null-byte.wonderhowto.com

BY KODY 12/07/2019

التجسس على حركة مرور الشبكة من الهاتف الذكي باستخدام Wireshark

ترجمة وتنقيح – الباحث المهندس احمد الربيعي

ربما تريد ان تعرف ما يفعله شخص على هاتفه في حال كنت تستخدم شبكة Wi-Fi نفسها . هذا بسيط في حال قمت باستخدام Wireshark وتكوين بعض الإعدادات. الان سنقوم باستخدامه لفك تشفير حركة مرور شبكة WPA2 حتى نتمكن من التجسس على التطبيقات التي يعمل بها هذا الهاتف في الوقت الفعلي . سيكون من الافضل استخدام شبكة مشفرة أفضل من استخدام شبكة مفتوحة ، اذ ستعمل على اخفاء ميزة وجود المهاجم على نفس الشبكة. فإذا كان شخص آخر يعرف كلمة مرور شبكة Wireshark التي تستخدمها ، فسيكون من السهل أن ترى ما تفعله في تلك اللحظة باستخدام لعمي المناحي . حيث يمكن أن يسمح للمهاجم بإنشاء قائمة بكل تطبيق يعمل على الجهاز المستهدف .

عملية فك تشفير الحزم المشفرة

عندما تكون على شبكة Wi-Fi تستخدم تشفير WPA2 ، فأن امانك يعتمد على شيئين : اولاً : كلمة المرور المستخدمة لإنشاء رقم أطول أو مفتاح PSK أو مفتاح مشترك مسبقًا. ثانياً : المصافحة الفعلية نفسها ، والتي يجب أن تحدث لإقامة اتصال. فإذا أحد المهاجمين يملك

ية . PSK على شبكة Wi-Fi ولاحظ انضمامك إلى الشبكة أو خروجك للحظة ، فيمكنه فك تشفير حركة مرور Wi-Fi لمعرفة ما تفعله.

لن يكون من الممكن رؤية محتوى مواقع HTTPS ، ولكن يمكن رؤية المواقع على HTTP التي تقوم بزيارتها او التطبيقات التي تعتمد عليها ، مما يجعل هاتفك في وضع سهل . قد لا يبدو هذا أمرًا كبيرًا ، لكن في عضون 60 ثانية فقط ، فمن السهل معرفة الكثير عن نوع الجهاز الذي نراقبه وما الذي يعمل عليه بالضبط ، كما سيكون من السهل رؤية طلبات DNS لحل المجالات التي تحتاج التطبيقات إلى التحدث إليها من أجل ان تعمل ، اضافةً الى تحديد التطبيقات والخدمات النشطة.

کيف يعمل ؟

للقيام هذا الهجوم ، يجب تلبية بعض الشروط. أولاً ، نحتاج إلى كلمة المرور ، كما يجب علينا أن نكون على مقربة من الضحية حتى نتمكن من تسجيل حركة المرور ، ويجب أن نكون قادرين على اخراج الجهاز المستهدف من الشبكة وانتظار إعادة الاتصال . ثم سنقوم بفتح وانتظار حزم Wireshark والوصول إلى القائمة لفك تشفير حزم Wi-Fi ، وإضافة PSK لتمكين فك التشفير وانتظار حزم EAPOL من الجهاز المستهدف المتصل بالشبكة. للتعرف على ماهية الجهاز المستهدف ، سنستخدم عوامل فلترة الالتقاط لتسليط الضوء على حزم DNS و التطلا على نبحث عنها. للاطلاع على قائمة كاملة بكل مجال دخله الجهاز ، كما يمكننا أيضًا الاطلاع على ملخص للنطاقات التي تم حلها بعد اكتمال الالتقاط. حيث يمكننا استخدام هذه المعلومات لاختيار الخدمات التي يتم تشغيلها بسهولة ، حتى لو كانت تعمل في الخلفية ولم يتم تشغيل التطبيق في بعض الوقت.

