

التحليل الجنائي لأنظمة Windows والتحقيق المتقدم في NTFS

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

التحليل الجنائي لأنظمة Windows والتحقيق المتقدم في NTFS

نظرة عامة على الدورة

تطور دورة التحليل الجنائي لأنظمة Windows والتحقيق المتقدم في NTFS المهارات العملية اللازمة للتحقيق في أنظمة التشغيل، وإعادة بناء أنشطة المستخدمين، ودعم الاستجابة للحوادث السيبرانية. يدرس المشاركون الأدلة الجنائية المستمدة من سجل النظام، وسجلات الأحداث، والملفات التمهيدية، وذاكرة التخزين المؤقت، وآثار التصفح، والملفات المرتبطة بالمستخدمين، وأجهزة USB، والتطبيقات السحابية. تعزز الدورة التدريبية المعايير التقليدية للتحقيق الرقمي من خلال التركيز على نظام ملفات NTFS، بما في ذلك تحليل جدول الملفات الرئيسي، وسجلات التغيير، والملفات المحذوفة، والطوابع الزمنية، والخط الزمني لأنظمة Windows. يتعلم المشاركون كيفية ربط الأدلة المتعددة بدلاً من الاعتماد على مصدر واحد لضمان دقة النتائج. تغطي سيناريوهات التحقيق الواقعية التهديدات الداخلية، وتسريب البيانات، وأنشطة البرمجيات الخبيثة، والوصول غير المصرح به، والملفات المُعاد تسميتها، والأدلة المحذوفة، والوسائط القابلة للإزالة، وسلوكيات مكافحة الأدلة الجنائية. توضح دراسة حالة تسريب البيانات من المعهد الوطني للمعايير والتقنية كيفية دمج أدلة البريد الإلكتروني، والمتصفحات، والبحث، والتخزين السحابي، ونظام الملفات في خط زمني تحقيقي واحد متكامل.

الفئة المستهدفة

- محللو الأدلة الرقمية
- أخصائيو الاستجابة للحوادث والاستجابة السيبرانية
- محللو مراقبة العمليات الأمنية والأمن السيبراني
- فاحصو الأدلة الجنائية للكمبيوتر
- محققو جرائم الكمبيوتر
- صائدو التهديدات
- محترفو أمن نقاط النهاية
- فرق التدقيق الداخلي والتحقيقات المؤسسية
- محترفو أمن تكنولوجيا المعلومات

AGILE LEADERS
Training Center

الإدارات المستهدفة

- التحقيقات الرقمية والاستجابة للحوادث
- الأمن السيبراني وعمليات مراقبة أمن المعلومات
- الأمن المؤسسي والتحقيقات
- التدقيق الداخلي والامتثال
- الشؤون القانونية والاكتشاف الإلكتروني
- إدارة الاحتيال والمخاطر الداخلية
- البنية التحتية لتكنولوجيا المعلومات وأمن نقاط النهاية

القطاعات المستهدفة

- الخدمات المصرفية والمالية
- القطاع الحكومي والدفاع
- النفط والغاز والطاقة
- الاتصالات
- الرعاية الصحية
- البنية التحتية الحرجة
- تكنولوجيا المعلومات والخدمات السحابية
- التصنيع

أهداف الدورة

بنهاية هذه الدورة، سيكون المشاركون قادرين على:

- شرح عملية التحقيق الجنائي لأنظمة التشغيل
- تحديد مواقع الأدلة الرئيسية وملفات النظام المختلفة
- وصف آليات الفرز السريع لأدلة نقاط النهاية
- مناقشة هندسة نظام الملفات وبياناته الوصفية
- تمييز دور جداول الملفات الرئيسية وسجلات التغيير
- تصنيف الملفات المحذوفة والمنقولة والمعاد تسميتها
- مقارنة أدلة سجل نظام التشغيل وملفات التنفيذ
- توضيح آلية فحص الوسائط القابلة للإزالة وأجهزة التخزين
- تلخيص طرق تحليل سجلات الأحداث والخطوط الزمنية

AGILE LEADERS
Training Center

محاور الدورة

اليوم الأول: التحقيق الجنائي لأنظمة التشغيل وفرز الأدلة

- فهم عملية التحقيق الجنائي لأنظمة التشغيل
- تحديد الأدلة الرئيسية ومواقع الملفات المرتبطة بها
- جمع وترتيب أولويات الأدلة أثناء الفرز الجنائي
- تثبيت وفحص صور الأدلة الجنائية لأنظمة التشغيل
- تحليل البيانات الوصفية للملفات

اليوم الثاني: التحقيق المتقدم في نظام الملفات والبيانات الوصفية

- دراسة هندسة نظام الملفات NTFS بعمق
- تحليل جدول الملفات الرئيسي وسجلات التغيير
- فحص الملفات المحذوفة واستعادة الآثار الرقمية
- فهم وتفسير الطوابع الزمنية بدقة
- إنشاء وتحليل الخطوط الزمنية لأنظمة التشغيل

اليوم الثالث: تحليل سجل النظام وأدلة تنفيذ البرامج

- فحص الهيكل الداخلي لسجل النظام
- تحديد آثار تنفيذ البرامج والتطبيقات
- دراسة الملفات المرتبطة بالارتباطات والقوائم المختصرة
- تتبع نشاط المستخدمين عبر مسارات التصفح والمجلدات
- تحليل سجلات الأجهزة الموصلة والوسائط القابلة للإزالة

