UJIAN AKHIR SEMESTER

KEAMANAN INFORMASI

TI-PAGI

MOCH. SHOHEBUL CHAFFI BRANTANAKA 1310651005

KELAS E

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH JEMBER

2015

1. RESUME EBOOK CISSP

TELEKOMUNIKASI DAN KEAMANAN JARINGAN

Telekomunikasi dan Jaringan Keamanan adalah dasar kehidupan modern kita. Internet, World Wide Web, online banking, instant messaging e-mail, dan teknologi lainnya mengandalkan Keamanan Jaringan: dunia modern kita tidak bisa ada tanpa itu. Telekomunikasi dan Keamanan Jaringan (sering disebut "kation Teleko-," singkatnya) berfokus pada kerahasiaan, integritas, dan ketersediaan data dalam gerakan. Telekomunikasi adalah salah satu domain terbesar di Tubuh umum Pengetahuan dan mengandung lebih banyak konsep dari domain lainnya. Domain ini juga merupakan salah satu domain yang paling teknis yang mendalam, yang membutuhkan pengetahuan teknis ke paket, segmen, frame, dan header mereka. Memahami domain ini sangat penting untuk memastikan keberhasilan pada ujian.

JARINGAN ARSITEKTUR DAN DESAIN

Bagian pertama kami adalah arsitektur jaringan dan desain. Kita akan membahas bagaimana jaringan harus dirancang dan kontrol mereka mungkin berisi, dengan fokus pada penggelaran pertahanan-mendalam strategi dan menimbang biaya dan kompleksitas jaringan con trol versus manfaat yang disediakan.

KONSEP JARINGAN DASAR

Sebelum kita dapat membahas spesifik Telekomunikasi dan Keamanan Jaringan konsep, kita perlu memahami konsep dasar di belakang mereka. Istilah seperti broadband yang sering digunakan secara informal
LAN, WAN, MAN, dan PAN LAN adalah Local Area Network.

A. LAN adalah jaringan yang relatif kecil, biasanya terbatas pada bangunan atau area dalam satu RUANG. Sebuah MAN adalah Metropolitan Area Network, yang biasanya terbatas pada sebuah kota, kode pos, kampus, atau office park.
B. WAN adalah Wide Area Network, biasanya meliputi kota, negara, atau negara. Di ujung lain dari spektrum, yang terkecil dari jaringan ini adalah PAN: Per- sonal Area Networks, dengan kisaran 100 m atau kurang. Rendah daya teknologi nirkabel yang seperti Bluetooth digunakan untuk membuat PANS.

Internet, Intranet, dan Extranet Internet adalah kumpulan jaringan global mengintip menjalankan TCP / IP, memberikan pelayanan yang terbaik-usaha. Intranet adalah jaringan milik pribadi menjalankan TCP / IP, seperti jaringan perusahaan. Extranet adalah hubungan antara intranet pribadi, seperti koneksi ke mitra bisnis intranet.

Model Open sistem interkoneksi (OSI) memiliki tujuh lapisan.

- Aplikasi
- Presentasi
- Sesi
- Transpor
- Jaringan
- Data Link
- Fisik

FUNGSI OSI LAYER

A. Layer Physical

Ini adalah layer yang paling sederhana; berkaitan dengan electrical (dan optical) koneksi antar peralatan. Data biner dikodekan dalam bentuk yang dapat ditransmisi melalui media jaringan, sebagai contoh kabel, transceiver dan konektor yang berkaitan dengan layer Physical. Peralatan seperti repeater, hub dan network card adalah berada pada layer ini.

B. Layer Data-link

Layer ini sedikit lebih “cerdas” dibandingkan dengan layer physical, karena menyediakan transfer data yang lebih nyata. Sebagai penghubung antara media network dan layer protocol yang lebih high-level, layer data link bertanggung-jawab pada paket akhir dari data binari yang berasal dari level yang lebih tinggi ke paket diskrit sebelum ke layer physical. Akan mengirimkan frame (blok dari data) melalui suatu network. Ethernet (802.2 & 802.3), Tokenbus (802.4) dan Tokenring (802.5) adalah protocol pada layer Data-link.

