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 Wi-Fi التي تستخدمها ، فسيكون من السهل أن ترى ما تفعله في تلك اللحظة باستخدام Wireshark. 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 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.

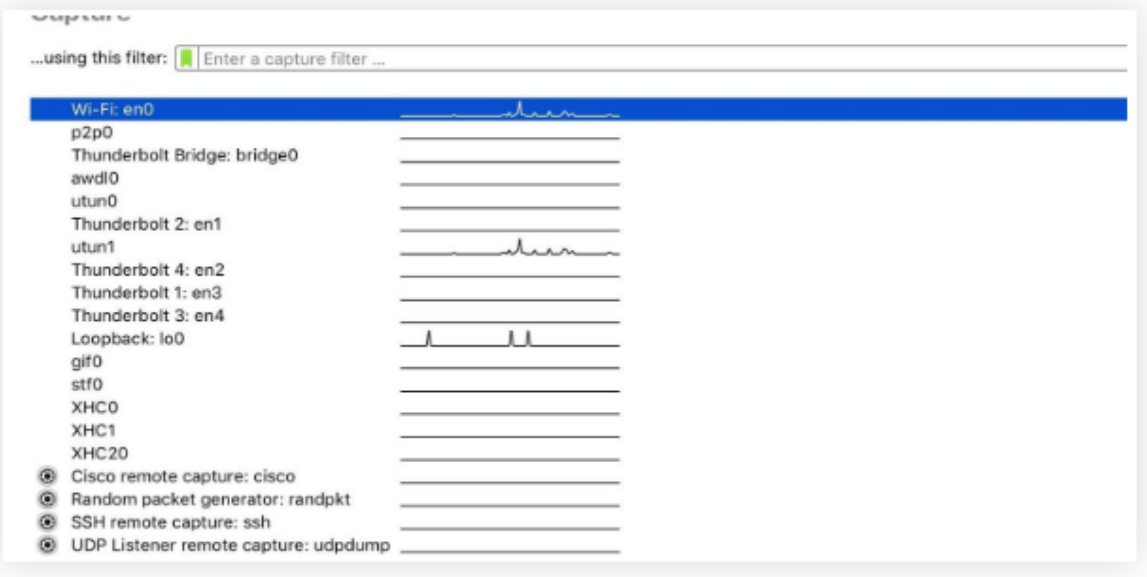
كيف يعمل ؟

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 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 HTTP التي 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.