ماذا ستحتاج ؟

للقيام بذلك ، ستحتاج إلى بطاقة محول شبكة لاسلكية قادرة على وضع الجهاز في وضع المراقبة كما يجب ان يكون متوافقاً مع Kali ويدعم وضع المراقبة . بعد ذلك ، ستحتاج إلى هاتف ذكي يعمل بنظام iOS أو Android ويكون متصل بشبكة Wi-Fi التي تراقبها. اذ يمكنك ممارسة هذا على شبكة Wi-Fi مفتوحة لمعرفة ما يفترض أن تراه ، حيث قد لا يعمل فك ممارسة هذا على شبكة Wi-Fi منتحتاج أيضًا إلى معرفة كما يقترض أن تراه ، حيث قد لا يعمل مله التشفير في بعض الأحيان. كما ستحتاج أيضًا إلى معرفة كمة المرور واسم الشبكة Wi-Fi التي تراقبها. اذ يمكنك معارسة وين متصل بشبكة Wi-Fi التي تراقبها. اذ يمكنك ممارسة هذا على شبكة Wi-Fi مفتوحة لمعرفة ما يفترض أن تراه ، حيث قد لا يعمل فك مارسة وي بعض الأحيان. كما ستحتاج أيضًا إلى معرفة كلمة المرور واسم الشبكة لشبكة Fi التشفير في بعض الأحيان. كما ستحتاج أيضًا إلى معرفة كلمة المرور واسم الشبكة لشبكة Fi

١. قم بتنزيل Wireshark والاتصال بشبكة Wi-Fi : قم بتنزيل Wireshark وتثبيته إذا لم يكن مثبتًا بالفعل ، ثم قم بالاتصال بشبكة Wi-Fi التي تستهدفها. إذا كنت تخطط لاستخدام مثبتًا بالفعل ، ثم قم بالاتصال بشبكة وسابة باستخدام أداة Wireshark لاستخدام أداة Wireshark ، فيجب عليك حسابة باستخدام أداة Wireshark وقبل القيام بذلك ، لأنه قد لا تتمكن من الوصول إلى الإنترنت أثناء الالتقاط ، اعتمادًا على بطاقتك. وبمجرد تنزيل Wireshark ، قم بفتحه ، ثم ألق نظرة على واجهات الشبكة. قبل القيام بذلك ، لأنه قد لا تتمكن من الوصول إلى الإنترنت أثناء الالتقاط ، اعتمادًا التي القيام بذلك ، لأنه قد لا تتمكن من الوصول إلى الإنترنت أثناء الالتقاط ، اعتمادًا على بطاقتك. وبمجرد تنزيل Wireshark ، قم بفتحه ، ثم ألق نظرة على واجهات الشبكة. قبل البدء في الالتقاط ، سنحتاج إلى إعداد بعض الأشياء للتأكد من التقاط السبكة.

proto-			
ng this filter:			
Enter a capture litter			
Wi-Fi: en0	h		
p2p0			
Thunderbolt Bridge: bridge0			
awdl0			
utun0			
Thunderbolt 2: en1			
utun1	lin		
Thunderbolt 4: en2			
Thunderbolt 1: en3			
Thunderbolt 3: en4		-	
Loopback: Io0			
gif0		-	
stf0		-	
XHC0			
XHC1		-	
XHC20			
Cisco remote capture: cisco		-	
Random packet generator: randpkt			
SSH remote capture: ssh			
UDP Listener remote capture: udpdump			

٢. إعداد Wireshark لالتقاط : ضمن خيار قائمة Wireshark ، انقر على قائمة
 ٢. إعداد Capture options) . كما في النافذة التالية :

• • •					Τ	he Wi
) 🗖 🚺	×	0	9		
Apply a display fi	Ite Capture options]				
	Welcome to	Wires	hark			
	Open					
	/Users/skickar/I	Docume	ents/Inte	ercepts	/CAMC	CAPTL
	/Users/skickar/l	Docume	ents/Inte	ercepts	/Only t	to and

سيؤدي ذلك إلى فتح نافذة التقاط الواجهات ، كما هو موضح أدناه.

nterface	Traffic	Link-layer Header	Promisci	Snaplen (B)	Buffer (MB)	Monitor Capture Filter
Wi-Fi: en0	-1	B02.11 plus radiotap header	8	default	2	2
p2p0		Raw IP	23	default	2	-
Thunderbolt Bridge: bridge0		Ethernet	22	default	2	
► awdi0		Ethernet		default	2	
▶ utun0	_	BSD loopback	82	default	2	-
Thunderbolt 2: en1		Ethernet	C	default	2	
► utun1	J.	BSD loopback	63	default	2	
Thunderbolt 4: en2		Ethernot	2	default	2	
Thunderbolt 1: en3		Ethernet	8	default	2	
Thunderbolt 3: en4		Ethernet	63	default	2	
Loopback: io0		BSD loopback		default	2	-
gif0	_	BSD loopback	83	default	2	-
Enable promiscuous mode on all int	erfaces					Manage Interfaces
acture filter for selected interfaces:	Enter a conture filter				+	Compile BPFs

