Copyright © September 2023

PERTEMUAN 14

KEAMANANAN WIRELESS NETWORKING

A. Wireless Technology
   - Celluler-based wireless data solutions
     i. Mempergunakan saluran komunikasi celluler yang sudah ada untuk mengirimkan data (CDMA/GPRS)
   - WLAN Solutions
     i. Hubungan wireless dalam lingkup area yang terbatas, biasanya 10 s/d 100 meter dari base station ke Access Point (AP)
     ii. Mulai meningkat sampai ke 15 mil (WiMax)

B. WLAN

- Sebuah teknologi yang memungkinkan pengiriman data dengan kecepatan antara 11- 54 Megabyte per second. Teknologi ini dikenal dengan sebutan Wireless Fidelity (Wi-Fi), yang bekerja pada jaringan 3G dan dapat membantu pengguna internet berkomunikasi data secara nirkabel.
- Wireless Local Area Network sebenarnya hampir sama dengan jaringan LAN, akan tetapi setiap node pada WLAN menggunakan wireless device untuk berhubungan dengan jaringan.

Copyright © September 2023

- node pada WLAN menggunakan channel frekuensi yang sama dan SSID yang menunjukkan identitas dari wireless device.
- Jaringan wireless memiliki dua mode yang dapat digunakan : infastruktur dan Ad-Hoc.
    i. Konfigurasi infrastruktur adalah komunikasi antar masing-masing PC melalui sebuah access point pada WLAN atau LAN.
    ii. Komunikasi Ad-Hoc adalah komunikasi secara langsung antara masing-masing komputer dengan menggunakan piranti wireless.
- Komponen WLAN
    i. Access Point, berfungsi mengkonversikan sinyal frekuensi radio (RF) menjadi sinyal digital yang akan disalurkan melalui kabel, atau disalurkan ke perangkat WLAN yang lain dengan dikonversikan ulang menjadi sinyal frekuensi radio.
    ii. Access Point, berfungsi mengkonversikan sinyal frekuensi radio (RF) menjadi sinyal digital yang akan disalurkan melalui kabel, atau disalurkan ke perangkat WLAN yang lain dengan dikonversikan ulang menjadi sinyal frekuensi radio.
    iii. Access Point, berfungsi mengkonversikan sinyal frekuensi radio (RF) menjadi sinyal digital yang akan disalurkan melalui kabel, atau disalurkan ke perangkat WLAN yang lain dengan dikonversikan ulang menjadi sinyal frekuensi radio.

C. Standar IEEE 802.11

- Komponen *logic* dari Access Point (AP) adalah ESSID (*Extended Service Set IDentification*). Pengguna harus mengkoneksikan *wireless adapter* ke *AP* dengan ESSID tertentu supaya transfer data bisa terjadi.
- ESSID menjadi *autentifikasi* standar dalam komunikasi wireless. Dalam segi keamanan beberapa vendor tertentu membuat kunci autentifikasi tertentu untuk proses autentifikasi dari klien ke *AP*.
- Rawannya segi keamanan ini membuat IEEE mengeluarkan standarisasi *Wireless Encryption Protocol* (WEP), sebuah aplikasi yang sudah ada dalam setiap PCMCIA card.
- WEP ini berfungsi meng-*encrypt* data sebelum ditransfer ke sinyal Radio Frequency (RF), dan men-*decrypt* kembali data dari sinyal RF.

