Starting Wireshark

Arsyad Dwiyankuntoko
11ipa3.arsyad@gmail.com
http://arsyaddwiyankuntoko.blogspot.com

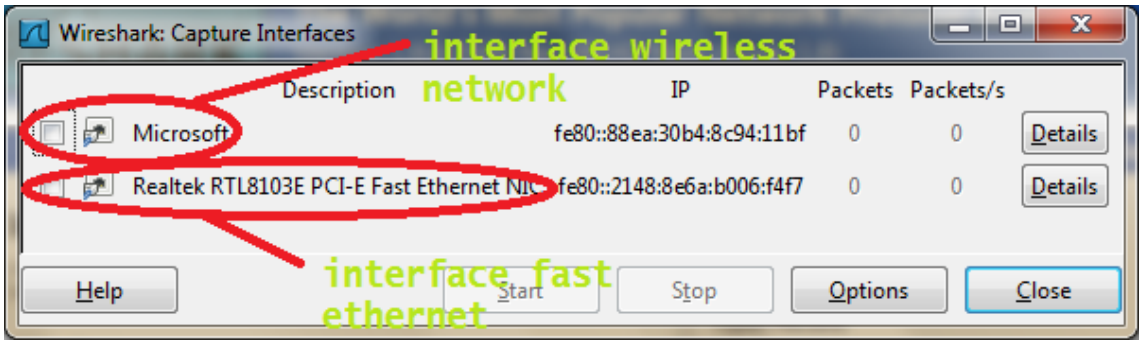
Pendahuluan

Network protocol Analyzer adalah suatu program komputer yang bisa digunakan untuk menangkap dan mencatat traffic paket-paket data yang dikirim melalui suatu jaringan komputer. Seperti yang telah diketahui, setiap kali terjadi komunikasi antar device pada suatu jaringan komputer, pasti ada paket-paket data yang dikirim dimana paket-paket ini terdiri dari beberapa layer tertentu dan menggunkan protocol tertentu juga sesuai dengan tujuan paket tersebut dikirimkan. Network protocol analyzer inilah yang nantinya akan menangkap tiap-tiap paket tersebut dan menampilkanya secara visual detail paket dari tiap layer dan protocol yang digunakan agar administrator jaringan pengguna software ini dapat dengan mudah menganalisa kondisi traffic dari suatu jaringan. pada tulisan ini akan dijelaskan salah satu software network protocol analyzer tersebut yaitu Wireshark.

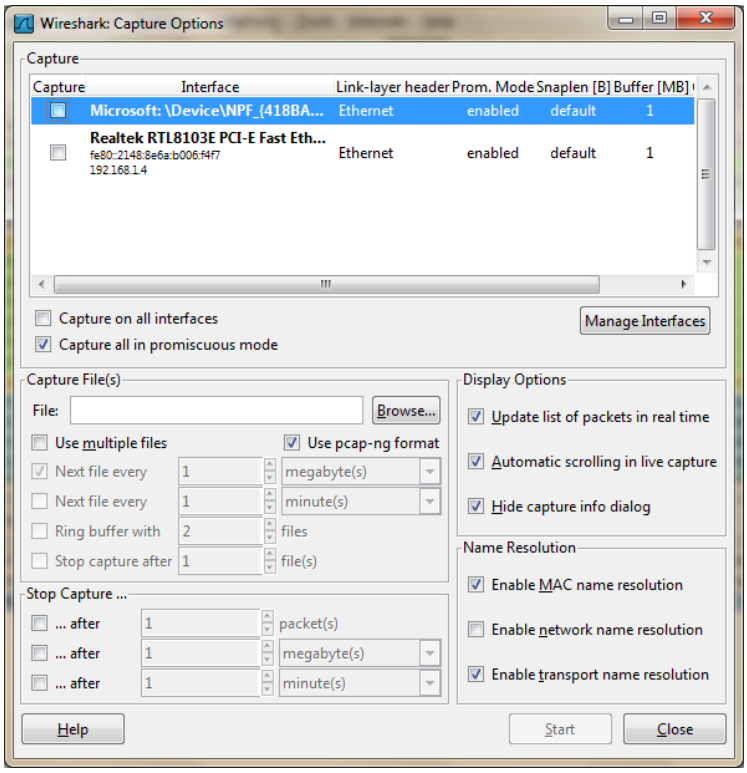
Wireshark merupakan salah satu network protocol analyzer yang populer dan sering digunakan oleh para network engineer. Software ini bersifat freeware sehingga bisa di-download secara gratis di situs resminya.

