Nama : Rendy Sapta Ramadhan

NIM : 131 065 1098

Kelas : D

Tugas : 1

Domain 5:

Cryptography

KONSEP KRIPTOGRAFI CORNERSTONE

Konsep kriptografi dasar yang diwujudkan oleh semua enkripsi yang kuat dan harus dipahami sebelum belajar tentang implementasi spesifik.

Istilah kunci

Kriptologi adalah ilmu komunikasi yang aman.Kriptografi menciptakan pesan yang maknanya tersembunyi,Banyak yang menggunakan kriptografi jangka di tempat kriptologi,Sebuah cipher adalah algoritma kriptografi.Sebuah plaintext adalah pesan terenkripsi.Enkripsi mengubah plaintext ke ciphertext a.Dekripsi ternyata ciphertext kembali ke plaintext a.

ENCRYPTION SYMMETRIC

Enkripsi simetris menggunakan satu kunci untuk mengenkripsi dan mendekripsi.Jika Anda mengenkripsi file zip dan kemudian mendekripsi dengan kunci yang sama, Anda menggunakan enkripsi simetris.Enkripsi simetris juga disebut "kunci rahasia" enkripsi: kunci harus dirahasiakan dari pihak ketiga.Kekuatan termasuk kecepatan dan kekuatan kriptografi per bit dari kunci.Kelemahan utama adalah bahwa kunci harus aman bersama sebelum kedua pihak dapat berkomunikasi secara aman.Kunci simetris sering bersama melalui metode out-of-band, seperti melalui tatap muka diskusi.

Tanda tangan digital

Tanda tangan digital digunakan untuk dokumen tanda kriptografi.Tanda tangan digital memberikan nonrepudiation, yang mencakup otentikasi identitas penandatangan, dan bukti integritas dokumen (membuktikan dokumen tidak berubah).Ini berarti pengirim tidak dapat menyangkal nanti (atau menolak) menandatangani dokumen.

Infrastruktur Kunci Publik

Public Key Infrastructure (PKI) memanfaatkan semua tiga bentuk enkripsi untuk menyediakan dan mengelola sertifikat digital.Sebuah sertifikat digital adalah kunci publik ditandatangani dengan tanda tangan digital.Sertifikat digital mungkin berdasarkan server atau

client berbasis.Jika keduanya digunakan bersama-sama, mereka menyediakan saling otentikasi dan enkripsi.

Asosiasi keamanan dan ISAKMP

AH dan ESP dapat digunakan secara terpisah atau dalam kombinasi.Asosiasi Keamanan IPsec (SA) adalah simpleks (satu arah) koneksi, yang dapat digunakan untuk bernegosiasi ESP atau AH parameter.Jika dua sistem berkomunikasi melalui ESP, mereka menggunakan dua DS (satu untuk setiap arah).Jika sistem leverage yang AH selain ESP, mereka menggunakan dua DS, untuk total empat.Sejumlah 32-bit yang unik disebut Parameter Indeks Keamanan (SPI) mengidentifikasi setiap simpleks SA koneksi.Asosiasi Internet Security dan Key Management Protocol (ISAKMP) mengelola proses pembuatan SA.

Mode tunnel dan transportasi

IPsec dapat digunakan dalam mode tunnel atau mode transportasi.Mode tunnel digunakan oleh gateway keamanan (yang dapat memberikan point-to-point terowongan IPsec).ESP mode tunnel mengenkripsi seluruh paket, termasuk paket header asli.Modus transportasi ESP hanya mengenkripsi data (dan bukan header asli);ini umumnya digunakan ketika sistem mengirim dan menerima dapat "berbicara" IPsec native.