D. Masalah Keamanan

- Cloning handphone AMPS untuk curi pulsa
- Cloning SIM card

Copyright © September 2023

- Airsnort dapat menyadap paket WLAN. Tools lain seperti Netstumbler, WEPcrack, dll mulai banyak tersedia
- NIST di Amerika melarang penggunakan WLAN untuk sistem yang memiliki data-data confidential
- Bluetooth jacking, bluestumbler: mencuri data-data melalui bluetooth
- Pencurian fisik (perangkat wireless yang biasanya kecil ukurannya) dan data Penyadapan, man-in-middle attack, passive attack dapat dilakukan. Contoh: informasi seperti daftar nomor telepon, calendar, dan data-data lainnya bisa dibaca melalui bluetooth tanpa pengamanan
- Resource perangkat wireless yang terbatas (CPU, memory, kecepatan) sehingga menyulitkan pengamanan dengan encryption misalnya
- Pengguna tidak dapat membuat sistem sendiri, bergantung kepada vendor
- Dos, active attack, injection of new (fake) traffic, mengirim pesan sampah (blue jacking), hijacking information
- Fokus utama dari wireless adalah transfer data secepat mungkin. Pengamanan dengan enkripsi (apalagi dengan resources terbatas) menghambat kecepatan sehingga menjadi nomor dua.
- Pengguna tidak tahu ada masalah keamanan
- Fokus
    i. Identity & Authentication, belum pada confidentiality
    ii. Biasanya yang dideteksi adalah device (perangkat) bukan usernya >> ditambahi dengan PIN. Biometrics. (biometrik lebih sering dipakai sebagai alat otentikasi dengan cara menganalisis karakteristik tubuh manusia yang digunakan, misalnya sidik jari, retina mata, bentuk wajah, cetakan tangan, suara dan lain-lain.)
    iii. Pengelolaan sistem dengan banyak Acces Point menyulitkan (misalnya bagaimana dengan single sign-on, pengguna dynamics firewall untuk akses ke jaringan internal

E. Pengamanan Jaringan WiFi

Copyright © September 2023

- Segmentasi Jaringan
    i. Memasukkan wireless ke sisi extranet yang dianggap kurang aman
- Aktivasi MAC Address Filtering
    i. Setiap peralatan Wi-Fi pastilah memiliki suatu identifikasi yang unik yang dinamakan "physical address" atau MAC address
- Ganti Password Default
    i. Bila perlu ganti pula usernamenya, Jantung dari jaringan Wi-Fi di rumah Anda adalah access point atau router
- Aktivasi Enkripsi
    i. Semua peralatan Wi-Fi pasti mendukung beberapa bentuk dari keamanan data. Intinya enkripsi akan mengacak data yang dikirim pada jaringan nirkabel sehingga tidak mudah dibaca oleh pihak lain
    ii. Standar umum security yang digunakan adalah WEP karena konfigurasi Zero configuration atau sistem setup network Windows dapat langsung mengunakan sistem pengaman dengan WEP. Sedangkan sistem pengaman lain adalah WPA.
    iii. Penggunaan *end-to end encyption* pada level aplikasi
- Ganti SSID Default
    i. Access point atau router menggunakan suatu nama jaringan yang disebut dengan SSID. Vendor biasanya memberi nama produk access point mereka dengan suatu default SSID
- Matikan Broadcast dari SSID
    i. Dalam jaringan Wi-Fi, maka access point atau router biasanya akan membroadcast SSID secara reguler
- Berikan Alamat IP Statis Kepada Piranti WiFi