Capturing Live Network Data

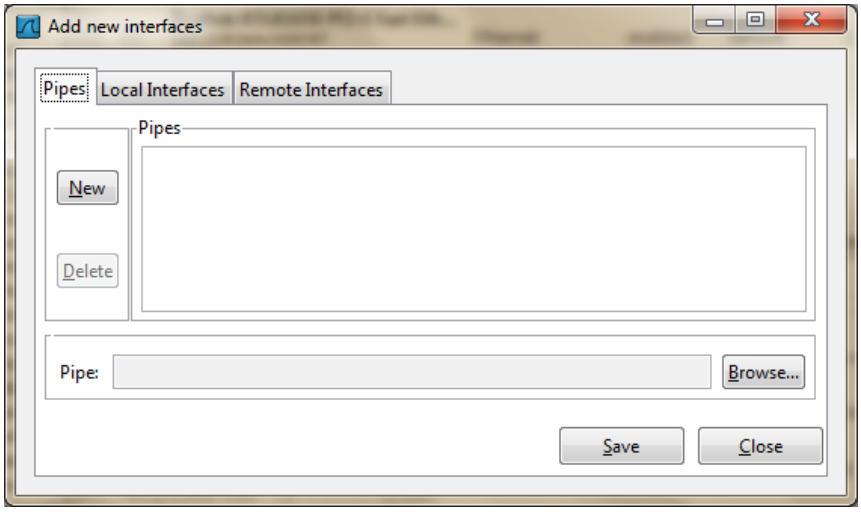
Capturing live network data merupakan fitur utama wireshark yang digunakan untuk menangkap paket-paket data secara langsung dari sebuah traffic dimana banyak komunikasi antar device yang berlangsung disitu. Wireshark ini bisa dugunakan untuk meng-capture berbagai macam jaringan seperti jaringan nirkabel (wireless), Ethernet, token ring, ATM, dll. Oleh karena itu, untuk memulai meng-capture paket dengan menggunakan wireshark hal pertama yang harus dilakukan adalah memilih interface mana yang akan digunakan, dengan syarat interface tersebut harus terhubung dengan jaringan yang akan dimonitor paket-paketnya. Untuk melakukanya, klik menu capture kemudian pilih interfaces. Kemudian akan muncul kotak dialog yang berisi pilihan interface



Pada gambar di atas terlihat jika wireshark telah mendeteksi dua interface yang ada pada komputer tersebut. Pilih salah satu interface tersebut kemudian klik start untuk memulai meng-capture paket. Selain itu, bisa juga dilakukan pengaturan pada peng-capture-an yang akan dilakukan dengan menggunakan option pada gambar diatas. Klik menu option maka akan muncul tampilan seperti pada gambar di bawah ini. Pada gambar tersebut terlihat jika terdapat pilihan interface seperti pada menu capture interface sebelumnya, tetapi pada box kali ini terlihat jika terdapat opsi lain yang bisa di atur seperti display options, name resolution, penggunaan multiple files, pengaturan berhentinya capture (stop capture), dll.

