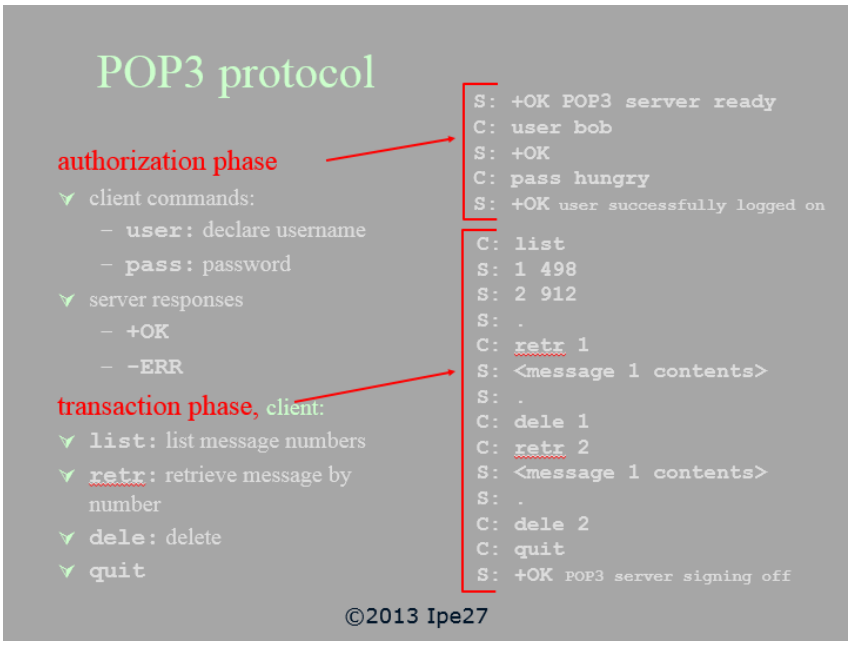
Monitoring Protokol POP Menggunakan Wireshark

Imam Prasetyo
imp.masiv@gmail.com
http://superman-kartini.blogspot.com

Apa sih Protokol POP?

Protokol POP *(Post Office Protocol)* adalah protokol yang banyak digunakan di internet untuk mengambil surat elektronik (email) dari server email. Untuk saat ini protokol POP berkembang sampai generasi ke-3 atau sering disebut POP3, karena sebelumnya ada POP2 (pada awal tahun 80an) dan POP1. Protokol ini erat hubungannya dengan protokol SMTP dimana protokol SMTP berguna untuk mengirim surat elektronik dari komputer pengirim ke server. Post Office Protocol - Version 3 (POP3) dimaksudkan agar workstation untuk secara dinamis mengakses maildrop pada server email dengan cara yang efisien. POP3 itu sendiri listen pada port TCP port 110. Protokol ini dispesifikasikan pada RFC 1939 (http://www.faqs.org/rfcs/rfc1939.html)

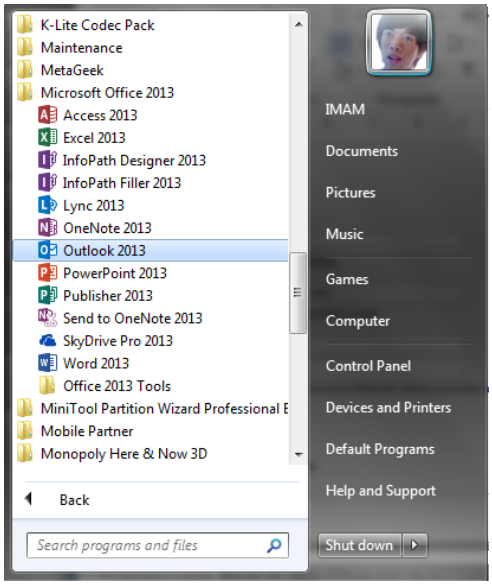
Ada dua fase dalam protokol POP3 yaitu authorization phase dan transaction phase.