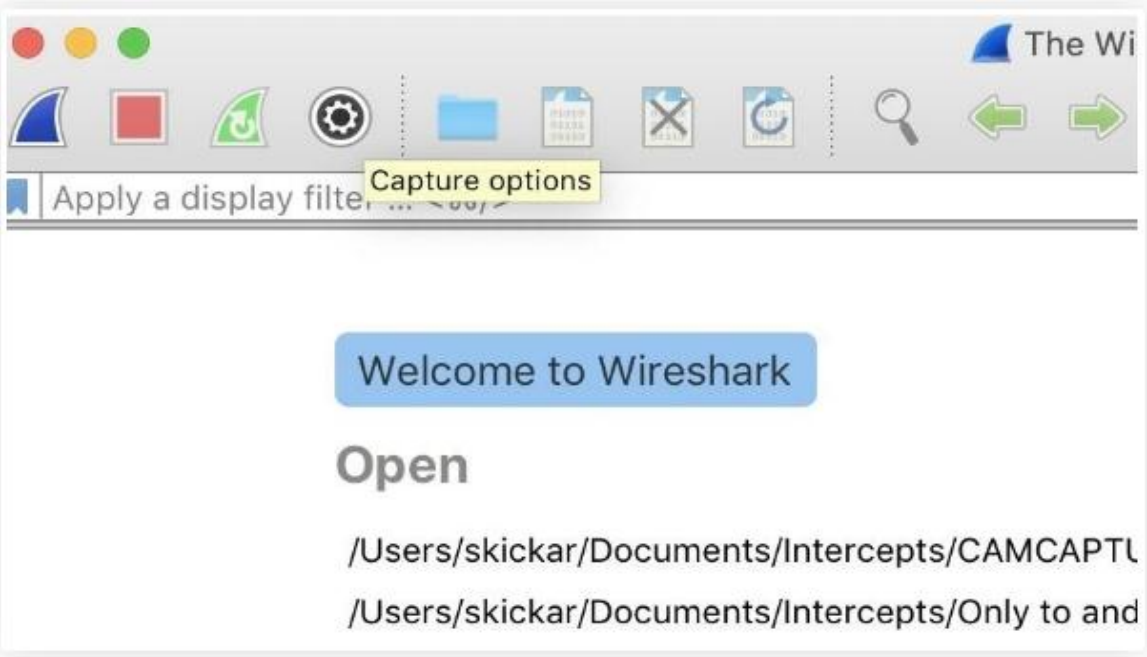
ماذا ستحتاج ؟

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 التشفير في بعض الأحيان. كما ستحتاج أيضًا إلى معرفة كلمة المرور واسم الشبكة لشبكة Wi-Fi التي ترغب في مراقبتها. حيث سيتيح لك ذلك حساب المفتاح المشترك مسبقًا ، وهذا سيسمح لنا بفك تشفير حركة المرور في الوقت الفعلي. ثم القيام بالخطوات التالية :

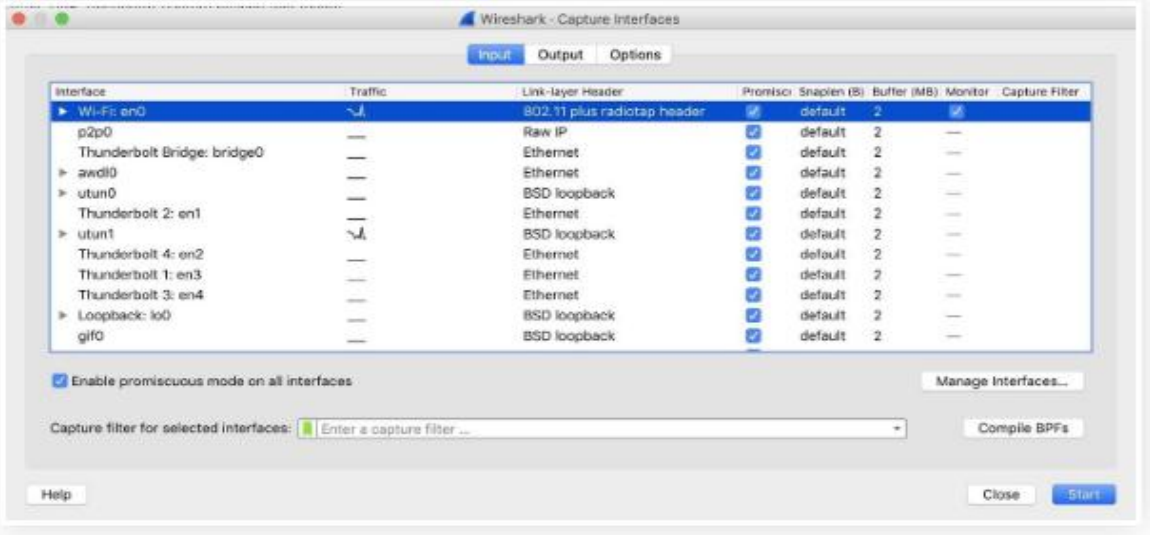
١. **قم بتنزيل Wireshark والاتصال بشبكة Wi-Fi :** قم بتنزيل Wireshark وتثبيته إذا لم يكن مثبتًا بالفعل ، ثم قم بالاتصال بشبكة Wi-Fi التي تستهدفها. إذا كنت تخطط لاستخدام PSK بدلاً من مفتاح الشبكة ، فيجب عليك حسابه باستخدام أداة Wireshark قبل القيام بذلك ، لأنه قد لا تتمكن من الوصول إلى الإنترنت أثناء 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 البطاقة في الوضع الصحيح. كما في الشكل التالي :



٢. **إعـداد Wireshark لالتقـاط** : ضـمن خيـار قائمـة Wireshark ، انقـر علـى قائمـة (Capture options) . كما في النافذة التالية :

