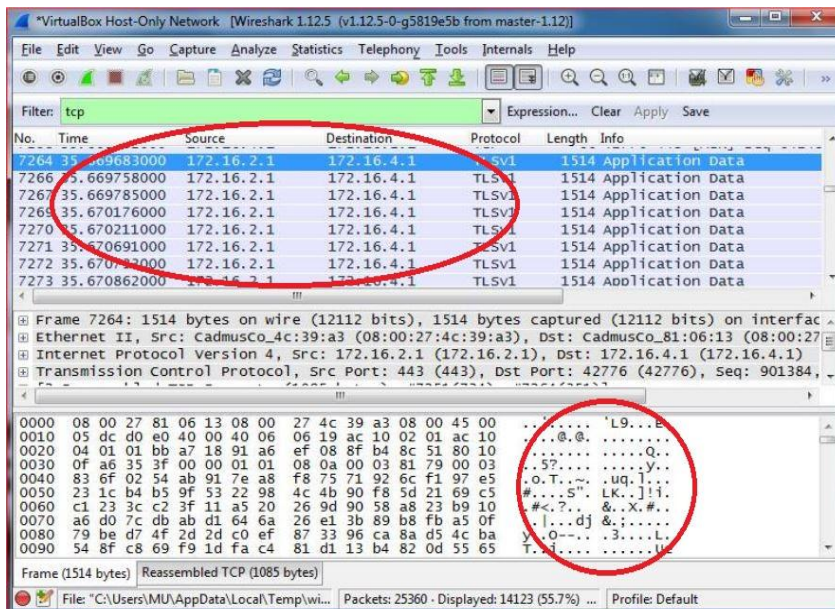
Hasil pengujian diperoleh melakukan ping test dan testing sharing data antar client pada jaringan VPN IPsec dengan network yang berbeda menggunakan tools TCPDump yang berfungsi untuk melakukan capture, membaca atau mendumping paket yang sedang ditransmisikan melalui jalur TCP saat pengujian koneksi menggunakan VPN IPsec, Hasil capture yang didapat dengan menggunakan aplikasi TCPCump diperoleh hasil dimana penggunaan protokol keamanan Authentication Header (AH) dan Encapsulating Security Payload (ESP) dimana protokol tersebut menawarkan autentikasi pengguna dan perlindungan dari beberapa), dan juga menyediakan fungsi autentikasi terhadap data serta integritas terhadap data serta melakukan enkapsulasi serta enkripsi terhadap data pengguna untuk meningkatkan kerahasiaan data

### 3.2 PEMBAHASAN

Peneliti melakukan pengujian Akhir dengan beberapa serangan terhadap jaringan di Universitas Muhammadiyah Palembang, dengan hasil pengujian beberapa serangan sebagai berikut :

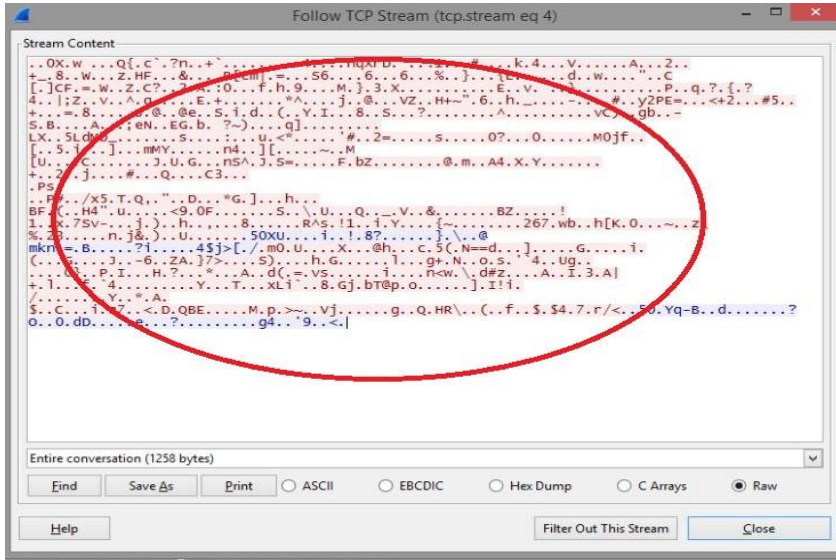
#### 3.2.1 Sniffing Jaringan IPsec dengan Wireshark

Proses sniffing menggunakan Wireshark pada kedua pengujian yaitu sebelum dan sesudah diimplementasikan protocol AH dan ESP Isec. Diperoleh hasil yang berbeda dianantara keduanya. Sniffing yang dilakukan pada VPN PPTP hanya menunjukkan aktivitas tunnel VPN hal itu ditunjukkan pada kolom info yaitu encapsulated PPP dan compressed data, sehingga tidak dapat menunjukkan tahap selanjutnya yaitu “follow tcp stream”. Hasil penangkapan menunjukkan bahwa paket data yang dikirim telah dienkapsulasi melalui tunnel VPN dan hal ini membuktikan bahwa enkripsi telah berjalan dengan baik dan aman untuk digunakan di jalur internet publik dapat dilihat pada gambar 3.



