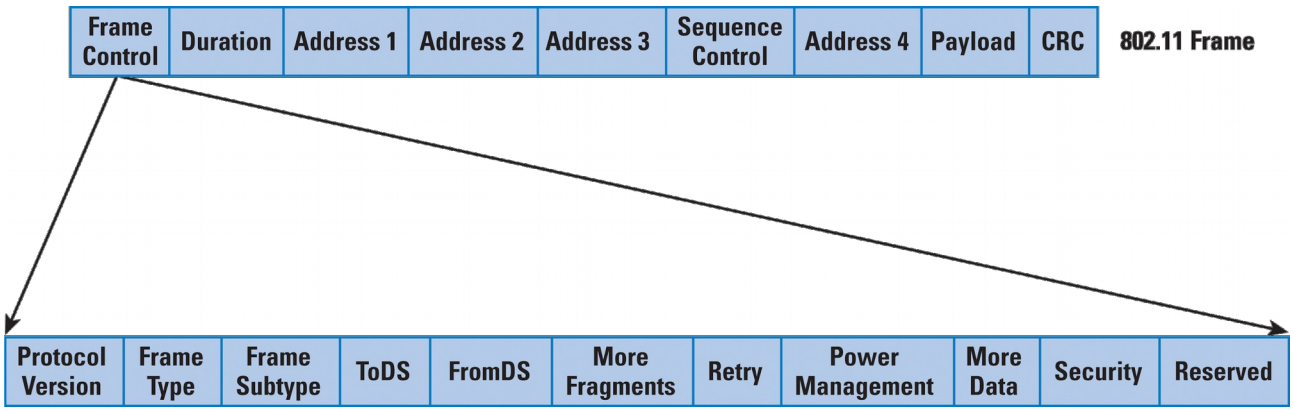
Wireshark'tan USB Dongle'ın Yakaladığı Paketleri Görüntüleme

Wireshark yazılımının USB Dongle'ın yakaladığı paketleri görüntüleyebilmesi için USB Dongle'ı monitör moda geçirmemiz gerekmektedir. Böylece Wireshark'tan USB Dongle'ı seçerek USB Dongle'ın havada yakaladığı tüm paketleri görüntüleyebiliriz ve hatta bunların içinde filtreleme yaparak sadece spesifik bir paket türünün görüntülenmesini sağlayabiliriz. Bu yazıda USB Dongle monitör moda geçirilecektir, ardından Wireshark USB Dongle'ı dinler vaziyete getirilecektir ve Nokia Lumia 620 telefonumun ayarlarındaki Wireless Erişimini kapalı moddan açığa çevirerek telefonun ürettiği Probe Request adlı frame Wireshark'tan görüntülenecektir. Öncelikle Probe Request Frame'i nedir ondan bahsetmek için bir background verelim. Daha sonra Wireshark'tan cep telefonumun ürettiği Probe Request Frame'ini filtrelerle yakalamayı gösterelim.

Background

Kablosuz ağlarda haberleşme işlemi frame'ler (çerçeveler) üzerinden gerçekleşir. 802.11 standartlarına uygun bir frame'in iç yapısı aşağıdaki gibidir.

Frame'in ilk iki byte'lık kısmına Frame Control adı verilir. Bu alan aşağıdaki resimden de görebileceğiniz üzere alt bölümlere sahiptir. Bu ayrılan alt bölümlerden Frame Tpe ve Frame Subtype bu yazının konusudur.



Frame Type Field'ı
Frame Type Wireless LAN frame'lerinin (paketlerinin) tipini belirleyen kısımdır. Wireless LAN frame'leri Management, Control ve Data olmak üzere 3 çeşit frame'e sahiptirler. Frame'lerin Frame Type field'ı bunlardan birinin sayısal değerini tutarak frame'in tipini belirler. Aşağıda frame tiplerinin sayısal değerlerini ve Wireshark'ta frame tipine göre filtreleme uygulamayı sağlayan ilgili filtre kodlarını görmektesiniz.