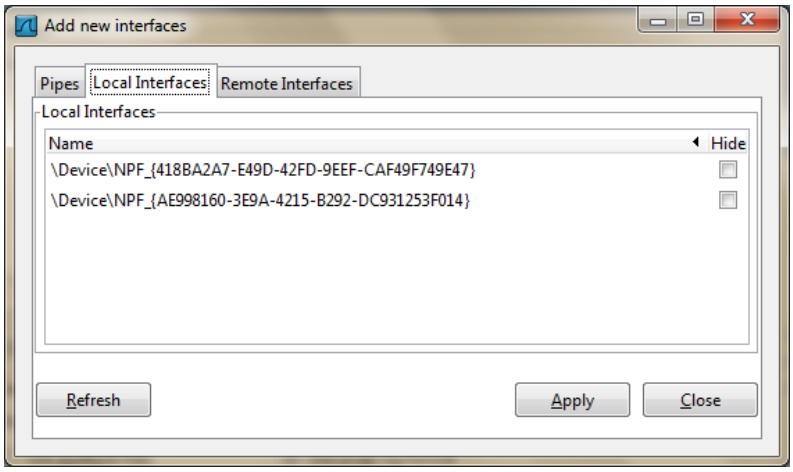


Selain itu bisa juga ditambahkan interface baru apabila ada interface yang belum muncul pada list dengan cara manage interface. Klik manage interface maka akan muncul gambar berikut

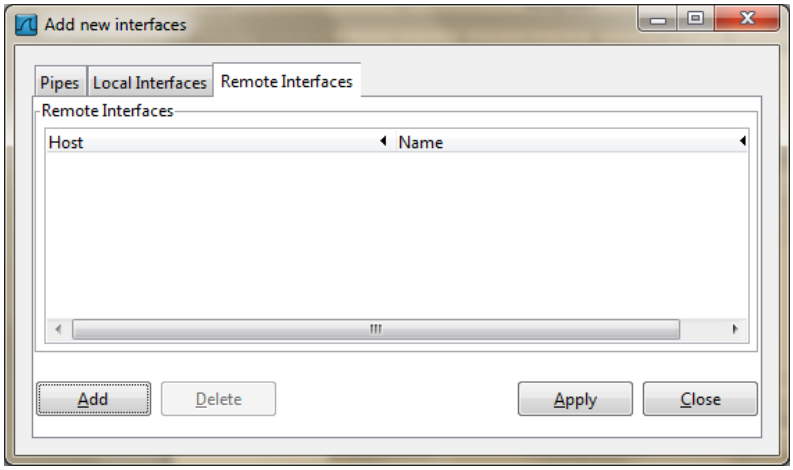


Pada gambar tersebut terdapat 3 tabs, yaitu pipes, local interface, dan remote interface. Pada pipes, tuliskan nama pipe baru beserta path dimana pipe tersebut berada kemudian klik new atau bisa juga klik browse dan pilih dimana pipe tersebut dibuat. Setelah telah itu klik save. Untuk tab local interface, disitu terdapat semua interface termasuk yang

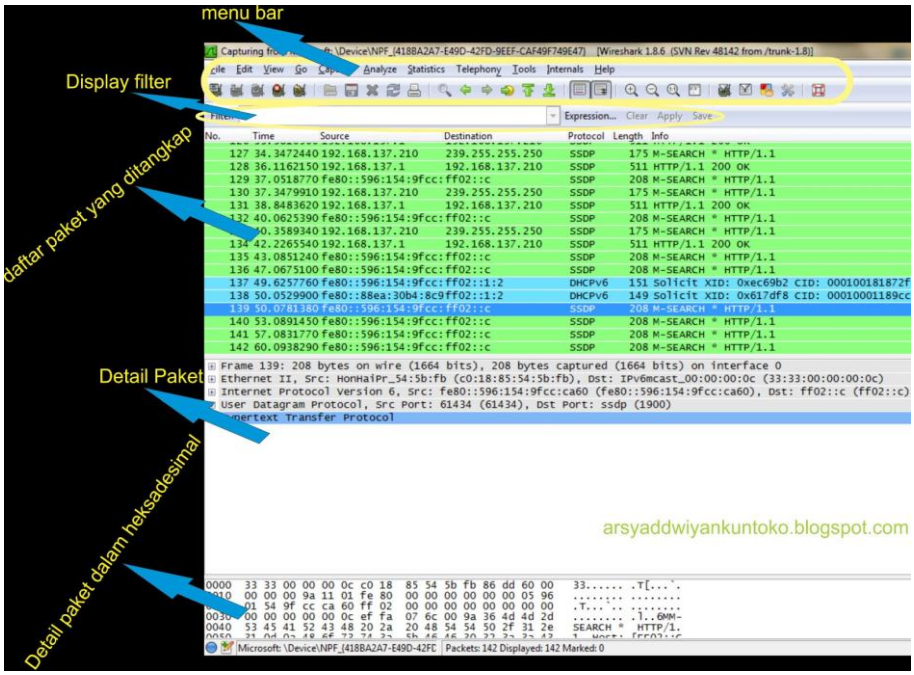
masih hidden atau tersembunyi. Untuk mengaktifkan atau menyembunyikan interface, klik kotak checkbox yang berada di kanan pada kolom hide.