- ٣. ابدأ التقاط الشبكة ومسح لحزم EAPOL : إذا لم تكن متصلاً بالشبكة التي يعمل بها هدفك ، فلن تتمكن من رؤية أي حزم لأنك قد تكون في قناة عشوائية أخرى. حيث لا يمكن له Wireshark بالفعل من تغيير القناة التي يعمل عليها محول الشبكة اللاسلكية ، لذلك إذا لم تحصل على أي شيء ، فقد يكون ذلك هو السبب.
- ٤. فك تشفير حركة مرور الشبكة باستخدام PSK : الآن وقد أصبح لدينا مصافحات ، يمكننا فك تشفير المحادثة من هذه النقطة فصاعدًا. وللقيام بذلك ، سنحتاج إلى إضافة كلمة مرور الشبكة أو PSK. ما عليك سوى الانتقال إلى القائمة المنسدلة في Wireshark وحدد خيار (Preferences) وبمجرد تحديده ، انقر فوق (Protocols) كما في النافذة التالية :

Layout Columns Font and Colors Capture Filter Buttons Name Resolution Protocols 104apci 29West 2dparityfec 3GPP2 A11 6LoWPAN 802.11 Radio 802.11 Radio 802.11 Radio 802.11 Radiotap 9P A-bis OML A21 ACAP	Protocols Display hidden protocol items Display byte fields with a space character between bytes Look for incomplete dissectors	
ACN ACR 122		
ACtrace		

ضمن البروتوكولات ، قم بتحديد (IEE 802.11) ، ثم انقر فوق (Enable decryption) لإضافة مفتاح الشبكة ، ثم انقر فوق (Edit) ثم بعدها على (ecryption keys) لفتح النافذة لإضافة كلمات المرور و PSKs. كما في النافذة التالية :

HiQnet		
HISLIP HL7 HNBAP HP_ERM HPFEEDS HSMS HSRP HTTP HTTP2 IAPP IAX2 IB ICAP ICEP ICMP ICP ICQ IEEE 802.11	IEEE 802.11 wireless LAN	
IEEE 802.1AH		

حدد (wpa-psk) من القائمة ، ثم الصق مفتاحك. بعدها اضغط على Tab ، ثم احفظ بالنقر فوق (OK) . كما في النافذة التالية :

wep wpa-pwd ✓ wpa-psk f7c1a67c97d232e44d	39ce973a34f5463a77cae2eaf48c1e6f98
+ - Po	/Users/skickar/.config/wireshark/80211_keys
Help	Cancel OK

٥

بمجرد اكتمال ذلك ، انقر فوق (OK)في قائمة التفضيلات ، هنا ينبغي على Wireshark إعادة فحص جميع الحزم التي تم التقاطها ومحاولة فك تشفيرها. هذا قد لا يعمل لمجموعة متنوعة من الأسباب. لكني تمكنت من جعله يعمل في معظم الوقت من خلال التأكد من حصولي على مصافحة جيدة (EAPOL) والتبديل بين استخدام كلمة مرور الشبكة و PSK. إذا نجحت ، فيمكننا الانتقال إلى خطوة تحليل حركة المرور لاختيار التطبيقات قيد الاستخدام.

