



الدورة التدريبية: البحث الجنائي والتحليل والتتبع الرقمي

Ref: #LAW38552269



مقدمة الدورة التدريبية / لمحة عامة:

يشهد العالم اليوم تحولاً جذرياً في طبيعة الجريمة وأساليب ارتكابها، إذ لم تعد الأدلة محصورة في مسرح الجريمة المادي، بل امتدت إلى الهواتف الذكية والحواسيب والخوادم السحابية وشبكات التواصل الاجتماعي ومعاملات العملات المشفرة. وأمام هذا الواقع، أصبحت تقنيات البحث الجنائي الحديثة وأدوات التحليل والتتبع الرقمي ركيزة أساسية لكل جهة تسعى إلى كشف الحقيقة وتقديم أدلة سليمة ومقبولة أمام الجهات القضائية. وتأتي هذه الدورة التدريبية لتمنح المشاركين فهماً شاملاً ومتكاملاً لدورة حياة الدليل الجنائي، بدءاً من معاينة مسرح الجريمة وتأمينه، مروراً بجمع الأدلة المادية والرقمية وحفظها وفق سلسلة حياة موثقة، وصولاً إلى تحليلها وربطها وإعداد التقارير الفنية القادرة على الصمود أمام المراجعة القانونية. وتستند الدورة إلى أطر علمية رصينة، من أبرزها أعمال Eoghan Casey في كتابه Digital Evidence and Computer Crime، إلى جانب المنهجيات التي عرضها Brian Carrier في كتابه File System Forensic Analysis، مما يمنح المتدرب أساساً أكاديمياً متيناً يوازن بين النظرية والتطبيق. كما تتناول الدورة تقنيات تحليل الهواتف المحمولة، واستخراج البيانات المحذوفة، وتحليل سجلات الشبكات، وتتبع المعاملات المالية الرقمية، والاستفادة من المصادر المفتوحة في التحريات، مع مراعاة الضوابط القانونية والأخلاقية وحماية الخصوصية. ويقدم BIG BEN Training Center هذه الدورة بأسلوب تطبيقي معمق يعتمد على قضايا واقعية ومحاكاة لسيناريوهات تحقيق متكاملة، ليخرج المشاركون قادراً على قيادة عمليات البحث الجنائي بثقة ودقة واحترافية عالية.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- المحققون الجنائيون وضباط البحث والتحري.
- خبراء الأدلة الجنائية والعاملون في مختبرات التحليل الجنائي.
- محللو الأدلة الرقمية ومختصو الطب الشرعي الرقمي.
- أعضاء النيابة العامة والمستشارون القانونيون المعنيون بالقضايا الجنائية.
- مسؤولو الأمن السيبراني وفرق الاستجابة للحوادث.
- محققو الاحتيال المالي ومكافحة غسل الأموال.
- مدققو الالتزام والرقابة الداخلية المعنيون بالتحقيقات.
- رؤساء الأقسام والمشفرون على وحدات التحقيق والتحري.
- المحللون الاستخباريون وباحثو المصادر المفتوحة.



القطاعات والصناعات المستهدفة:

- الهيئات الحكومية والأجهزة الأمنية والشرطية وما في حكمها.
- الجهات القضائية والنيابات العامة.
- البنوك والمؤسسات المالية وشركات الدفع الإلكتروني.
- شركات الاتصالات ومزودو خدمات الإنترنت.
- شركات التأمين وإدارات مكافحة الاحتيال.
- شركات الأمن السيبراني والاستشارات التقنية.
- الجمارك وهيئات المنافذ الحدودية.
- المؤسسات الكبرى ذات الأنظمة الرقمية الحساسة.

الأقسام المؤسسية المستهدفة:

- إدارات التحقيق والبحث الجنائي.
- إدارات الأدلة الجنائية والمختبرات.
- إدارات الأمن السيبراني وأمن المعلومات.
- إدارات مكافحة الاحتيال والجرائم المالية.
- إدارات الشؤون القانونية.
- إدارات التدقيق الداخلي والالتزام.
- إدارات المخاطر والاستخبارات المؤسسية.



