

# دورة الأدلة الجنائية الرقمية للأجهزة المحمولة



## دورة الأدلة الجنائية الرقمية للأجهزة المحمولة

المرجع: 157333\_753 التاريخ: 23 - 27 مايو 2027 المكان: نيروبي الرسوم: Euro 4500

### نظرة عامة

دورة الأدلة الجنائية الرقمية للأجهزة المحمولة دورة متوسطة لمدة 5 أيام لممارسي الأدلة الرقمية ووظائف الاستجابة للحوادث والتحقيق والتحليل الأمني وإدارة الأجهزة والدعم القانوني، ويعود المشاركون منها بملف فحص أدلة الأجهزة المحمولة. تربط الدورة الصلاحية النظامية وحفظ الدليل وخطة الاكتساب وآثار iOS و Android وأدلة التطبيقات والاتصالات وبناء الخط الزمني والتحقق وإعداد التقارير عبر قرارات قابلة للتتبع. تطور أجايل للتدريب ممارسة الأدلة الجنائية الرقمية للأجهزة المحمولة.

### الفئة المستهدفة

- وظائف الأدلة الرقمية المسؤولة عن اكتساب بيانات الأجهزة المحمولة وفحصها
- وظائف الاستجابة للحوادث المسؤولة عن حفظ الأجهزة ودعم التحقيقات
- وظائف التحقيق المسؤولة عن ربط آثار الجهاز بأسئلة القضية
- وظائف إدارة الأجهزة المحمولة المسؤولة عن حالة الجهاز والنسخ الاحتياطية والبيانات المتزامنة
- وظائف الدعم القانوني والتدقيق المسؤولة عن سجلات الأدلة والجاهزية للمراجعة

تفترض الدورة أن المشاركين يتعاملون في العمل مع الأدلة الأمنية أو سجلات الأجهزة أو إجراءات التحقيق، وتستبعد تطوير أساليب الاستغلال وتعليم تجاوز رموز الدخول والتحضير للشهادات والمشورة القانونية.

### الإدارات والقطاعات المستهدفة

تدعم الدورة الإدارات والقطاعات التي تفحص أدلة الأجهزة المحمولة ضمن التحقيقات المصرح بها والاستجابة للحوادث.

- الأدلة الجنائية الرقمية والاستجابة للحوادث
- العمليات السيبرانية والتحقيقات الداخلية
- الدعم القانوني والتدقيق والامتثال
- الخدمات المالية والاتصالات
- الرعاية الصحية والعمليات الصناعية والخدمات الرقمية



## أهداف التعلم

بنهاية هذه الدورة، سيتمكن المشاركون من:

- تطبيق ضوابط الصلاحية والحفظ وسلسلة الحيازة على أدلة الأجهزة المحمولة
- مقارنة خيارات الاكتساب المنطقي ونظام الملفات والنسخ الاحتياطية والوسائط الخارجية والسحابة
- تحليل آثار Android و iOS وفق أسئلة القضية المحددة
- بناء خطوط زمنية للاتصالات والتطبيقات والمواقع والنشاط
- تقييم مخرجات أدوات الفحص عبر التحقق ومراجعة النظراء
- بناء ملف فحص أدلة الأجهزة المحمولة بنتائج قابلة للدفاع

## جدول الدورة

### اليوم 1: التصريح بفحص أدلة الأجهزة المحمولة وحفظها

- سجل صلاحية الفحص ونطاقه
- ورقة توثيق حالة الجهاز والموقع
- سجل معرف الدليل وسلسلة الحيازة
- شجرة قرار حفظ الجهاز المشغل والمتوقف
- قائمة عزل الشبكة وسلامة الدليل

### اليوم 2: تخطيط اكتساب الدليل والتحقق منه

- مصفوفة الاكتساب المنطقي والنسخ الاحتياطي ونظام الملفات
- خريطة الوسائط الخارجية والمصادر المتزامنة
- ملف طراز الجهاز ونظام التشغيل وحالة الوصول
- سجل اختبار أداة الاكتساب والتحقق منها
- سجل مبررات أسلوب الاستخراج والاستثناءات



### اليوم 3: فحص أدلة Android

- خريطة آثار التخزين والتطبيقات في Android
- ورقة ربط المكالمات والرسائل وجهات الاتصال والحسابات
- مراجعة المتصفح والموقع والبيانات الوصفية للوسائط
- منهج تفسير قواعد بيانات التطبيقات والطوابع الزمنية
- ورقة التحقق من نتائج Android