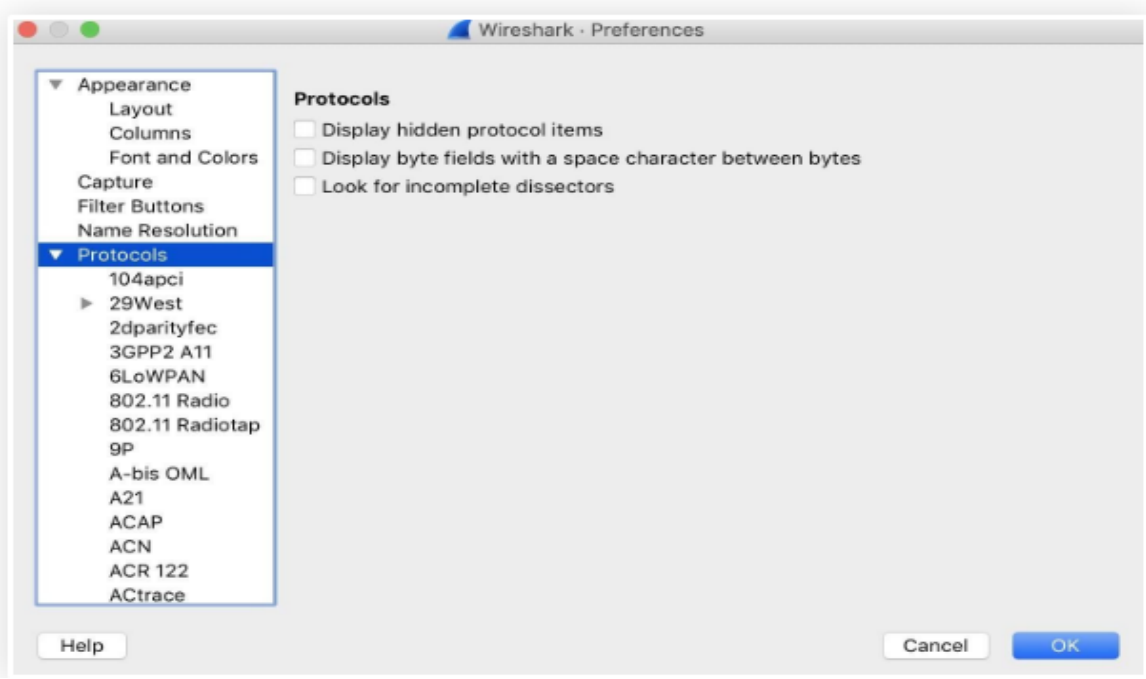


سيؤدي ذلك إلى فتح نافذة التقاط الواجهات ، كما هو موضح أدناه.

