Nama : RIYAN SUDIBYO

Nim : 1310651074

Kelas : E

Soal nomer 1

Cryptography

Cryptography berasal dari kata *crypto* yang berarti ”*hidden, secret*” dan pada bidang studi informatika dapat diartikan dengan studi mengenai menyembunyikan informasi atau informasi yang disembunyikan (*hiding information*). Pada saat ini, ilmu ini berkembang dan dapat dikategorikan menjadi tiga kelompok utama, yaitu:

1. Penggunaan operasi matematika yang mengubah *plaintext* (sumber informasi atau informasi aslinya) ke dalam bentuk ciphertext (informasi yang sudah dikodekan) menggunakan kunci enkripsi.
2. Apakah dibentuk sebuah block atau sebuahstream cipher.
3. Penggunaan satu atau dua kunci sistem.

Tujuan kriptografi: 1. *Deter* (menghalangi)
2. *Prevent* (mencegah)
3. *Detect* (menemukan)
4. *Correct* (membetulkan)

atas pelanggaran keamanan, termasuk pada saat melakukan pengiriman (*transmission*) informasi.

- Karakteristik cryptosytem yang baik sebagai berikut :
  - Keamanan sistem terletak pada kerahasiaan kunci dan bukan pada kerahasiaan algoritma yang digunakan.
  - Cryptosystem yang baik memiliki ruang kunci (keyspace) yang besar.
  - Cryptosystem yang baik akan menghasilkan ciphertext yang terlihat acak dalam seluruh tes statistik yang dilakukan terhadapnya.
  - Cryptosystem yang baik mampu menahan seluruh serangan yang telah dikenal sebelumnya
- Macam Cryptosytem

- Symmetric Cryptosystem

  Dalam symmetric cryptosystem ini, kunci yang digunakan untuk proses enkripsi dan dekripsi pada prinsipnya identik, tetapi satu buah kunci dapat pula diturunkan dari kunci yang lainnya.
- Assymmetric Cryptosystem

  Dalam assymmetric cryptosystem ini digunakan dua buah kunci. Satu kunci yang disebut kunci publik (public key) dapat dipublikasikan, sedang kunci yang lain yang disebut kunci privat (private key) harus dirahasiakan. Proses menggunakan sistem ini dapat diterangkan secara sederhana sebagai berikut : bila A ingin mengirimkan pesan kepada B, A dapat menyandikan pesannya dengan menggunakan kunci publik B, dan bila B ingin membaca surat tersebut, ia perlu mendekripsikan surat itu dengan kunci privatnya. Dengan demikian kedua belah pihak dapat menjamin asal surat serta keaslian surat tersebut, karena adanya mekanisme ini. Contoh : sistem ini antara lain RSA Scheme dan Merkle-Hellman Scheme.

- Protokol Cryptosystem

  Cryptographic protocol adalah suatu protokol yang menggunakan kriptografi. Protokol ini melibatkansejumlah algoritma kriptografi, namun secara umum tujuan protokol lebih dari sekedar kerahasiaan.Pihak-pihak yang berpartisipasi mungkin saja ingin membagi sebagian rahasianya untuk menghitungsebuah nilai, menghasilkan urutan random, atau pun menandatangani kontrak secara bersamaan.

  Penggunaan kriptografi dalam sebuah protokol terutama ditujukan untuk mencegah atau pun mendeteksi adanya eavesdropping dan cheating.
- Jenis Penyerangan Pada Protokol
  - Ciphertext-only attack. Dalam penyerangan ini, seorang cryptanalyst memiliki ciphertext dari sejumlah pesan yang seluruhnya telah dienkripsi menggunakan algoritma yang sama.
  - Known-plaintext attack. Dalam tipe penyerangan ini, cryptanalyst memiliki akses tidak hanya ke ciphertext sejumlah pesan, namun ia juga memiliki plaintext pesan-pesan tersebut.
  - Chosen-plaintext attack. Pada penyerangan ini, cryptanalyst tidak hanya memiliki akses atas ciphertext dan plaintext untuk beberapa pesan, tetapi ia juga dapat memilih plaintext yang dienkripsi.