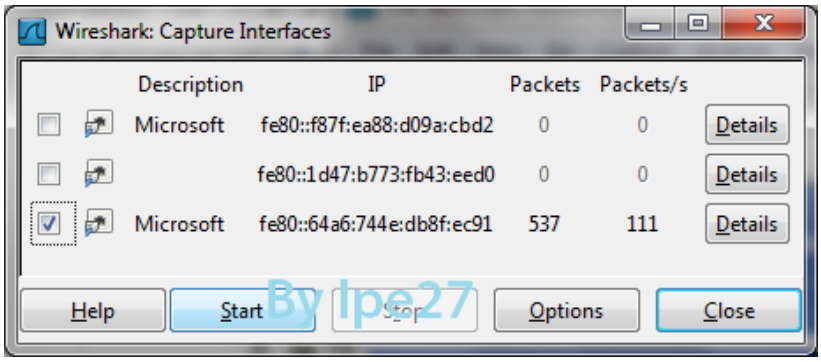
Pada analisis dengan wireshark yang akan dilakukan adalah authorization phase. Dimana kita mencoba login dan mensinkronisasi sebuah alamat email dengan menggunakan Ms. Outlook.

Analisis Protokol POP (authorization phase) dengan Wireshark

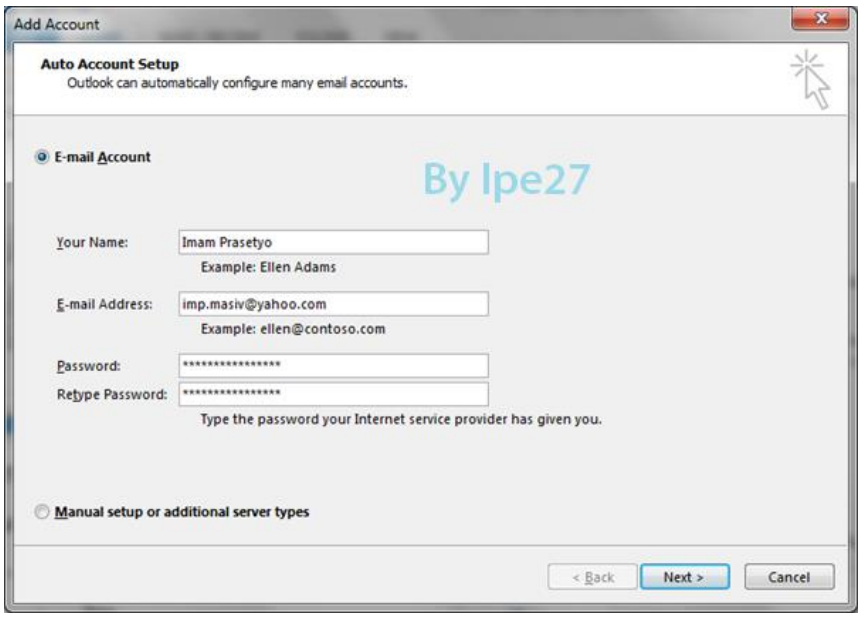
1. Bukalah aplikasi Ms. Outlook



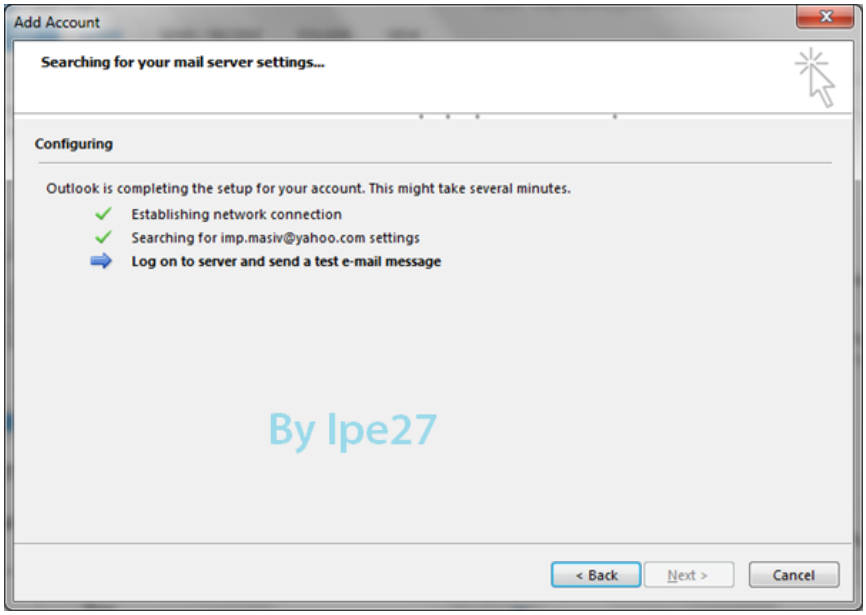
2. Jalankan wireshark dan pilih interface yang akan digunakan kemudia start capture.

