LAPORAN TUGAS KRIPTOGRAFI

MITM

Oleh :

- Muhammad Azriansyah 09011281320006
- Muhammad Ridwan 09011281320009
- Ratih Gustifa 09011281320007

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

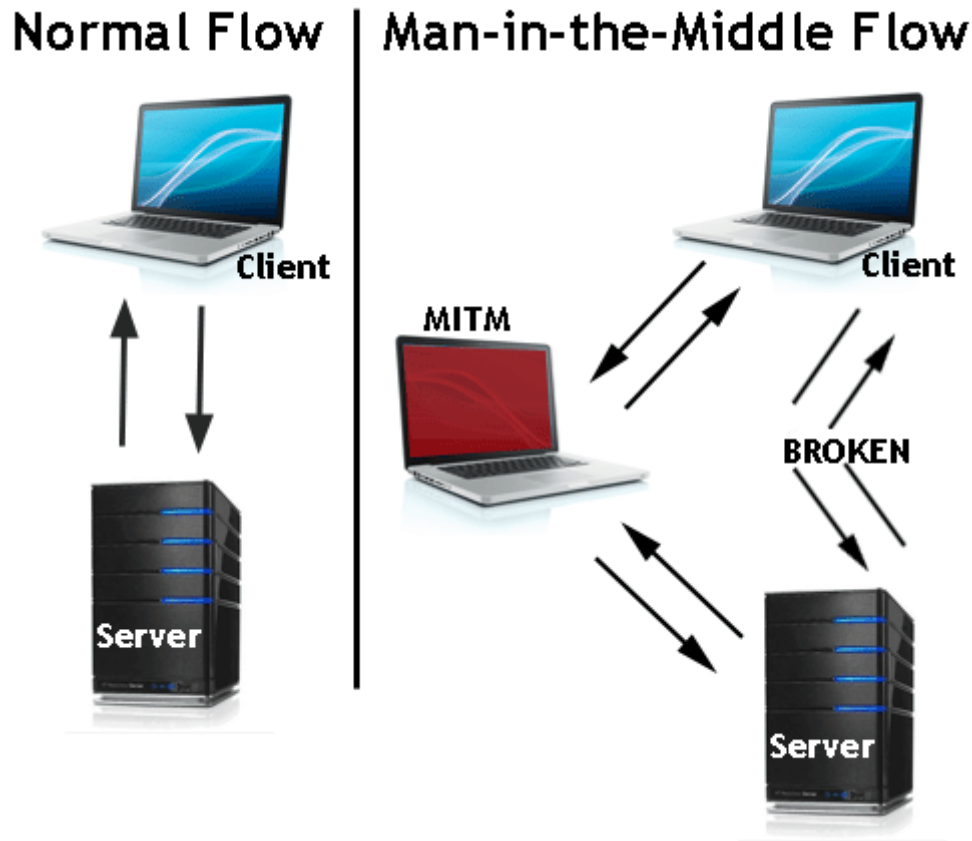
2016

1. Penjelasan MITM (*Man-In-The-Middle*)

MITM adalah Sebuah serangan MITM adalah jenis serangan cyber di mana seseorang berbahaya mendaftarkan dirinya sendiri dalam sebuah percakapan antara dua pihak, impersonates kedua belah pihak dan memperoleh akses terhadap informasi bahwa kedua pihak sedang berusaha untuk mengirim satu sama lain.

MITM memungkinkan seseorang berbahaya untuk mencegat, mengirim, dan menerima data dimaksudkan untuk orang lain, atau tidak dimaksudkan untuk dikirim sama sekali, tanpa baik di luar pihak mengetahui sampai terlambat. Serangan Man in the Middle Attack dapat disingkat dalam banyak cara termasuk, MITM, MitM, Mim, atau MIM

MITM adalah jenis serangan menguping yang terjadi ketika seseorang berbahaya menyisipkan dirinya sebagai relay / proxy ke sesi komunikasi antara orang atau sistem. Sebuah serangan MITM memanfaatkan pengolahan real time transaksi, percakapan, atau transfer data lainnya.
Sebuah serangan Man-in-the-Middle memungkinkan penyerang untuk mencegat, mengirim, dan menerima data tidak pernah dimaksudkan untuk menjadi bagi mereka tanpa mengetahui baik di luar partai sampai terlambat.