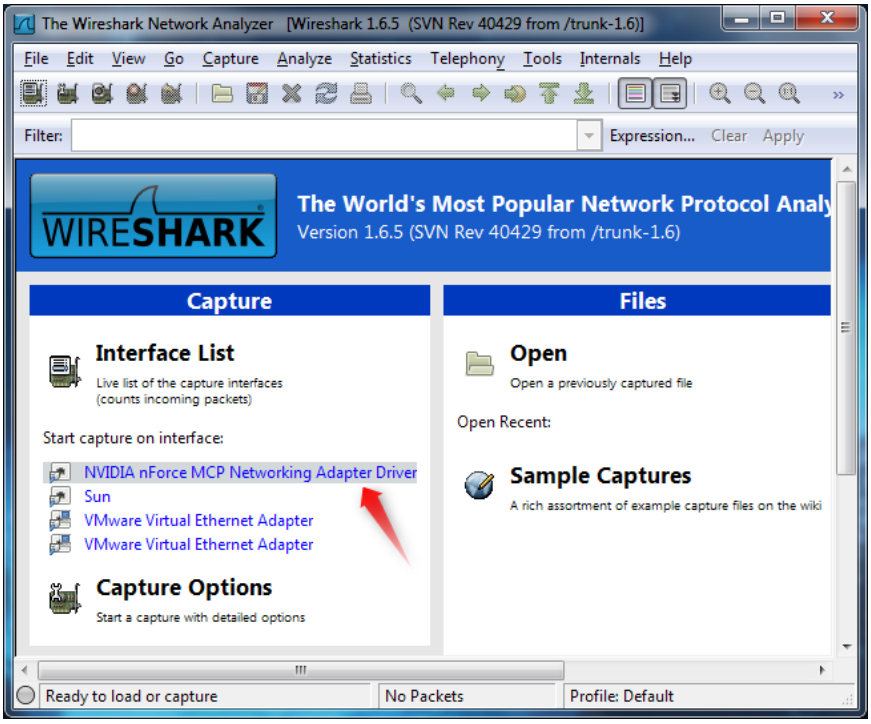
CRUNCH WAKTU

AH mengotentikasi header IP asli, sehingga sering digunakan (bersama dengan ESP) dalam mode transportasi karena header asli tidak dienkripsi.Mode tunnel biasanya menggunakan ESP sendiri (header asli akan dienkripsi, dan dengan demikian dilindungi, oleh ESP).

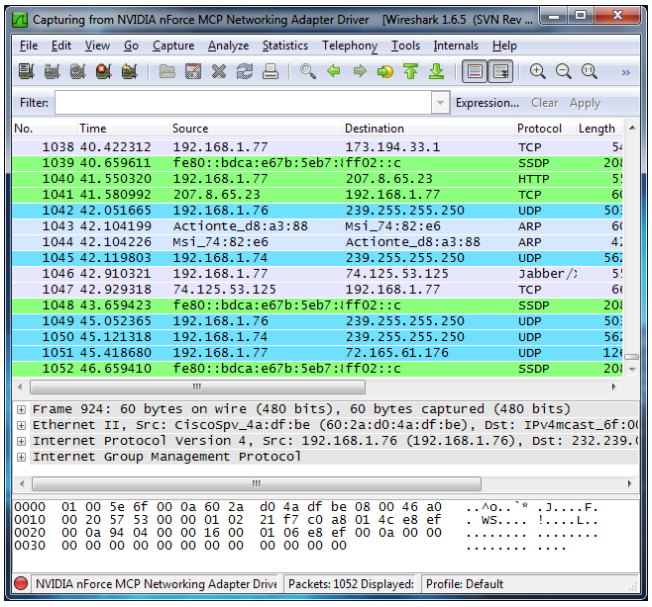
Tugas : 2

Wireshark Menangkap Paket Data

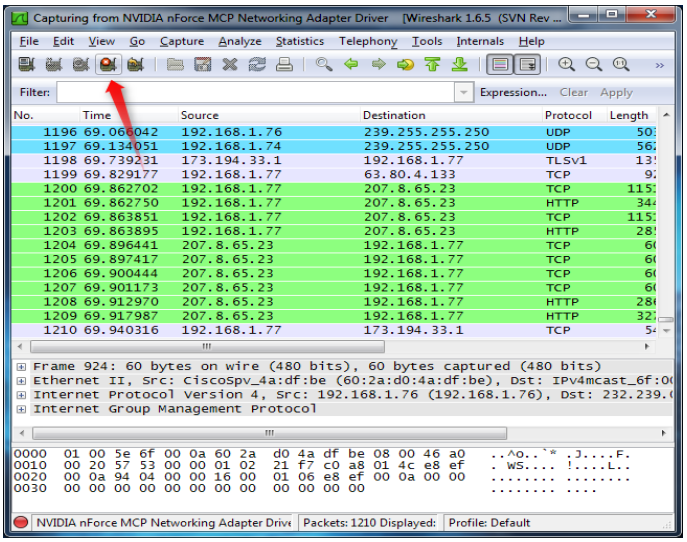
Setelah mengunduh dan memasang Wireshark, Anda bisa menjalankannya dan mengklik nama dari sebuah *interface* pada *Interface List* untuk mulai menangkap paket data pada *interface* tersebut. Contohnya, jika Anda ingin menangkap paket data dari jaringan nirkabel, klik *interface* nirkabel Anda.



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.

