# 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 Duration Address 1 Address	2 Address 3 Sequence Control	Address 4 Payloa	I CRC
----------------------------------	------------------------------	------------------	-------

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.



😢 🖨 🖬	See Capturing from mon0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)] File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help								
•	) 🦾 🗖 🔬	X C Q (	< > > 7 1 📃 🖻 🗉 🖉 🔛 🐚 🔀 🖉						
Filter:			▼ Expression Clear Apply Save						
No.	Time Source	Destination	Protocol Length Info						
115	2 90.4949HuaweiTe 9a:4a:d0	Broadcast	802.11 359 Beacon frame, SN=1108, FN=0, Flags=C, BI=100, SSID=TTNET HUAWEI 4AC7						
115	3 90.5972HuaweiTe 9a:4a:d0	Broadcast	802.11 359 Beacon frame, SN=1109, FN=0, Flags=C, BI=100, SSID=TTNET HUAWEI 4AC7						
115	4 90.6214AirtiesW_fa:64:1a	Broadcast	802.11 364 Beacon frame, SN=256, FN=0, Flags=C, BI=250, SSID=AirTies_Air5341						
115	5 90.699€HuaweiTe_9a:4a:d0	Broadcast	802.11 359 Beacon frame, SN=1110, FN=0, Flags=C, BI=100, SSID=TTNET_HUAWEI_4AC7						
115	6 90.8019HuaweiTe_9a:4a:d0	Broadcast	802.11 359 Beacon frame, SN=1111, FN=0, Flags=C, BI=100, SSID=TTNET_HUAWEI_4AC7						
115	7 90.8774AirtiesW_fa:64:1a	Broadcast	802.11 364 Beacon frame, SN=257, FN=0, Flags=C, BI=250, SSID=AirTies_Air5341						
115	8 91.0068HuaweiTe_9a:4a:d0	Broadcast	802.11 359 Beacon frame, SN=1113, FN=0, Flags=C, BI=100, SSID=TTNET_HUAWEI_4AC7						
115	9 91.137€AirtiesW_fa:64:1a	Broadcast	802.11 364 Beacon frame, SN=258, FN=0, Flags=C, BI=250, SSID=AirTies_Air5341	_					
116	0 91.3139 HuaweiTe_9a:4a:d0	Broadcast	802.11 359 Beacon frame, SN=1116, FN=0, Flags=, BI=100, SSID=TTNET_HUAWEI_4AC7						
116	1 91.3894AirtiesW_fa:64:1a	Broadcast	802.11 364 Beacon frame, SN=259, FN=0, Flags=C, BI=250, SSID=AirTies_Air5341						
116	2 91.5187 HuaweiTe_9a:4a:d0	Broadcast	802.11 359 Beacon frame, SN=1118, FN=0, FLags=C, BI=100, SSID=TTNET_HUAWEI_4AC7						
116	3 91.6211HuaweiTe_9a:4a:d0	Broadcast	802.11 359 Beacon frame, SN=1119, FN=0, Flags=C, BI=100, SSID=TTNET_HUAWEI_4AC7						
116	4 91.6454AirtiesW_fa:64:1a	Broadcast	802.11 364 Beacon frame, SN=260, FN=0, Flags=C, BI=250, SSID=Arfles Arf3341						
116	5 91.7230 HuaweiTe_9a:4a:d0	Broadcast	802.11 359 Beacon frame, SN=1120, FN=0, FLags=C, BI=100, SSID=TTNET_HUAWE1_4AC7						
▶Frame ▶Radio	1: 364 bytes on wire (2912 b tap Header v0, Length 26	oits), 364 bytes c	captured (2912 bits) on interface 0						
▶ IEEE 8	802.11 Beacon frame, Flags:	C							
▼ IEEE	802.11 wireless LAN managemer	nt frame							
▶ F1xe	d parameters (12 bytes)								
▶ Tagg	ed parameters (298 bytes)								
0000 0 0010 1 0020 1 0030 1	00         00         1a         00         2f         48         00         00         6f         a           10         02         7b         09         a0         00         c8         00         00         6           10         02         7b         09         a0         00         c8         00         00         6           ff         ff         ff         18         28         61         fa         64         1           f0         f4         13         21         f6         87         22         01         00         6	0 f7 87 22 01 00 0 80 00 00 00 ff a 18 28 61 fa 64 0 fa 00 11 04 00	00/H o" ff{ la(a. d(a.d. of!."						

