

Kaeamanan Informasi  
Tugas UAS



Disusun oleh:  
Nama : Sonia Eka Pratiwi  
Nim : 1310651025  
Kelas : A

JURUSAN TEKNIK INFORMATIKA  
FAKULTAS TEKNIK  
UNIVERSITAS MUHAMMADIYAH JEMBER  
2015

## **Tugass 1**

### **1. Access Control**

Istilah Access Control umumnya mengacu pada system yg dapat mengontrol, memantau dan membatasi pergerakan orang, asset, atau kendaraan, di, keluar dan sekitar bangunan atau situs.

Access control bertujuan untuk memungkinkan pengguna yg berwenang untuk mengakses data yg sesuai dan menolak akses ke pengguna yg tidak sah. Access control dalam kenyataanya terkait dengan segala kejadian yang kita alami dalam kehidupan sehari-hari. Contohnya sebuah kunci pada pintu mobil pada dasarnya adalah sebuah bentuk Access control. Sebuah PIN pada sistem ATM di bank adalah cara lain dari Access control. Kepemilikan Access control dirasakan sangat penting untuk dimiliki ketika orang tersebut berusaha untuk mengamankan sesuatu hal / wilayah yang dianggap penting / vital dan bersifat mengandung informasi rahasia. Dan adapun manfaatnya menggunakan akses control meliputi pencegahan kehilangan atau kerusakan asset dan mengurangi resiko cedera pribadi. Ada 6 jenis control access : pencegahan, detektif, perbaikan, pemulihan, pencegah, kompensasi.

Jenis control akses biasa jatuh ke dalam 3 kategori :

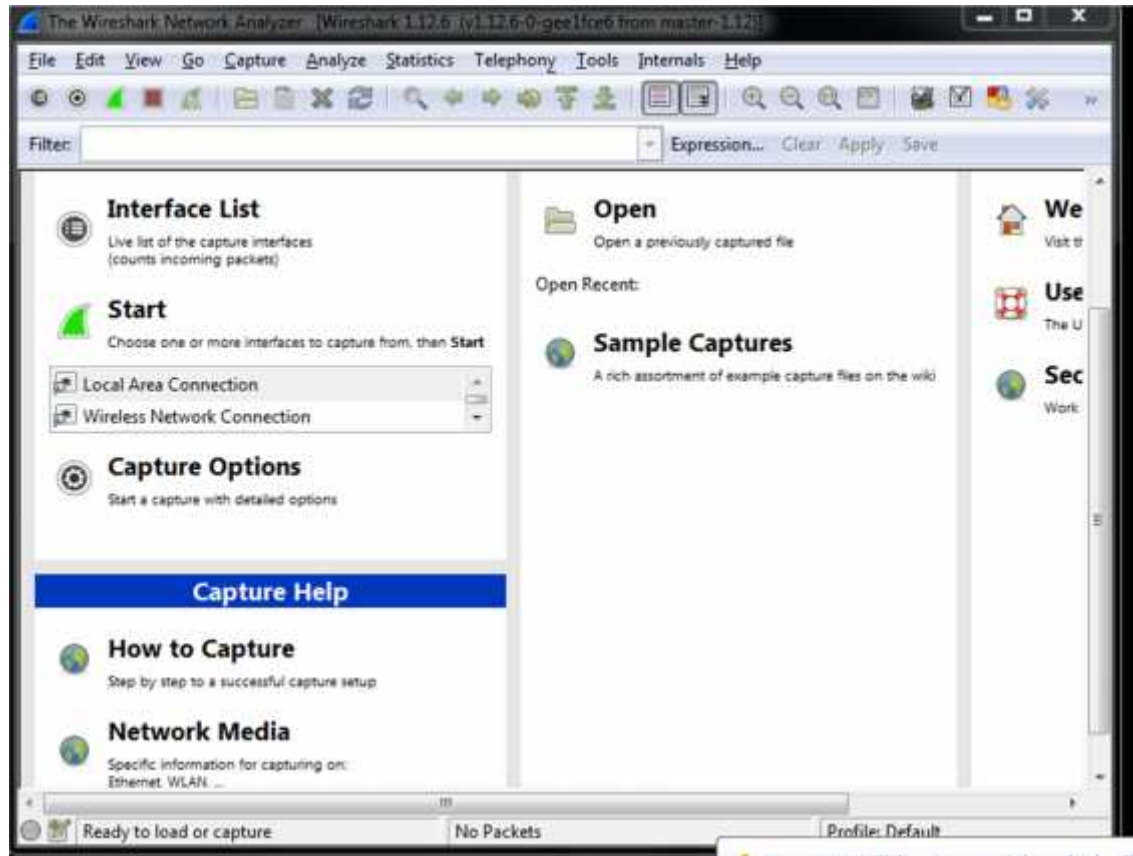
1. **Administrasi**  
Di laksanakan dengan menciptakan dan mengikuti kebijakan organisasi, prosedur dan peraturan.
2. **Teknis**  
Di implementasikan menggunakan perangkat lunak, perangkat keras, atau firmware yg membatasi akses logis pada system teknologi. Seperti firewall, router dan enkripsi.
3. **Fisik**  
Di implementasikan dengan perangkat fisik seperti kunci, pagar, gerbang dan penjaga keamanan

