الدورة التدريبية: التحقيق الجنائي الرقمي وجمع الأدلة الإلكترونية



29 نوفمبر - 03 ديسمبر 2026
عمان
3800 € (للشخص الواحد)
Ref: #LEG9565_411876

مقدمة الدورة التدريبية / لمحة عامة:

في العصر الرقمي الحالي، تتزايد الجرائم التي تعتمد على التكنولوجيا بشكل مطرد، مما يجعل التحقيق الجنائي الرقمي وجمع الأدلة الإلكترونية من المجالات الحيوية في مكافحة الجريمة. تُقدم هذه الدورة التدريبية من BIG BEN Training Center فهمًا شاملاً لمبادئ التحقيق الرقمي، بدءًا من مفاهيم الأدلة الرقمية والطب الشرعي الرقمي وصولاً إلى الجوانب العملية للحفاظ على سلسلة الحضانة وتحليل البيانات الجنائية. سنتناول بالتفصيل أنواع الجرائم السيبرانية، الاستجابة للحوادث الأمنية، تقنيات استعادة البيانات، والتعامل مع الأدلة في بيئات مختلفة كالحوسبة السحابية والأجهزة المحمولة. تهدف الدورة إلى تزويد المشاركين بالمعرفة والأدوات اللازمة لإجراء تحقيقات رقمية فعالة، وضمان قبول الأدلة في المحكمة، مما يسهم في تحقيق العدالة. إن فهم هذه الجوانب التقنية والقانونية ضروري للمحققين، مسؤولي الأمن السيبراني، والمتخصصين في إنفاذ القانون. يمكن الإشارة هنا إلى أعمال أكاديميين بارزين مثل البروفيسور إيفان كيسي (Eoghan Casey)، الذي يُعد مرجعًا في الطب الشرعي الرقمي ويسلط الضوء على أهمية الدقة والمنهجية في جمع الأدلة الرقمية، مما يؤكد على ضرورة هذه الدورة للمحققين وخبراء الأمن.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- المحققون الجنائيون.
- مسؤولو الأمن السيبراني.
- خبراء الطب الشرعي الرقمي.
- المحللون الجنائيون الرقميون.
- أفراد إنفاذ القانون (الشرطة، النيابة العامة).
- المستشارون القانونيون المتخصصون في الجرائم الإلكترونية.
- المدققون الأمنيون.

القطاعات والصناعات المستهدفة:

- الجهات الحكومية وإنفاذ القانون.
- قطاع الأمن السيبراني.
- الخدمات القانونية والاستشارية.
- القطاع المالي والمصرفي.
- الشركات التقنية ومقدمي الخدمات السحابية.
- الشركات التي تتعامل مع بيانات حساسة.
- مؤسسات البحث والتطوير في الأمن الرقمي.

الأقسام المؤسسية المستهدفة:

- إدارات التحقيقات الجنائية.
- أقسام الأمن السيبراني.
- وحدات الجرائم الإلكترونية.
- الإدارات القانونية.
- أقسام التدقيق الداخلي.
- إدارات المخاطر.
- الموارد البشرية (في قضايا سوء الاستخدام).

أهداف الدورة التدريبية:

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

- فهم المبادئ الأساسية للتحقيق الجنائي الرقمي والطب الشرعي الرقمي.
- تحديد أنواع الأدلة الإلكترونية ومصادرها.
- تطبيق منهجيات جمع الأدلة الرقمية بشكل قانوني وسليم.
- الحفاظ على سلسلة الحضانة للأدلة لضمان قبولها في المحكمة.
- استخدام الأدوات والتقنيات الأساسية في تحليل الأدلة الرقمية.
- التعامل مع الحوادث الأمنية السيبرانية بفعالية.
- إعداد التقارير الفنية والقانونية للتحقيقات الرقمية.

