Keamanan Informasi

Asyrofi Fadhil Al-Ahadi
1310651182/TI-E

1. Aspek keamanan informasi mempunyai ruang lingkup yang luas. Menurut referensi dari ebook CISSP, ruang lingkup materi dari keamanan informasi terdiri dari 10 pokok permasalahan. Dari 10 pokok permasalahan tersebut, silakan buatlah resume salah satu pokok permasalahan dari keamanan informasi mengacu terhadap ebook CISSP yang sudah saya upload di elearning.

- **Access Control**

  Access control meliputi identifikasi, otentifikasi, otorisasi, model model pengendalia akses, teknik kendali akses, metode pengedalian akses, administrasi pengedalian akses, dan ancaman-ancaman pengedalian akses. Contoh implementasinya adalah dengan melakukan identifikasi username, tanda tangan, sidik jari, dan kartu anggota, kemudian melakukan otentifikasi dengan menggunaakn password serta mengotorisasi hak akses.Tujuan dari kontrol akses untuk memungkinkan pengguna yang berwenang mengakses data yang sesuai dan menolak akses ke pengguna yang tidak sah. Kontrol akses melindungi terhadap ancaman seperti akses yang tidak sah, modifikasi yang tidak pantas data, dan hilangnya kerahasiaan.

- **Telecommunications and Network Security**

  Telekomunikasi dan Jaringan Keamanan meliputi pengamanan pada tujuah lapisan jaringan OSI layer, model rujukan protocol TCP/IP, topologi LAN, MAN, WAN, VPN, perangkat jaringan kabel dan nirkabel serta firewall.Telekomunikasi dan Keamanan Jaringan (sering disebut "telecommunikation, "singkatnya) berfokus pada kerahasiaan, integritas, dan ketersediaan data digerak.

- **Information Security Governance and Risk Management**

  Meliputi alur pertanggung jawaban, administrasi, model keamaan organisasi, keperluan keamanan untuk bisnis, pengelolaan resiko, analisis resiko, prosedur, kebijakan, lapisan keamanan, klasifikasi data, dan sosialisasi aspek keamanan, contoh implementasi nya adalah dengan melakukan klasifikasi terhadap hak akses pada suatu berkas/file melalui mengatur status berkas dengan mode R (Read), W (Write) atau X (Execute).

  ANALISIS RISIKO

  Analisis Risiko adalah keterampilan penting untuk keamanan informasi profesional. Kita harus menahan diri untuk standar yang lebih tinggi ketika menilai risiko.keputusan risiko akan menentukan yang pengamanan kita menyebarkan untuk melindungi aset dan jumlah uang dan sumber daya yang kami habiskan melakukannya.

  KEAMANAN INFORMASI TATA

  Keamanan Informasi Pemerintahan adalah keamanan informasi di tingkat organisasi : manajemen senior, kebijakan, proses, dan staf.Organisasi sebagian besar disediakan oleh kepemimpinan senior, yang diperlukan untuk informasi yang berhasil program keamanan.

- **Software Development Security**

  Software Development Security meliputi Tingkatan Kerumitan Fungsi dan Aplikasi, Data, Pengelolaan Keamanan Basis Data, SDLC(Systems

Development Life Cycle) dari suatu aplikasi, metodology pengembangan aplikasi dan pengendalian perubahan perangkat lunak.

- **Cryptography**

  Komunikasi yang aman yang dapat dipahami oleh penerima yang dimaksud saja. Sementara fakta bahwa data sedang dikirim mungkin diketahui, isi data yang harus tetap tidak diketahui kepada pihak ketiga. Data dalam gerakan (bergerak pada jaringan) dan saat istirahat (yang tersimpan pada perangkat seperti disk) dapat dienkripsi.Cryptography merupakan metode untuk menyembunyikan informasi dengan cara melakukan enkripsi atau pengacakan informasi agar tidak dapat dibaca oleh pengguna yang tidak terotorisasi. Pengamaan dapat dilakukan dengan banyak metode kriptografi, diantaranya kriptografi simetrik dan asimetrik. Implementasinya otorisasi dan identifikasi dapat dilakukan dengan tanda tangan digital.