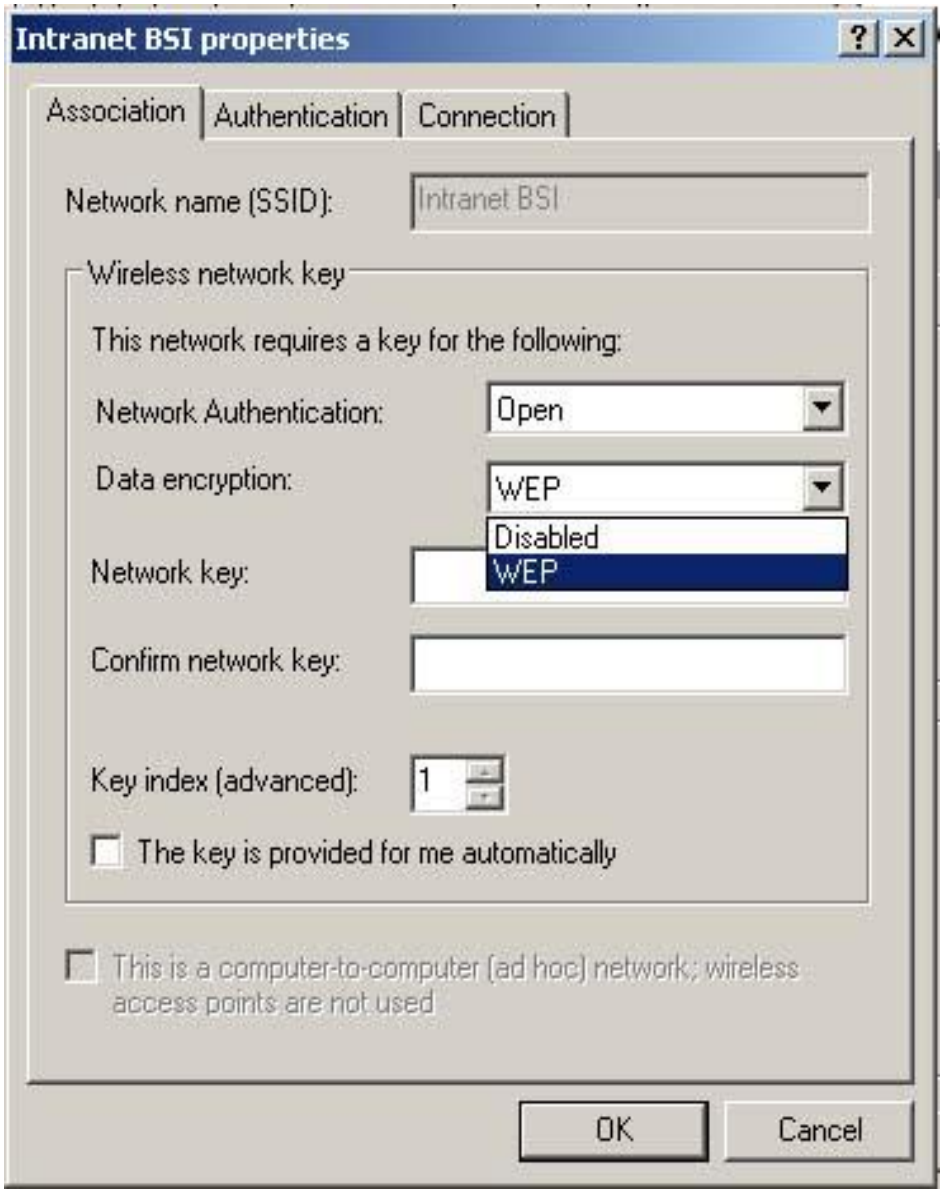
Copyright © September 2023

i. Saat ini cenderung orang memanfaatkan DHCP untuk memberikan alamat IP secara otomatis kepada klien yang ingin terhubung ke jaringan nirkabel.

F. Contoh Dasar Wireless Security Pada AP

- Wireless Network Mode : Mixed (default Access Point yang akan support pada standard 802.11b dan 802.11g)
- Wireless Network Name : Lab Wireless (Nama Access Point yang akan (SSID) terdeteksi di jaringan wireless)
- Wireless Channel : 6-2.437 GHz (default kanal yang digunakan)
- Wireless SSID Broadcast : Enabled (SSID akan dibroadcast ke jaringan wireless)
- Penjelasan:
    i. Pada Network Authentication terdapat Open atau Open system, diartikan network tidak memiliki authentication dan mengijinkan perangkat / computer lain dan bebas memasuki network yang ada tanpa adanya pengaman.
    ii. Dan Shared key, diartikan setiap perangkat atau computer yang ingin bergabung akan ditanyakan kunci pengaman.