- م. البحث عن حزم DNS و HTTP : الآن وبعد أن قمنا بتجريد الحماية المحيطة بحركة المرور ، يمكن لـ Wireshark فك تشفير ها وإخبارنا عن الأجهزة الموجودة على شبكة Wi-Fi التي لدينا مصافحة للقيام بها في الوقت الفعلي. وتنقسم الى قسمين :
- طلبات DNS : لرؤية الحزم المهمة ، سنبدأ بطلبات DNS. التي تتأكد من التطبيقات و عناوين IP التي من المفترض أن تتصل بها لم تتغير. و هنا سيتم توجيههم إلى أسماء النطاقات التي تحتوي عادةً على اسم التطبيق ، مما يجعل من السهل مشاهدة التطبيق الذي يتم تشغيله على هاتف iPhone أو Android وتقديم الطلبات. وللاطلاع على هذه الطلبات ، سنستخدم مرشح الالتقاط ، DNS و مما يجعل مما سيرينا المسارات الأكثر وضوحًا التي يقوم التطبيق بتركها عبر شبكة iPi أو Wi-Fi. أو لأ ، قم بكتابة dns في المحارات في الأكثر وضوحًا التي يقوم التطبيق بتركها عبر شبكة iPi و Wi-Fi.

إذا كان هدفك وحيداً ، فقد ترى الرد :

Tinder calls the Tindersparks.com domain بالإضافة إلى الكثير من الخدمات الأخرى. وهذا الطلب هو واحد من الأكثر وضوحا. كما في النافذة التالية :