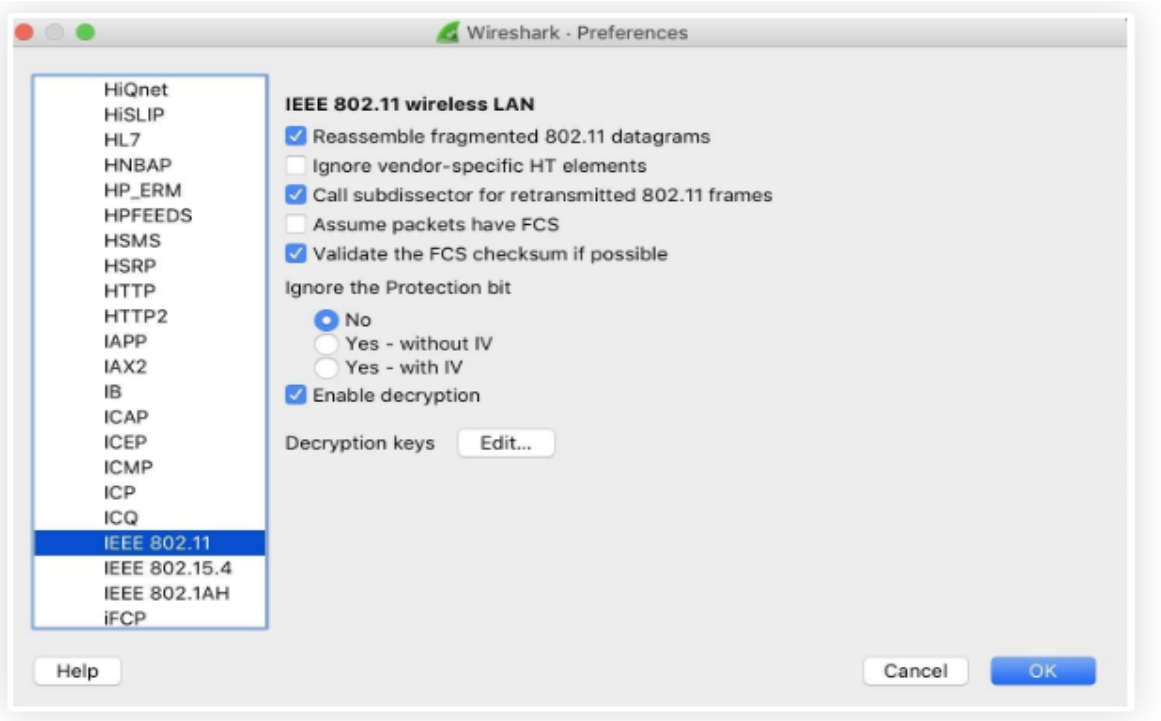


٣. **ابدأ التقاط الشبكة ومسح لحزم EAPOL** : إذا لم تكن متصلاً بالشبكة التي يعمل بها هدفك ، فلن تتمكن من رؤية أي حزم لأنك قد تكون في قناة عشوائية أخرى. حيث لا يمكن لـ Wireshark بالفعل من تغيير القناة التي يعمل عليها محول الشبكة اللاسلكية ، لذلك إذا لم تحصل على أي شيء ، فقد يكون ذلك هو السبب.

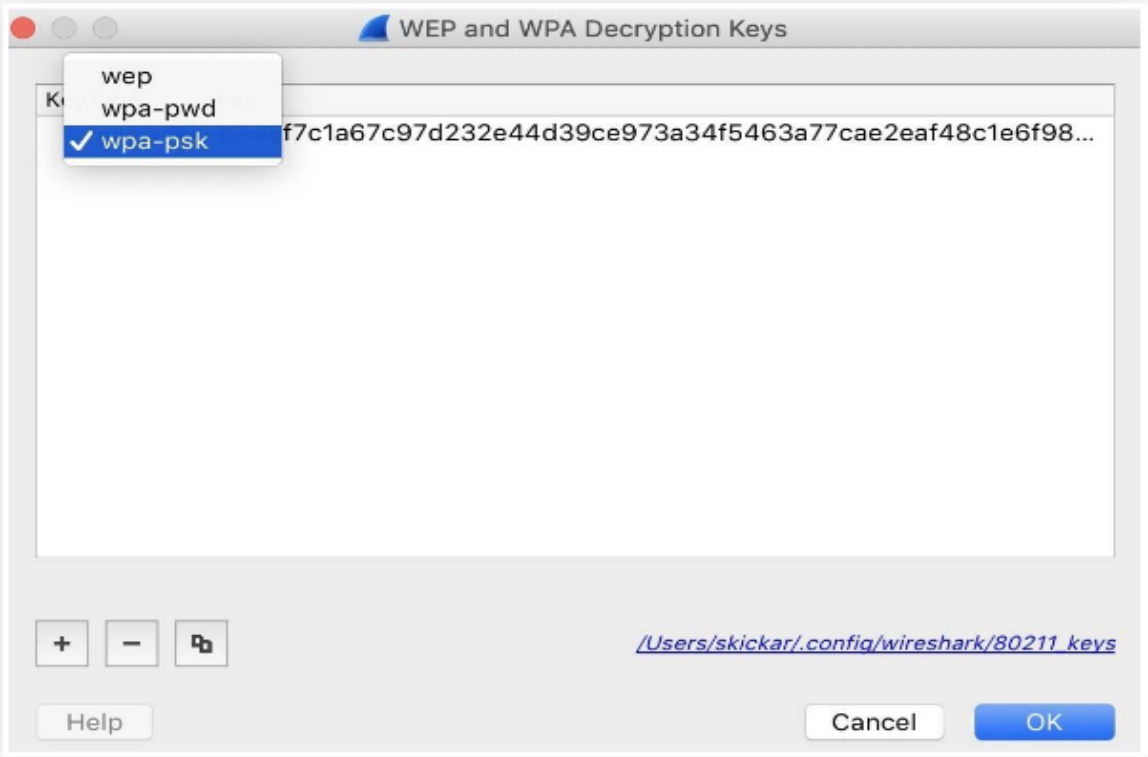
٤. **فك تشفير حركة مرور الشبكة باستخدام PSK** : الآن وقد أصبح لدينا مصافحات ، يمكننا فك تشفير المحادثة من هذه النقطة فصاعدًا. وللقيام بذلك ، سنحتاج إلى إضافة كلمة مرور الشبكة أو PSK. ما عليك سوى الانتقال إلى القائمة المنسدلة في Wireshark وحدد خيار(Preferences) وبمجرد تحديده ، انقر فوق (Protocols) كما في النافذة التالية :