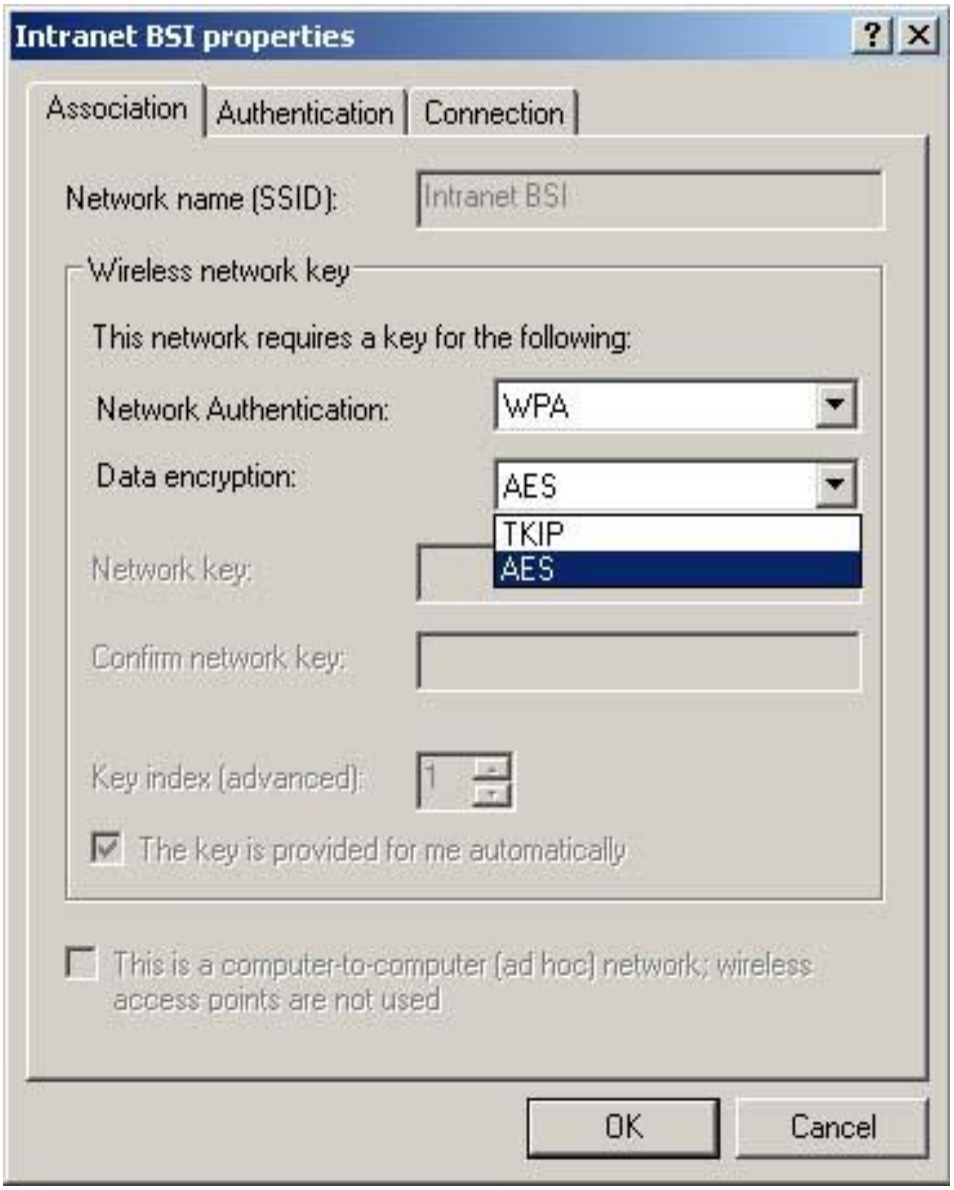
Copyright © September 2023



iii. WPA (Wi-Fi Protected Access)

- Pengamanan jaringan nirkabel dengan menggunakan metoda WPA-PSK jika tidak ada authentikasi *server* yang digunakan. Access point dapat dijalankan dengan mode WPA tanpa menggunakan bantuan komputer lain sebagai server.
- Dua algoritma WPA yang disediakan, terdiri dari algoritma TKIP atau algoritma AES.

Copyright © September 2023



iv. Temporal Key Integrity Protocol (TKIP)

- Sebuah protokol yang didefinisikan oleh IEEE 802.11i yang mengkhususkan untuk jaringan nirkabel untuk menggantikan WEP. TKIP didesain untuk menggantikan WEP tanpa mengubah / mengganti perangkat keras. Hal ini diperlukan karena "buruknya" jenis pengamanan WEP meninggalkan jaringan nirkabel tanpa aktif mengamankan link-layer.
- TKIP, seperti WEP, menggunakan skema kunci berdasarkan RC4, tetapi tidak seperti WEP, TKIP meng-enkripsi semua paket data yang dikirimkan dengan kunci enkripsi yang unik.