- **Security Architecture and Design**

  Arsitektur keamanan dan Desain menggambarkan hardware logis fundamental, operasi sistem, dan komponen keamanan perangkat lunak dan bagaimana menggunakan komponen-komponen untuk desain, arsitek, dan mengevaluasi sistem komputer aman.Arsitektur keamanan dan Desain melputi konsep, prinsip dan standar untuk merancang dan implementasi aplikasi, sistem operasi dan sistem yang aman.

- **Operations Security**

  Operasi keamanan adalah tentang orang, data, media, perangkat keras, dan ancaman yang terkait dengan masing-masing dalam lingkungan produksi.Operasi keamanan berkaitan dengan ancaman terhadap lingkungan operasi produksi.Agen ancaman bisa menjadi aktor internal atau eksternal, dan keamanan operasi harus memperhitungkan kedua sumber ancaman tersebut agar efektif. Membahas tentang cakupan pemisahan tugas dan wewenang, alur tanggung jawab (akutabilitas), perekrutan sumber daya manusia, pengedalian keluaran/masukan, pengedalian pengelolaan perubahan, penyerangan (Attack), penyusupan, penanggulangan virus dan worm

- **Business Continuity and Disaster Recovery Planning**

  Meliputi Indentifikasi Sumber Daya Bisnis, Penentuan Nilai Bisnis, Analisa Kegagalan (impact) Bisnis (BIA), Analisa Kerugian, Pengelolaan Prioritas dan Krisis, Rencana Pengembangan, Rencana Implementasi dan Rencana Pemeliharaan

- **Legal, Regulations, Investigations, and Compliance**

  Membahas tentang Hukum, Aturan, dan Etika, Transaksi Elektronis perusahaan, Hak Kekayaan Intelektual, Pembajakan, Undang-undang keamanan dan eksport, Penyelidikan Kejahatan Komputer dan Privasi

- **Physical (Environmental) Security**

  Mendefiniskan berbagai ancaman, resiko dan kontrol untuk pengamanan fasilitas sistem informasi. Pengamanan serta kesiagaan dari adanya ancaman kerusakan fisik akibat bencana atau kecelakaan teknis yang tidak terduga, seperti kebakaran, sabotase hardware dll.

2. Cari software atau tools pendukung keamanan informasi kemudian cobalah fungsional software tersebut untuk menangani kasus tertentu. Buatlah step by step yang terdiri dari screenshot, keterangan gambar, dan analisis. Misalnya penggunaan wireshark dalam melakukan analisis paket data jaringan (pcap file), penggunaan ftk forensic untuk mengetahui file steganografi, dan lain sebagainya.

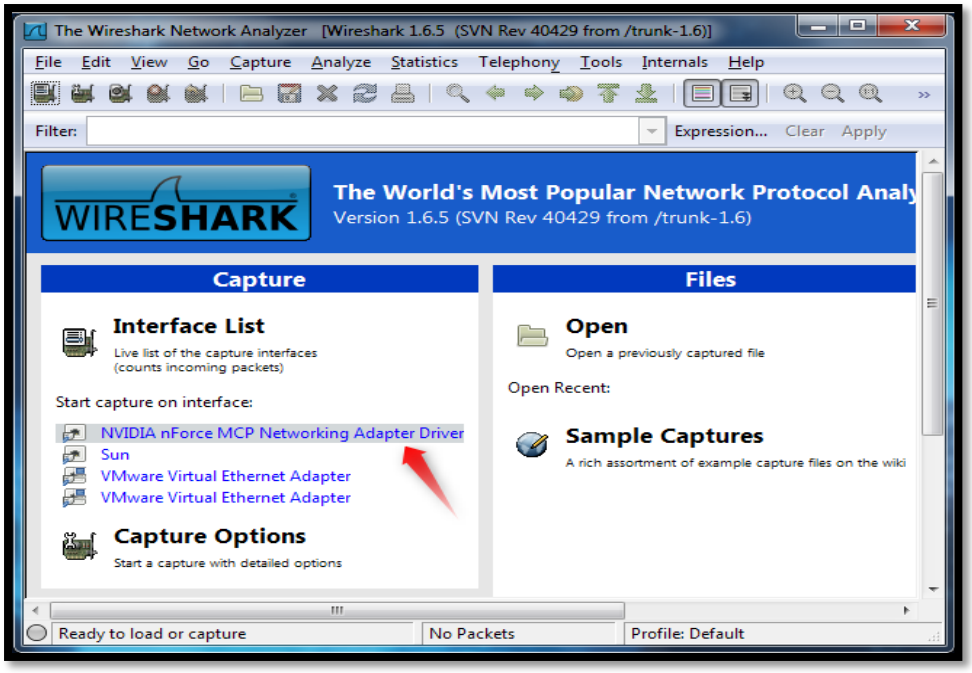
Penggunakan Wireshark Untuk Menangkap, Memfilter Dan Menginspeksi Paket Data