اليوم الرابع: تحليل سجلات الأحداث والأنشطة الشبكية والسحابية

- استعراض وتحليل سجلات الأحداث لنظام التشغيل
- تتبع أنشطة المتصفحات واستخراج الأدلة الرقمية
- فحص أدلة البريد الإلكتروني والتطبيقات السحابية
- ربط أدلة الأجهزة الطرفية بالأنشطة المشبوهة
- دراسة سلوكيات مكافحة الأدلة الجنائية وكشفها

اليوم الخامس: التطبيقات العملية ودراسات الحالة المتقدمة

- تطبيق سيناريو تسريب البيانات العملي للمعهد الوطني للمعايير والتقنية
- ربط أدلة البريد الإلكتروني والبحث والتخزين السحابي
- اختبار الفرضيات التحقيقاتية وإعادة بناء الحوادث
- تقييم أدلة التهديدات الداخلية والملفات المُعاد تسميتها
- صياغة وتقديم النتائج التحقيقية بشكل احترافي

الأسئلة الشائعة

- **هل تتطلب الدورة خبرة مسبقة في الأمن السيبراني؟**

تفضل وجود خلفية أساسية في مفاهيم الشبكات وأنظمة التشغيل لضمان الاستفادة القصوى من المحتوى المتقدم.

- **هل يتم توفير تراخيص برامج تحليل جنائي خلال التدريب؟**

لا يتم توفير برامج أو تراخيص تجارية، ولكن تركز الدورة على المنهجيات التحقيقية مع استعراض أمثلة توضيحية للأدوات ذات الصلة.

- **كيف تساعد الدورة في سيناريوهات العمل اليومية؟**

تزود المشاركين بالقدرة على ربط الأدلة المتعددة واستخدام التحقيق المتقدم في نظام NTFS لمواجهة الحوادث المعقدة بكفاءة.

AGILE LEADERS
Training Center

فئات الدورات التدريبية

الأعمال الزراعية والأمن الغذائي	الدورات التدريبية في مجال البيئة والاستدامة
دورات إدارة الأزمات واستمرارية الأعمال	دورات إدارة الجودة وتطوير العمليات
دورات إدارة الرعاية الصحية	دورات إدارة المرافق والعقارات
دورات إدارة المنظمات غير الحكومية والعمل الإنساني والتنمية	دورات إدارة و تحليل البيانات ودورات علم البيانات
دورات إدارة و تطوير الموارد البشرية	دورات إدارة وعمليات الطيران
دورات الأمن السيبراني ودورات تقنية المعلومات	دورات الاتصال الجماهيري و السياسات والعلاقات العامة
دورات التدريب القانوني والمشتريات والتعاقدات	دورات التسويق وإدارة علاقات العملاء وإدارة المبيعات
دورات التعليم وتطوير التعلم	دورات الحكومة الرقمية والخدمات العامة
دورات الحوكمة وإدارة المخاطر والامتثال	دورات السكرتارية و إدارة المكاتب
دورات الشحن والملاحة البحرية والموانئ	دورات الصحة والسلامة والأمن المهني
دورات الصيانة ودورات المجالات الهندسية المتنوعة	دورات الضيافة والسياحة
دورات المحاسبة و التمويل و دورات الإدارة المالية	دورات المهارات الشخصية وتطوير الذات
دورات حفظ التراث وإدارة المتاحف	دورات في مجالات القيادة والإدارة

AGILE LEADERS
Training Center

فئات الدورات التدريبية

- دورات قطاع النفط والغاز ودورات تقنية متنوعة
- دورات معتمدة من قبل هيئات دولية
- دورات مكتب إدارة المشاريع وإدارة المشاريع الرشيقة

AGILE LEADERS
Training Center

مدن التدريب

أبوظبي الإمارات العربية المتحدة	**أثينا** اليونان	**أديس أبابا** إثيوبيا
أكرا غانا	**أمستردام** هولندا	**اسطنبول** تركيا
الدار البيضاء المغرب	**الدوحة** قطر	**القاهرة** مصر
الكويت الكويت	**المنامة** مملكة البحرين	**باريس** فرنسا
باكو أذربيجان	**بالي** جمهورية إندونيسيا	**بانكوك** تايلند
براغ جمهورية التشيك	**برشلونة** إسبانيا	**برلين** ألمانيا
بورت لويس موريشيوس	**بورتو** البرتغال	**بوكيت** تايلاند
تبليسي جورجيا	**تورنتو** كندا	**جاكرتا** جمهورية إندونيسيا
جنيف سويسرا	**جوهانسبرغ** جنوب إفريقيا	**دبي** الإمارات العربية المتحدة
روما إيطاليا	**زنجبار** تنزانيا	**زيورخ** سويسرا
سان دييغو الولايات المتحدة الأمريكية	**سنغافورة** سنغافورة	**سيول** كوريا الجنوبية
شرم الشيخ مصر	**شيكاغو** الولايات المتحدة الأمريكية	**طرابزون** تركيا

AGILE LEADERS
Training Center

مدن التدريب

طشقند أوزبكستان	**طوكيو** اليابان	**عمان** المملكة الأردنية الهاشمية
عن بعد منصة زووم	**فرانكفورت** ألمانيا	**فيينا** النمسا
كوالالمبور ماليزيا	**كيب تاون** جنوب إفريقيا	**لاغوس** نيجيريا
لانكاوي ماليزيا	**لشبونة** البرتغال	**لندن** المملكة المتحدة
ماربيا اسبانيا	**مدريد** إسبانيا	**مسقط** سلطنة عمان
مونترو سويسرا	**ميلان** إيطاليا	**ميونخ** ألمانيا
نيروبي كينيا	**نيس** فرنسا	**نيويورك** الولايات المتحدة الأمريكية