Gambar 3. Hasil Capture Sniffing IPsec

Pada saat melakukan tahap selanjutnya yaitu follow tcp stream diperoleh hasil yang tidak jelas atau acak seperti yang terlihat pada gambar 4 yang menunjukkan data random atau acak dari hasil capture dengan wireshark. Maka data tidak bisa di curikarne sudah terenkripsi.

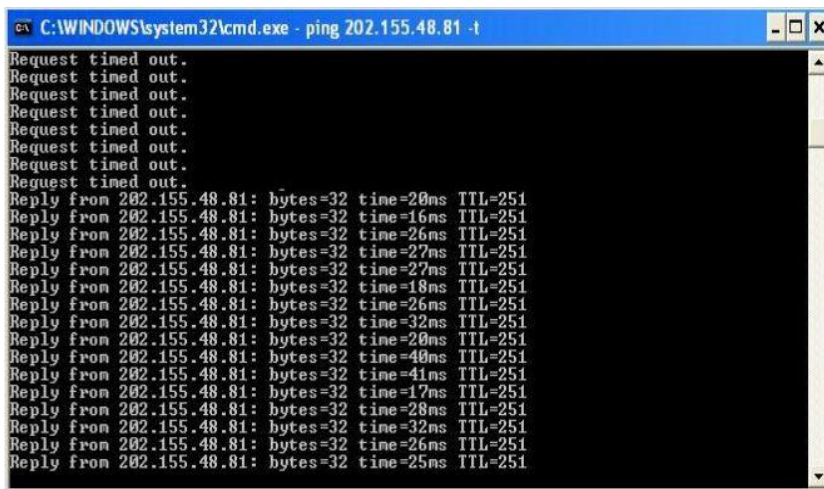


Gambar 4. tcp stream

### 3.2.2 DoS Pingflood

Pada pengujian sebelum nya dapat dilihat bahwa terjadi terputusnya koneksi karena pada saat mengirim ping dengan jumlah besar maka koneksi akan terputus. Yang semula koneksinya lancar tiba-tiba mengalami down dengan adanya *request time out*.

Setelah diterapkannya protocol Authentication Header (AH) dan Encapsulating Security Payload (ESP) maka hasil pengujian dengan serangan Dos Pingflood menunjukkan bahwa koneksi nya juga terputus karena pingflood hanya mengganggu koneksi sementara tidak mematikan koneksi. Apabila sudah mencapai total paket yaitu 100000, maka koneksi kembali normal. dapat dilihat pada gambar 5 dibawah ini :



Gambar 5. Koneksi IP target Normal kembali

#### 4. KESIMPULAN

Berdasarkan pembahasan dan evaluasi dari bab-bab sebelumnya, maka diperoleh kesimpulan sebagai berikut:

1. Penggunaan IPSec akan meningkatkan keamanan pada jaringan komputer karena IPSec melakukan enkripsi terhadap data yang dikirim pada jaringan tersebut. Seandainya terjadi penyadapan data oleh pihak ketiga, maka data asli tidak dapat dilihat dengan mudah tanpa mengetahui kunci enkripsi yang digunakan.
2. Setelah diimplementasikan Protokol AH dan ESP pada router KPA maka data yang dikirim melalui server akan terenkripsi dan terautentikasi dengan baik.
3. Dengan melakukan serangan yaitu dengan Sniffing packet data, Dos Pingflood dan TCPCDump maka hasil yang didapat paket tidak bisa dicuri karena packet data sudah dibungkus dengan protokol AH dan ESP, Kecuali Dos Pingflood karena sistem pengujian konektivitas hanya terganggu pada saat terjadi pingflood.

#### DAFTAR PUSTAKA

- [1] H. Wijaya, *Belajar Sendiri: Cisco ADSL Router Pix Firewall dan VPN*, Jakarta: Penerbit Elex Media Komputindo, 2006.
- [2] N. Kock, *Information Systems Action Research*, United State: Springer US, 2007.
- [3] M. G. Martinsons and N. Kock, "Principles of canonical action research," *Information Systems Journal*, vol. 4, pp. 65-86, 2004.