Pada gambar di atas Anda akan melihat bahwa penyerang yang dimasukkan-nya, di-antara arus lalu lintas antara klien dan server. Sekarang bahwa penyerang telah memasuki komunikasi antara dua endpoint, ia dapat menyuntikkan informasi palsu dan mencegat data yang ditransfer antara mereka.

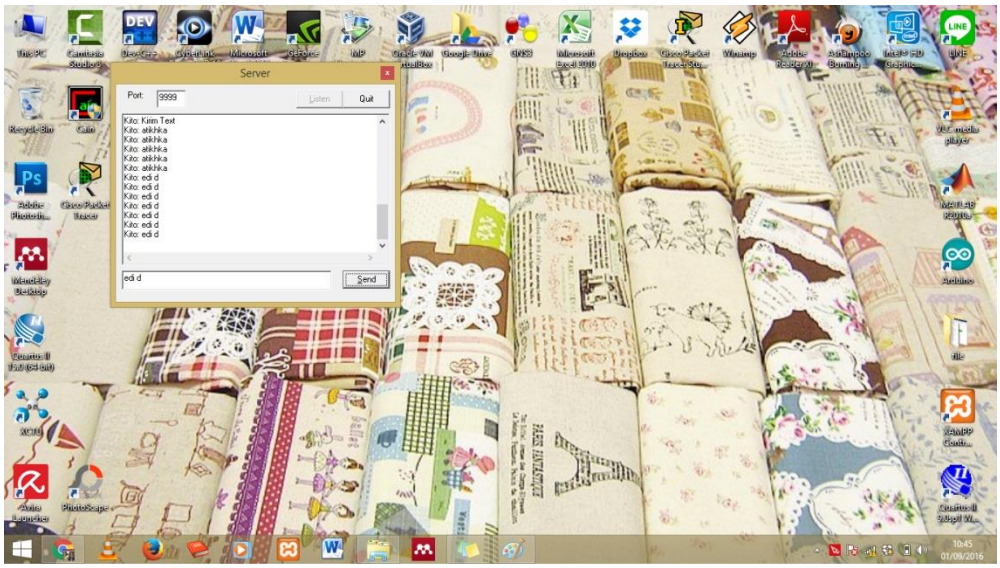
2. Software Yang Di Gunakan Untuk MITM

- 3 Laptop
- Software Wireshark
- Software Cain and Able
- Software Aplikasi Chatting Sederhana
- Software Xampp