Frame Type	Sayısal Değeri	Filtre
Management Frames	0	wlan.fc.type == 0
Control Frames	1	wlan.fc.type == 1
Data Frames	2	wlan.fc.type == 2

0 değeri eğer bir frame'in frame type field'ında yer alıyorsa o frame Management Frame'dir. 1 değeri eğer frame'in frame type field'ında yer alıyorsa o frame Control Frame'dir ve aynı şekilde 2 değeri frame type field'ında yer alıyorsa o frame Data Frame'dir. Filtre sütunundaki kodlar ile Wireshark dinlediği interface'ten gelen tüm paketler içerisinden sadece belirtilen frame türüne ait frame'leri sıralamayı sağlar.

Management Frame tipindeki frame'ler alt tiplere ayrılırlar. Bunlardan öne çıkanları Authentication Frame, Deauthentication Frame, Beacon Frame ve Probe Request Frame'dir. Bu yazının konusu Probe Request frame'i olduğu için sadece Probe Request Frame'lerden bahsedilecektir. Diğer frame'ler hakkındaki bilgilere BGA/İncelenmiş Makaleler/Pentest Çalışmalarında Kablosuz Ağ Güvenliği Testleri.docx belgesinin 4 nolu maddesinde bulabilirsin.

Probe Request Frame'leri
İstemciler daha önce bağlandıkları ve otomatik olarak bağlan dedikleri kablosuz ağlar için etrafa sürekli Probe Request frame'lerinden yollarlar. Bu yaptıkları yayın cihaz internet bağlantısı elde edene kadar ya da cihazın Wifi'ı kapatılana kadar devam eder. Örneğin bir router'a bağlanan cep telefonu ayarlarından router'a otomatik bağlan yaparsa ve router'ın kapsam alanı dışına çıkarsa etrafa durmadan Probe Request frame'i yollayacaktır. Cep telefonu ne zaman tekrar kapsam alanına girerse yaydığı Probe Request frame'leri router tarafından algılanacaktır ve router cep telefonunu otomatikmen authenticate edip kendine bağlayacaktır. Böylece kullanıcı cep telefonundan router'a bağlan adımlarını yapmadan router'a bağlanmış, internete erişim elde etmiş olacaktır.

Eğer cep telefonu kapsam alanı dışındaysa sürekli boş yere etrafa Probe Request frame'leri yollarlar. Dolayısıyla cep telefonunun wireless erişimini açık tutmak neden bataryayı tüketir diye bir soru akla gelirse nedenlerinden biri bu probe request frame'lerinin yayınının internet erişimi elde edilene kadar sürüyor oluşundan dolayıdır.

Önceden de denildiği gibi Probe Request Frame'leri Management Frame'lerin bir alt tipidir. Dolayısıyla Probe Request Frame'lerini Wireshark'ta yakalayabilmek için subtype keyword'ü kullanılır ki birazdan bu bahse gelinecektir.

Uygulama
Öncelikle cep telefonunun Wireless Erişimini kapatalım. Sonra TP-Link WN722N adlı usb wifi dongle'ımızı bilgisayara takalım ve interface adını öğrenelim:

```
> iwconfig

Output:
        eth0        Link encap:Ethernet  HWaddr 20:cf:30:64:a9:d5
                    inet addr:192.168.2.201  Bcast:192.168.2.255  Mask:255.255.255.0
                    ….....….

        lo          Link encap:Local Loopback
                    inet addr:127.0.0.1  Mask:255.0.0.0
                    ….....….
```

wlan0 Link encap:Ethernet HWaddr 48:5d:60:38:0a:ff
inet addr:192.168.2.70 Bcast:192.168.2.255 Mask:255.255.255.0
…….…….
wlan2 Link encap:Ethernet HWaddr ec:08:6b:17:c4:24
UP BROADCAST MULTICAST MTU:1500 Metric:1
…….…….

Normalde eth0 ve wlan0 usb dongle takılmadan önce de var olan interface'lerdir. USB dongle takıldıktan sonra wlan2 interface'i belirdiğine göre wlan2 usb dongle'ın interface'idir deriz. Şimdi bu interface'i monitör moda geçirelim ki havadaki tüm paketleri yakalayabilsin. Bu işlem için aircrack tool'unun bir alt bileşeni olan airmon-ng kullanılacaktır.