Wireshark, *tool* analisis jaringan yang dulunya bernama Ethereal, menangkap paket data serta menampilkannya dengan format yang dapat dibaca oleh manusia. Wireshark, memiliki *filter*, *coding* berwarna, dan fitur lainnya yang mampu membuat Anda mendalami *traffic* jaringan serta menginspeksi paket data individual.

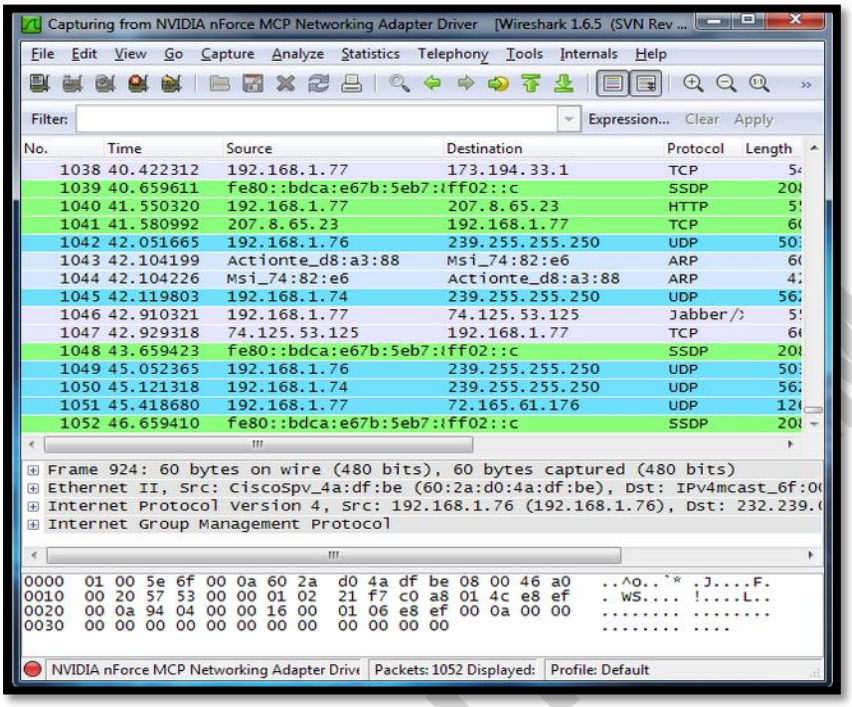
Artikel ini akan menjelaskan kepada Anda cara menggunakan Wireshark untuk menangkap, memfilter dan menginspeksi paket data. Anda bisa menggunakan Wireshark untuk menginspeksi *traffic* jaringan dari program yang mencurigakan, menganalisa aliran *traffic* jaringan Anda, serta melakukan *troubleshoot* masalah jaringan.

