



**التدريبية: تحليل الطب الشرعي الرقمي -
التحقيق في الجرائم السيبرانية الدورة
الأدوات وتقنيات:**

Ref: #CYB4827





مقدمة الدورة التدريبية / لمحة عامة:

أداة لا غنى عنها للتحقيق في السببية أكثر تعقيداً وتواتراً، مما يجعل تحليل في عالمنا الرقمي المتسارع، أصبحت الجرائم جنائية تقدم هذه الدورة التدريبية المتخصصة للمحترفين الحوادث الأمنية وجمع الأدلة الجنائية الرقمية. الطب الشرعي الرقمي البيانات المعقدة وتقديم التقارير رقمية شاملة، بدءاً من الحفاظ على الأدلة وحتى المعرفة والمهارات اللازمة لإجراء تحقيقات الأجهزة. سيكتسب الشرعي الرقمي، أدوات التحليل المتقدمة، وتقنيات القانونية. سنتناول في هذه الدورة مبادئ الطب التحليل وكشف البرمجيات الخبيثة، والتعامل مع المشاركون القدرة على تتبع المسارات الرقمية استعادة البيانات من مختلفاً تهدف الدورة إلى إعداد المتخصصين لمواجهة التحديات الأدلة الرقمية بطريقة تضمن صلاحيتها في المحاكم. للمهاجمين، الرقمي، مع رقمي قوية. يستند المحتوى إلى أحدث المعايير وأفضل في التحقيق بالجرائم السيبرانية وبناء قدرات تحقيق كيسي (Eoghan Casey)، مؤلف الاستفادة من إسهامات خبراء أكاديميين بارزين مثل الممارسات في مجال الطب الشرعي الرقمي. يقدم Big Ben Training Center هذه الدورة العديد من الأعمال المرجعية في التحقيق الجنائي البروفيسور إيفان السيبرانية لتعزيز قدرات المحترفين في مكافحة الجريمة



لأ الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- محققو الطب الشرعي الرقمي.
- متخصصو الأمن السيبراني.
- أفراد فرق الاستجابة للحوادث الأمنية.
- المحققون الجنائيون وضباط إنفاذ القانون.
- مدققو أمن المعلومات.
- الحوادث الأمنية. أي مهني مسؤول عن جمع الأدلة الرقمية وتحليل

القطاعات والصناعات المستهدفة:

- القطاع الحكومي والهيئات القضائية وما في حكمها.
- وكالات إنفاذ القانون والأمن الوطني.
- شركات الأمن السيبراني وخدمات الاستشارات الأمنية.
- السيبراني. القطاع المالي والمصرفي للتحقيق في الاحتيال
- شركات المحاماة المتخصصة في الجرائم التقنية.
- البيانات. المؤسسات الكبرى التي تتعامل مع حوادث اختراق

الأقسام المؤسسية المستهدفة:

- إدارة الأمن السيبراني.
- إدارة المخاطر والامتثال.
- القسم القانوني.
- التحقيقات الداخلية.
- فرق الاستجابة للحوادث.



أهداف الدورة التدريبية:

أتقن المهارات التالية: بنهاية هذه الدورة التدريبية، سيكون المتدرب قد

- للأدلة، فهم مبادئ الطب الشرعي الرقمي وسلسلة الحضانة
- (أجهزة الكمبيوتر، الأجهزة المحمولة، الشبكات)، القدرة على جمع الأدلة الرقمية من مختلف المصادر
- التحقيقات، استخدام أدوات وتقنيات الطب الشرعي الرقمي لإجراء
- الأنشطة المشبوهة، تحليل سجلات الأنظمة وحركة مرور الشبكة لاكتشاف
- الصلابة، استعادة البيانات المحذوفة والمخفية من الأقراص
- فحص البرمجيات الخبيثة وتحليل السلوكيات الضارة
- في المحاكم، إعداد تقارير الطب الشرعي الرقمي القابلة للاستخدام

منهجية الدورة التدريبية:



سيتمكن المتدربون من تركيز على تزويد المشاركين بالخبرة المباشرة في تعتمد هذه الدورة التدريبية منهجية عملية ومكثفة، وورش العمل التطبيقية من استخدام أدوات خلال المحاكاة العملية لسيناريوهات الجرائم تحليل الطب الشرعي الرقمي. تحليل مفصل تتضمن المنهجية دراسات حالة، Volatility وFTK Imager وAutopsy الطب الشرعي الرقمي الرائدة مثل السيرانية مع الأدلة الرقمية بطريقة تضمن لعمليات جمع الأدلة وتقنيات التحليل. سيتم التركيز حقيقية لتحقيقات جنائية رقمية، مع بالجرائم هذه الدورة لتمكين BIG BEN Training Center سلامتها وقبولها في الإجراءات القانونية. يقدم على التعامل السيرانية ودعم العدالة الرقمية المتخصصين من أن يصبحوا خبراء في التحقيق