C. Layer Network

Tugas utama dari layer network adalah menyediakan fungsi routing sehingga paket dapat dikirim keluar dari segment network lokal ke suatu tujuan yang berada pada suatu network lain. IP, Internet Protocol, umumnya digunakan untuk tugas ini. Protocol lainnya seperti IPX, Internet Packet eXchange. Perusahaan Novell telah memprogram protokol menjadi beberapa, seperti SPX (Sequence Packet Exchange) & NCP (Netware Core Protocol). Protokol ini telah dimasukkan ke sistem operasi Netware. Beberapa fungsi yang mungkin dilakukan oleh Layer Network

- Membagi aliran data biner ke paket diskrit dengan panjang tertentu
- Mendeteksi Error
- Memperbaiki error dengan mengirim ulang paket yang rusak
- Mengendalikan aliran

D. Layer Transport

Layer transport data, menggunakan protocol seperti UDP, TCP dan/atau SPX (Sequence Packet eXchange, yang satu ini digunakan oleh NetWare, tetapi khusus untuk koneksi berorientasi IPX). Layer transport adalah pusat dari mode-OSI. Layer ini menyediakan transfer yang reliable dan transparan antara kedua titik akhir, layer ini juga menyediakan multiplexing, kendali aliran dan pemeriksaan error serta memperbaikinya.

E. Layer Session

Layer Session, sesuai dengan namanya, sering disalah artikan sebagai prosedur logon pada network dan berkaitan dengan keamanan. Layer ini menyediakan layanan ke dua layer diatasnya, Melakukan koordinasi komunikasi antara entiti layer yang diwakilinya. Beberapa protocol pada layer ini: NETBIOS: suatu session interface dan protocol, dikembangkan oleh IBM, yang menyediakan layanan ke layer presentation dan layer application. NETBEUI, (NETBIOS Extended User Interface), suatu pengembangan dari NETBIOS yang digunakan pada produk Microsoft networking, seperti Windows NT dan LAN Manager. ADSP (AppleTalk Data Stream Protocol). PAP (Printer Access Protocol), yang terdapat pada printer Postscript untuk akses pada jaringan AppleTalk.

F. Layer Presentation

Layer presentation dari model OSI melakukan hanya suatu fungsi tunggal: translasi dari berbagai tipe pada syntax sistem. Sebagai contoh, suatu koneksi antara PC dan mainframe membutuhkan konversi dari EBCDIC character-encoding format ke ASCII dan banyak faktor yang perlu dipertimbangkan. Kompresi data (dan enkripsi yang mungkin) ditangani oleh layer ini.

G. Layer Application

Layer ini adalah yang paling “cerdas”, gateway berada pada layer ini. Gateway melakukan pekerjaan yang sama seperti sebuah router, tetapi ada perbedaan diantara mereka. Layer Application adalah penghubung utama antara aplikasi yang berjalan pada satu komputer dan resources network yang membutuhkan akses padanya. Layer Application adalah layer dimana user akan beroperasi padanya, protocol seperti FTP, telnet, SMTP, HTTP, POP3 berada pada layer Application.

MAC ADDRESS

Media Access Control (MAC) alamat adalah alamat hardware yang unik dari gawang kartu antarmuka jaringan Ether- (NIC). Alamat MAC dapat diubah dalam perangkat lunak.

IPV4

IPv4 adalah Internet Protocol versi 4, yang biasa disebut "IP." Ini adalah protocol dasar internet, yang dirancang pada tahun 1970 untuk mendukung packet-switched jaringan untuk AS Defense Advanced Research Projects Agency (DARPA). IPv4 digunakan untuk ARPAnet, yang kemudian menjadi Internet.

IPV6

IPv6 adalah penerus IPv4, menampilkan ruang jauh lebih besar alamat (alamat 128-bit dibandingkan dengan IPv4 yang 32 bit), sederhana routing, dan alamat sederhana tugas. Kurangnya alamat IPv4 adalah faktor utama yang menyebabkan penciptaan IPv6.

TCP

TCP adalah Transmission Control Protocol, Layer 4 protokol yang handal. TCP menggunakan three-way handshake untuk membuat koneksi yang dapat diandalkan di seluruh jaringan. TCP dapat reor-segmen der yang tiba rusak dan memancarkan kembali segmen yang hilang.

UDP

UDP adalah User Datagram Protocol, lebih cepat untuk TCP. UDP adalah Kendala ini com- digunakan untuk aplikasi yang "lossy" (dapat menangani beberapa packet loss), seperti streaming audio dan video. Hal ini juga digunakan untuk aplikasi permintaan-respon, seperti query DNS.