أهداف الدورة التدريبية:

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

- فهم المبادئ العلمية والقانونية للبحث الجنائي الحديث ومراحل التحقيق المتكاملة.
- إدارة مسرح الجريمة وتأمينه وتوثيقه وفق المعايير الدولية المعتمدة.
- جمع الأدلة المادية والرقمية وحفظها مع الالتزام بسلسلة الحيازة.
- استخدام أدوات التحليل الجنائي الرقمي لاستخراج البيانات وتحليلها من الحواسيب والهواتف.
- استرجاع البيانات المحذوفة وتحليل البيانات الوصفية والسجلات الزمنية.
- تتبع الأنشطة عبر الشبكات والبريد الإلكتروني ومنصات التواصل الاجتماعي.
- تتبع المعاملات المالية الرقمية والعملات المشفرة وكشف أنماط الاحتيال.
- توظيف تقنيات التحري من المصادر المفتوحة OSINT بطريقة قانونية وأخلاقية.
- ربط الأدلة وبناء التسلسل الزمني للأحداث وتحليل الروابط بين الأطراف.
- إعداد تقارير فنية جنائية واضحة ومقبولة أمام الجهات القضائية.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية على منهجية تفاعلية تطبيقية تجمع بين العمق الأكاديمي والممارسة الميدانية، حيث يحرص BIG BEN Training Center على أن يعيش المشارك تجربة التحقيق بكل مراحلها لا أن يكتفي بسماعها. وتبدأ كل جلسة بعرض مفاهيمي مركز يشرح الأسس العلمية والقانونية للموضوع، ثم ينتقل المدرب إلى عروض عملية توضح آلية عمل أدوات التحليل والتتبع الرقمي خطوة بخطوة، مع شرح نقاط القوة والقيود لكل أداة وأثرها على موثوقية الدليل. وتشكل دراسات الحالة محوراً رئيساً في الدورة، إذ يجري تحليل قضايا واقعية في مجالات الاحتيال المالي والجرائم الإلكترونية والتحقيقات الداخلية، ويُطلب من المشاركين استخلاص الأخطاء والدروس وطرح بدائل أفضل. كما يُوزع المشاركون على فرق عمل تحاكي وحدات التحقيق الحقيقية، تتولى كل فرقة معالجة سيناريو تحقيق متكامل يبدأ بمعاينة مسرح جريمة افتراضي وينتهي بإعداد تقرير فني وعرضه أمام لجنة تحاكي جلسة قضائية. ويعتمد التدريب كذلك على التمارين الفردية القصيرة، وحلقات النقاش المفتوح، وجلسات العصف الذهني لربط المعارف بواقع عمل المشاركين في مؤسساتهم. وتُقدم التغذية الراجعة بشكل مستمر وبناء بعد كل نشاط، مع تقييم موضوعي لأداء الفرق والأفراد، مما يضمن تثبيت المهارات وقياس التقدم طوال أيام الدورة، ويجعل المشارك قادراً على نقل ما تعلمه مباشرة إلى بيئة العمل.



خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أسس البحث الجنائي الحديث وإدارة مسرح الجريمة

- تطور علم البحث الجنائي من الأساليب التقليدية إلى التقنيات الحديثة.
- المبادئ العلمية للأدلة الجنائية ومبدأ التبادل Locard's Exchange Principle.
- مراحل التحقيق الجنائي المتكامل من البلاغ حتى الإحالة القضائية.
- معاينة مسرح الجريمة وتأمينه ومنع تلوث الأدلة.
- التوثيق الفوتوغرافي والرسم الهندسي لمسرح الجريمة.
- تصنيف الأدلة المادية والبيولوجية والرقمية.
- سلسلة الحيازة Chain of Custody وأهميتها القانونية.
- الإطار القانوني والأخلاقي لجمع الأدلة واحترام الخصوصية.

الوحدة الثانية: جمع الأدلة الرقمية وحفظها وفق المعايير الدولية

- مفهوم الدليل الرقمي وخصائصه وهشاشته.
- المعايير الدولية لمعالجة الأدلة الرقمية ISO/IEC 27037.
- التعامل الأولي مع الأجهزة الرقمية في مسرح الجريمة.
- النسخ الجنائي للأقراص Forensic Imaging والتحقق بـ Hash.
- الاستحواذ على الذاكرة الحية Live Memory Acquisition.
- استخدام أدوات الحجب ضد الكتابة Write Blockers.
- جمع الأدلة من البيئات السحابية والخوادم.
- توثيق إجراءات الجمع والحفظ بما يضمن قبول الدليل.