Copyright © September 2023

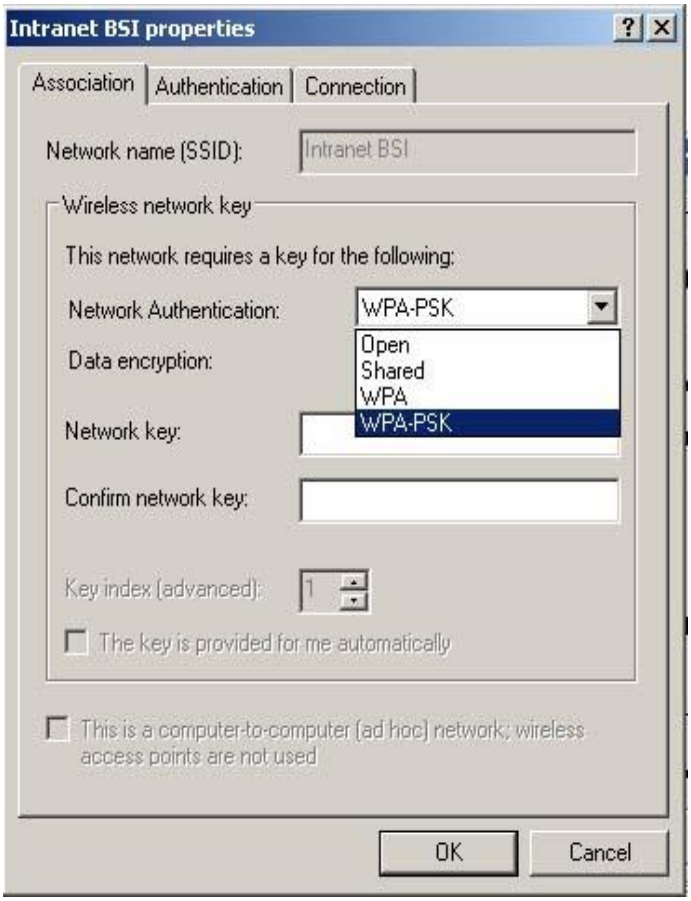
- Setelah Shared-Key didapat, maka client yang akan bergabung dengan *access point* cukup memasukkan angka/kode yang diijinkan dan dikenal oleh *access point*. Prinsip kerja yang digunakan WPA-PSK sangat mirip dengan pengamanan jaringan nirkabel dengan menggunakan metoda Shared-Key.

v. Advanced Encryption Standard (AES)

- diperkenalkan pada Desember 2001 yang merupakan algoritma yang lebih efisien dibanding algoritma sebelumnya. Mempunyai 9, 11 atau 13 kitaran untuk kunci 128 bit, 192 dan 256 bit.