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.

See Capturing from mon0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]															
File Ed	it view	Go Capture A	natyze Sta	itistics lelep	nony loois	Incernals He	elp		,						
	) (			KCC	2 < >	<b>4 7</b>	<u></u>		÷	- 1	÷ +			🗙 🕐	
Filter:	wlan.fc	type_subtype==	0x04		• E	xpression	Clear	Apply	Save						
No.	Time	Source		Destinatio	n	Protocol	Lengtł	Info							
722	3 479.73	8778:f8:82:b5:	b9:6f	Broadcast		802.11	130	Probe Re	equest,	SN=1453,	FN=0,	Flags=.	c,	SSID=Broad	cast
722	7 479.76	6678:f8:82:b5:	b9:6f	Broadcast		802.11	130	Probe Re	equest,	SN=1454,	FN=0,	Flags=.	c,	SSID=Broad	cast
723	1 479.77	7778:f8:82:b5:	b9:6f	Broadcast		802.11	130	Probe Re	equest,	SN=1456,	FN=0,	Flags=.	c,	SSID=Broad	cast
723	2 479.78	3778:f8:82:b5:	b9:6f	Broadcast		802.11	130	Probe Re	equest,	SN=1457,	FN=0,	Flags=.	c,	SSID=Broad	cast
723	5 479.81	L€ 78:f8:82:b5:	b9:6f	Broadcast		802.11	130	Probe Re	equest,	SN=1458,	FN=0,	Flags=.	c,	SSID=Broad	cast
735	9 490.93	3€80:6a:b0:7e:	ee:f2	Broadcast		802.11	112	Probe Re	equest,	SN=3117,	FN=0,	Flags=.	c,	SSID=Broad	cast
745	4 501.87	278:f8:82:b5:	b9:6f	Broadcast		802.11	130	Probe Re	equest,	SN=1490,	FN=0,	Flags=.	c,	SSID=Broad	cast
745	7 501.87	778:f8:82:b5:	b9:6f	Broadcast		802.11	130	Probe Re	equest,	SN=1491,	FN=0,	Flags=.	c,	SSID=Broad	cast
746	9 501.88	8578:f8:82:b5:	b9:6f	Broadcast		802.11	130	Probe Re	equest,	SN=1492,	FN=0,	Flags=.	c,	SSID=Broad	cast
746	3 501.89	0578:f8:82:b5:	b9:6f	Broadcast		802.11	130	Probe Re	equest,	SN=1493,	FN=0,	Flags=.	c,	SSID=Broad	cast
746	4 501.92	2278:f8:82:b5:	b9:6f	Broadcast		802.11	130	Probe Re	equest,	SN=1494,	FN=0,	Flags=.	c,	SSID=Broad	cast
746	7 501.92	2878:f8:82:b5:	b9:6f	Broadcast		802.11	130	Probe Re	equest,	SN=1495,	FN=0,	Flags=.	c,	SSID=Broad	cast
747	1 501.94	€ 78:f8:82:b5:	b9:6f	Broadcast		802.11	130	Probe Re	equest,	SN=1497,	FN=0,	Flags=.	c,	SSID=Broad	cast
7/7	5 5 A 1 A	77 78 • f8 • 87 • h5 •	ha.et	Broadcast		802 11	130	Drohe Re		CM-1/00	EN-0	Flanc-	C	SSTD-Broad	cast
▶Frame 7212: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface 0 ▶Radiotap Header v0, Length 26 ▶IEEE 802.11 Probe Request, Flags:C ▼IEEE 802.11 wireless LAN management frame															
►Tagg	ed para	neters (76 byt	es)												
0000 0	0 00 1a	00 2f 48 00 (	90 24 ce	8d a4 22 01	00 00	/H \$									

 0000
 00
 00
 24
 ce
 80
 a4
 22
 01
 000
 ..../H.. \$..."...