- **Menangkap Paket Data**

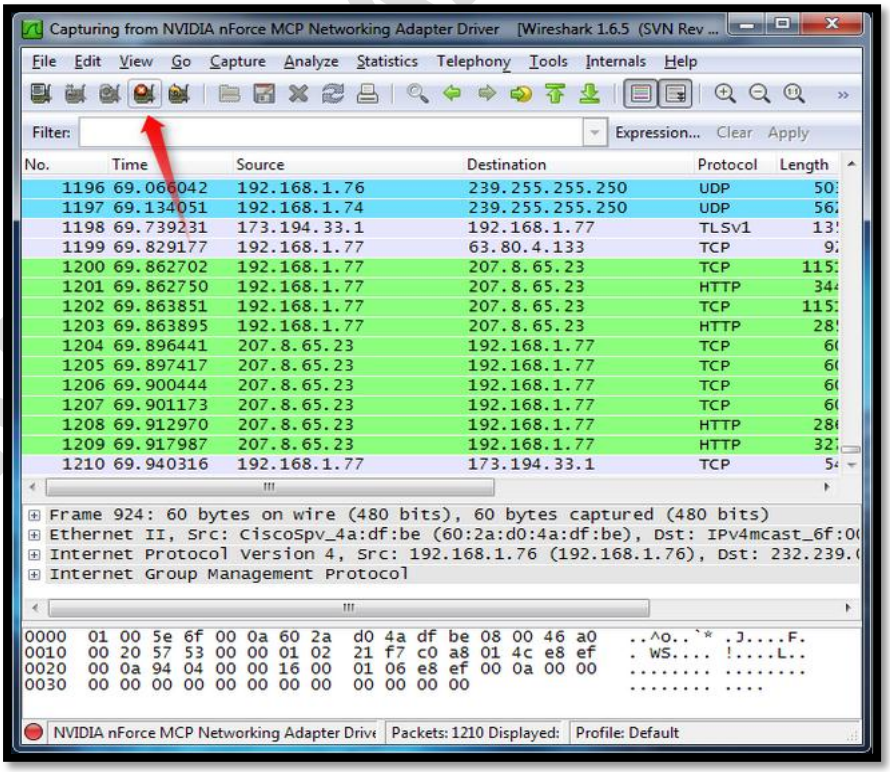
Setelah mengunduh dan memasang Wireshark, Anda bisa menjalankannya dan mengklik nama dari sebuah *interface* pada*Interface List* untuk mulai menangkap paket data pada *interface* tersebut. Contohnya, jika Anda ingin menangkap paket data dari jaringan nirkabel, klik *interface* nirkabel Anda.



Segera setelah Anda mengklik nama *interface*, Anda akan melihat paket data mulai muncul pada jendela Wireshark. Program ini menangkap tiap paket data yang dikirim ke atau dari sistem Anda. Jika Anda menangkap paket data dari*interface* nirkabel, dan mengaktifkan *promiscuous mode* pada opsi *capture*, Anda juga akan melihat paket lainnya yang ada pada jaringan.

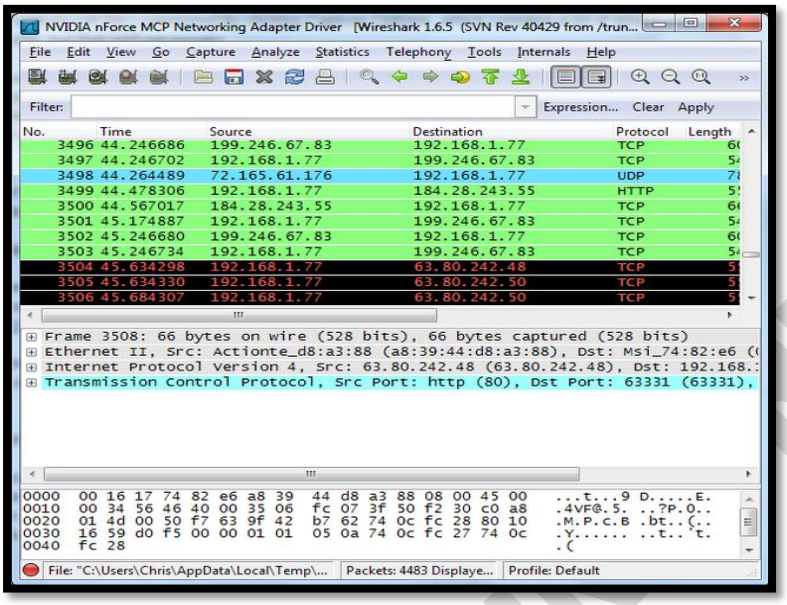


Klik tombol *stop capture* yang ada pada bagian sudut kiri atas jendela jika Anda ingin berhenti menangkap paket data.