ضمن البروتوكولات ، قم بتحديد (IEEE 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 :



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



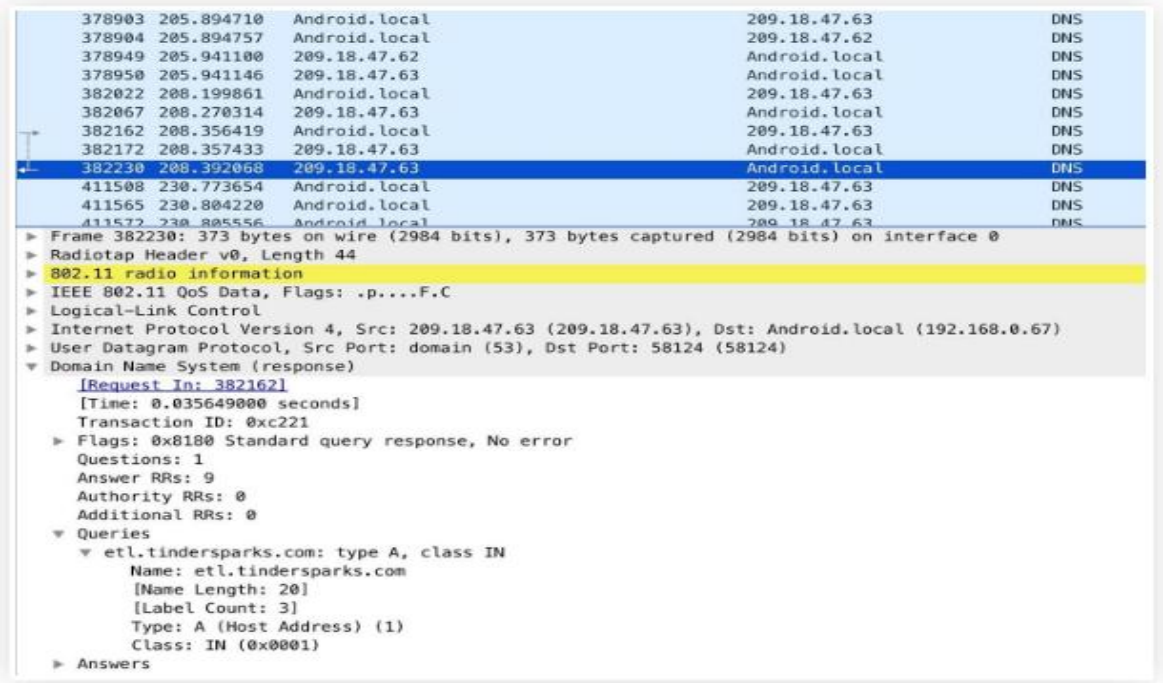
بمجرد اكتمال ذلك ، انقر فوق (OK)في قائمة التفضيلات ، هنا ينبغي على Wireshark إعادة فحص جميع الحزم التي تم التقاطها ومحاولة فك تشفيرها. هذا قد لا يعمل لمجموعة متنوعة من الأسباب. لكني تمكنت من جعله يعمل في معظم الوقت من خلال التأكد من حصولي على مصافحة جيدة (EAPOL) والتبديل بين استخدام كلمة مرور الشبكة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