ICMP

ICMP adalah Internet Control Message Protocol, protokol pembantu yang membantu Lapisan 3. ICMP digunakan untuk memecahkan masalah dan melaporkan kondisi kesalahan: Tanpa ICMP untuk membantu, IP akan gagal ketika menghadapi routing yang loop, port, host, atau jaringan yang turun , dll ICMP tidak memiliki konsep port, TCP dan UDP lakukan, melainkan menggunakan jenis dan kode.

Aplikasi-Layer protokol TCP / IP dan konsep A banyak protokol ada pada TCP / IP Application Layer, yang menggabungkan Presentasi, Sesi, dan Layers Penerapan model OSI.

TELNET

Telnet menyediakan emulasi terminal melalui jaringan. Server Telnet mendengarkan pada port TCP 23. Telnet adalah cara standar untuk mengakses perintah shell interaktif lebih suatu jaringan selama lebih dari 20 tahun. Telnet lemah karena tidak memberikan kerahasiaan: semua data yang dikirimkan selama sesi Telnet adalah plaintext, termasuk username dan password yang digunakan untuk otentikasi ke sistem.

FTP

FTP adalah File Transfer Protocol, digunakan untuk mentransfer file ke dan dari server. Seperti Tel-bersih, FTP tradisional tidak memiliki kerahasiaan atau integritas dan tidak boleh digunakan untuk trans- fer data sensitif melalui saluran tidak aman.

SSH

SSH dirancang sebagai pengganti yang aman untuk Telnet, FTP, dan UNIX "R" mands com- (rlogin, rshell, dll). Ini menyediakan kerahasiaan, integritas, dan tication melakukan otentikasi aman, antara fitur-fitur lainnya. SSH juga dapat digunakan untuk aman terowongan protokol lain, seperti HTTP. Server SSH mendengarkan pada TCP port 22 secara default.

SMTP, POP, dan IMAP SMTP adalah Simple Mail Transfer Protocol, digunakan untuk mentransfer e-mail antara server. Server SMTP mendengarkan pada TCP port 25. POPv3 (Post Office Protocol) dan IMAP (Inter net Message Access Protocol) digunakan untuk client-server akses e-mail, yang menggunakan port TCP 110 dan 143, masing-masing.

DNS

DNS adalah Domain Name System, database hirarki global yang terdistribusi yang menerjemahkan nama ke alamat IP dan sebaliknya. DNS menggunakan TCP dan UDP: jawaban kecil menggunakan UDP port 53; jawaban besar (seperti transfer zona) menggunakan port TCP 53.

HTTP DAN HTTPS

HTTP adalah Hypertext Transfer Protocol, yang digunakan untuk mentransfer data berbasis Web tidak terenkripsi.
HTTPS (Hypertext Transfer Protocol Secure) transfer data dienkripsi berbasis Web melalui SSL / TLS. HTTP menggunakan port TCP 80, dan HTTPS menggunakan port TCP 443. HTML (Hypertext Markup Language) digunakan untuk menampilkan konten Web.

TEKNOLOGI LAN DAN PROTOKOL

konsep Local Area Network fokus pada Layer 1-3 teknologi seperti jaringan jenis kabel, topologi jaringan fisik dan logis, Ethernet, FDDI, dan lain-lain.

ETHERNET

Ethernet beroperasi pada Layer 2 dan merupakan dominan lokal teknologi Jaringan di Area yang transmitsnetworkdataviaframes.Ethernetisbaseband (onechannel), masalah soitmustaddress seperti tabrakan, di mana dua node mencoba untuk mengirimkan data secara bersamaan

BRIDGES

Bridges dan switch adalah Layer 2 perangkat. Sebuah jembatan memiliki dua port dan menghubungkan segmen pekerjaan net- bersama-sama. Setiap segmen biasanya memiliki beberapa node, dan jembatan belajar alamat MAC node di kedua sisi. Lalu lintas dikirim dari dua node di sisi yang sama dari jembatan tidak akan diteruskan di jembatan. Lalu lintas yang dikirim dari sebuah node di salah satu sisi jembatan ke sisi lain akan meneruskan seluruh. Jembatan pro vides lalu lintas isolasi dan membuat keputusan forwarding dengan mempelajari alamat MAC node terhubung. Sebuah jembatan memiliki dua domain tabrakan..