Untuk tab ketiga yaitu remote interface, isinya merupakan interface untuk remote hosts. Pada tab ini bisa ditambahkan remote interface baru dengan cara klik add ataupun juga menyembunyikan dan menampilkan remote interface yang ada dengan klik checkbox pada kolom hide yang terletak paling kanan.



Apabila interface jaringan yang akan di-capture sudah ditentukan beserta dengan opsi-opsi lainya, klik start untuk memulai capture traffic jaringan. wireshark akan terus melakukan aktifitas menangkap paket-paket yang dikirim melalui interface tersebut hingga waktu yang ditentukan atau bisa juga dihentikan dengan masuk ke menu capture kemudian klik stop. Setelah di-stop, maka paket-paket yang telah tertangkap dapat dianalisa detail-nya dengan lebih mudah. gambar berikut merupakan contoh tampilan dari wireshark saat sedang melakukan capture. Pada tampilan tersebut terdapat beberapa kolom, yaitu Menu bar, Display filter, daftar paket yang ditangkap, detail paket, dan detail paket dalam hexadesimal.



Gambar di atas merupakan tampilan saat wireshark mulai melakukan capture. Berikut penjelasan lebih lanjut dari tiap bagiannya :

1. Menu bar---> Menu bar berisi tools yang bisa digunakan untuk membantu dalam meng-capture paket data. Selain itu juga terdapat menu-menu yang bisa digunakan untuk setting wireshark itu sendiri

2. Display filter---> Display filter merupakan kolom yang digunakan untuk menuliskan command untuk filter. Commad untuk filter sendiri bisa bermacam-macam sesuai dengan protocol apa yang ingin di filter

3. Daftar paket yang ditangkap ----> Daftar paket yang ditangkap akan diperlihatkan secara terus menerus selama jaringan dan computer yang di filter dalam keadaan aktif. Daftar ini berisi bermacam-macam kolom, yaitu ;
   - Time --> berisikan waktu kapan paket tersebut di-capture
   - Source -->berisikan IP sumber dari paket tersebut
   - Destination-->berisikan Ip tujuan dari paket tersebut
   - Protocol -->berisikan protocol apa yang digunakan paket tersebut