6. Jenis Penyerangan Pada Jalur Komunikasi.

- Sniffing: secara harafiah berarti mengendus, tentunya dalam hal ini yang diendus adalah pesan (baik yang belum ataupun sudah dienkripsi) dalam suatu saluran komunikasi. Hal ini umum terjadi pada saluran publik yang tidak aman. Sang pengendus dapat merekam pembicaraan yang terjadi.
- Replay attack [DHMM 96]: Jika seseorang bisa merekam pesan-pesan handshake (persiapan komunikasi), ia mungkin dapat mengulang pesan-pesan yang telah direkamnya untuk menipu salah satu pihak.

- Spoofing [DHMM 96]: Penyerang – misalnya Maman – bisa menyamar menjadi Anto. Semua orang dibuat percaya bahwa Maman adalah Anto. Penyerang berusaha meyakinkan pihak-pihak lain bahwa tak ada salah dengan komunikasi yang dilakukan, padahal komunikasi itu dilakukan dengan sang penipu/penyerang. Contohnya jika orang memasukkan PIN ke dalam mesin ATM palsu – yang benar-benar dibuat seperti ATM asli – tentu sang penipu bisa mendapatkan PIN-nya dan copy pita magentik kartu ATM milik sang nasabah. Pihak bank tidak tahu bahwa telah terjadi kejahatan.
- Man-in-the-middle [Schn 96]: Jika spoofing terkadang hanya menipu satu pihak, makadalam skenario ini, saat Anto hendak berkomunikasi dengan Badu, Maman di mata Anto seolah-olah adalah Badu, dan Maman dapat pula menipu Badu sehingga Maman seolah-olah adalah Anto. Maman dapat berkuasa penuh atas jalur komunikas ini, dan bisa membuat berita fitnah.

Soal Nomer 2

WireShark

WireShark adalah sebuah free software yang digunakan untuk analisis jaringan yang biasa digunakan oleh network administrator untuk menganalisa kinerja jaringan termasuk protocol di dalamnya. Tujuan dari monitoring dengan wireshrak adalah,

- Memecahkan masalah jaringan
- Memerikasa Keamanan Jaringan
- Men-debug implementasi protocol
- Mempelajari protocol jaringan internal

Wireshark ini memiliki beberapa keuntungan, diantaranya dapat memantau paket paket data yang diterima dari internet. WireShark ini bekerja pada layer Aplikasi. Yaitu layer terakhir dari OSI Layer. Dengan menggunakan protocol protocol di layer application HTTP, FTP, TELNET, SMTP, DNS kita dengan mudah memonitoring jaringan yang ada.

HTTP (*Hypertext Transfer Protocol*)

HTTP adalah suatu protocol dari Layer Aplikasi yang mementukan aturan dalam pengambilan dokumen di web browser server sehingga dokumen tersebut bisa di akses dalam bentuk HTML.
Pada HTTP termasuk ke dalam jenis fungsi sebagai client-server. Client adalah browser yang meminta,menerima,dan menampilkan objek web. Sedangkan, server adalah browser yang mengirimkan objek atas suatu request dari client.

FTP (*File Transfer Protocol*)

FTP adalah suatu protocol yang berfungsi untuk tukar menukar file dalam sauatu network. Ada dua hal penting dalam FTP yaitu FTP server dan FTP client.
Tujuan FTP server adalah sebagai berikut :
1. Untuk mensharing data.
2. Untuk menyediakan indirect atau implicit remote computer.
3. Untuk menyediakan tempat penyimpanan bagi user.
4. Untuk menyediakan transfer data yang reliable dan efisien.

FTP sebenarnya cara yang tidak aman untuk mentransfer file karena file tersebut ditransfer tanpa melalui enkripsi terlebih dahulu tetapi melalui clear text.

Telnet

Telnet adalah aplikasi remote login Internet. Telnet digunakan untuk login ke komputer lain di Internet dan mengakses berbagai macam pelayanan umum, termasuk katalog perpustakaan dan berbagai macam database. Telnet memungkinkan pengguna untuk duduk didepan komputer yang terkoneksi ke internet dan mengakses komputer lain yang juga terkoneksi ke internet.
Telnet menggunakan 2 program, yang satu adalah client (telnet) dan server (telnetd). Yang terjadi adalah ada dua program yang berjalan, yaitu software client yang dijalankan pada komputer yang meminta pelayanan tersebut dan software server yang dijalankan oleh computer yang menghasilkan pelayanan tadi.

