# Protokol 802.11 pada Wireshark

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



## Pendahuluan

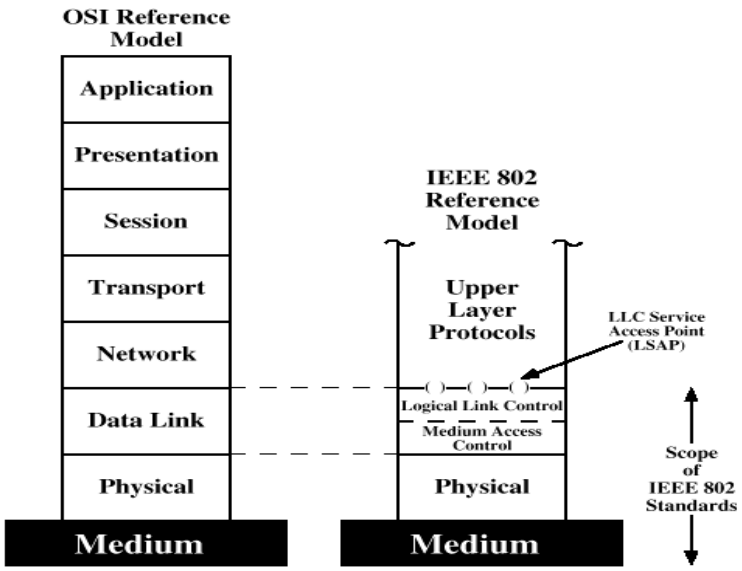
Wireless network merupakan salah satu metode dalam pembangunan jaringan komputer yang praktis karena dalam implementasinya tidak menggunakan kabel untuk komunikasi datanya melainkan menggunakan media udara. hal itu bisa terjadi karena pada tiap-tiap device yang digunakan tersebut terdapat antena yang mengirim dan menerima sinyal radio yang dikirim. Jadi data-data yang akan dikirim dari suatu device akan diubah terlebih dahulu menjadi sinyal radio dan baru setelah itu dikirim ke device tujuan. Dan setelah diterima oleh device tujuan, sinyal radio tersebut diubah kembali menjadi data-data yang ditampilkan.

Sinyal radio sendiri sebenarnya merupakan gelombang elektromagnetik yang terlepas ke udara. Dan seperti yang telah diketahui, terdapat aturan-aturan dalam penggunaan gelombang elektromagnetik tersebut sebagai media untuk pengiriman data. Terdapat parameter-parameter yang perlu diperhatikan dalam penggunaanya seperti daya yang digunakan, frekuensi, channel, dll karena apabila tidak ada protokol atau aturan tertentu yang mengatur penggunaan gelombang radio tersebut akan terjadi tabrakan antar gelombang yang dapat menyebabkan hilangnya data. Protokol yang mengatur gelombang radio tersebut adalah protokol 802.11. pada tulisan ini akan dicoba capturing protocol tersebut menggunakan wireshark agar dapat diketahui parameter apa

saja yang ada didalamnya.

## Jenis-Jenis Protokol 802.11

Seperti yang telah dijelaskan sebelumnya bahwa protokol 802.11 ini merupakan protokol yang mengatur gelombang radio yang digunakan data sebagai medium pengiriman. Oleh sebab itu, Protokol 802.11 ini pada model OSI terdapat pada layer fisik hingga layer LLC (Logical Link Control). Berikut merupakan gambar yang menunjukkan perbandingan layer-layer pada protocol 802 dengan model OSI




Sumber Gambar: http://budi.insan.co.id/courses/ec7010/dikmenjur/hari-report.doc

Protokol 802.11 sendiri selalu berkembang dari waktu ke waktu, berikut merupakan jenis-jenis protokol 802.11 yang ada :

**802.11b**

Digunakan mulai akhir tahun 1999 dengan menggunakan frekuensi 2,4 Ghz. Maksimum bandwidth yang bisa dicapai adalah 11Mbps (Megabit per second). Pada koneksi ini, modulasi yang digunakan adalah DSSS (Direct Sequence Spread Spectrum). Kanal yang tidak overlapping berjumlah 3, yaitu kanal 1, kanal 6 dan kanal 11. Protokol ini kompatibel dengan tipe 802.11g jika tipe 802.11g beroperasi pada mode mixed.