الوحدة الثالثة: أدوات التحليل الجنائي للحواسيب والهواتف الذكية

- تحليل أنظمة الملفات وهياكل التخزين.
- استرجاع البيانات المحذوفة وتقنية Data Carving.
- تحليل البيانات الوصفية Metadata والطوابع الزمنية.
- تحليل سجلات النظام وسجل Windows Registry.
- بناء الخط الزمني للأحداث Timeline Analysis.
- استخراج بيانات الهواتف الذكية وتحليل التطبيقات والمحادثات.
- تحليل بيانات الموقع الجغرافي وسجلات الاتصال.
- مقارنة أدوات التحليل الجنائي التجارية والمفتوحة المصدر.

الوحدة الرابعة: التتبع الرقمي عبر الشبكات والمصادر المفتوحة والمعاملات المالية

- تحليل حركة الشبكات وسجلات الخوادم والجدران النارية.
- تتبع عناوين IP وتحليل رؤوس رسائل البريد الإلكتروني.
- التحري من المصادر المفتوحة OSINT ومنهجيته.
- تحليل منصات التواصل الاجتماعي وكشف الهويات الوهمية.
- التحقق من الصور ومقاطع الفيديو وكشف التلاعب الرقمي.
- تتبع المعاملات المالية الرقمية وأنماط الاحتيال الإلكتروني.
- تحليل سلاسل الكتل Blockchain Analysis وتتبع العملات المشفرة.
- تحليل الروابط بين الأشخاص والكيانات Link Analysis.

الوحدة الخامسة: ربط الأدلة وإعداد التقارير الجنائية والشهادة الفنية

- منهجيات ربط الأدلة المادية والرقمية لبناء رواية متماسكة.
- توظيف الذكاء الاصطناعي وتحليل البيانات الضخمة في التحقيقات.
- تقييم موثوقية الأدلة وتجنب التحيز المعرفي لدى المحقق.
- إعداد التقرير الفني الجنائي وهيكلته ولغته.
- عرض النتائج الفنية أمام الجهات القضائية بوضوح وحياد.
- الإدلاء بالشهادة الفنية والتعامل مع أسئلة الدفاع.
- محاكاة تحقيق متكامل من مسرح الجريمة حتى التقرير النهائي.
- بناء خطة لتطوير وحدة البحث الجنائي الرقمي داخل المؤسسة.



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:

إذا كانت أدوات التحليل الرقمي والذكاء الاصطناعي تكشف ما لم يكن ممكناً كشفه من قبل، فكيف يضمن المحقق أن تبقى الحقيقة التي يقدمها نتاج عقل ناقد ومحايد، لا مجرد انعكاس لما تُظهره الخوارزميات؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بأنها لا تتعامل مع البحث الجنائي التقليدي والتحليل الرقمي بوصفهما مجالين منفصلين، بل تقدمهما منظومة واحدة متكاملة تعكس واقع الجريمة المعاصرة، حيث يلتقي الدليل المادي مع الدليل الرقمي في القضية الواحدة. فالمشارك لا يتعلم كيف يستخدم أداة بعينها فحسب، بل يتعلم كيف يفكر كمحقق محترف يعرف متى يجمع الدليل، وكيف يحفظه، ولماذا يختار منهجية تحليل دون أخرى، وكيف يحول النتائج الفنية إلى رواية قانونية متماسكة يصعب الطعن فيها. ويركز BIG BEN Training Center على الرؤى العملية المستخلصة من قضايا حقيقية، مثل كشف شبكات الاحتيال المالي عبر تتبع المعاملات الرقمية، وإعادة بناء التسلسل الزمني لحادثة اختراق من خلال سجلات الأنظمة، وكشف الهويات الوهمية على منصات التواصل الاجتماعي. كما تمنح الدورة اهتماماً خاصاً بمرحلة غالباً ما تُهمل في البرامج الأخرى، وهي إعداد التقرير الفني والإدلاء بالشهادة أمام القضاء، لأن قيمة الدليل لا تكتمل إلا حين يُقدم بلغة واضحة ومقنعة. وتختتم الدورة بمحاكاة تحقيق متكامل تضع المشارك أمام تحديات واقعية تتطلب العمل الجماعي واتخاذ القرار تحت الضغط، مع معالجة جادة لقضايا التحيز المعرفي والضوابط الأخلاقية وحماية الخصوصية. وبهذا يغادر المشارك الدورة وهو يمتلك عقلية تحليلية ناضجة وخطة واضحة لتطوير قدرات مؤسسته في البحث الجنائي والتتبع الرقمي.