الجرائم الإلكترونية
والتحقيقات الجنائية

د/ خالد السيد عبدالحق
د/ دعاء محمود عبدالعال

جدول المحتويات

مقدمة: ٧
الفصل الأول: مقدمة في الجرائم الإلكترونية والتحقيقات الجنائية ٩
١. تعريف الجرائم الإلكترونية وأنواعها ١٣
٢. أهمية التحقيقات الجنائية الرقمية ٣٧
٣. أدوات وتقنيات الجريمة الإلكترونية ٤٠
٤. تحديات التحقيق في الجرائم الإلكترونية ٥٤
الفصل الثاني: أساسيات شبكات الحاسوب والأدلة الرقمية ٥٧
١. بنية شبكات الحاسوب ودورها في التحقيقات الجنائية ٦١
٢. مفاهيم الازدواجية وتأثيرها على الأدلة الرقمية ٦٨
٣. جمع الأدلة الرقمية وتحليلها ٧٢
٤. أدوات وتقنيات تحليل الشبكات في التحقيقات ٨١
الفصل الثالث: المراقبة والكشف عن التسلل والاستجابة للحوادث ٨٥
١. تقنيات مراقبة الشبكة وتحليل البيانات ٨٩
٢. أنظمة الكشف عن الاختراق (IDS) ومنع الاختراق (IPS) ٩٧
٣. استراتيجيات الاستجابة للحوادث وتتبع المصدر ١٠٤
٤. التوقيع الرقمي وخوارزميات مطابقة النمط ١١١
الفصل الرابع: الفيروسات والبرمجيات الخبيثة وطرق الكشف عنها ١٢٣
١. أنواع الفيروسات والبرمجيات الخبيثة ١٢٧
٢. تقنيات تحليل الفيروسات والكشف عنها ١٤٤
٣. أساليب انتشار الفيروسات والهجمات السيبرانية ١٤٨
٤. استراتيجيات الحماية من الفيروسات والبرمجيات الخبيثة ١٦١
الفصل الخامس: تقنيات إخفاء الهوية ووسائل التمويه الرقمي ١٦٧
١. تقنيات التصفح المجهول وإخفاء الهوية ١٧١
٢. استخدام الأسماء المستعارة والهويات المزيفة ١٨٦

٣. وسائل حماية الخصوصية والتشفير ١٩٥
٤. مخاطر وأساليب كشف هوية المستخدمين..... ١٩٩
الفصل السادس: الأطر القانونية والتشريعات الخاصة بالفضاء الإلكتروني ٢٠٥
١. قانون الفضاء الإلكتروني وأهم تشريعاته ٢٠٩
٢. سياسات الأمن السيبراني ومبادئ الحوكمة الرقمية ٢٢٨
٣. أثر القوانين على التحقيقات الجنائية الرقمية ٢٣٢
٤. التعاون الدولي في مكافحة الجرائم الإلكترونية ٢٣٥
الفصل السابع: التحقيقات الجنائية الرقمية والتقارير القضائية..... ٢٣٩
١. طرق تحليل ودراسة الحالات الجنائية الرقمية..... ٢٤٣
٢. إعداد التقارير الخاصة بالمحاكم وشهادات الخبراء ٢٤٥
٣. استخدام الأدلة الرقمية في القضايا القانونية ٢٤٩
٤. التحديات المستقبلية في التحقيقات الرقمية ٢٥٢

مقدمة

مع التطور الهائل في تكنولوجيا المعلومات والاتصالات، أصبح الفضاء الرقمي ساحة جديدة للجريمة، حيث لم تعد الجرائم مقتصرة على العالم المادي فقط، بل امتدت إلى الفضاء الإلكتروني لتشمل مجموعة واسعة من الأنشطة غير القانونية، مثل الاختراقات، والاحتيال الإلكتروني، وسرقة الهوية، ونشر البرمجيات الخبيثة، والتجسس الإلكتروني، وغيرها من الجرائم التي تهدد الأفراد والمؤسسات والدول على حدٍ سواء. لقد أحدث هذا التحول الرقمي ثورة في طريقة ارتكاب الجرائم، مما استدعى تطوير أساليب حديثة للتحقيق في هذه الجرائم والكشف عن مرتكبيها وملاحقتهم قانونيًا.

يهدف هذا الكتاب إلى تقديم رؤية شاملة حول الجرائم الإلكترونية، وأساليب التحقيق الجنائي الرقمي، والتحديات التي تواجه المحققين في هذا المجال، وذلك من خلال مناقشة مختلف الجوانب التقنية والقانونية المتعلقة بالجرائم الرقمية. فالتحقيقات الجنائية التقليدية لم تعد كافية لمواكبة التعقيد المتزايد في الجرائم الإلكترونية، خاصةً مع تطور أدوات وتقنيات التخفي الرقمي التي يستخدمها المجرمون لطمس آثارهم وإخفاء هوياتهم. لذا، أصبح من الضروري تبني منهجيات متطورة تعتمد على التحليل الرقمي، ومراقبة الشبكات، والكشف عن التسلل، بالإضافة إلى استخدام خوارزميات الذكاء الاصطناعي وتقنيات تعلّم الآلة لتعزيز قدرة المحققين على تعقب الجناة وجمع الأدلة الرقمية بطرق قانونية سليمة.

يتناول الكتاب مجموعة من الموضوعات الأساسية التي تشكل حجر الأساس في التحقيقات الرقمية، بدءًا من فهم بنية شبكات الحاسوب، مرورًا بأساليب جمع الأدلة الرقمية وتحليلها، ووصولًا إلى كتابة التقارير وعرض الأدلة أمام الجهات القضائية. كما يسلط الضوء على أنظمة الكشف عن التسلل (IDS)وأنظمة منع الاختراق(IPS) ، وأهمية الاستجابة السريعة للحوادث السيبرانية، فضلاً عن دراسة الفيروسات والبرمجيات الخبيثة، وطرق انتشارها، وكيفية مواجهتها.

علاوة على ذلك، يتناول الكتاب واحدة من أهم القضايا في الجرائم الإلكترونية، وهي تقنيات إخفاء الهوية ووسائل التمويه الرقمي التي يستخدمها المجرمون، مثل الشبكات المجهولة، والبروكسيات، والتشفير، والهوية المزيفة، والتي تشكل تحديًا كبيرًا أمام جهات إنفاذ القانون. كما يناقش الأساليب المستخدمة لتجاوز هذه العوائق وكشف هوية المتورطين في الأنشطة الإجرامية الرقمية.