CONCEPT

التحليل الجنائي للهواتف المحمولة: استخراج بيانات iOS وAndroidg وتحليل آثار التطبيقات والتقرير الجنائي

10 – 14 مايو 2027

دبي - فندق خمس نجوم في وسط الأعمال



التحليل الجنائي للهواتف المحمولة: استخراج بيانات iOS وAndroid وتحليل آثار التطبيقات والتقرير الجنائي

المرجع: 14414_471 **التاريخ:** 10 – 14 مايو 2027 **المكان:** دبي - فندق خمس نجوم في وسط الأعمال **الرسوم:** SAR 21450

مقدمة:

أصبح التحليل الجنائي للهواتف المحمولة مصدر الدليل الحاسم في قضايا الاحتيال والمضايقة وتسريب البيانات والحوادث الأمنية، ومع ذلك تضيع فحوص كثيرة لأن الجهاز بقي متصلا بالشبكة، أو لأن طريقة الاستخراج اختيرت دون مبرر مكتوب، أو لأن مخرجات الأداة نقلت إلى التقرير دون تحقق. تدرب هذه الدورة من كور كونسبت الفاحصين على حفظ أجهزة iOS وAndroid واستخراج بياناتها وتحليلها في قضايا نظامية مصرح بها، مع تعليل كل خطوة. ومن خلال العمل المخبري على صور اختبار، يعد المشاركون تقرير فحص الجهاز المحمول وسجل قرار الاستخراج جاهزين للتدقيق الإثباتي.

أهداف الدورة:

- عزل الهواتف وشرائح SIM وبطاقات الذاكرة المضبوطة وترقيمها وحفظها بحيث تبقى بياناتها دون تغيير من لحظة الضبط حتى الفحص
- شرح بنية التخزين والتشفير وعزل التطبيقات في نظامي iOS وAndroid وأثر كل منها على الأدلة القابلة للاسترجاع
- اختيار نوع الاستخراج المنطقي أو استخراج نظام الملفات أو نظام الملفات الكامل أو الاستخراج المادي وتبريره وفق حالة الجهاز وسؤال القضية
- تحليل آثار تطبيقات المراسلة والموقع والوسائط والمتصفح واسترجاع السجلات المحذوفة من قواعد بيانات SQLite على صور الاختبار
- التحقق من مخرجات أدوات التحليل الجنائي مقابل بيانات مرجعية معروفة ومطابقة النتائج بين أداتين مستقلتين
- كتابة تقرير فحص يبين المنهجية والنتائج والقيود ورأي الفاحص بمستوى يصلح للإثبات

الفئة المستهدفة:

- وظائف فحص الأدلة الرقمية التي تستخرج بيانات الهواتف والأجهزة اللوحية وتحللها في القضايا الجنائية والمدنية والداخلية
- وظائف التحقيق في الأجهزة الأمنية ومكافحة الاحتيال وأمن المؤسسات التي تحيل الهواتف للفحص وتبني على نتائجه
- وظائف الاستجابة للحوادث التي تحفظ أدلة الأجهزة المحمولة حين يكون جهاز أحد الموظفين طرفا في اختراق
- وظائف الجودة في المختبرات الجنائية المسؤولة عن التحقق من الأدوات وسجلات المنهجية ومراجعة الزملاء
- وحدات الجرائم الإلكترونية والأدلة الرقمية التي تعرض نتائج فحص الهواتف على جهات الادعاء واللجان والمحاكم

محاور الدورة:

اليوم 1: أسس أدلة الأجهزة المحمولة وضبط الهاتف

- نطاق التحليل الجنائي للأجهزة المحمولة: الهواتف والأجهزة اللوحية والأجهزة القابلة للارتداء وبطاقات الذاكرة
- مراجعة السند النظامي وطلب الفحص قبل التعامل مع الهاتف
- قرارات الضبط للأجهزة المشغلة والمطفأة والمقفلة الشاشة
- العزل اللاسلكي بحقائب فاراداي والحاويات المحجوبة مقارنة بوضع الطيران
- ترقيم الهاتف بوصفه حرزا وتصويره واستمرارية حيازة شرائح SIM وبطاقات الذاكرة

