الدورة التدريبية: التحقيق الجنائي الرقمي والأدلة الإلكترونية المتقدمة



16 - 20 نوفمبر 2026
كوالالمبور
5200 € (للشخص الواحد)
Ref: #SM3606_340754

مقدمة الدورة التدريبية / لمحة عامة:

في ظل التزايد المستمر للجرائم السيبرانية والحاجة الملحة لإثبات الحقائق في المحاكم، أصبح التحقيق الجنائي الرقمي والأدلة الإلكترونية المتقدمة مجالاً حيويًا يتطلب خبرة ومعرفة متعمقة. تتطلب عمليات جمع الأدلة الرقمية، تحليلها، وتقديمها في سياق قانوني فهمًا دقيقًا للمبادئ التقنية والقانونية على حد سواء. هذه الدورة التدريبية الشاملة مصممة لتزويد المتخصصين في الأمن السيبراني، إنفاذ القانون، القانون، ومدققي الطب الشرعي الرقمي بالمعرفة والمهارات المتقدمة اللازمة لإجراء تحقيقات جنائية رقمية فعالة. سنتعمق في تقنيات استعادة البيانات، تحليل البرمجيات الخبيثة، تأمين مسرح الجريمة الرقمي، وتقديم الأدلة في المحاكم. تستند الدورة إلى أعمال خبراء أكاديميين بارزين في مجال الطب الشرعي الرقمي، مثل البروفيسور Marcus Rogers Marcus Rogers، الذي يُعد مرجعًا في أبحاث الطب الشرعي الحاسوبي. يقدم BIG BEN Training Center هذه الدورة بهدف تمكين المهنيين من الكشف عن الجرائم الرقمية، استخلاص الأدلة الدقيقة، وتقديمها بشكل قانوني سليم، مما يعزز العدالة والأمن السيبراني. سيركز التدريب على الجوانب التطبيقية والعملية، مع تقديم دراسات حالة واقعية وتمارين محاكاة، لمساعدة المشاركين على تطبيق المفاهيم النظرية في بيئات عملهم المعقدة، وتعزيز قدراتهم على مواجهة التحديات القانونية والتقنية ببراعة.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- محققو الطب الشرعي الرقمي.
- ضباط إنفاذ القانون.
- متخصصو الأمن السيبراني.
- المستشارون القانونيون في القضايا الرقمية.
- مدققو الأنظمة.
- مسؤولو الاستجابة للحوادث.
- مديرو الأمن السيبراني.

القطاعات والصناعات المستهدفة:

- القطاع الحكومي وإنفاذ القانون.
- القطاع القضائي (المحامون، القضاة، المدعون العامون).
- المؤسسات المالية والمصرفية.
- شركات الأمن السيبراني.
- الشركات الكبرى التي تتعامل مع البيانات الحساسة.
- القطاع الدفاعي.
- شركات الاستشارات التقنية والقانونية.

الأقسام المؤسسية المستهدفة:

- وحدات الجرائم الإلكترونية.
- إدارة أمن المعلومات.
- القسم القانوني.
- إدارة المخاطر.
- التدقيق الداخلي.
- فرق الاستجابة للحوادث.
- إدارة تقنية المعلومات.

أهداف الدورة التدريبية:

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

فهم المبادئ الأساسية للتحقيق الجنائي الرقمي.
جمع الأدلة الرقمية بطرق قانونية وفنية سليمة.
تحليل البيانات من الأجهزة المختلفة (أقراص صلبة، هواتف، شبكات).
استخدام أدوات الطب الشرعي الرقمي المتخصصة.
التعامل مع البرمجيات الخبيثة والتهديدات المتقدمة (APTs).
كتابة التقارير الجنائية الرقمية وتقديمها كأدلة قانونية.
تأمين مسرح الجريمة الرقمي وسلسلة الحضانة (Chain of Custody).
فهم التشريعات والقوانين المتعلقة بالأدلة الإلكترونية.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية على منهجية تفاعلية وعملية مكثفة، تهدف إلى بناء قدرات احترافية في مجال التحقيق الجنائي الرقمي والأدلة الإلكترونية المتقدمة. تبدأ المنهجية بمحاضرات متعمقة يقدمها خبراء متخصصون في الطب الشرعي الرقمي والقانون السيبراني، يليها جلسات نقاش حيوية لتبادل الخبرات والتحديات في قضايا الجرائم الإلكترونية. تركز الدورة بشكل كبير على دراسات الحالة الواقعية، حيث يقوم المشاركون بتحليل سيناريوهات جرائم رقمية معقدة، من اختراقات الشركات إلى الاحتيال عبر الإنترنت، وتطوير استراتيجيات للتحقيق. تتضمن المنهجية ورش عمل تطبيقية ومختبرات افتراضية، تتيح للمتدربين استخدام أدوات الطب الشرعي الرقمي لجمع الأدلة، استعادتها، تحليلها، وتقديمها في تقارير مفصلة. يشجع BIG BEN Training Center العمل الجماعي والتعاون بين المتدربين لتعزيز التفكير النقدي وقدرات حل المشكلات المعقدة. يتم تقديم تغذية راجعة فردية ومستمرة لضمان تحقيق أقصى استفادة من الدورة. تهدف هذه المنهجية إلى تمكين المشاركين من العودة إلى مؤسساتهم وهم مسلحون بالمعرفة والأدوات والخبرة العملية اللازمة لإجراء تحقيقات جنائية رقمية دقيقة، وضمان قبول الأدلة الإلكترونية في الإجراءات القانونية بفعالية وكفاءة عالية.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: مقدمة في التحقيق الجنائي الرقمي ومبادئه