> sudo su
> airmon-ng stop wlan2
> ifconfig wlan2 down
> airmon-ng start wlan2

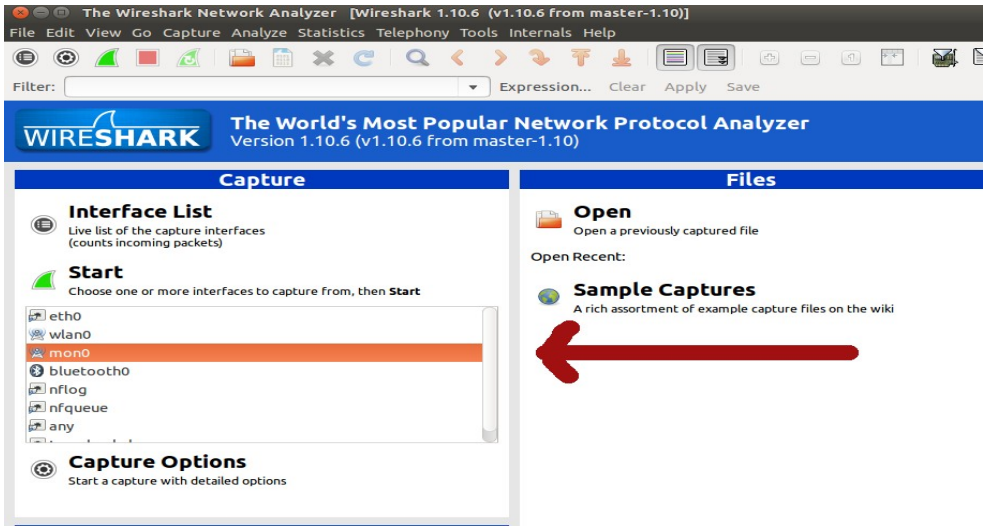
Output:

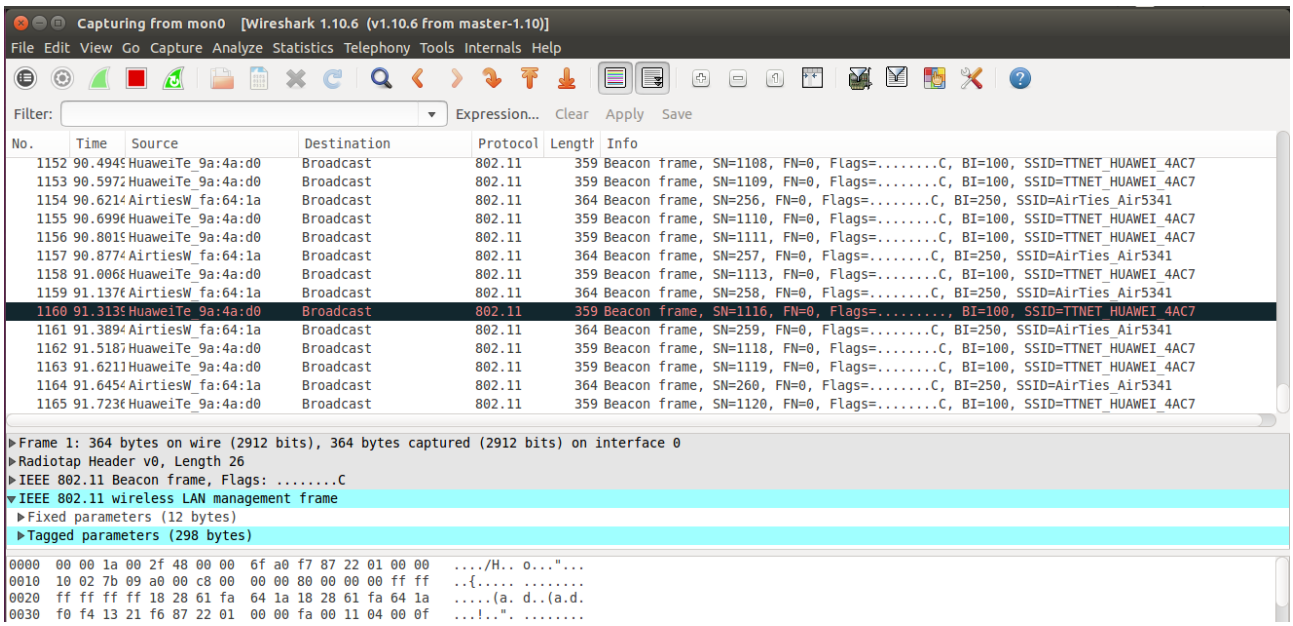
Interface	Chipset	Driver
wlan2	Atheros	ath9k - [phy7] (monitor mode enabled on mon0)
wlan0	Atheros	ath9k – [phy0]