**802.11a**

Digunakan mulai akhir 2001 dengan menggunakan frekuensi 5Ghz. Maksimum bandwidth yang bisa dicapai sebesar 54Mbps sementara modulasi sinyal yang digunakan adalah OFDM (Orthogonal Frequency Division Multiplexing). Kanal yang tidak overlapping berjumlah 12 (bisa lebih). T ipe ini tidak kompatibel denga tipe b maupun g.

**802.11g**

Digunakan mulai pertengahan tahun 2003 dengan menggunakan frekuensi 2,4Ghz. Maksimum bandwidth yang bisa dicapai sebesar 54Mbps. Modulasi yang dighunakan adalah OFDM. Kanal yang tidak overlapping berjumlah 3 buah. Protokol ini kompatibel dengan tipe b namun hasilnya mengikuti tipe b.

**802.11a/g**

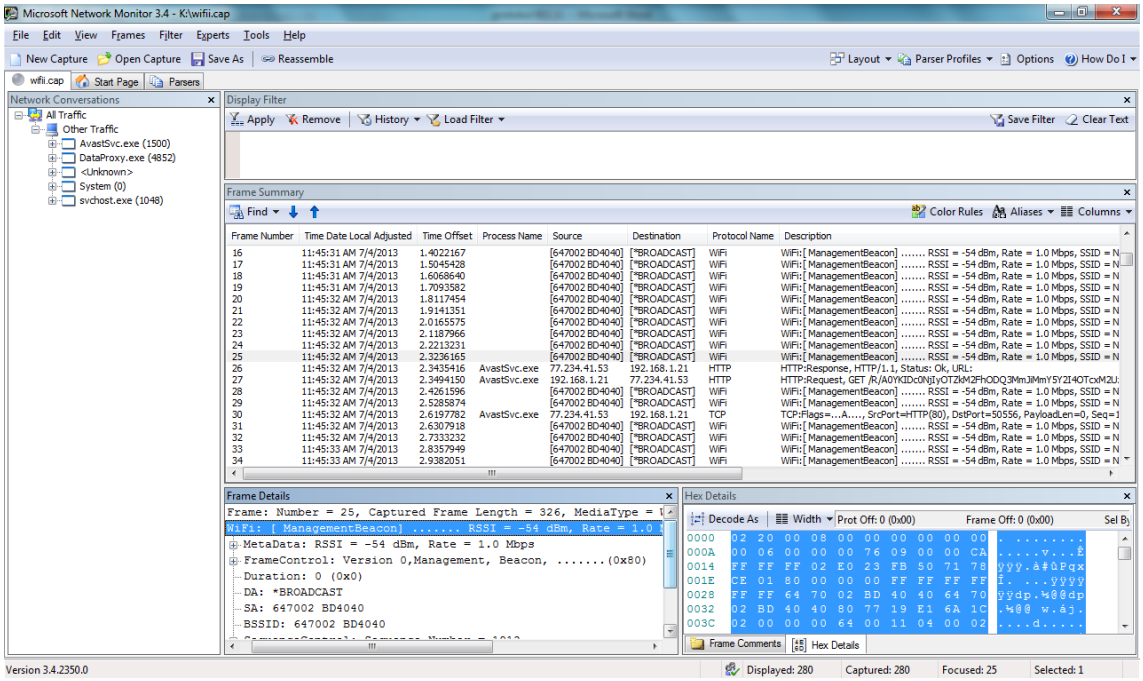
Tipe protokol ini mulai diperkenalkan pertengahan 2003 dengan menggunakan frekuensi 2,4 Ghz dan 5Ghz. Maksimum bandwidth yang bisa dicapai sebesar 54Mbps dengan menggunakan modulasi sinyal OFDM. Kanal yang tidak overlapping berjumlah 16 buah. Bila beroperasi pada modus a, maka protokol ini tidak kompatibel dengan tipe b dan g. Namun, jika beroperasi pada modus g, koneksinya akan kompatibel dengan tipe b.