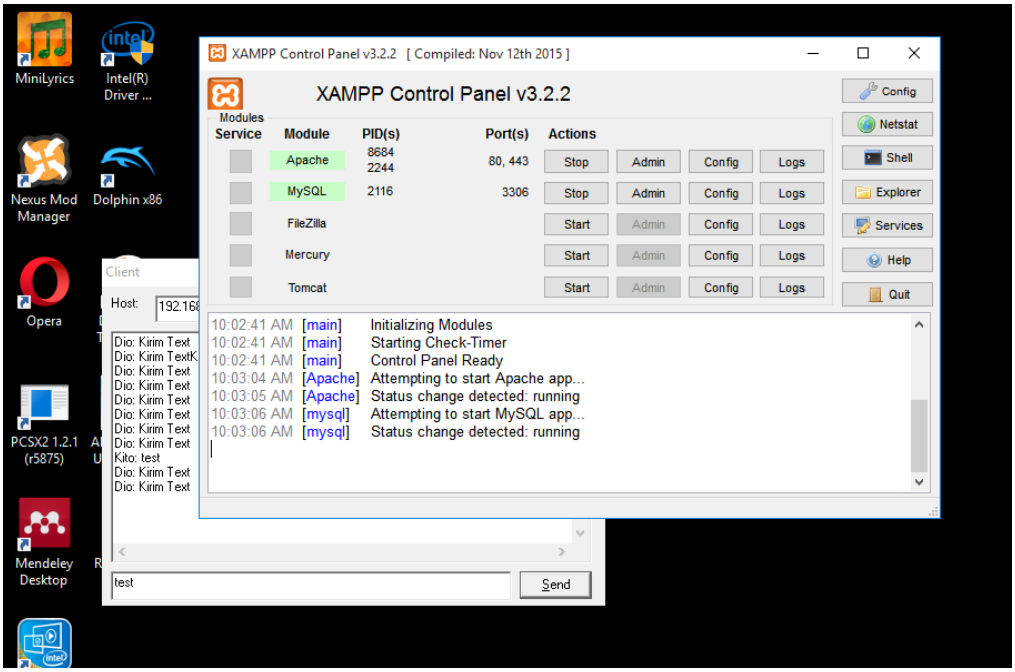
3. Percobaan

1. Koneksikan Client dan Server dan Attacker dalam satu Jaringan yang sama, matikan firewall agar hasil dapat maksimal. Siapkan masing-masing satu komputer satu peran

   Server (Komputer 1)

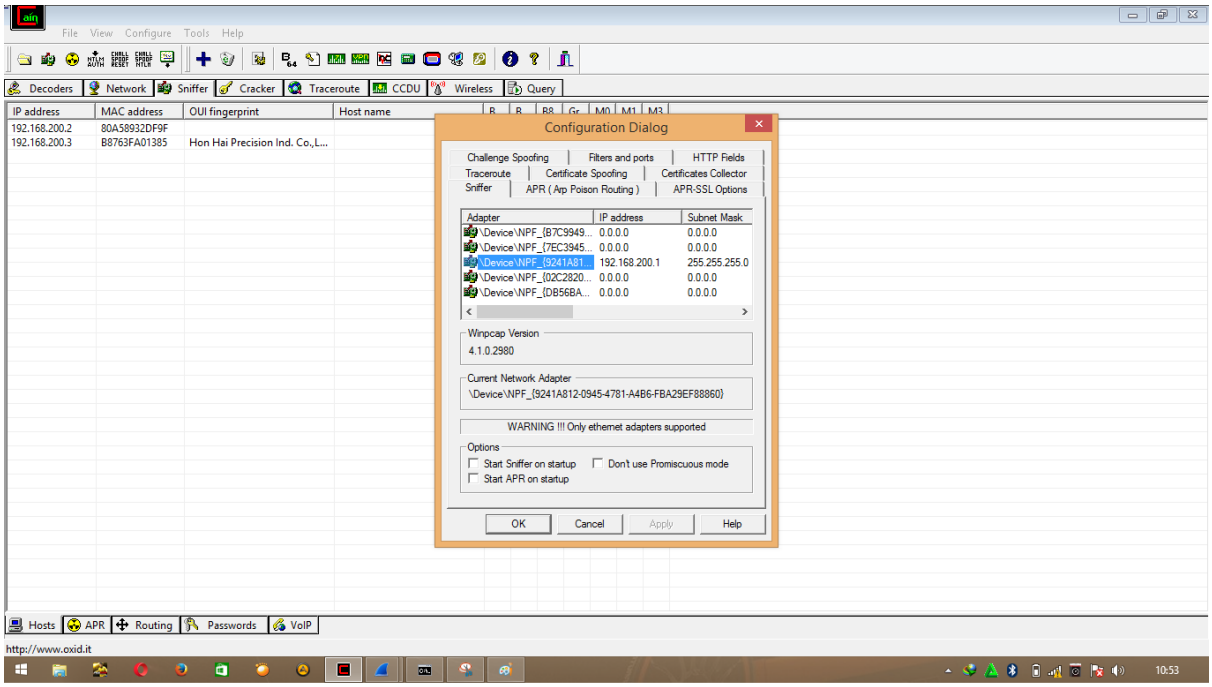


Client(Komputer 2)