Tugas dari client adalah:
• Membuat koneksi network TCP (Transfer Control Protocol) dengan server.
• Menerima inputan dari user
• Menformat kembali inputan dari user kemudian mengubah dalam bentuk format standard dan dikirim ke server.

• Menerima output dari server dalam format standard.
• Mengubah format output tadi untuk ditampilkan pada layar.

Tugas dari server adalah:
• Menginformasikan software jaringan bahwa komputer itu siap menerima koneksi.
• Menunggu permintaan dalam bentuk format standard.
• Melaksanakan permintaan tersebut.
• Mengirim kembali hasil ke client dalam bentuk format standard.
• Menunggu permintaan selanjutnya.

SMTP (*Simple Mail Transfer Protocol*)

SMTP merupakan salah satu protokol yang umum digunakan untuk pengiriman surat elektronik di Internet. Protokol ini dipergunakan untuk mengirimkan data dari komputer pengirim surat elektronik ke server surat elektronik penerima.
Protokol ini timbul karena desai dari sistem elektronik yang mengharuskan adanya server surat elektronik yang menampung sementara sampai surat elektronik diambil oleh yang berhak.
Sehingga nisa kita simpulkan bahwa terdapat 3(tiga) transfer pada SMTP:
1. Handshaking(greeting)
2. Transfer message
3. Penutup

DNS (*Domain Name System*)

DNS (Domain Name System, bahasa Indonesia: Sistem Penamaan Domain) adalah sebuah sistem yang menyimpan informasi tentang nama host maupun nama domain dalam bentuk basis data tersebar (distributed database) di dalam jaringan komputer, misalkan: Internet. DNS menyediakan alamat IP untuk setiap nama host dan mendata setiap server transmisi surat (mail exchange server) yang menerima surat elektronik (email) untuk setiap domain.

DNS menyediakan servis yang cukup penting untuk Internet, bilamana perangkat keras komputer dan jaringan bekerja dengan alamat IP untuk mengerjakan tugas seperti pengalamatan dan penjaluran (routing), manusia pada umumnya lebih memilih untuk menggunakan nama host dan nama domain, contohnya adalah penunjukan sumber universal (URL) dan alamat e-mail. DNS menghubungkan kebutuhan ini.

Keunggulan DNS antara lain:
1. Mudah, DNS sangat mudah karena user tidak lagi direpotkan untuk mengingat IP address. sebuah komputer cukup host name (nama Komputer).

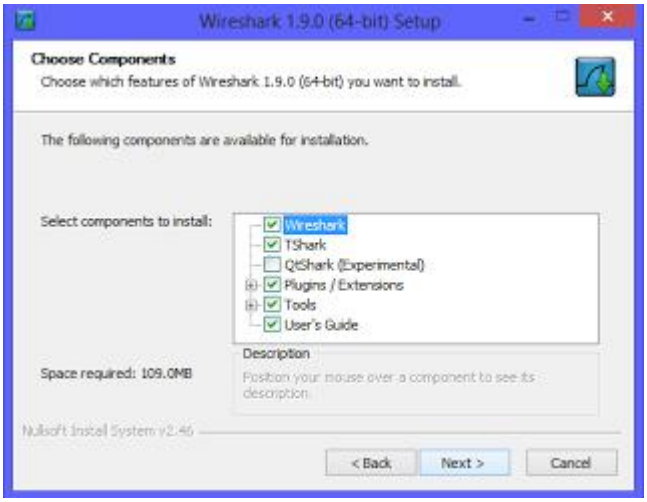
2. Konsisten, IP address sebuah komputer bisa berubah tapi host name tidak berubah.
3. Simple, user hanya menggunakan satu nama domain untuk mencari baik di Internet maupun di Intranet.