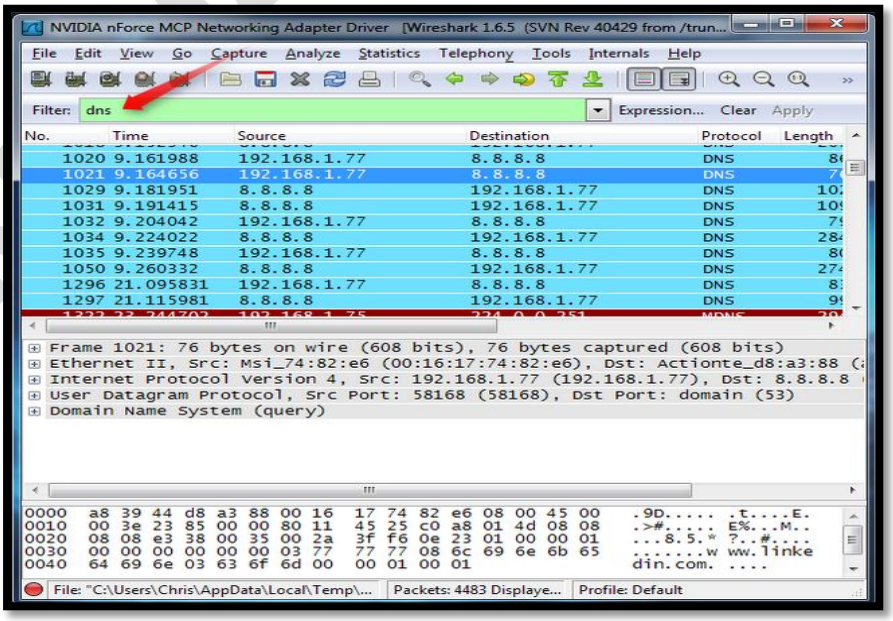
- **Coding Berwarna**

Anda akan melihat paket data yang berwarna hijau, biru, atau hitam. Wireshark menggunakan warna agar Anda dapat mengidentifikasi jenis data. Pada pengaturan awal, hijau artinya *traffic* TCP, biru gelap artinya *traffic* DNS, biru terang artinya *traffic* UDP dan hitam berarti paket TCP yang bermasalah.

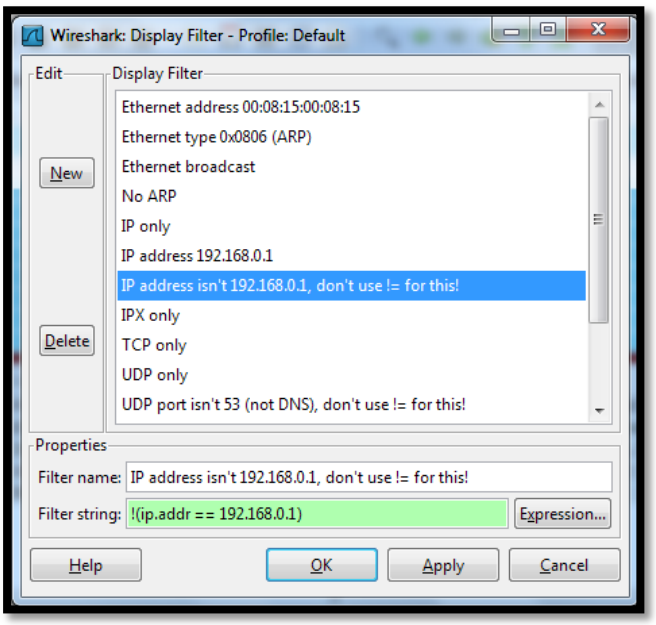


- **Memfilter Paket Data**

Jika Anda ingin menginspeksi hal tertentu, seperti *traffic* sebuah yang dikirim sebuah program ketika menelpon rumah, Wireshark dapat menutup semua aplikasi lainnya yang menggunakan jaringan sehingga Anda bisa menentukan *traffic*tertentu itu. Tetapi jika Anda cenderung memiliki jumlah data yang besar untuk diinspeksi, disini Anda bisa menggunakan filter untuk memilah-milah paket data.