٥. **البحث عن حزم DNS و HTTP** : الآن وبعد أن قمنا بتجريد الحماية المحيطة بحركة المرور ، يمكن لـ Wireshark فك تشفيرها وإخبارنا عن الأجهزة الموجودة على شبكة Wi-Fi التي لدينا مصافحة للقيام بها في الوقت الفعلي. وتنقسم الى قسمين :

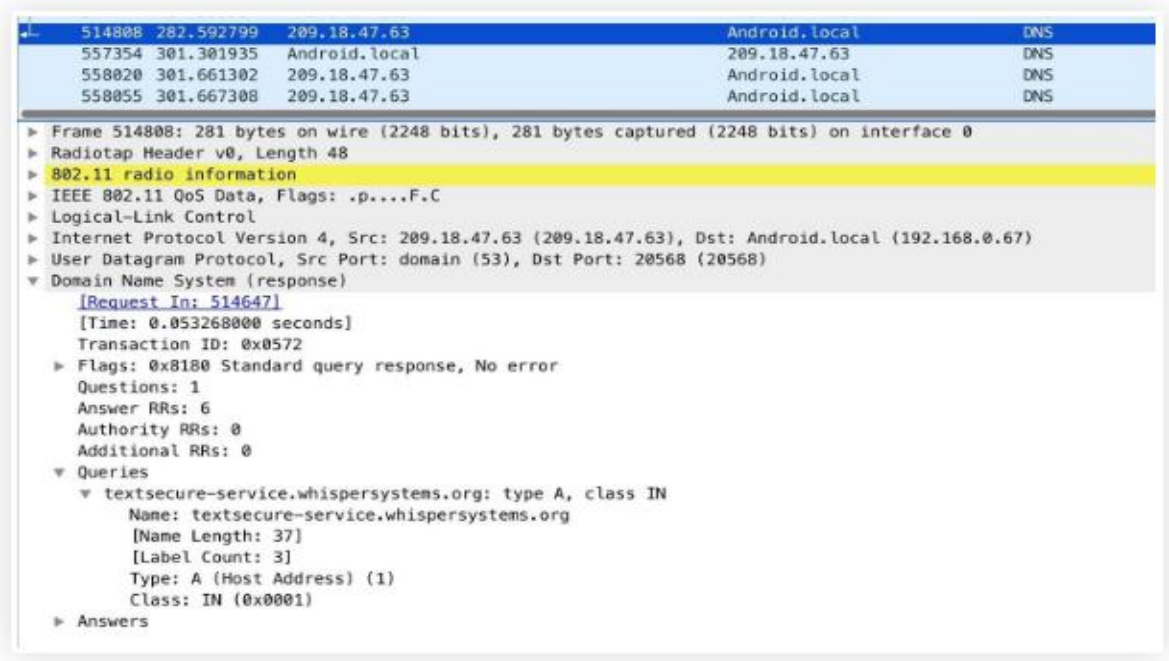
❖ **طلبات DNS** : لرؤية الحزم المهمة ، سنبدأ بطلبات DNS. التي تتأكد من التطبيقات وعناوين IP التي من المفترض أن تتصل بها لم تتغير. وهنا سيتم توجيههم إلى أسماء النطاقات التي تحتوي عادةً على اسم التطبيق ، مما يجعل من السهل مشاهدة التطبيق الذي يتم تشغيله على هاتف iPhone أو Android وتقديم الطلبات. وللاطلاع على هذه الطلبات ، سنستخدم مرشح الالتقاط ، DNS و http ، مما سيرينا المسارات الأكثر وضوحًا التي يقوم التطبيق بتركها عبر شبكة Wi-Fi. أولاً ، قم بكتابة dns في شريط فلترة الالتقاط واضغط على Enter. إذا لم ينجح ذلك ، فحاول التبديل بين PSK وكلمة المرور عدة مرات وسوف تبدأ العمل.