378903 205.894710	Android.local	209.18.47.63	DNS
378904 205,894757	Android.local	209, 18, 47, 62	DNS
378949 205.941100	209.18.47.62	Android.local	DNS
378950 205.941146	209.18.47.63	Android.local	DNS
382022 208.199861	Android.local	209.18.47.63	DNS
382067 208.270314	209.18.47.63	Android, local	DNS
382162 208.356419	Android.local	209.18.47.63	DNS
382172 208.357433	209.18.47.63	Android.local	DNS
382230 208.392068	209.18.47.63	Android.local	DNS
411508 230.773654	Android.local	289.18.47.63	DNS
411565 230.804220	Android.local	209.18.47.63	DNS
411572 230 805556	Android local	789 18 47 63	DMS
TEEE 902 11 0oc Data			
ILLE 002.11 QUS Data,	rugs: .pr.		
Logical-Link Control	rtagsp		
Logical-Link Control Internet Protocol Ver	sion 4, Src: 209.18.47.63 (20)	9.18.47.63), Dst: Android.local (192.	168.0.67)
Logical-Link Control Internet Protocol Ver User Datagram Protoco	rion 4, Src: 209.18.47.63 (20) 1, Src Port: domain (53), Dst	9.18.47.63), Dst: Android.local (192. Port: 58124 (58124)	168.0.67)
Logical-Link Control Internet Protocol Ver User Datagram Protoco Domain Name System (r	sion 4, Src: 209.18.47.63 (20) l, Src Port: domain (53), Dst esponse)	9.18.47.63), Dst: Android.local (192. Port: 58124 (58124)	168.0.67)
Logical-Link Control Internet Protocol Ver User Datagram Protoco Domain Name System (r <u>IRequest In: 38216</u> ; [Time: 0.035649000	sion 4, Src: 209.18.47.63 (20) 1, Src Port: domain (53), Dst esponse) 21 seconds] -231	9.18.47.63), Dst: Android.local (192. Port: 58124 (58124)	168.0.67)
Logical-Link Control Internet Protocol Ver User Datagram Protoco Domain Name System (r <u>IRequest In: 38216</u> [Time: 0.035649000 Transaction ID: 0x > Flags: 0x8180 Stand Questions: 1	riggs: ipric sion 4, Src: 209.18.47.63 (209 il, Src Port: domain (53), Dst response) 21 seconds] c221 dard query response, No error	9.18.47.63), Dst: Android.local (192. Port: 58124 (58124)	168.0.67)
Link Gos Data Logical-Link Control Internet Protocol Ver User Datagram Protoco Domain Name System (r <u>IRequest In: 38216</u>) [Time: 0.035649000 Transaction ID: 0x. > Flags: 0x8180 Stan Questions: 1 Answer RRs: 9 Authority RRs: 0	sion 4, Src: 209.18.47.63 (20) hl, Src Port: domain (53), Dst esponse) 21 seconds] c221 dard query response, No error	9.18.47.63), Dst: Android.local (192. Port: 58124 (58124)	168.0.67)
Logical-Link Control Internet Protocol Ver User Datagram Protoco Domain Name System (r <u>IRequest In: 38216</u> ; [Time: 0.035649000 Transaction ID: 0x; Flags: 0x8180 Stand Questions: 1 Answer RRs: 9 Authority RRs: 0 Additional RRs: 0	sion 4, Src: 209.18.47.63 (209 1, Src Port: domain (53), Dst esponse) 21 seconds] c221 dard query response, No error	9.18.47.63), Dst: Android.local (192. Port: 58124 (58124)	168.0.67)
Logical-Link Control Internet Protocol Ver User Datagram Protoco Domain Name System (r <u>IRequest In: 38216</u> [Time: 0.035649000 Transaction ID: 0x. > Flags: 0x8180 Stan Questions: 1 Answer RRs: 9 Authority RRs: 0 Additional RRs: 0 > Queries	sion 4, Src: 209.18.47.63 (20 1, Src Port: domain (53), Dst esponse) 21 seconds] c221 dard query response, No error	9.18.47.63), Dst: Android.local (192. Port: 58124 (58124)	168.0.67)
Link Control Logical-Link Control Internet Protocol Ver User Datagram Protoco Domain Name System (r <u>[Request In: 38216]</u> [Time: 0.035649000 Transaction ID: 0x. > Flags: 0x8180 Stand Questions: 1 Answer RRs: 9 Authority RRs: 0 Additional RRs: 0 > Queries > etl.tindersparks	sion 4, Src: 209.18.47.63 (20) hl, Src Port: domain (53), Dst esponse) 21 seconds] c221 dard query response, No error com: type A, class IN	9.18.47.63), Dst: Android.local (192. Port: 58124 (58124)	168.0.67)
Legical-Link Control Logical-Link Control Internet Protocol Ver User Datagram Protoco Domain Name System (r <u>IRequest In: 38216</u> ; [Time: 0.035649000 Transaction ID: 0x; Flags: 0x8180 Stan Questions: 1 Answer RRs: 9 Authority RRs: 0 Additional RRs: 0 V Queries v etl.tindersparks Name: etl.tin	sion 4, Src: 209.18.47.63 (20) l, Src Port: domain (53), Dst esponse) 21 seconds] c221 dard query response, No error s.com: type A, class IN dersparks.com	9.18.47.63), Dst: Android.local (192. Port: 58124 (58124)	168.0.67)
Legical-Link Control Internet Protocol Ver User Datagram Protoco Domain Name System (r <u>[Request In: 38216</u> , [Time: 0.035649000 Transaction ID: 0x; Flags: 0x8180 Stand Questions: 1 Answer RRs: 9 Authority RRs: 0 Additional RRs: 0 V Queries v etl.tindersparks Name: etl.tin [Name Length:	sion 4, Src: 209.18.47.63 (20) vol, Src Port: domain (53), Dst response) 21 seconds] c221 dard query response, No error c.com: type A, class IN dersparks.com	9.18.47.63), Dst: Android.local (192. Port: 58124 (58124)	168.0.67)
Link Control Logical-Link Control Internet Protocol Ver User Datagram Protoco Domain Name System (r <u>[Request In: 38216]</u> [Time: 0.035649000 Transaction ID: 0x. > Flags: 0x8180 Stan Questions: 1 Answer RRs: 9 Authority RRs: 0 Additional RRs: 0 Additional RRs: 0 Additional RRs: 0 v Queries v etl.tindersparks Name: etl.tin [Name Length: [Label Count:	sion 4, Src: 209.18.47.63 (20) h, Src Port: domain (53), Dst esponse) 21 seconds] c221 dard query response, No error c.com: type A, class IN dersparks.com 20] 3]	9.18.47.63), Dst: Android.local (192. Port: 58124 (58124)	168.0.67)
Legical-Link Control Logical-Link Control Internet Protocol Ver User Datagram Protoco Domain Name System (r <u>IRequest In: 38216</u> ; [Time: 0.035649000 Transaction ID: 0x; Flags: 0x8180 Stand Questions: 1 Answer RRs: 9 Authority RRs: 0 Additional RRs: 0 VQueries * etl.tindersparks Name: etl.tindersparks	sion 4, Src: 209.18.47.63 (20) l, Src Port: domain (53), Dst esponse) 21 seconds] c221 dard query response, No error s.com: type A, class IN dersparks.com 20] 31 Address) (1)	9.18.47.63), Dst: Android.local (192. Port: 58124 (58124)	168.0.67)
Legical-Link Control Logical-Link Control Internet Protocol Ver User Datagram Protoco Domain Name System (r <u>IRequest In: 38216</u> ITime: 0.035649000 Transaction ID: 0xx Flags: 0x8180 Stand Questions: 1 Answer RRs: 9 Authority RRs: 0 Additional RRs: 0 * etl.tindersparks Name: etl.tim [Name Length: Label Count: Type: A (Host Class: IN (0x)	sion 4, Src: 209.18.47.63 (20) vol, Src Port: domain (53), Dst response) 21 seconds] c221 dard query response, No error s.com: type A, class IN dersparks.com 20] 31 Address) (1) 0001)	9.18.47.63), Dst: Android.local (192. Port: 58124 (58124)	168.0.67)