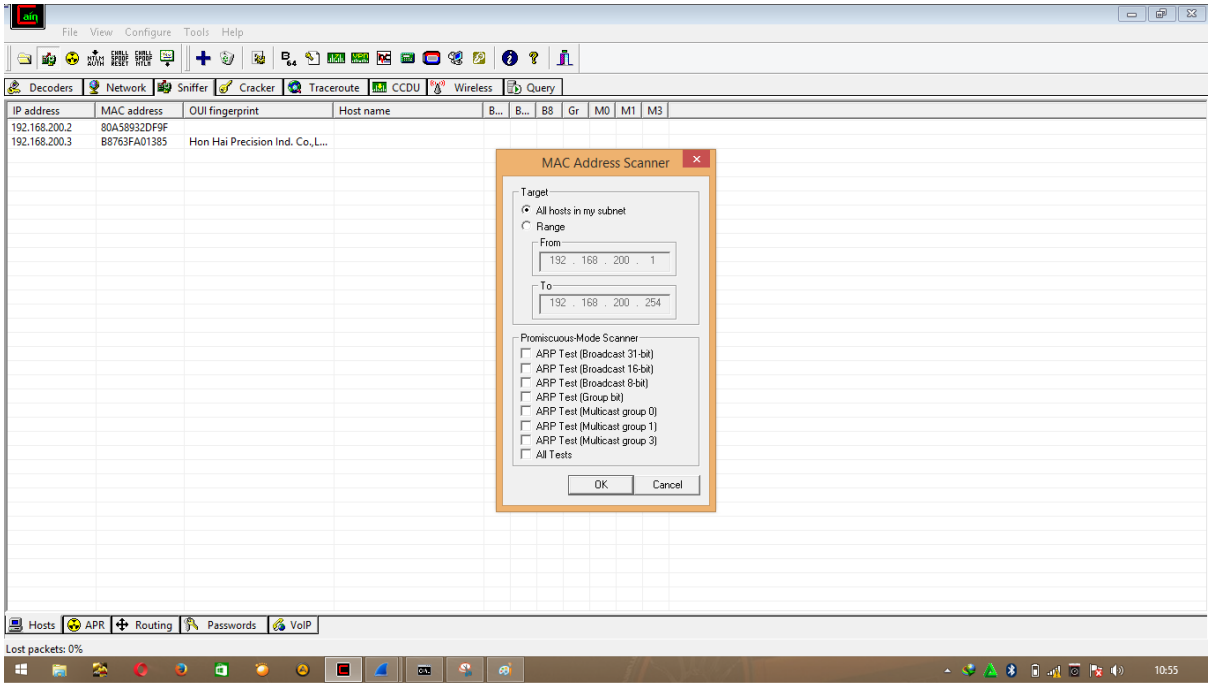


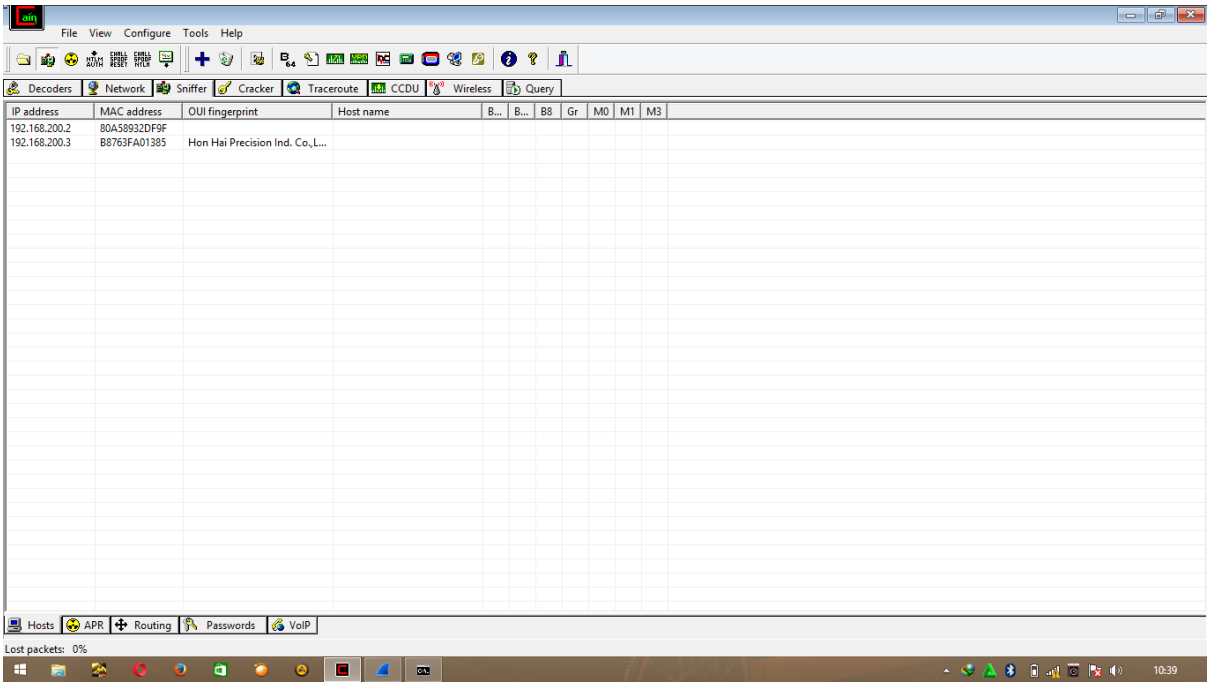
2. Sniffing yang dilakukan pada Komputer 3 (Attacker) menggunakan Software Cain and Able juga wireshark