## CAPTURING Protokol 802.11 dengan Wireshark

Berdasarkan Wiki.Wireshark.org, untuk bisa melakukan capture protokol 802.11 menggunakan wireshark harus mengaktifkan dulu fasilitas “monitor mode” pada wireshark. Padahal tidak semua OS support dengan fasilitas ini. OS windows yang sering digunakan juga termasuk OS yang tidak support untuk fasilitas “monitor mode” ini. Monitor mode ini hanya support pada wireshark 1.4 (atau versi selanjutnya) yang menggunakan OS BSD, Linux, dan Mac OS X system yang terdapat libpcap 1.0 (atau versi selanjutnya) didalamnya. Atau bisa juga dengan menggunakan AirPcap. AirPcap merupakan sebuah device tambahan berbentuk seperti USB yang digunakan untuk melakukan capture protokol 802.11 pada OS windows. Device ini merupakan buatan dari riverbed, berikut gambarnya

Oleh karena itu, diperlukan cara lain untuk melakukan capture protokol 802.11 ini, salah satunya adalah dengan menggunakan bantuan software network protocol analyzer yang lain. Karena OS yang digunakan pada komputer yang akan digunakan untuk melakukan capture ini adalah windows 7, maka akan digunakan network protocol analyzer "Microsoft Network Monitor" karena software ini keluaran dari vendor yang sama seperti windows 7 yaitu Microsoft jadi banyak program di dalamnya yang saling sinkron.

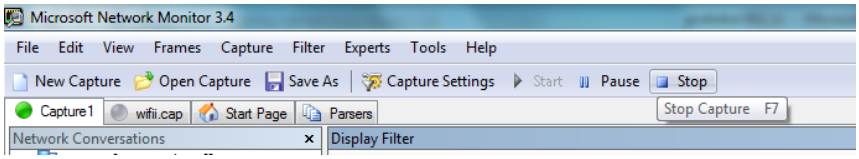
Microsoft network monitor sendiri tidak berbeda jauh dari wireshark, terdapat kolom filter, paket yang tercapture, detail paket, dan detail paket dalam hexadecimal. Berikut tampilan dari Microsoft network Monitor



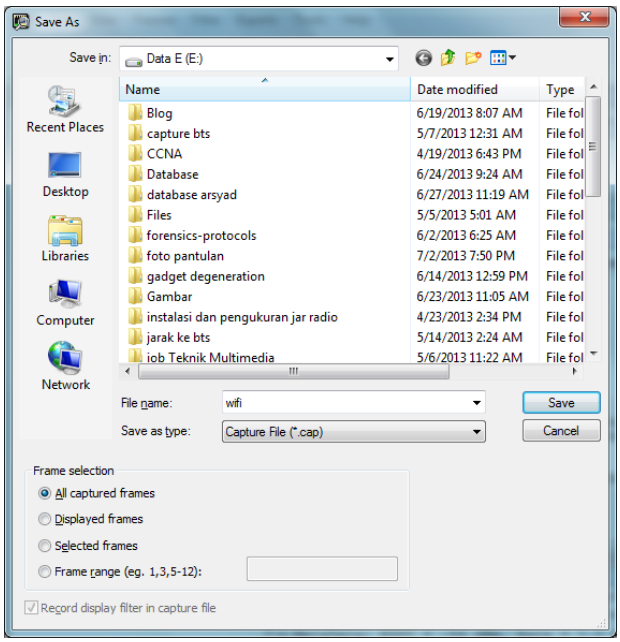

Pada gambar tersebut terlihat jika MNM dapat melakukan capture terhadap protocol 802.11 dimana pada gambar tersebut ditunjukan dengan nama protocol wifi. Di situ

sebenarnya juga sudah terdapat paket detail dari setiap paket yang ada meskipun agak sedikit berbeda tampilanya dengan tampilan yang ada pada wireshark.