إذا كان هدفك وحيداً ، فقد ترى الرد :

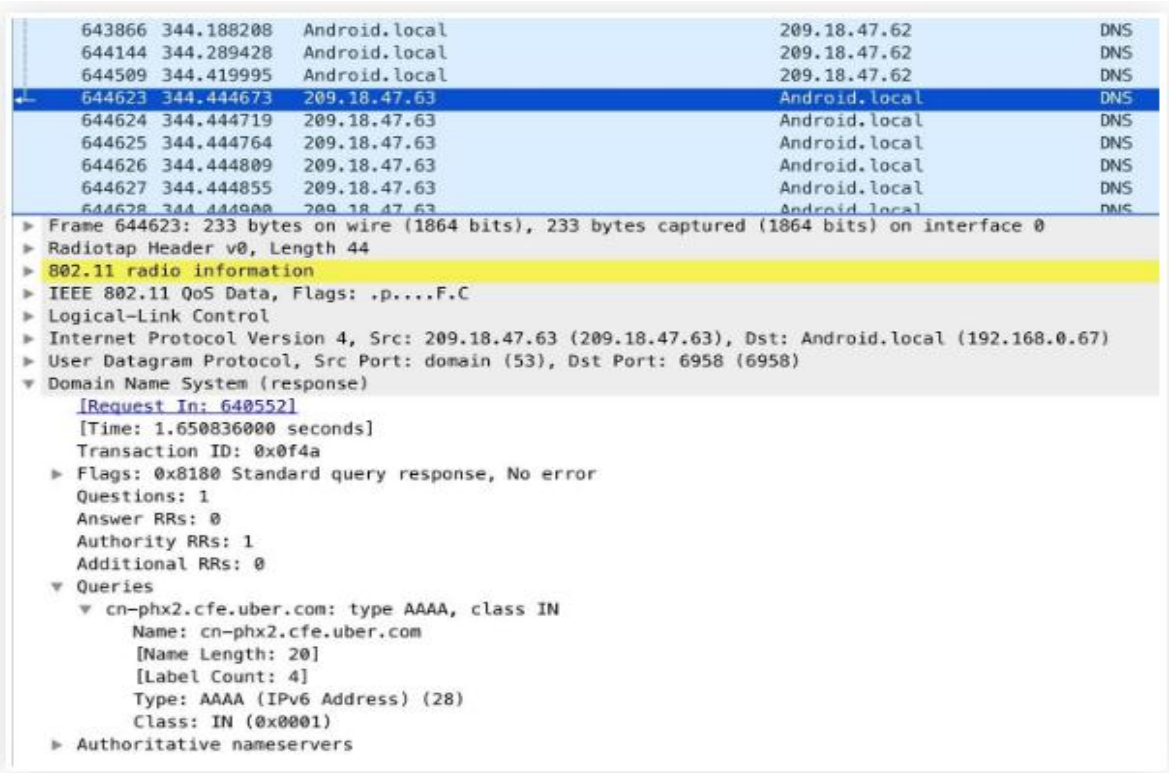
Tinder calls the Tindersparks.com domain بالإضافة إلى الكثير من الخدمات الأخرى. وهذا الطلب هو واحد من الأكثر وضوحا. كما في النافذة التالية :



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.



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



❖ **HTTP Packets** : بعد ذلك ، يمكننا أن نرى أن هناك العديد من طلبات الويب غير الآمنة باستخدام مرشح التقاط http. اذ 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 (Hypertext Transfer Protocol) .في المثال ادناه ، يمكننا رؤية طلبات HTTP غير الآمنة إلى خادم الدردشة. ما هو هذا ؟ انه مجرد فحص الحزمة وحل المجال سيعطينا الجواب على الفور. انها WeChat ! اذ قام هذا الهاتف بتثبيت WeChat ، علاوة على ذلك ، فإن الاتصالات الصادرة منه غير مشفرة بالكامل.

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 :

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.