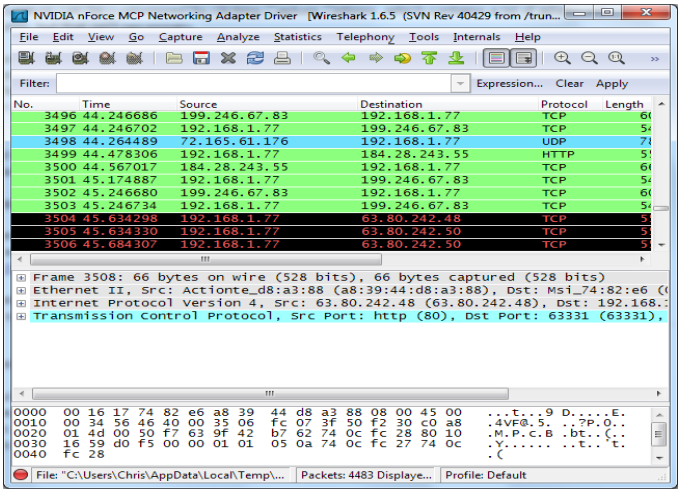


Klik tombol *stop capture* yang ada pada bagian sudut kiri atas jendela jika Anda ingin berhenti menangkap paket data.



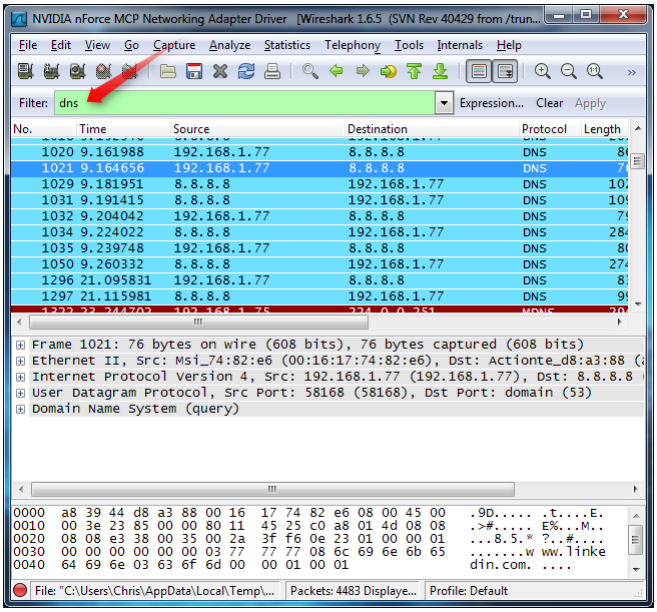
Coding Berwarna

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.

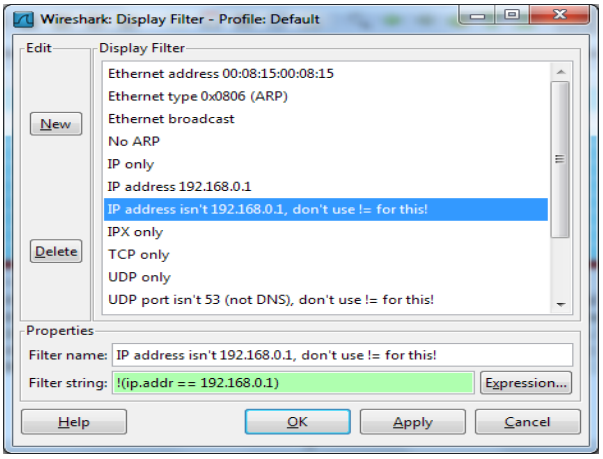


Memfilter Paket Data

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.

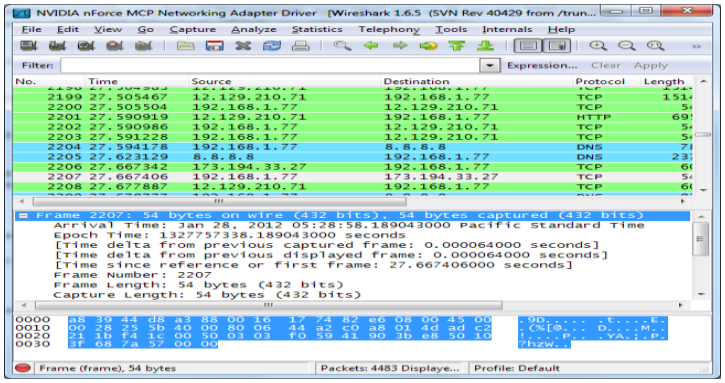


Cara yang paling dasar untuk menggunakan filter adalah dengan cara mengetikkannya pada kotak filter yang ada pada bagian paling atas jendela Wireshark. Contohnya, ketikkan ***dns*** jika Anda hanya ingin melihat paket DNS. Ketika Anda mulai mengetik, Wireshark akan membantu Anda dengan fitur *autocomplete.* 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.