- مفاهيم الطب الشرعي الرقمي ودوره في مكافحة الجرائم.
- المبادئ الأساسية للتحقيق الجنائي الرقمي.
- المتطلبات القانونية للأدلة الإلكترونية (القبول، الموثوقية).
- تأمين مسرح الجريمة الرقمي والحفاظ على الأدلة.
- سلسلة الحضانة (Chain of Custody) وأهميتها.
- أنواع الأدلة الرقمية ومصادرها.
- الأخلاقيات المهنية في الطب الشرعي الرقمي.

الوحدة الثانية: جمع الأدلة الرقمية من مختلف الأنظمة

- تقنيات جمع الأدلة من أنظمة التشغيل (Windows, Linux, macOS).
- استخلاص الأدلة من الأجهزة المحمولة (الهواتف الذكية، الأجهزة اللوحية).
- جمع الأدلة من الشبكات وحركة المرور (Network Forensics).
- الحصول على الأدلة من السحابة (Cloud Forensics).
- التعامل مع الأجهزة التالفة أو المشفرة.
- أدوات وتقنيات استنساخ الأقراص (Disk Imaging).
- مفاهيم استعادة البيانات المحذوفة.

الوحدة الثالثة: تحليل الأدلة الرقمية المتقدم والبرمجيات الخبيثة

- تحليل سجلات الأحداث (Log Analysis) وتتبع النشاط.
- التحليل الجنائي للذاكرة (Memory Forensics).
- تحليل البرمجيات الخبيثة (Malware Analysis) وتحديد وظائفها.
- تقنيات الهندسة العكسية (Reverse Engineering) للبرمجيات الخبيثة.
- اكتشاف الجذور الخفية (Rootkits) والبرمجيات الضارة المستمرة.
- تحليل الملفات المخفية والمشفرة.
- تقنيات البحث عن الأنماط والتوقيعات (Pattern and Signature Analysis).

الوحدة الرابعة: الطب الشرعي للشبكات والسحابة والجرائم المعقدة

- التحقيق في هجمات الشبكات وتحليل حركة البيانات المشبوهة.
- تتبع مصادر الهجمات السيبرانية.
- التحقيق في الجرائم السحابية وتحدياتها.
- التعامل مع الجرائم المالية الرقمية والاحتيال عبر الإنترنت.
- التحقيق في جرائم الملكية الفكرية.
- أدوات الطب الشرعي الشبكي المتقدمة.
- التحقيق في الجرائم التي تشمل العملات المشفرة.

الوحدة الخامسة: إعداد التقارير وتقديم الأدلة في المحكمة

- كتابة تقارير الطب الشرعي الرقمي الشاملة والموثوقة.
- تنسيق التقارير لتقديمها كأدلة قانونية.
- تقديم الشهادة الخبيرة في المحكمة.
- التعامل مع الاستجواب والأسئلة القانونية.
- ضمان مصداقية الأدلة وسلسلة الحضانة.
- التحديات القانونية في قضايا الجرائم الإلكترونية.
- التطورات المستقبلية في قوانين الأدلة الرقمية.

الأسئلة المتكررة:

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

لا توجد شروط مسبقة.

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

تمتد هذه الدورة التدريبية على مدار خمسة أيام، بمعدل يومي يتراوح بين 4 إلى 5 ساعات، تشمل فترات راحة وأنشطة تفاعلية، ليصل إجمالي المدة إلى 20-25 ساعة تدريبية.

سؤال للتأمل:

في ظل التطور المتسارع للتقنيات الرقمية والأساليب الإجرامية، كيف يمكن للمحققين الجنائيين الرقميين أن يضمنوا بقاءهم متقدمين بخطوة على المجرمين، مع الحفاظ على سلامة الأدلة وقبولها قانونيًا في بيئة رقمية متغيرة باستمرار؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها المتقدم والعملي على التحقيق الجنائي الرقمي والأدلة الإلكترونية المتقدمة، مما يميزها عن الدورات التي تقدم لمحة عامة فقط. نحن لا نكتفي بتقديم المفاهيم النظرية، بل نغوص في التطبيقات العملية من خلال ورش عمل مكثفة وتمارين مختبرية تحاكي سيناريوهات جرائم رقمية حقيقية، مما يمنح المشاركين خبرة مباشرة لا تقدر بثمن في جمع وتحليل الأدلة. يضمن المحتوى الأكاديمي المتقدم، المقدم من BIG BEN Training Center، أن يكون المشاركون على اطلاع بأحدث الأدوات والتقنيات وأفضل الممارسات في هذا المجال الحيوي. هذه الدورة لا تهدف فقط إلى تزويد المشاركين بالمعلومات، بل إلى بناء قدراتهم ليصبحوا خبراء قادرين على إجراء تحقيقات جنائية رقمية دقيقة، واستخلاص الأدلة الموثوقة، وتقديمها بشكل قانوني سليم، مما يعزز العدالة ويدعم جهود مكافحة الجريمة السيبرانية بفعالية استثنائية.