SWITCH

Switch adalah sebuah jembatan dengan lebih dari dua port. Juga, itu adalah praktek terbaik untuk hanya menghubungkan satu perangkat per port switch. Jika tidak, segala sesuatu yang benar tentang jembatan juga berlaku tentang switch. Gambar 2.1 menunjukkan switch jaringan. Switch menyediakan isolasi lalu lintas dengan mengasosiasikan alamat MAC dari setiap komputer dan server dengan port-nya. Switch menyusut tabrakan domain ke port tunggal. Anda biasanya akan memiliki tabrakan dengan asumsi satu perangkat yang terhubung per port (yang praktek terbaik). Batang digunakan untuk menghubungkan beberapa switch.

ROUTERS

Routers are Layer 3 devices that route traffic from one LAN to another. IP-based routers make routing decisions based on the source and destination IP addresses.

FIREWALL

Firewall Filter lalu lintas antara jaringan. TCP / IP packet filter dan firewall stateful membuat keputusan berdasarkan Layers 3 dan 4 (alamat IP dan port). Firewall Proxy juga dapat membuat keputusan berdasarkan Layers 5-7. Firewall multihomed: mereka memiliki beberapa NIC terhubung ke beberapa jaringan yang berbeda.

WIRELESS LOCAL AREA NETWORKS

Wireless Local Area (WLAN) mengirimkan informasi melalui gelombang elektromagnetik (seperti radio) atau cahaya. Secara historis, jaringan data nirkabel sudah sangat tidak aman, sering mengandalkan (dianggap) kesulitan dalam menyerang kerahasiaan atau integritas lalu lintas. Persepsi ini biasanya salah tempat. Bentuk yang paling umum dari jaringan data nirkabel 802.11 standar nirkabel, dan yang pertama 802.11 dard-standar keamanan yang wajar adalah 802.11i.

DESKTOP DAN APLIKASI VIRTUALISASI

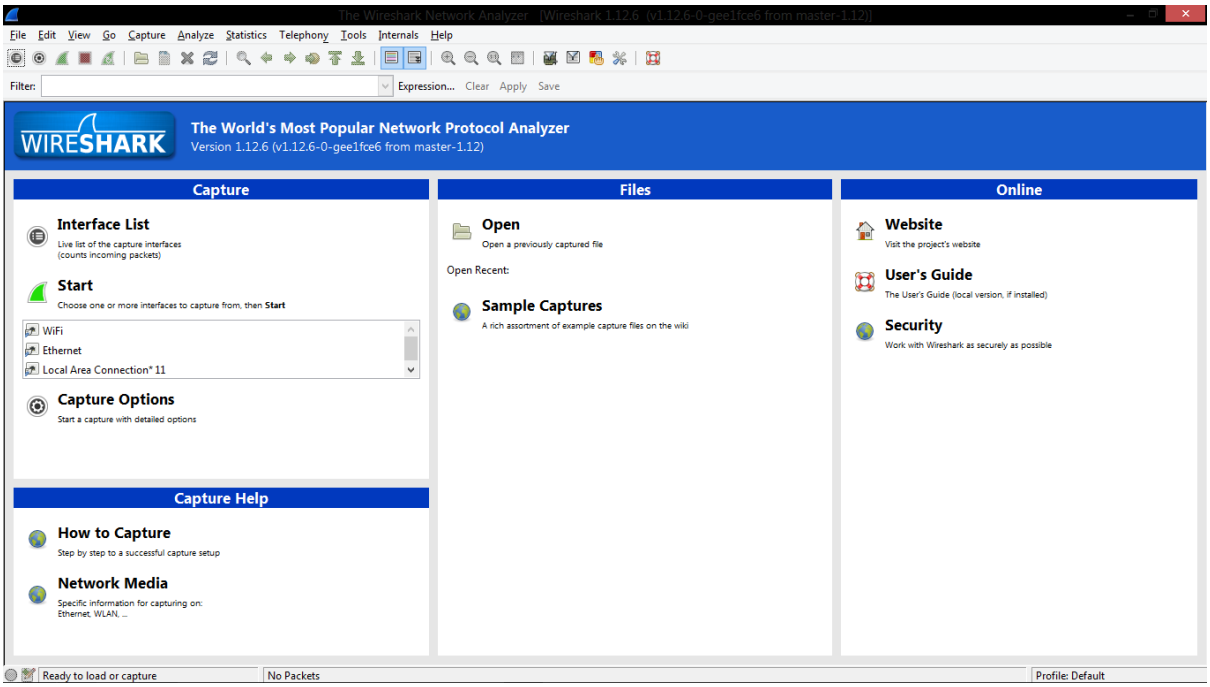
Selain mengakses sistem desktop yang berdiri sendiri dari jarak jauh, pendekatan lain untuk menyediakan akses remote ke sumber daya komputasi adalah melalui desktop dan aplikasi virtualisasi. Virtualisasi desktop adalah sebuah pendekatan yang menyediakan infrastruktur terpusat yang host gambar desktop yang dapat jarak jauh memanfaatkan oleh tenaga kerja. Virtualisasi desktop sering disebut sebagai VDI.