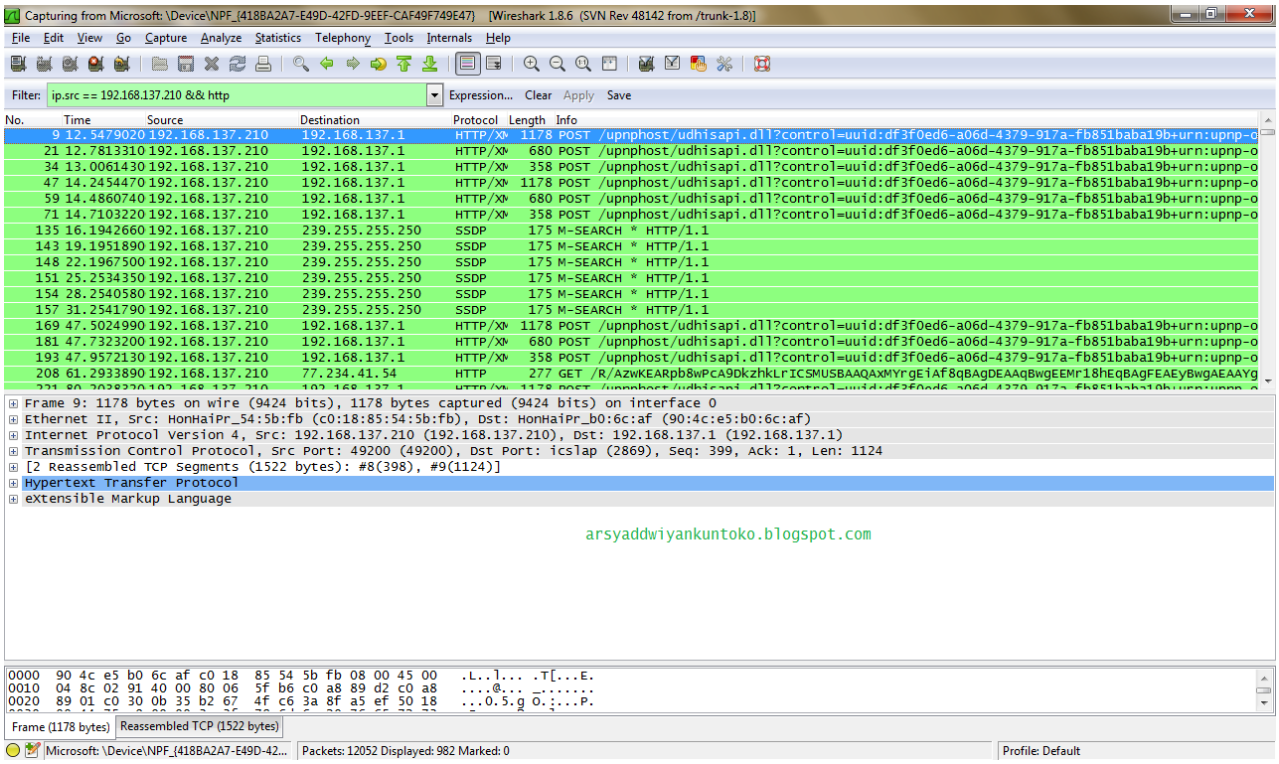
- Info -->berisikan detail informasi dari paket tersebut

4. Detail paket ---> Pada bagian ini ditampilkan detail paket dari paket yang di sorot pada daftar paket yang di tangkap. Detail ini berisi frame, Ethernet II, media type, dll. Tiap paket memiliki detail yang berbeda-beda.

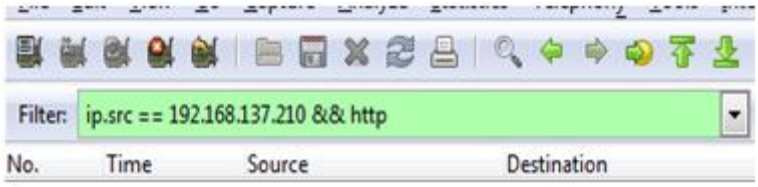
5. Detail paket heksa---> Bagian ini sama dengan detail paket, hanya saja detail paketnya dituliskan dalam bentuk heksadesimal