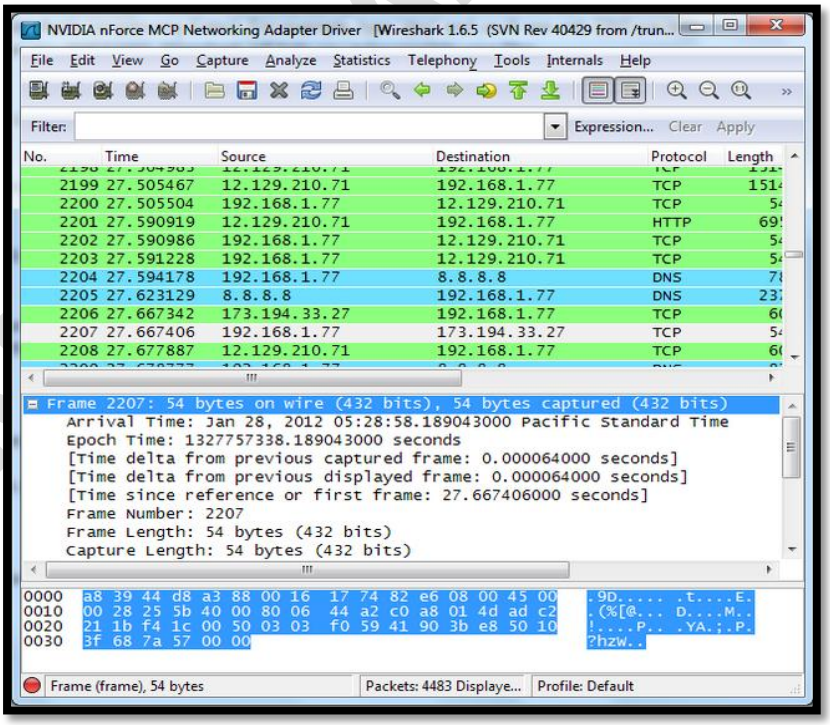


Cara yang paling dasar untuk menggunakan filter adalah dengan cara mengetikkannya pada kotak filter yang ada pada bagian paling atas jendela Wireshark. Contohnya, ketikkan ***dns*** jika Anda hanya ingin melihat paket DNS. Ketika Anda mulai mengetik, Wireshark akan membantu Anda dengan fitur *autocomplete.* Anda juga bisa mengklik menu Analize dan memilih*Display Filters* untuk membuat sebuah filter baru.

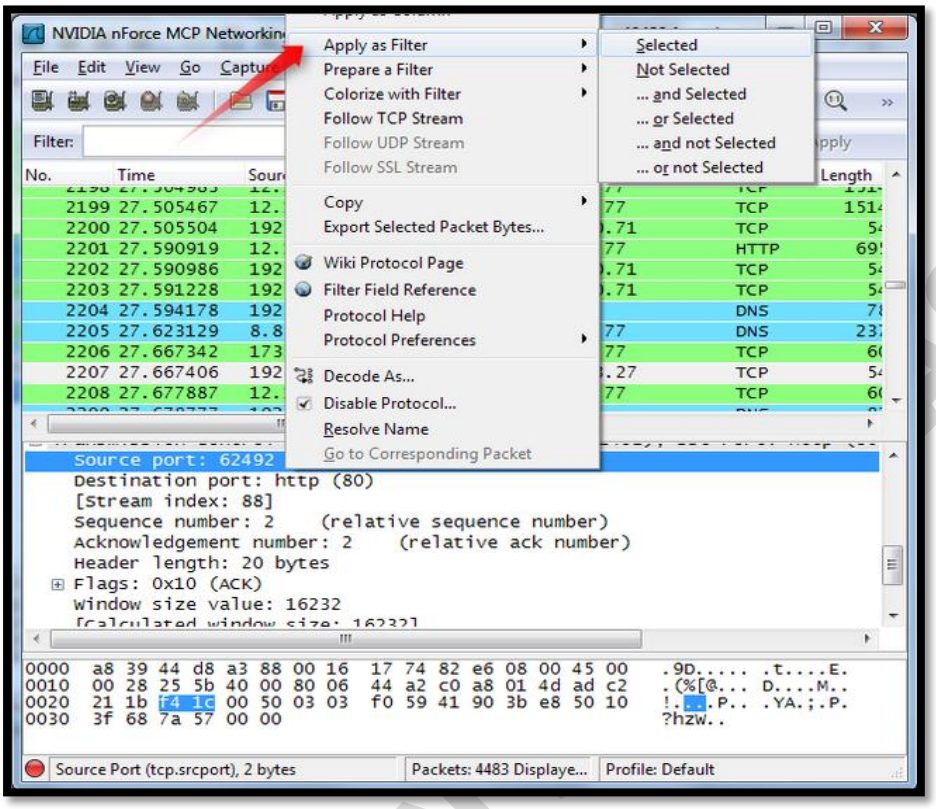


- **Menginspeksi Paket**

Klik paket data untuk memilihnya, serta menampilkan detail paket tersebut.



Anda juga bisa membuat filter dari sini. Kli kanan pada satu dari detail dan gunakan submenu *Apply as Filter* untuk membuat filter dari sini.



Sekian Terima Kasih ☺