منهجية الدورة التدريبية:

يعتمد BIG BEN Training Center في هذه الدورة التدريبية على منهجية عملية ومكثفة لضمان استيعاب شامل للتحقيق الجنائي الرقمي وجمع الأدلة الإلكترونية. يتم تقديم المفاهيم النظرية من خلال محاضرات تخصصية، يليها تدريبات عملية مكثفة في بيئات محاكاة لمسارح الجريمة الرقمية، مما يتيح للمشاركين تطبيق التقنيات والأدوات في سيناريوهات واقعية. سيشارك المتدربون في ورش عمل جماعية تتيح لهم فرصة جمع الأدلة من أجهزة مختلفة، تحليل البيانات، وإعداد تقارير الطب الشرعي الرقمي. سيتم التركيز على الجلسات التفاعلية التي تشجع على النقاش وتبادل الخبرات بين المشاركين، مما يعزز قدرتهم على اتخاذ قرارات مستنيرة في مواقف التحقيق المعقدة. توفر الدورة تغذية راجعة فردية لضمان تحقيق أقصى استفادة، وتمكين المشاركين من تطبيق المهارات المكتسبة بفعالية في عملهم.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات التحقيق الجنائي الرقمي.

- مفهوم التحقيق الجنائي الرقمي وأهميته.
- تعريف الأدلة الرقمية وأنواعها.
- مبادئ الطب الشرعي الرقمي ومراحله.
- الفرق بين التحقيق التقليدي والرقمي.
- المتطلبات القانونية لجمع الأدلة الإلكترونية.
- أخلاقيات التحقيق الرقمي.
- دور المحقق الرقمي في القضايا الحديثة.

الوحدة الثانية: جمع وحماية الأدلة الإلكترونية.

- تحديد مصادر الأدلة الرقمية.
- تقنيات الاستحواذ على البيانات (Acquisition).
- الحفاظ على سلسلة الحضانة (Chain of Custody).
- التعامل مع الأدلة في الأجهزة المتوقفة والتشغيلية.
- تحديات جمع الأدلة من الحوسبة السحابية.
- تأمين الأدلة من التلف أو التغيير.
- الأدوات الأساسية لجمع الأدلة الرقمية.

الوحدة الثالثة: تحليل الأدلة الرقمية.

- مراحل تحليل الأدلة الإلكترونية.
- تقنيات استعادة البيانات المحذوفة.
- التحليل الجنائي للشبكات.
- التحليل الجنائي للأجهزة المحمولة.
- التحليل الجنائي للبرمجيات الخبيثة.
- أدوات تحليل الأدلة الرقمية الشائعة.
- استخلاص المعلومات ذات الصلة بالتحقيق.

الوحدة الرابعة: الاستجابة للحوادث الأمنية السيبرانية.

- مفهوم الحادث الأمني السيبراني.
- مراحل الاستجابة للحوادث.
- دور التحقيق الرقمي في الاستجابة للحوادث.
- إدارة الأزمات بعد الاختراقات الأمنية.
- وضع خطة الاستجابة للحوادث.
- التعاون مع الفرق الداخلية والخارجية.
- الدروس المستفادة من الحوادث السيبرانية.

الوحدة الخامسة: إعداد التقارير والشهادة في المحكمة.

- أهمية التوثيق في التحقيق الرقمي.
- بناء تقرير الطب الشرعي الرقمي.
- تقديم النتائج بوضوح وموضوعية.
- الشهادة أمام المحكمة كخبير رقمي.
- الدفاع عن الأدلة المستخلصة.
- التحديات القانونية والفنية في الشهادة.
- أفضل الممارسات في إعداد التقارير الجنائية 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 وتزايد تعقيد الجرائم السيبرانية، كيف يمكن للمحققين الرقميين الحفاظ على مواكبتهم لأحدث الأدوات والأساليب لضمان فعالية جمع وتحليل الأدلة الإلكترونية وتقديمها بشكل مقنع أمام العدالة؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة التدريبية من BIG BEN Training Center بتركيزها العملي والمكثف على التحقيق الجنائي الرقمي وجمع الأدلة الإلكترونية، مما يجعلها فريدة في مجالها. ما يميزها هو قدرتها على دمج المفاهيم النظرية مع التدريبات العملية المكثفة في بيئات محاكاة واقعية، مما يمنح المشاركين خبرة عملية لا تقدر بثمن في التعامل مع الأدلة الرقمية. تعتمد الدورة على أحدث الأدوات والتقنيات المستخدمة في الطب الشرعي الرقمي، وتوفر للمتدربين الفرصة لتطبيقها بأنفسهم. يتم التركيز على سلسلة الحضانة للأدلة لضمان قبولها القانوني، وعلى كيفية إعداد التقارير الفنية التي تدعم التحقيقات. هذه الدورة لا تقتصر على نقل المعلومات، بل تهدف إلى بناء كفاءات حقيقية تسهم في تعزيز قدرات المشاركين على مكافحة الجرائم السيبرانية بفعالية.