 0010
 10
 02
 7b
 09
 a0
 00
 co
 a4
 a2
 01
 00
 00
 ..../H.. \$..."...

 0010
 10
 02
 7b
 09
 a0
 00
 co
 a4
 a0
 00
 00
 ff
 .......................
 .......................

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.

😕 亘 🗊 Capturing from mon0 [Wiresl	nark 1.10.6 (v1.10.6 from	n master-1.10)]					
File Edit View Go Capture Analyze St	atistics Telephony Tool	s Internals He	elp				
• • 🖉 📕 🔏   🚞 🗎	X C 🔍 🔇	> 🗣 Ŧ	🛓 🗐 📑 6 o 6 🕾 👹 M 🐚 🔀 👔				
Filter: wlan.fc.type_subtype==0x04	•	Expression	Clear Apply Save				
No. Time Source	Destination	Protocol	Length Info				
100 11.2994 Nokia_5e:ed:c8 171 11.3633 Nokia_5e:ed:c8 183 11.4754 Nokia_5e:ed:c8 184 11.5415 Nokia_5e:ed:c8 187 11.5475 Nokia_5e:ed:c8 190 11.612C Nokia_5e:ed:c8 201 11.7457 Nokia_5e:ed:c8 203 11.8196 Nokia_5e:ed:c8 204 11.8633 Nokia_5e:ed:c8 206 11.9092 Nokia_5e:ed:c8	Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast	802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11	<pre>100 Probe Request, SN=606, FN=0, Flags=C, SSID=Broadcast 100 Probe Request, SN=606, FN=0, Flags=C, SSID=Broadcast 100 Probe Request, SN=610, FN=0, Flags=C, SSID=Broadcast 100 Probe Request, SN=611, FN=0, Flags=C, SSID=Broadcast 100 Probe Request, SN=612, FN=0, Flags=C, SSID=Broadcast 100 Probe Request, SN=613, FN=0, Flags=C, SSID=Broadcast 100 Probe Request, SN=613, FN=0, Flags=C, SSID=Broadcast 100 Probe Request, SN=616, FN=0, Flags=C, SSID=Broadcast 100 Probe Request, SN=618, FN=0, Flags=C, SSID=Broadcast 100 Probe Request, SN=618, FN=0, Flags=C, SSID=Broadcast 100 Probe Request, SN=619, FN=0, Flags=C, SSID=Broadcast 100 Probe Request, SN=619, FN=0, Flags=C, SSID=Broadcast</pre>				
207 11.9530 Nokia_5e:ed:c8	Broadcast	802.11	100 Probe Request, SN=621, FN=0, Flags=C, SSID=Broadcast				
233 14.3675 Nokia_5e:ed:c8	AirtiesW_fa:64:1a	802.11	115 Probe Request, SN=627, FN=0, Flags=C, SSID=AirTies_Air5341				
Frame 233: 115 bytes on wire (920 bits), 115 bytes captured (920 bits) on interface 0 Radiotap Header v0, Length 26 IEEE 802.11 Probe Request, Flags:C ✓IEEE 802.11 wireless LAN management frame							
▶Tagged parameters (61 bytes)							
0000 00 00 1a 00 2f 48 00 00 6a c8 0010 10 02 7b 09 a0 00 f3 00 00 00	e7 af 22 01 00 00 40 00 3a 01 18 28	/H j	· " · · · ·				

0020 61 fa 64 la 3c c2 43 5e ed c8 18 28 61 fa 64 la a.d.<.c^ ...(a.d. AARA 3A 27 AA Af 41 64 72 54 64 65 73 5f 41 64 72 35 A' AirT iec Air5

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.