WireShark adalah sebuah free software yang digunakan untuk analisis jaringan yang biasa digunakan oleh network administrator untuk menganalisa kinerja jaringan termasuk protocol di dalamnya. Tujuan dari monitoring dengan wireshrak adalah,
- Memecahkan masalah jaringan
- Memerikasa Keamanan Jaringan
- Men-debug implementasi protocol
- Mempelajari protocol jaringan internal

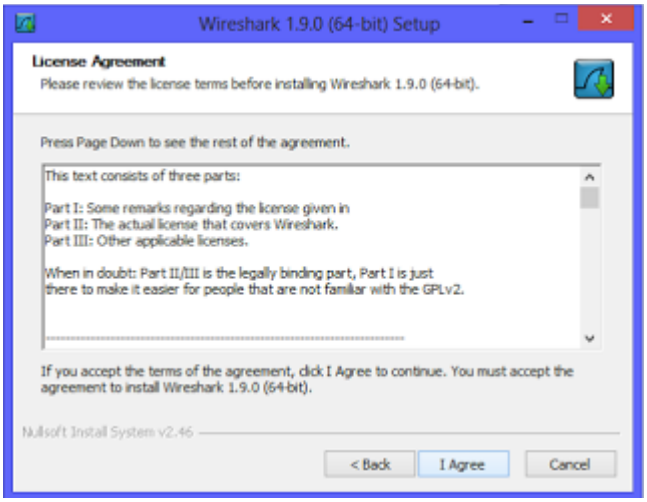
Berikut ini langkah menginstal WireShark :