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

والمبادئ القانونية الوحدة الأولى: أساسيات الطب الشرعي الرقمي

- مقدمة إلى الطب الشرعي الرقمي ودورها
- مراحل التحقيق الجنائي الرقمي
- الرقمية، سلسلة الحضانة (Chain of Custody) للأدلة
- الرقمي، المبادئ القانونية والأخلاقية في الطب الشرعي
- أنواع الجرائم السيرانية وكيفية التحقيق فيها
- الاستعداد للتحقيق في الحوادث
- تخطيط الاستجابة لحوادث الأمن السيراني

الوحدة الثانية: جمع الأدلة الرقمية والحفاظ عليها



- تقنيات جمع الأدلة من أجهزة الكمبيوتر.
- الحصول على صور الأقراص الصلبة ((Disk Imaging)).
- ((Forensics)) جمع الأدلة من الذاكرة العشوائية (RAM).
- جمع الأدلة من الأجهزة المحمولة.
- جمع الأدلة من الشبكات.
- أدوات جمع الأدلة الرقمية.
- توثيق عملية جمع الأدلة.

الأدلة الوحدة الثالثة: تحليل البيانات الرقمية واستعادة

- تحليل أنظمة الملفات ((File System Analysis)).
- استعادة البيانات المحذوفة والبيانات المخفية.
- تحليل سجلات الأحداث ((Log Analysis)).
- تحليل سجلات المتصفح والبريد الإلكتروني.
- التعامل مع البيانات المشفرة والمضغوطة.
- أدوات تحليل البيانات الرقمية.
- بناء مخطط زمني للحوادث.

الخبیثة الوحدة الرابعة: الطب الشرعي للشبكات والبرمجيات



- (Forensics) مقدمة إلى الطب الشرعي للشبكات (Network)
- تحليل حزم البيانات (Packet Analysis)
- كشف الاختراقات عبر تحليل الشبكة
- (Malware) مقدمة إلى تحليل البرمجيات الخبيثة
- أنواع البرمجيات الخبيثة وسلوكياتها
- أدوات تحليل البرمجيات الخبيثة
- تتبع مصادر الهجمات السيبرانية

الخبراء الوحدة الخامسة: إعداد التقارير القانونية وشهادة

- كتابة تقارير الطب الشرعي الرقمي الاحترافية
- هيكلية التقرير والمحتوى المطلوب
- تقديم الأدلة في المحاكم
- الشهادة كخبير في الطب الشرعي الرقمي
- التحديات القانونية في قضايا الجرائم السيبرانية
- التحسين المستمر لمهارات التحقيق
- مستقبل الطب الشرعي الرقمي

الأسئلة المتكررة:

التسجيل في الدورة؟ ما هي المؤهلات أو المتطلبات اللازمة للمشاركين قبل

لا توجد شروط مسبقة

الإجمالي لساعات الدورة التدريبية؟ كم تستغرق مدة الجلسة اليومية، وما هو العدد

المدة إلى ٢٥٢٠- بمعدل يومي يتراوح بين ٤ إلى ٥ ساعات، تشمل فترات تمتد هذه الدورة التدريبية على مدار خمسة أيام،

ساعة تدريبية راحة وأنشطة تفاعلية ليصل إجمالي



سؤال للتأمل:

السيبرانية، ليس المهاجمين، كيف يمكن لمحقق الطب الشرعي الرقمي أن يظل التطور السريع للتقنيات الرقمية وأساليب للأنظمة المستقبلية وتأثيرها على فقط من خلال الأدوات والتقنيات الحالية، بل من خلال يظل متقدماً بخطوة على الجرائم جمع وتحليل الأدلة؟ تطوير فهم عميق

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

في الجرائم السيبرانية. تحليل الطب الشرعي الرقمي، مما يوفر للمشاركين تتميز هذه الدورة بتركيزها العملي والمعمق على لأدوات وتقنيات الطب الشرعي الرقمي، مما بدلاً من مجرد سرد المفاهيم، نغوص في التطبيق مهارات حقيقية للتحقيق لا تقدر بثمن في سيناريوهات تحقيق واقعية ودراسات حالة مفصلة، مما يميزها عن الدورات النظرية. تقدم الدورة العملي على كيفية إعداد تقارير الطب الشرعي القابلة التعامل مع الأدلة الرقمية واستعادة البيانات. نركز يمنح المشاركين خبرة عملية خبراء تحقيق هذا المجال. إنها ليست مجرد دورة لتعلم الأدوات، بل للاستخدام القانوني، وهي مهارة حاسمة للمحترفين في العالم الرقمي. رقمي قادرين على كشف الحقيقة ودعم العدالة في هي برنامج تدريبي شامل يهدف إلى بناء