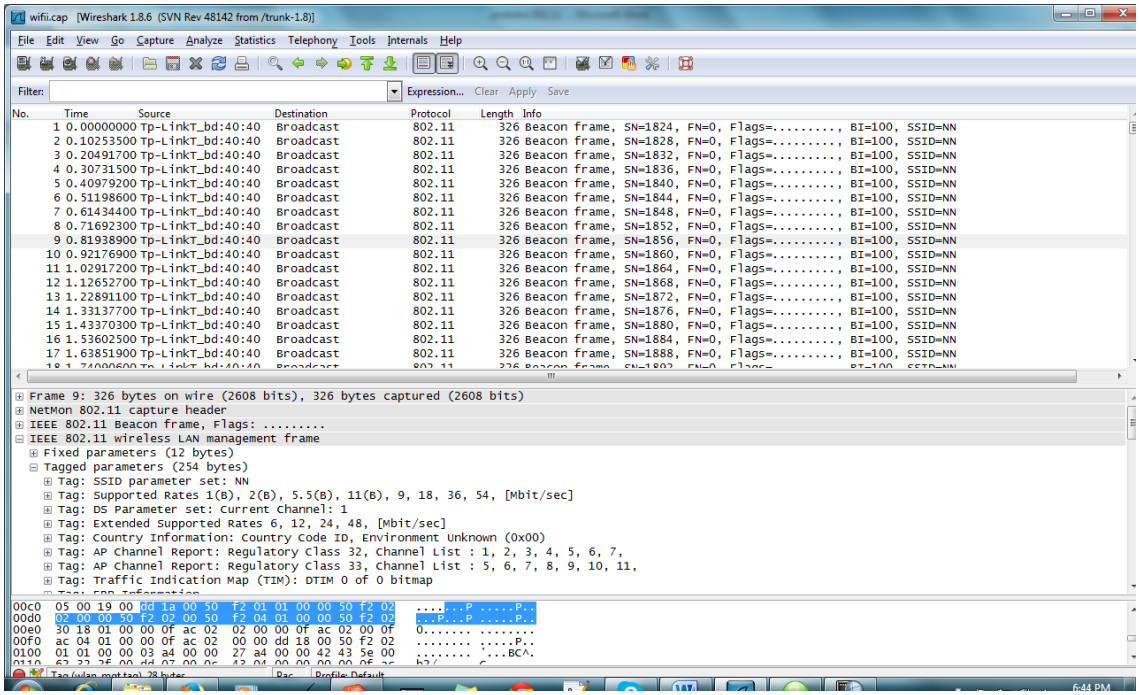
Untuk melihat protocol tersebut melalui wireshark, pertama-tama stop dulu proses capture yang sedang berlangsung dengan cara klik stop pada toolbar