Pertama konfigurasikan dialog cain and able dalam range IP dari Client dan Server

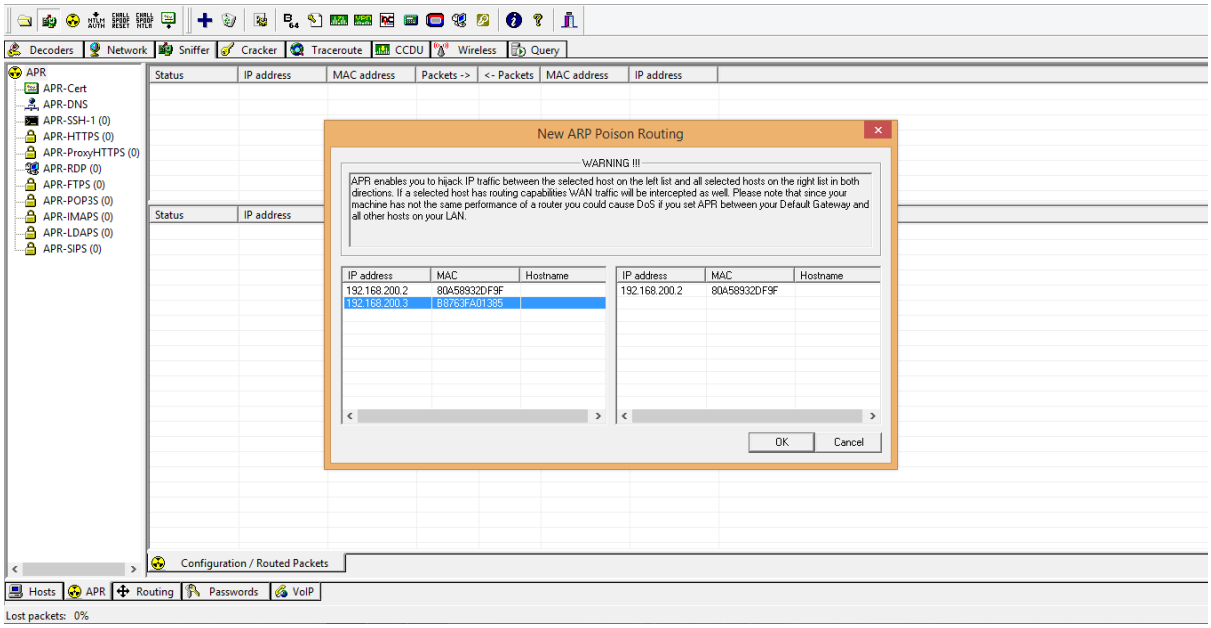


Selanjutnya klik start Sniffing dan scan MAC Address

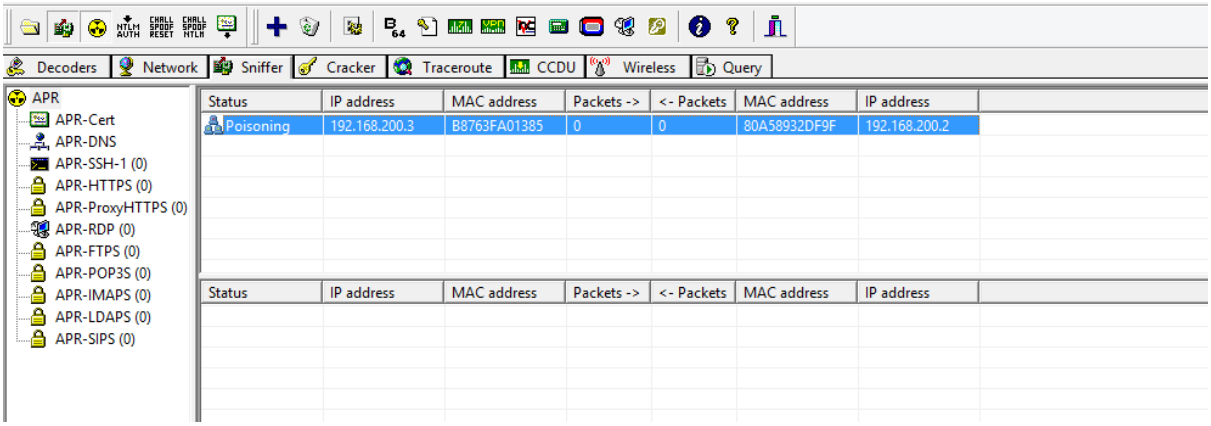




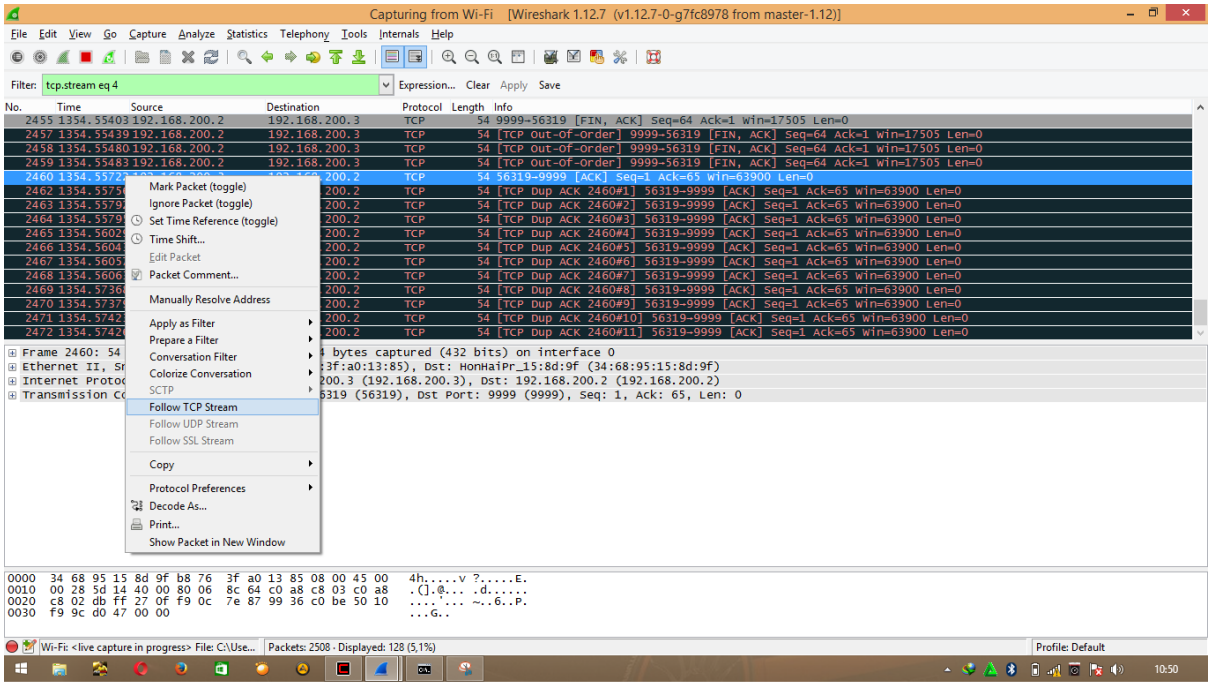
Setelah IP Client dan Server detect, maka klik ARP untuk membelokkan Komunikasi ke Attacker



Tentukan Client atau Server yang akan di belokkan



Selanjutnya buka Wireshark dan lihat isi komunikasi yang dilakukan oleh Client dan Server



Hasil Sniffing