Dibawah ini adalah enam type akses kontrol:

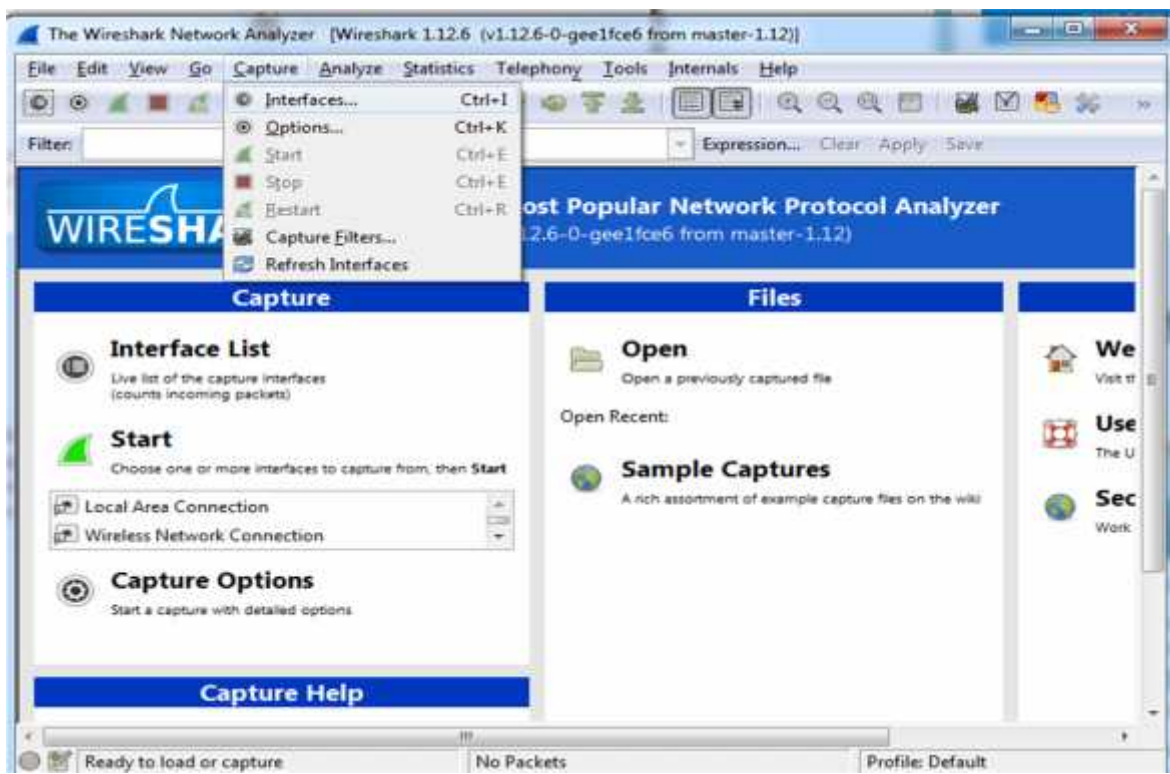
- Preventive
- Detective
- Corrective
- Recovery
- Deterrent
- Compensating