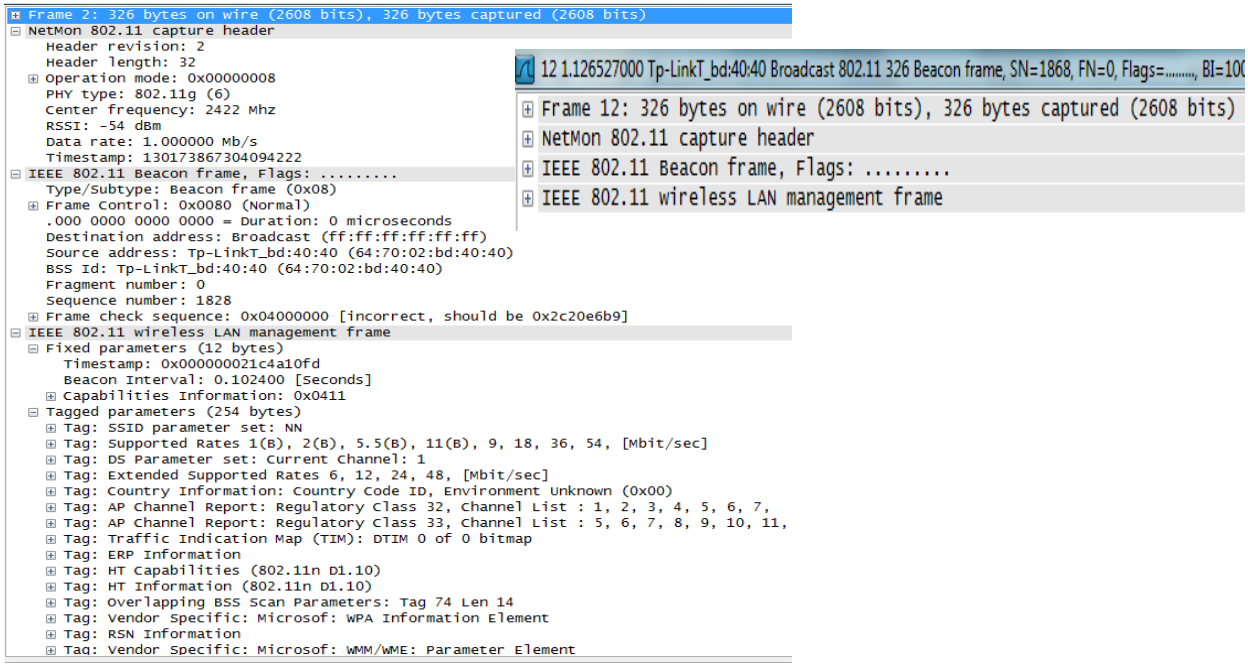

Kemudian save hasil capture protokol wifi tersebut dengan format yang bisa dibaca oleh wireshark yaitu format .cap




Save file tersebut pada folder yang diinginkan kemudian bukalah wireshark dan buka file .cap yang telah di-save tadi dengan cara klik file, open kemudian cari di folder tempat menyimpan file tersebut kemudian klik open.




Gambar di atas merupakan tampilan dari hasil capture protocol wifi yang telah dilakukan pada MNM tadi melalui wireshark. Disitu terlihat nama protokolnya tidak lagi wifi melainkan protokol 802.11. berikut merupakan detail dari paket yang telah tercapture tersebut



Pada gambar tersebut terdapat empat layer pada detail paketnya yaitu frame, netmon 802.11 capture header, IEEE 802.11 beacon frame, dan IEEE 802.11 Wireless LAN Management Frame. Pada gambar terlihat jika frame tersebut merupakan frame ke 12 dan jika dilihat pada keterangan di dalamnya, terdapat detail-detail dari frame tersebut seperti frame number, frame length, capture length, dll.

Kemudian selanjutnya adalah netmon 802.11 capture header, berisi parameter-parameter dari protokol 802.11 yang digunakan. Disitu terlihat jika PHY type yang digunakan adalah 802.11g. PHY type merupakan tipe dari physical layer yang digunakan. Berarti paket tersebut menggunakan 802.11g sebagai layer fisiknya dimana seperti yang telah diketahui pada teori di atas jika 802.11g merupakan protokol 802.11 yang memiliki frekuensi 2,4Ghz dan Maksimum bandwidth yang bisa dicapai sebesar 54Mbps. Hal itu ditunjukan pada keterangan dibawahnya pada "center frequency" yang menunjukan 2422 MHz (2.422GHz) yang berarti komunikasi data yang digunakan pada pengiriman paket data tersebut bekerja pada frekuensi 2.4 GHz. Selain itu terdapat juga keterangan RSSI, Data rate, dan Timestamp.

RSSI merupakan besarnya sinyal radio yang diterima oleh komputer penerima, disitu tertulis besarnya RSSI adalah -54 dBm yang berarti sinyal yang diterima cukup kuat dan bisa digunakan untuk komunikasi data. Kemudian data rate pada gambar tersebut tertulis 1.0000 Mb/s yang berarti data yang dikirim dengan menggunkan sinyal radio tersebut bisa mengirim 1Mb data pada setiap detiknya. Dan timestamp sendiri merupakan suatu tanda yang diberikan ke tiap paket oleh WinPcap.

## Referensi

http://wiki.wireshark.org/CaptureSetup/WLAN#Management_Packets
http://www.khaerulanwar.com/jaringan/2012/03/24/23/protokol--wlan/
http://budi.insan.co.id/courses/ec7010/dikmenjur/hari-report.doc

## Biografi Penulis

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