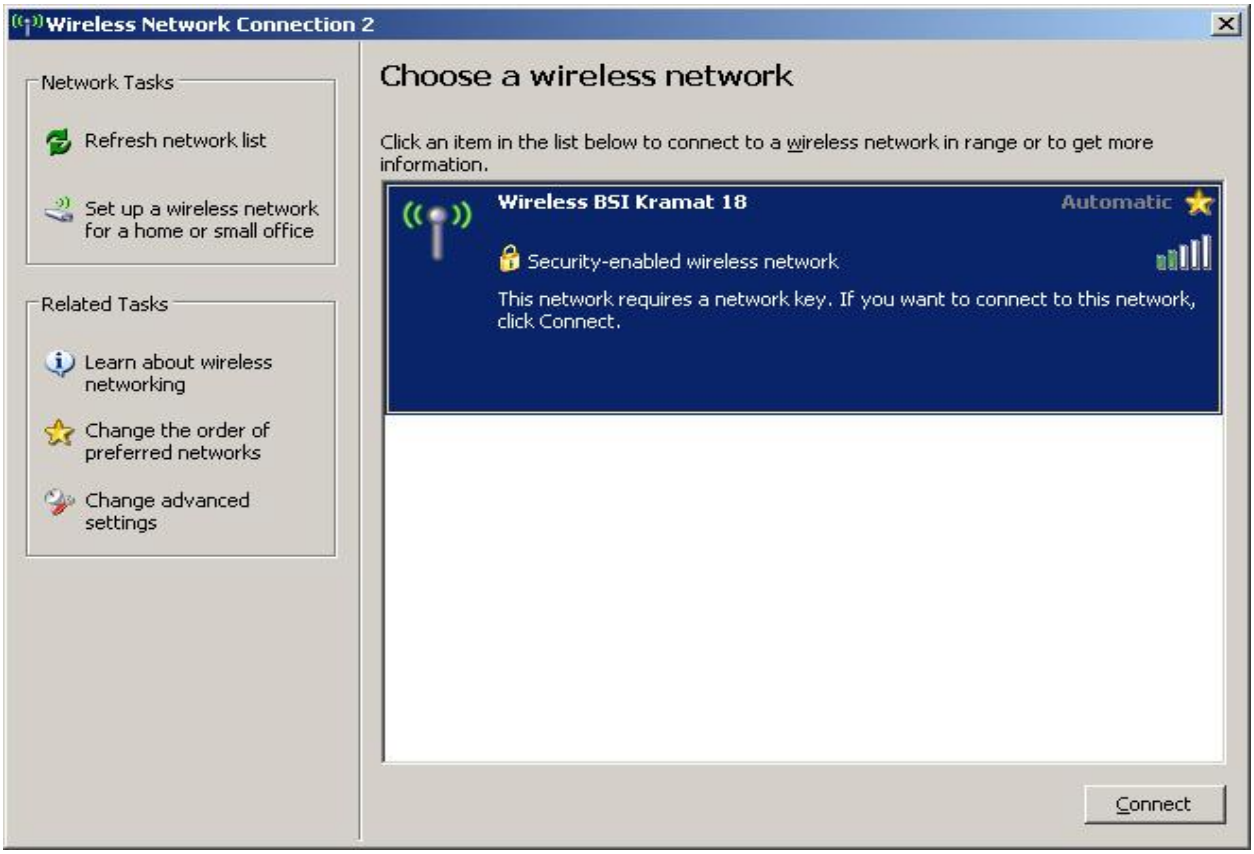
vi. WPA-PSK (WiFi Protected Access – Pre Shared Key)

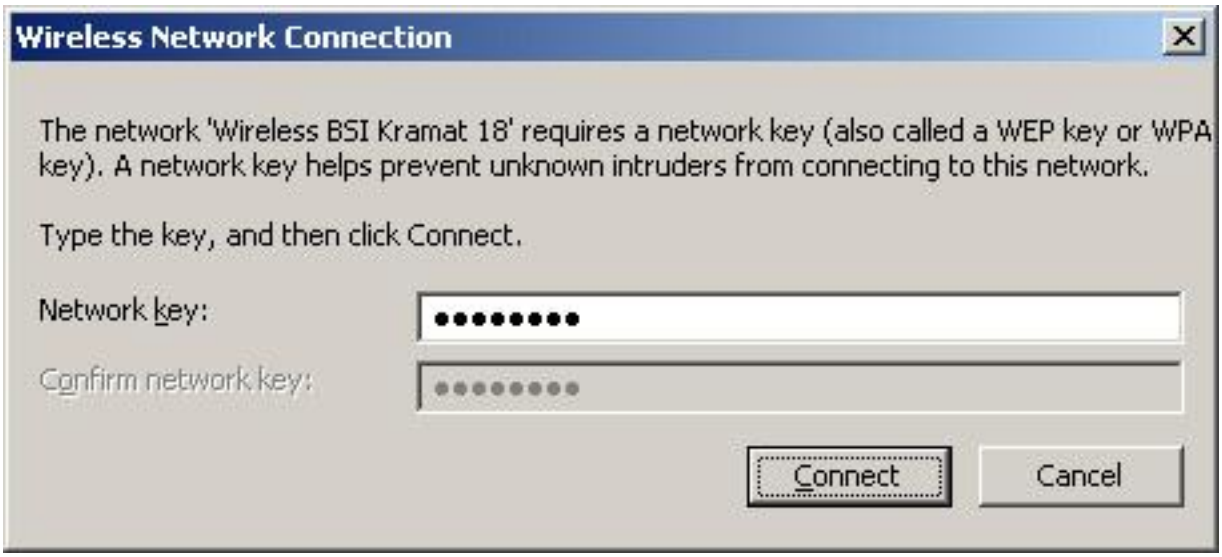
- pengamanan jaringan nirkabel dengan menggunakan metoda WPA-PSK jika tidak ada authentikasi *server* yang digunakan. Access point dapat dijalankan dengan mode WPA tanpa menggunakan bantuan komputer lain sebagai server.