REMOTE MEETING TECHNOLOGY

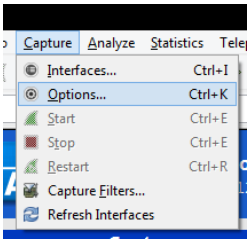
Remote meeting technology adalah teknologi baru yang memungkinkan pengguna untuk melakukan pertemuan online melalui internet, termasuk fungsi desktop sharing. Teknologi ini biasanya termasuk menampilkan slide PowerPoint pada semua PC yang terhubung ke sebuah pertemuan, berbagi dokumen seperti spreadsheet, dan juga berbagi audio atau video. Banyak dari solusi ini dirancang untuk terowongan keluar SSL atau TLS lalu lintas, yang sering dapat lulus melalui firewall dan setiap proxy Web. Penggunaan teknologi pertemuan jarak jauh harus dipahami, dikendalikan, dan sesuai dengan semua kebijakan yang berlaku.

2. ANALISA SOFTWARE WIRESHARK

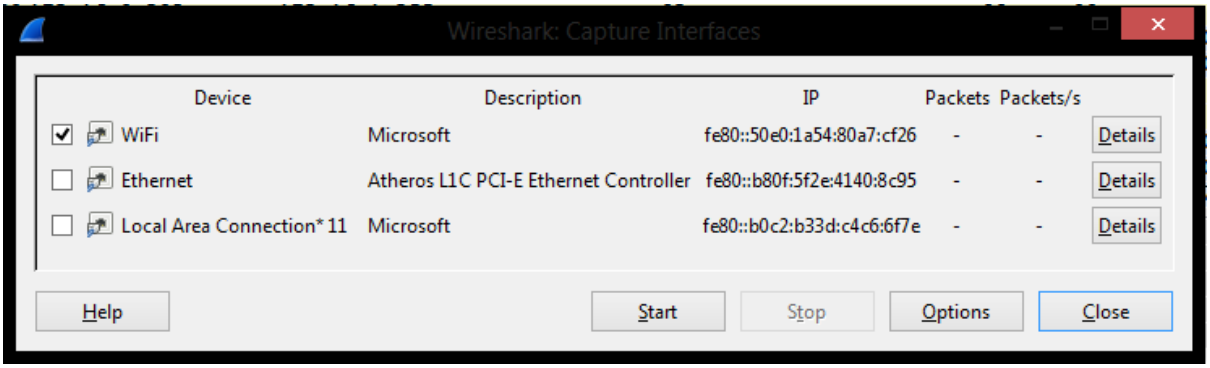
Buka software terlebih dahulu



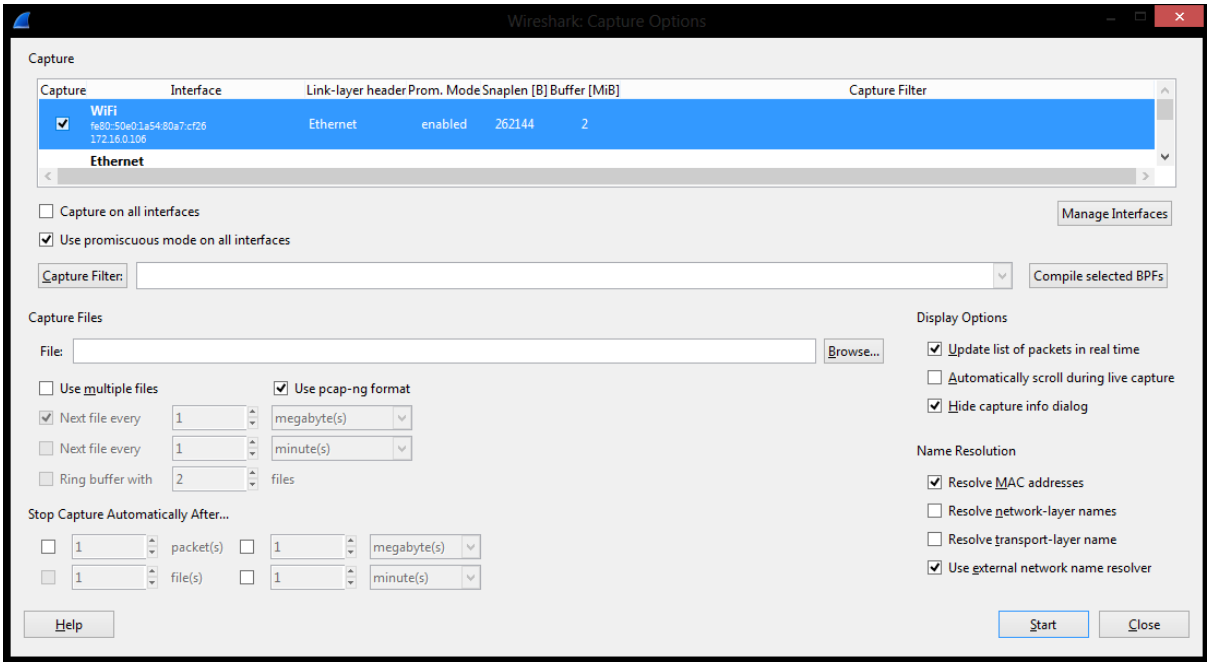
Pertama masuk pada Capture – Option atau menekan tombol Capture Interfaces



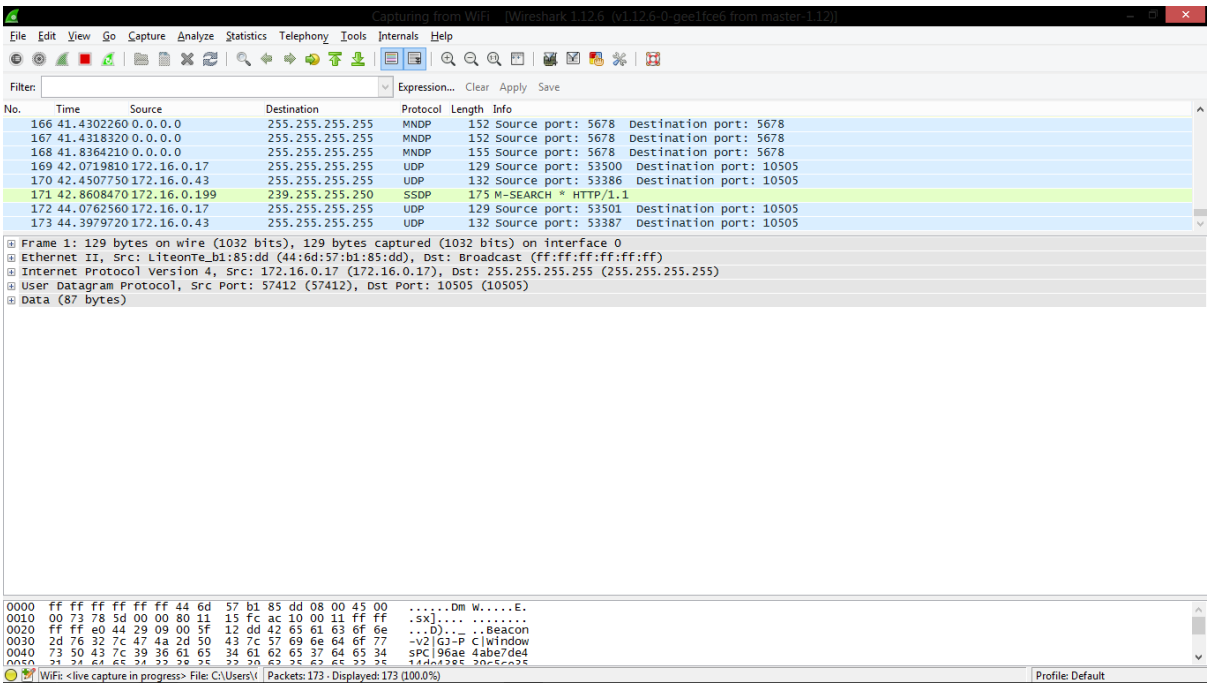
Kemudian akan muncul tampilan window Capture Interfaces. Pilih Option pada Ethernet yang terpakai / yang tersambung dengan jaringan.