1. Downlaod Wireshark
2. Ekstrak file dan jalankan WireShark.exe
3. Lakukan proses Instalasi

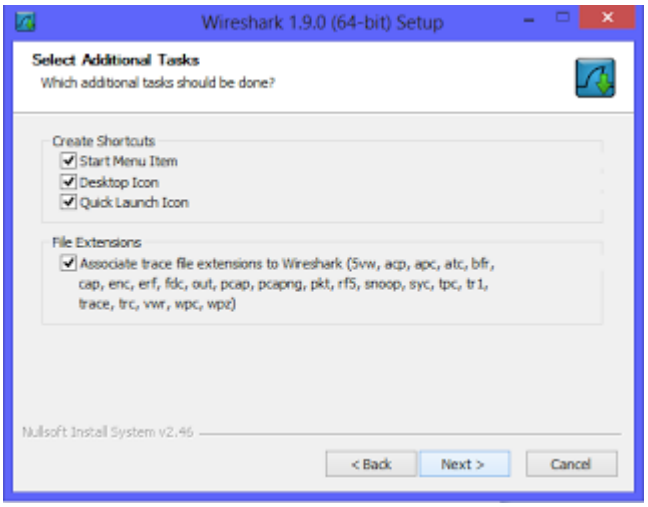
Gambar 1



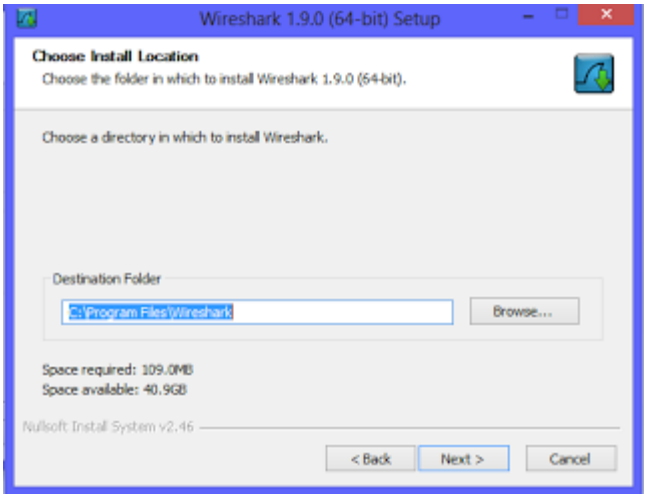
Gambar 2



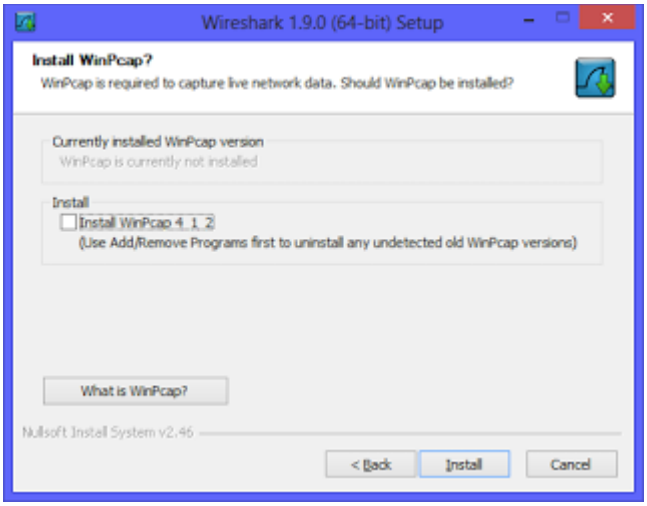
Gambar 3



Gambar 4



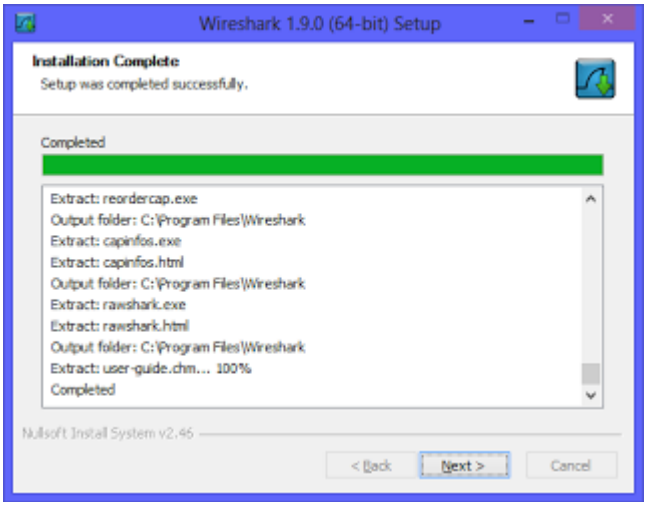
Gambar 5



Gambar 6

Instal Wincap untuk mendeteksi diver yang kalian gunakan.

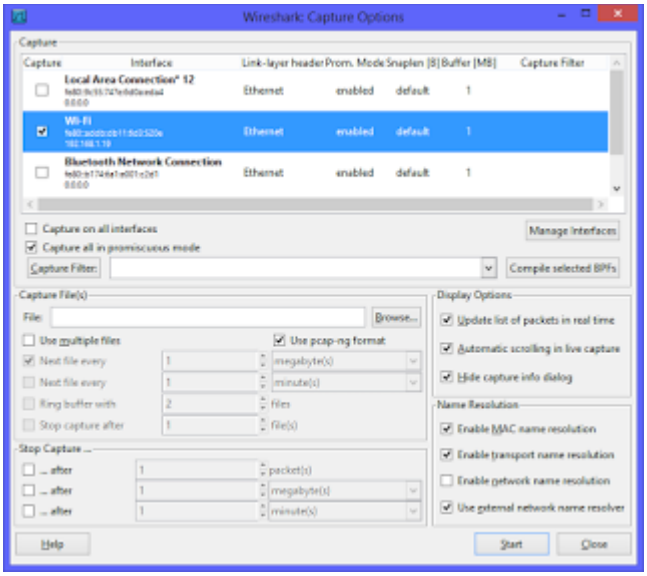
Gambar 7



Gambar

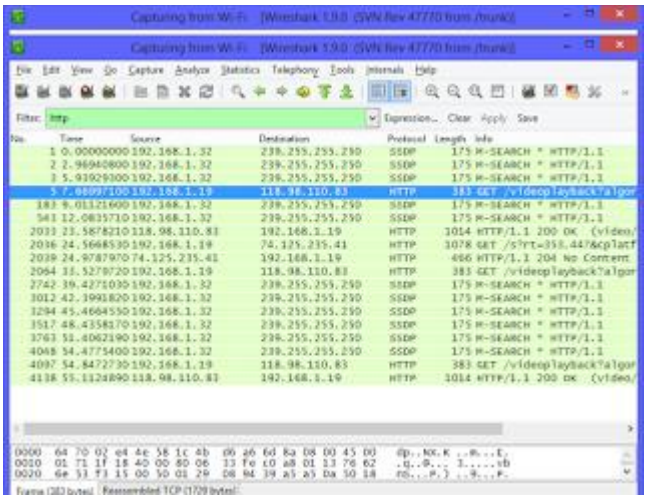
ANALISA

Disini saya mencoba menggunakan wireshark untuk memantau akses browser yang saya jalankan. Namun disini saya mencoba memonitor jaringan wi-fi. langkah pertama untuk memilih driver wireless. saat ditampilan awal kita bisa menenkan tombol **Ctrl +K**