Menerapkan Filter pada saat Capture File

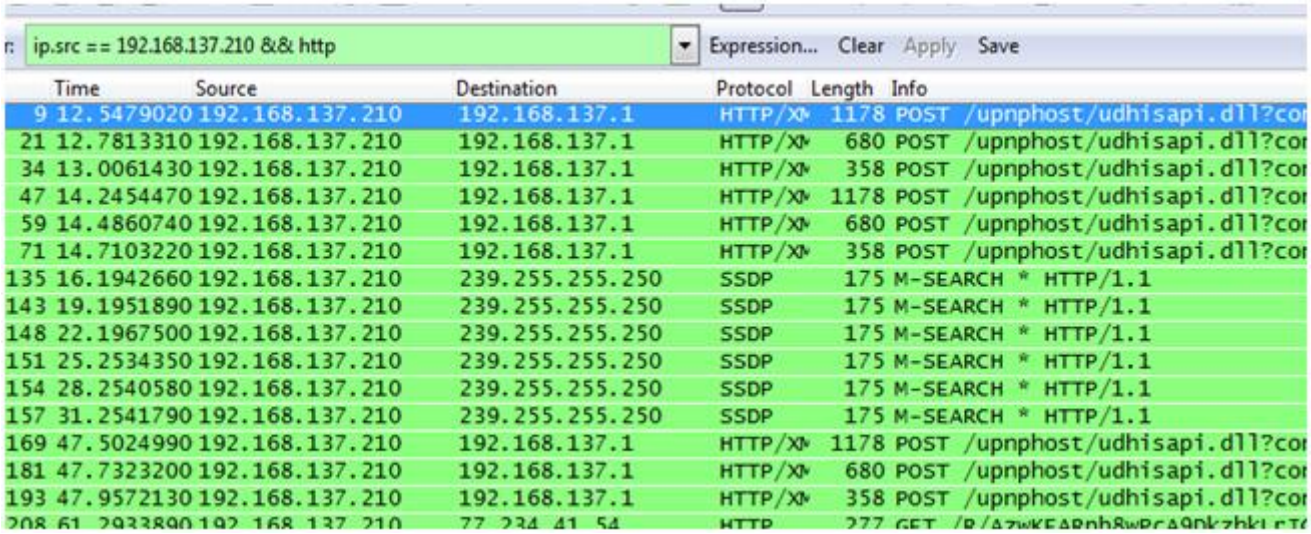
Seperti yang terlihat pada gambar sebelumnya, dalam suatu jaringan terdapat bermacam-macam paket yang dikirim dan dapat di-capture oleh wireshark. Pada table daftar paket yang ditangkap terdapat berbagai macam paket dan terkadang membuat kita bingung saat kita ingin melihat paket tertentu saja. oleh karena itu, wireshark menyediakan suatu tool untuk memudahkan hal tersebut, yaitu filter. Filter ini digunakan dengan cara memasukan command filter yang akan dipakai pada kolom display filter kemudian klik apply kemudian wireshark akan memilih paket berdasarkan protocol yang anda inginkan. Ada berbagai macam filter yang tersedia di wireshark seperti http,icmp,snmp,udp, dan masih banyak lagi. Berikut contoh penerapan filter pada wireshark



Gambar di atas merupakan hasil capture dengan menggunakan filter ip source dan protocol http. Hal itu dapat kita lihat pada kolom display filter. Pada kolom tersebut tertulis :



Ip.src == 192.168.137.210 ---->berarti wireshark hanya akan menampilkan paket dengan Ip source 192.168.137.210



&& http →tanda && disini merupakan suatu command yang digunakan untuk melakukan lebih dari satu filter. Setelah tanda && terdapat http, berarti selain filter ip source, wireshark juga melakukan filter terhadap paket-paket dengan protocol http saja. tetapi, pada table daftar paket yang ditangkap terdapat protocol SSDP juga selain HTTP. Ini terjadi karena SSDP sebenarnya merupakan protocol yang mirip dengan HTTP tetapi protocol ini juga tidak terdapat pada filter wireshark. Pada detail paketnya pun pada layer aplikasi yang digunakan merupakan HTTP. untuk melakukan filter tersendiri terhadap SSDP saja bisa digunakan filter pada port-nya.

Referensi

http://cisco.tu-sofia.bg/uploads/Additional/wireshark.pdf

Biografi Penulis

Biografi Penulis

Arsyad Dwiyankuntoko. Sedang menjalankan program D4 Teknik Telekomunikasi di Politeknik Negeri Semarang angkatan 2010