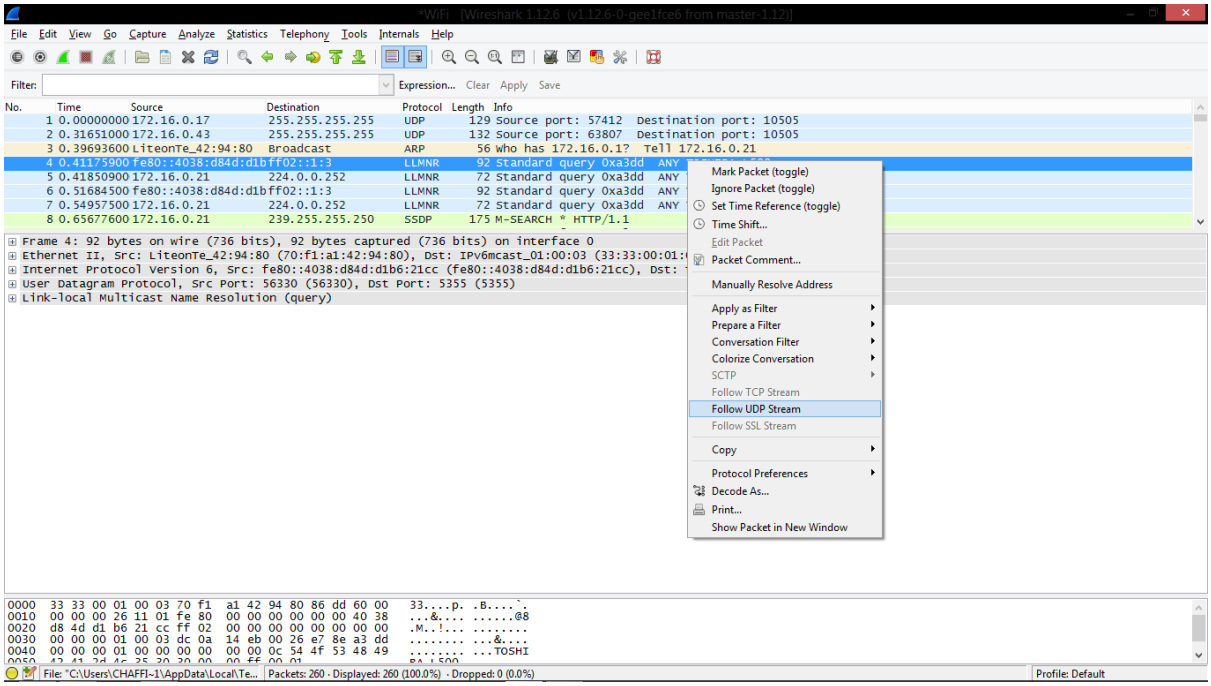
Pilih interface (network card) yang tersambung ke internet



Untuk menyimpan record yang tercapture, bisa mengaktifkan kolom File, pada bagian Capture File(s). Pilih tombol Start untuk memulai merecord packet data yang masuk



Klik tombol stop (Alt+E) setelah anda merasa yakin bahwa ada password yang masuk selama anda menekan tombol start. Pasti akan ada banyak sekali packet data yang merecord. Dari sini kita mulai menganalisa packet tersebut. Karena yang kita butuhkan adalah men-sniffing password, maka pada kolom Filter kita ketikkan http untuk lebih memudahkan pengelompokan packet data.



Klik kanan pada packet tersebut, pilih Follow TCP Stream

Maka akan muncul informasi tentang packet data yang kita pilih. Disini lah kita bisa menemukan username dan password dari halaman administrator blog uad. Biasanya ditanda dengan tulisan berwarna merah.

Jika kita bisa menganalisa packet tersebut satu per satu maka kita akan tau data yang kita cari. Klik find cari kata log / pwd. Pada kasus ini tidak ditemukan.