يعد استخدام Signal فكرة جيدة ، إلا أن استخدامه مع VPN يعد فكرة أفضل. السبب؟ لأنه يؤدي فتح الإشارة إلى إنشاء التبادل أدناه ، حيث يحدد بوضوح أن المستخدم يتواصل مع رسول مشفر.

→ 514808 282.592799 209.18.47.63	Android.local	DNS
557354 301.301935 Android.local	209,18,47.63	DNS
558020 301.661302 209.18.47.63	Android.local	DNS
558055 301.667308 209.18.47.63	Android.local	DNS
▶ Frame 514808: 281 bytes on wire (2248 bits), 281 b	ytes captured (2248 bits) on interfac	2 0
Radiotap Header v0, Length 48		
B02.11 radio information		
> IEEE 802.11 QoS Data, Flags: .pF.C		
Logical-Link Control		
Internet Protocol Version 4, Src: 209.18.47.63 (20)	9.18.47.63), Dst: Android.local (192.)	168.0.67)
> User Datagram Protocol, Src Port: domain (53), Dst	Port: 20568 (20568)	
v Domain Name System (response)		
[Request In: 514647]		
[Time: 0.053268000 seconds]		
Transaction ID: 0x0572		
▶ Flags: 0x8180 Standard query response, No error		
Questions: 1		
Answer RRs: 6		
Authority RRs: 0		
Additional RRs: 0		
v Queries		
v textsecure-service.whispersystems.org: type A	, class IN	
Name: textsecure-service.whispersystems.org	9	
[Name Length: 37]		
[Label Count: 3]		
Type: A (Host Address) (1)		
Class: IN (0x0001)		
▶ Answers		

يؤدي فتح التطبيق للاتصال بـ Uber إلى إنشاء الطلبات التي تراها أدناه.

1	643866 344.188208	Android.local	209.18.47.62	DNS
	644144 344.289428	Android.local	209,18,47,62	DNS
	644509 344.419995	Android.local	209.18,47,62	DNS
	644623 344,444673	209.18.47.63	Android, Local	DNS
	644624 344.444719	209.18.47.63	Android, local	DNS
	644625 344,444764	209.18.47.63	Android, local	DNS
	644626 344,444809	209.18.47.63	Android, local	DNS
	644627 344 444855	209.18.47.63	Android, local	DNS
	644628 344 444988	200 18 47 63	Android local	DAIS
▶ Fra	me 644623: 233 byte	es on wire (1864 bits), 233	bytes captured (1864 bits) on interface	2 0
► Rad	iotap Header v0, L	ength 44		
▶ 802	.11 radio informat	ion		
► IEE	E 802.11 QoS Data,	Flags: .pF.C		
> Log	ical-Link Control			
► Int	ernet Protocol Ver	sion 4, Src: 209.18.47.63 (209.18.47.63), Dst: Android.local (192.1	168.0.67)
► Use	r Datagram Protoco	. Src Port: domain (53), D	st Port: 6958 (6958)	
T Don	ain Name System (re	sponse)		
11/1/10/2010/10	Request In: 640552	1		
-	Time: 1.650836000	seconds]		
	Transaction TD: 0x0	f4a		
	Flags: 0x8180 Stand	and query response. No erro		
1 1	Questions: 1	and query response; no erre		
	Ancuer PRc · A			
	Authority PPc: 1			
	Additional PPc: 0			
	Querier			
	wertes	come tune AAAA class Th		
	Vones co aby?	com: type AAAA, class IN		
	Name: cn-prix2.	cre.uber.com		
	Iname Length:	201		
	Laber Count:	4]		
	Type: AAAA (IF	V6 Address) (28)		
02.3	Class: IN (0x0	2001)		
P .	Authoritative names	ervers		