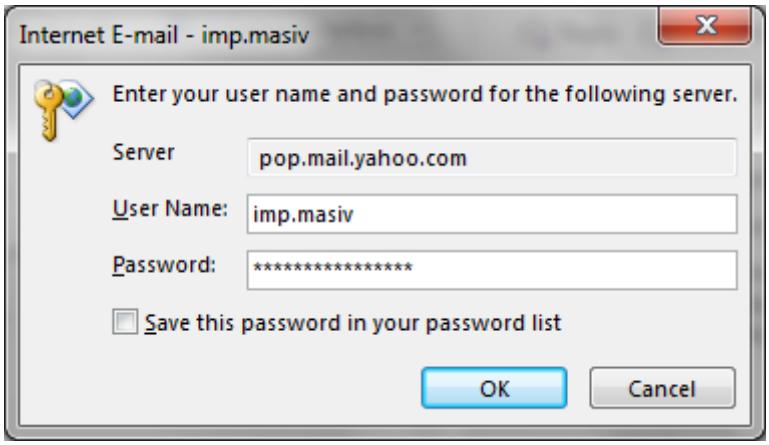


3. Login atau tambah account email pada Ms. Outlook

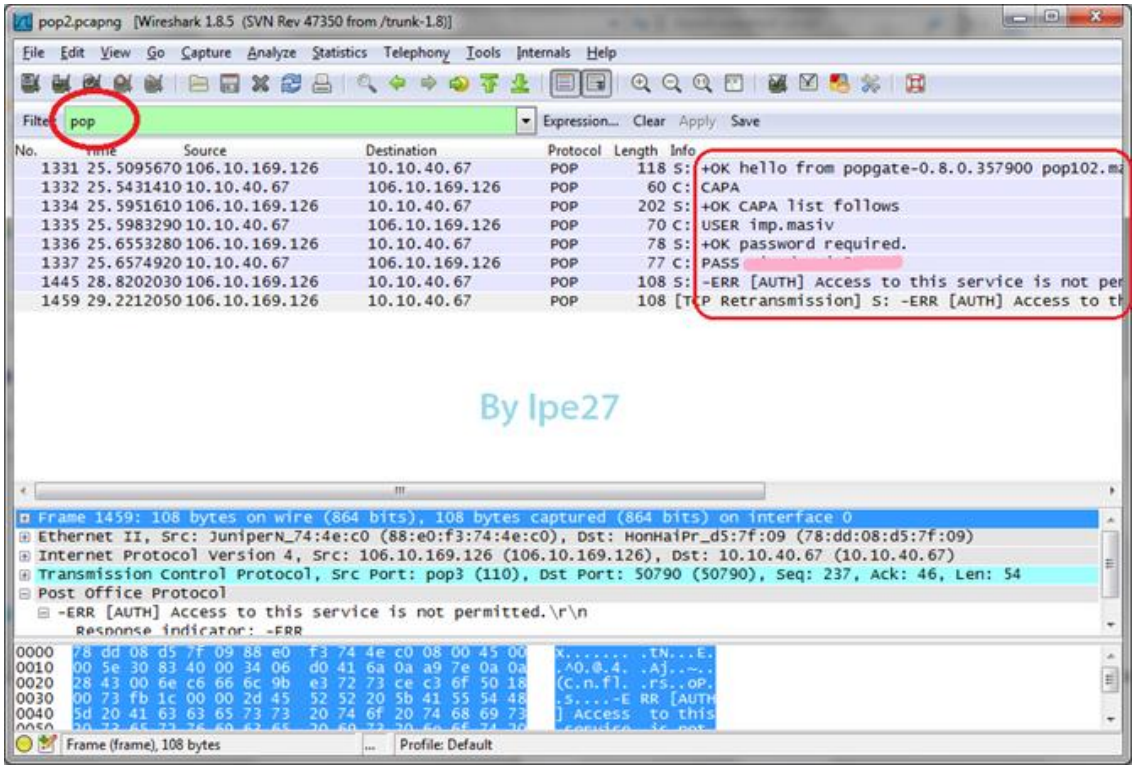


4. Tunggu server email merespon permintaan login.





5. Setelah autentifikasi alamat email selesai stop capture pada wireshark. Kemudian buatlah filter "POP" untuk menganalisis protokol POP yang telah tercapture oleh wireshark.