wlan2 interface'inin Driver sütunundan da görülebileceği üzere wlan2 monitör moda geçirilmiştir. Fakat dikkat ederseniz monitör modun mon0 adlı interface üzerinden enable edildiği söylenmektedir. Dolayısıyla wireshark'ta dinleyeceğimiz interface mon0 olacaktır. Şimdi wireshark'ı başlatalım.

> sudo wireshark

Ardından sıralı interface'lerden mon0'yu seçelim ve start düğmesine tıklayalım.

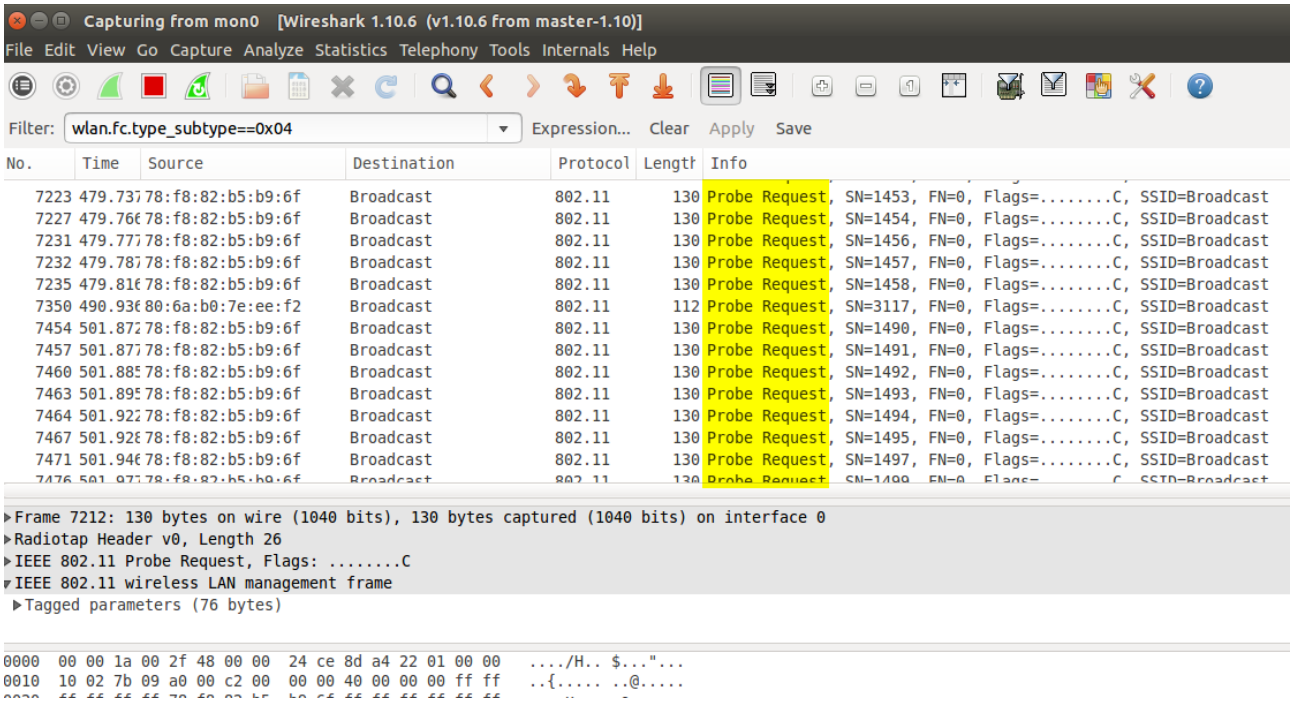




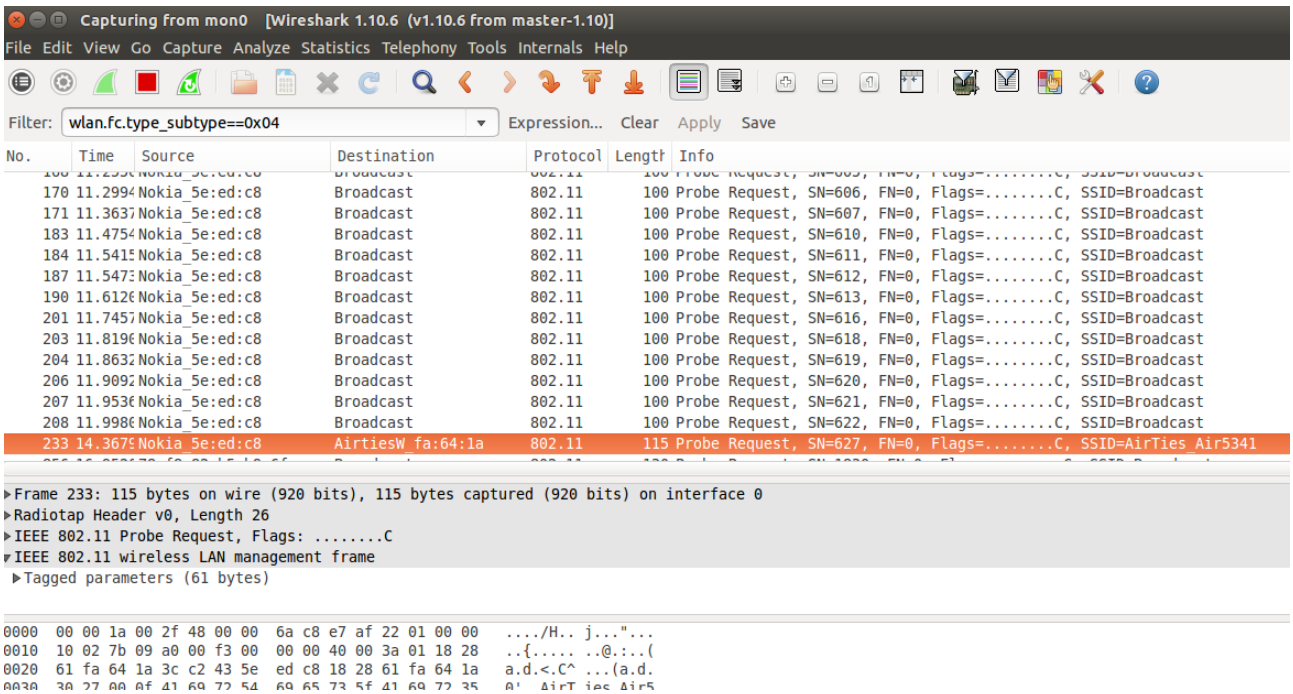
Ardından açılan penceredeki filtre kutusuna aşağıdaki kodu girelim:

> wlan.fc.type_subtype==0x04

4 numarası Probe Request frame'lerinin numarasını temsil eder. Yukarıdaki kod filtreye konulduğu takdirde etrafta yakalanan tüm probe request frame'lerini görüntülüyor olacağız.



Görüldüğü üzere girdiğimiz filtre sayesinde sadece Probe Request frame'leri ekranda sıralanmaktadır. Şimdi wireless erişimine kapalı olan Nokia Lumia 620 model cep telefonumuzu Wireles Erişimine açalım ve Wireshark ekranını gözlemleyelim.



Ekranda sıralı paketlere baştan aşağıya doğru bakacak olursak Nokia kaynağından yapılan Probe Request frame tipinde bir yayının yapıldığını görebiliriz. Yani telefonumuz durmadan probe request frame'i etrafa saçmaktadır. Bu yayın ile Nokia telefonun aslında yapmaya çalıştığı şey etrafta otomatik olarak bağlanabilecek kendinde kayıtlı, daha önce bağlandığı router'ları yoklamak ve bulabilirsa otomatikmen bağlanabilmektir. Yoklama işlemi ekranda seçilmiş satırda belirtilen son paketten de görülebileceği üzere işe yarıyor ve daha önce bağlanılmış, beni otomatik bağla ayarının yapıldığı router'a (Airties'e) otomatikmen bağlantı kuruluyor.

Sonuç

Bu yazıda cep telefonunun wireless erişimini aç kapa yaparak bir paket üretmiş olduk ve bu paketi Wireshark'ta görüntülemiş olduk.