HTTP Packets : بعد ذلك ، يمكننا أن نرى أن هناك العديد من طلبات الويب غير الأمنة باستخدام مرشح التقاط ملات الذ تحتوي عوامل تصفية الالتقاط هذه على معلومات مثل useragent ، والتي سوف تخبرنا بنوع الجهاز المتصل. كما يمكننا فحص ذلك عن طريق النقر فوق (packets) ثم النقر على علامة التبويب فحص ذلك عن طريق النقر فوق (http المثال ادناه ، يمكننا رؤية طلبات HTTP غير الأمنة إلى خادم الدردشة. ما هو هذا ؟ انه مجرد فحص الحزمة وحل المجال ، wechat يعلي المواب على علامة المتعال المتعال ولي على على على على على على معلومات مثل عن طريق النقر فوق (backet) فحص ذلك عن طريق النقر فوق (backet) معلومات مثل المتعال .



إذا كنا نريد أن نرى كل شيء ، فيمكننا النقر فوق علامة تبويب قائمة (Statistics) وتحديد (Resolved Addresses) لرؤية جميع المجالات التي تم حلها خلال فترة الالتقاط. يجب أن تكون هذه قائمة تضم الخدمات التي يتصل بها الجهاز عبر التطبيقات التي تعمل عليه. كما في النافذة التالية :

🖻 💿 🔵 🗾 🛋 Wi	reshark · Resolved Addresses · /var/folders/n1/l_2ynlx91lv57t122lq8lkyh0000gn
24 225 240 172	
54.225.240.175	constitute version 199925126 ou unit 1 old anagonaut con
74 125 142 100	apps/tyer-web-10100/51/0.eu-west-1.etb.amazonaws.com
74.125.142.100	mobile-glack.l.google.com
52 0 00 206	www.google.com
52.9.00.200	etb-p-gtu-dts-uwi-964236364.us-west-1.etb.ama20naws.com
34.233.233.10/	events-enopoint-j-obooo2941.us-east-1.etb.amazonaws.com
33.227.224.91	ch-phx2.cte.uber.com
15.35.99.0	alwor83br95ng.cloudfront.net
151.101.66.133	contig2.mparticle.com
23.53.253.29	el69/3.a.akamaleoge.net
54.225.133.120	Settings.crashtytics.com
210.58.193.202	googleapis. L.google.com
52.31.14.184	appsrlyer-web-7-644333284.eu-west-1.elb.amazonaws.com
52.31.109.158	appstlyer-web-7-644333284.eu-west-1.elb.amazonaws.com
54.243.211.28	settings.crashlytics.com
54.235.130.153	settings.crashlytics.com
52.1.179.65	a92c0bbf24f7811e985630ec70d216ec-405837804.us-east-1.elb.amaz
172.217.4.138	googleapis.l.google.com
54.225.208.144	settings.crashlytics.com
172.217.5.212	venmopics.appspot.com
172.217.14.110	android.l.google.com
54.153.16.101	elb-p-gld-dls-uw1-984238364.us-west-1.elb.amazonaws.com
13.35.99.100	cdn.branch.io
35.169.3.40	textsecure-service.whispersystems.org
108.128.134.25	appsflyer-web-10-1289156558.eu-west-1.elb.amazonaws.com
54.171.104.162	appsflyer-web-10-1289156558.eu-west-1.elb.amazonaws.com
54.197.255.121	events-endpoint-j-660082941.us-east-1.elb.amazonaws.com
50.19.124.76	settings.crashlytics.com
13.35.103.215	d1w2poirtb3as9.cloudfront.net

Wireshark يجعل شبكات Wi-Fi شيئاً محفوفًا بالمخاطر

قد يبدو هذا النوع من المراقبة القاهرة ، وإذا كنت ترغب في منع هذا النوع من التطفل ، يجب أن تحصل على VPN مثل Mullvad أو PIA الذي يسمح لك بإخفاء حركة المرور المحلية وراء تشفير قوي. في مكان قد تفعل فيه شيئًا حساسًا عبر اتصال البيانات ، يجب عليك أيضًا استخدام البيانات الخلوية كلما كان ذلك ممكنًا لمنع هذا النوع من الهجوم.