اليوم 2: الإرشادات الجنائية للأجهزة المحمولة وبنية نظامي Androidg iOS

- إرشادات NIST للتحليل الجنائي للأجهزة المحمولة: الحفظ والاستخراج والفحص وإعداد التقرير
- تطبيق ISO/IEC 27037، إرشادات تحديد الأدلة الرقمية وجمعها واستخراجها وحفظها، على الهواتف
- بنية نظام iOS: وحدات تخزين APFS وحاويات التطبيقات المعزولة وملفات الخصائص plist
- بنية نظام Android: الأقسام وأنظمة الملفات ext4 وF2FSg ومجلدات بيانات كل تطبيق
- التشفير أثناء التخزين وحالات القفل وأثرها على البيانات القابلة للاسترجاع

اليوم 3: أنواع الاستخراج وأدلة SIM والنسخ الاحتياطية والسحابة

- تسلسل أنواع الاستخراج: المنطقي ونظام الملفات ونظام الملفات الكامل والمادي على مستوى المفهوم
- مصفوفة قرار الاستخراج وفق حالة الجهاز والسند النظامي وسؤال القضية
- النسخ الاحتياطية المحلية للجهاز بوصفها دليلا: بنية النسخة والتعامل مع النسخ المشفرة
- أدلة شريحة SIM وUICCg: رقم ICCID ورقم IMSI وجهات الاتصال والرسائل النصية المخزنة
- بيانات الحساب السحابي والمحتوى المتزامن: الإجراء النظامي وحدود النطاق ومصدر البيانات

اليوم 4: آثار التطبيقات والبيانات المحذوفة والتحقق من الأدوات

- قواعد بيانات تطبيقات المراسلة: المحادثات والمرفقات وعضوية المجموعات وحالات القراءة
- آثار الموقع: الوسوم الجغرافية EXIF في الصور وسجل اتصالات Wi-Fi وسجلات الأبراج الخلوية
- سجل المتصفح وبيانات الوسائط الوصفية وذاكرة الصور المصغرة بوصفها آثارا داعمة
- استرجاع السجلات المحذوفة من SQLite: قوائم الصفحات الحرة وسجلات الكتابة المسبقة والصفحات غير المخصصة
- التحقق من أدوات التحليل الجنائي بصور اختبار مرجعية ومقارنة النتائج بين الأدوات

اليوم 5: حالات مخبرية لفحص الهواتف وإعداد التقرير الإثباتي

- حالة مخبرية: إعادة بناء المراسلات والمواقع من صورة اختبار لجهاز Android
- حالة مخبرية: استرجاع الوسائط وسجل المتصفح والرسائل المحذوفة من صورة اختبار لجهاز iOS
- بناء الخط الزمني لأحداث الهاتف مع توحيد المناطق الزمنية وفروق ساعة الجهاز
- صياغة تقرير فحص الجهاز المحمول وسجل قرار الاستخراج
- مراجعة الزملاء ومحاكاة استجواب الخبير حول نتائج فحص الهاتف

المهارات التي ستكتسبها:

- ضبط الهاتف وعزله
- بنية منصات الأجهزة المحمولة
- اختيار طريقة الاستخراج
- تحليل آثار التطبيقات
- استرجاع سجلات SQLite
- التحقق من الأدوات الجنائية
- إعادة بناء الخط الزمني للهاتف
- كتابة تقارير الخبرة

لماذا تحضر هذه الدورة:

- العودة بتقرير فحص الجهاز المحمول وسجل قرار الاستخراج المعدين من حالات مخبرية كاملة على صور اختبار لنظامي iOS Androidg
- الدفاع عن اختيار طريقة الاستخراج وعن كل قيد بعبارات واضحة أثناء المناقشة والاستجواب
- كشف ثغرات التحليل الآلي والآثار المنسوبة خطأ قبل وصولها إلى التقرير بمطابقة أداة بأخرى
- مقارنة ممارسات فحص الهواتف مع فاحصين ومحققين من الأجهزة الأمنية والمصارف والاتصالات وأمن المؤسسات

الخاتمة:

لا يكون لنتيجة فحص الهاتف وزن إلا حين يعزل الجهاز ويبرر نوع الاستخراج وتفحص مخرجات الأداة. تنتقل الدورة من الضبط والعزل اللاسلكي، إلى إرشادات NIST ومعيار ISO/IEC 27037 وبنية نظامي iOS وAndroidg، ثم إلى أنواع الاستخراج وأدلة SIM والنسخ الاحتياطية والسحابة، فآثار التطبيقات واسترجاع سجلات SQLite والتحقق من الأدوات. ويطبق اليوم الأخير المنهجية على حالات مخبرية تنتهي بتقرير فحص الجهاز المحمول وسجل قرار الاستخراج للاستخدام الإثباتي.