### اليوم 4: فحص أدلة iOS والمصادر المتصلة

- خريطة آثار النسخ الاحتياطية ونظام الملفات في iOS
- مراجعة أدلة التطبيقات والاتصالات والإشعارات
- سجل مصادر السحابة والحاسوب والأجهزة القابلة للارتداء والمزامنة
- مصفوفة الخط الزمني والإسناد عبر المصادر
- اختبار قيود النتيجة والتفسير البديل

### اليوم 5: ممارسة إعداد تقارير أدلة الأجهزة المحمولة

- تمرين: حفظ سيناريو جهاز محمول وتوثيقه
- تمرين: اختيار استراتيجية اكتساب الدليل وتبريرها
- تمرين: ربط الخطوط الزمنية لآثار Android و iOS
- تمرين: التحقق من النتائج وتسجيل القيود
- المشروع الختامي: ملف فحص أدلة الأجهزة المحمولة

### التمارين التطبيقية

تستخدم الدورة أنشطة مقترحة من الخدمات المالية والاتصالات والرعاية الصحية والعمليات الصناعية والخدمات الرقمية.

- نشاط مقترح: تسجيل صلاحية الفحص وحالة الجهاز وخيارات العزل وسلسلة الحياة لهاتف مضبوط.
- نشاط مقترح: مقارنة خيارات الاكتساب وتوثيق الأسلوب المختار وفحوص التحقق والاستثناءات.
- نشاط مقترح: ربط آثار التطبيقات والاتصالات والوسائط ضمن خط زمني للقضية.
- نشاط مقترح: إعداد النتائج والقيود وملاحظات مراجعة النظراء وتقرير فحص قابل للتتبع.



## الأسئلة الشائعة

### لمن تناسب دورة الأدلة الجنائية الرقمية للأجهزة المحمولة، وماذا تفترض؟

تناسب وظائف الأدلة الرقمية والاستجابة للحوادث والتحقيق والتحليل الأمني وإدارة الأجهزة والدعم القانوني والتدقيق، وتفترض خبرة في الأدلة الأمنية أو سجلات الأجهزة أو إجراءات التحقيق.

### كيف تختلف دورة الأدلة الجنائية للأجهزة المحمولة عن تدريب الأدلة الجنائية الرقمية العام؟

تركز أدلة الأجهزة المحمولة على حالة الهاتف وأنظمة التشغيل وآثار التطبيقات والمصادر المتزامنة وخيارات الاكتساب والتحقق الخاص بالجهاز، بينما يمتد التدريب العام إلى الحواسيب ووسائل التخزين والشبكات والأنظمة السحابية.

### كيف يختار الفاحص أسلوب اكتساب أدلة الأجهزة المحمولة؟

يختار الفاحص أسلوب الاكتساب بمقارنة الصلاحية وحالة الجهاز ونظام التشغيل وظروف الوصول والأدوات المتاحة والآثار المطلوبة ومخاطر تغيير البيانات وخيارات التحقق واحتياجات القضية الموثقة.

### لماذا يجب التحقق من مخرجات أدوات فحص الأجهزة المحمولة؟

يجب التحقق لأن محلات الأدوات قد تغفل الآثار أو تصنفها أو تفسرها على نحو غير دقيق؛ لذلك يقارن الفاحصون البيانات المصدرة والطوابع الزمنية والأدوات أو الأساليب البديلة ومراجعة النظراء عند الحاجة.

### ماذا يتضمن ملف فحص أدلة الأجهزة المحمولة؟

يتضمن الملف الصلاحية والنطاق وحالة الجهاز وسجلات الحياة ومبررات الاكتساب ونتائج التحقق وملاحظات الآثار والخطوط الزمنية والنتائج والقيود وسجلات المراجعة وتقريراً يربط الاستنتاجات بالأدلة.

## الخاتمة

يعود المشاركون بملف فحص أدلة الأجهزة المحمولة الذي يربط الصلاحية والحفظ والاكتساب والتحليل والتحقق والتقرير. يحول الملف مخرجات الأدوات المتفرقة إلى سجل فحص قابل للتتبع. ويدعم نتائج قابلة للمراجعة وقيوداً واضحة وتسليمات منضبطة واتصالاً ثابتاً بشأن القضية.