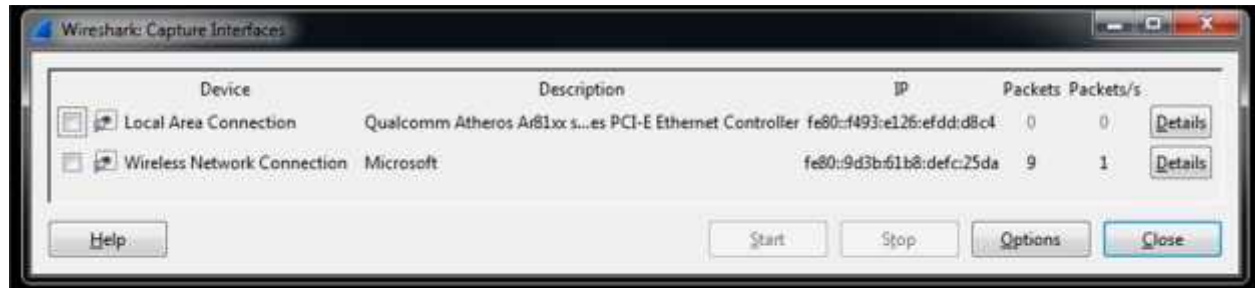
## Tugas 2

1. Buka program wireshark.



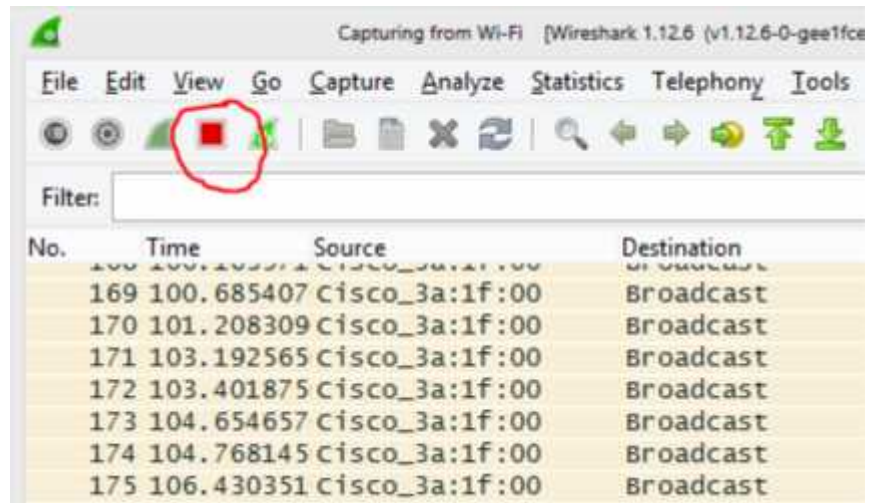
2. Pertama masuk pada Capture – Option atau menekan tombol Capture Interfaces





3. Keluar Kunjungi website yg berisi form login, contoh: [www.mywapblog.com](http://www.mywapblog.com) (CONTOH)





Masukkan username dan kata sandi lalu login seperti biasa...  
Ketika Selesai LOGIN, STOP Wreshark

4. Lihat Ipnnya melalui cmd

```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Toni>ping nywapblog.com

Pinging nywapblog.com [107.161.181.166] with 32 bytes of data:
Reply from 107.161.181.166: bytes=32 time=266ms TTL=49
Reply from 107.161.181.166: bytes=32 time=268ms TTL=49
Reply from 107.161.181.166: bytes=32 time=287ms TTL=49
Reply from 107.161.181.166: bytes=32 time=280ms TTL=49

Ping statistics for 107.161.181.166:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 266ms, Maximum = 287ms, Average = 275ms
```

5. Filter ip nya dengan kode "ip.dst=="alamat IP" Cari di info yg ada login.phpnya Lihat di HTML Form URL Decoded

The image shows a Wireshark packet capture of a login attempt. The packet list shows an HTTP POST to /login.php. The packet details show the HTML form URL decoded, with fields: username='noorohita', password='1htorhnt', and login='Masuk'. The packet bytes show the raw data, with the password field highlighted.

Maka akan terlihat passwordnya