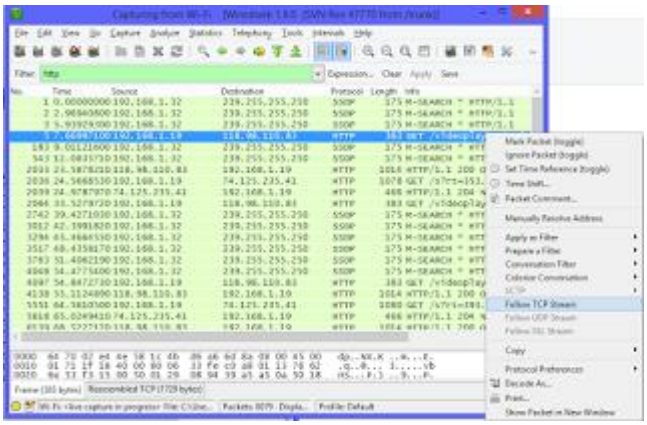
Gambar 9. List driver

Setelah menekan Tombol Strat, maka WireShark akan langsung menampilkan packet packet data yang masuk. Untuk mempermudah monitoring gunakan filter *http*. Filter *http* ini dimaksudkan untuk menampilkan packet data yang berbasis HTTP. Dari hasil yang saya peroleh (Yang saya Block) menunjukkan bahwa ada paket yang diterima dari youtube. kebetulan saat itu saya sedang streaming video di youtube.



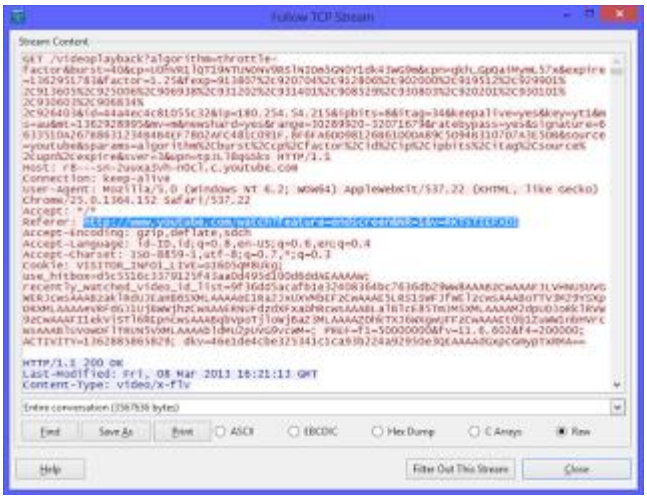
Gambar 10. Hasil Paket Data dengan Filter HTTP

Namun dari data diatas belum bisa menunjukkan hasil junlah packet data, alamat web yang sedang buka maka dari itu packet yang telah dipilh tersebut kita klik kanan, pilih ***follow TCP stream***.



Gambar 11. Follow TCP Stream

Seperti Gambar 12. Bahwa alamat youtube yang sedang saya streaming tertangkap pada wireshark. Jadi dengan wireshark ini bisa memantau alamat alamat web yang kita kunjungi. Namun Video yang sedang saya tonton di youtube saat itu sudah saya play sebelum saya mengaktifkan WireShark. Dengan Kata lain untuk jaringan Wireless, Kemapuan Wireshark ini agak berkurang yaitu WireShark hanya menampilkan data Cookie yang lama sedangkan untuk menampilkan data cookie yang baru dibutuhkan waktu yang cukup lama.



Gambar 12. Hasil dari Follow TCP Stream

Pada follw TCP Stream ini juga ditampilkan Content Type, Date, dan cache control yang digunakan. seperti pada hasil data wireshrak
Content type : Video
Date : Sun, 10 Mar 2013
Cache control privat.