G. Contoh Pengamanan WEP

Copyright © September 2023



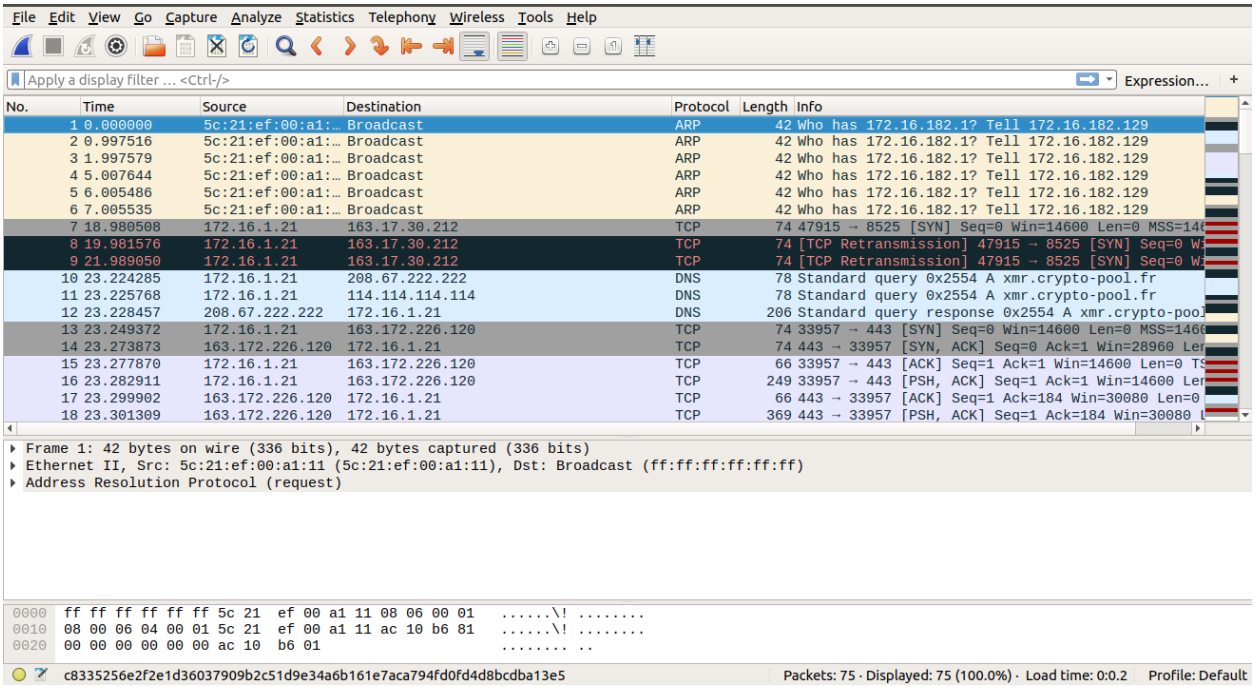


H. Scanning Tools

- Redfang,
- Kismet,
- THC- WarDrive v2.1,
- PrismStumbler,

Copyright © September 2023

- MacStumbler,
- Mognet v1.16,
- WaveStumbler,
- StumbVerter v1.5,
- NetChaser v1.0 for Palm tops
- AP Scanner,
- Wavemon,
- Wireless Security Auditor (WSA),
- AirTraf 1.0
- Wifi Finder

I. Sniffing Tools
- AiroPeek,
- NAI Sniffer Wireless,
- Ethereal,
- Aerosol v0.65
- vxSniffer,
- EtherPEG,
- Drifnet,
- AirMagnet,
- WinDump 3.8,
- Alpha,
- ssidsniff

Copyright © September 2023