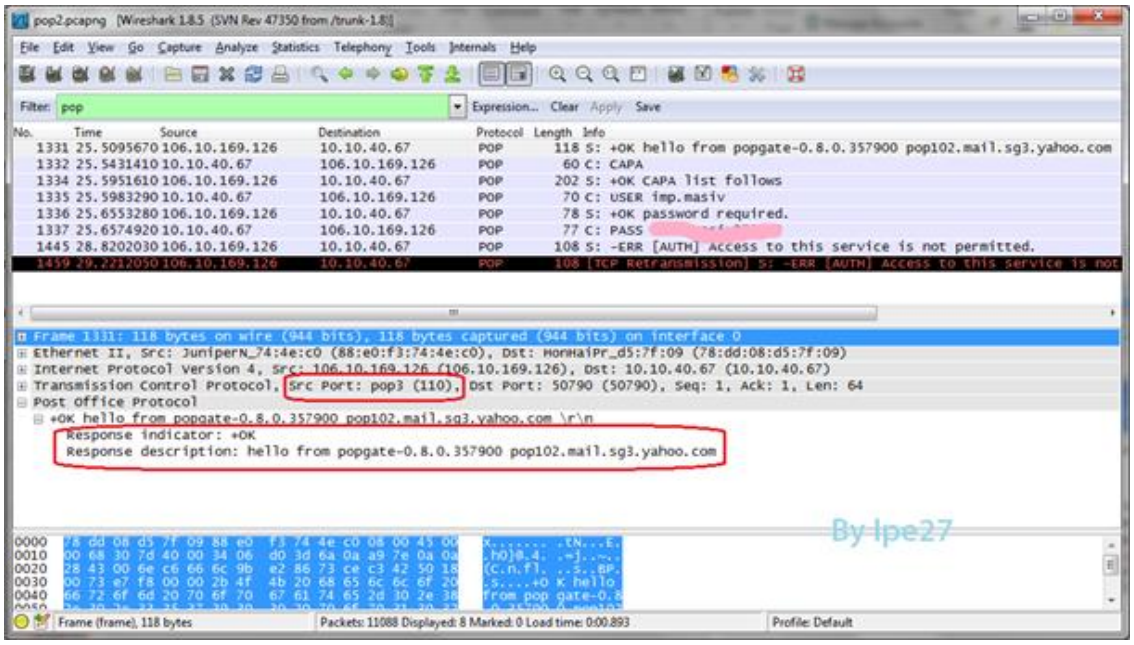


Analisis:

authorization phase dimulai dari sumber yaitu server yahoo mail memberikan respon +OK, respon ini berarti menginformasikan bahwa server oke dan akan melanjutkan ke proses autentifikasi berikutnya. Dapat dilihat bahwa IP kita adalah 10.10.40.67 dan IP server yahoo mail adalah 106.10.169.126.

Jika dibuka detail paket dari +OK akan kita ketahui bahwa hostname server yahoo mail

yang merespon adalah gerbang POP pop102.mail.sg3.yahoo.com yang memberi indikator ok. Diketahui pula generasi POP yang digunakan adalah POP3 dan listen to port TCP 110 seperti gambar dibawah.



CAPA ini adalah request dari Ms. Outlook untuk autentifikasi berikutnya dan terlihat bahwa server membalas dengan indikator +OK yang berarti siap melanjutkan proses berikutnya.

Client memberikan informasi berupa ID user (imp.masiv) dan server merespon bahwa user ID tersebut valid dan diperlukan password untuk masuk ke akredensialnya, yang kemudian klien memberikan password yang diminta server (**********).

Server memberi jawaban baik itu +OK yang berarti telah masuk ke akredensial akun maupun +ERR yang menunjukan pesan eror. Pada contoh diatas pesan dari server adalah +ERR karena yahoo mail dengan user ID imp.masiv belum dikonfigurasi untuk disinkronisasi dengan Ms. Outlook.

Biografi Penulis

Imam Prasetyo. Kuliah D4 Teknik Telekomunikasi di Politeknik Negeri Semarang. Lulusan SMA Negeri 1 Pati tahun 2010 dan SMP Negeri 1 Pati tahun 2007. Dari kecil sangat tertarik pada ilmu pengetahuan alam dan teknologi. Untuk informasi maupun tulisan menarik lain dapat diakses di situs blog *http://www.superman-kartini.blogspot.com*