

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

سایبر فارنزیک

تألیف: آلبرت جی مارسلو و داگلاس مندنز

مترجم: امیر توکلی



عنوان و نام پدیدآور	: سایبر فارنژیک / تالیف [اصحیح: ویراستار] آلبرت جی مارسلا و داگلاس منندز؛ مترجم: امیر توکلی.
مشخصات نشر	: تهران : نیروی انتظامی جمهوری اسلامی ایران، پلیس فتا، ۱۳۹۲.
مشخصات ظاهری	: ۶۶۲ ص. مصور.
شابک	: ۹۷۸-۶۰۰-۹۳۴۰۱-۳-۲
وضعیت فهرست نویسی	: فیپا
موضوع	: جرائم کامپیوتری - پی جویی - دستنامه ها
شناسه افزوده	: توکلی، امیر، ۱۳۶۵ - مترجم
شناسه افزوده	: مارسلا، آلبرت ج.، ۱۹۶۵ - م.
شناسه افزوده	: منندز، دوگ، ویراستار
شناسه افزوده	: Menendez, Doug
شناسه افزوده	: Marcella, Albert J.
شناسه افزوده	: نیروی انتظامی جمهوری اسلامی ایران، پلیس فتا
رده بندی کنگره	: HV ۸۰۷۹ / ک۲ ج۴ ۱۳۹۲
رده بندی دیویی	: 363/25968
شماره کتابشناسی ملی	: 3271129



نام کتاب	: سایبر فارنژیک
ناشر	: پلیس فتا
مولفان	: آلبرت جی مارسلا و داگلاس منندز
مترجم	: امیر توکلی
ویراستار	: اباذر محرمی
نظارت	: محسن خداپرست
چاپ اول	: ۱۳۹۲
تیراژ	: ۱۰۰۰ جلد
لیتوگرافی، چاپ و صحافی	: چاپ و نشر حدیث کوثر
قیمت	: ۲۹۰۰۰۰ ریال
شابک	: ۹۷۸-۶۰۰-۹۳۴۰۱-۳-۲
ISBN	: 978-600-93401-3-2

فهرست مطالب

۱۵	پیشگفتار
۱۹	فصل ۱: معرفی
۲۰	اثرات سوءاستفاده از فناوری بر امنیت افراد و سازمان‌ها
۲۶	تعریف سایبر فارنزیک
۲۷	تعاریف عملی برای تشریح پیشرفت‌های این حرفه
۲۷	فرآیندهای تحقیقات سایبر فارنزیک
۳۰	فعالیت‌های غیرقانونی هشدار دهنده
۳۱	سایبر فارنزیک: خنثی سازی ریسک شرکت
۳۴	گرایش‌ها: نیاز فزاینده به کسب توانایی‌های موثر سایبر فارنزیک
۳۹	مدرك: جداسازی گندم از کاه
۴۱	چه کسانی باید در مورد سایبر فارنزیک آگاهی داشته باشند؟
۴۳	ضرورت به‌کارگیری تحلیل‌های سایبر فارنزیک
۴۴	فشار بر سازمان‌ها در جهت کسب توانایی‌های سایبر فارنزیک
۴۴	قانون سربانز-اکسلی ۲۰۰۲ یا (SoX)
۴۶	قانون گرام-میچ-بیلی
۴۷	قانون نقص امنیت اطلاعات کالیفرنیا
۴۸	قانون پاسخگویی و کاربری بیمه درمانی، مصوب ۱۹۹۶
۴۹	پیمان سرمایه بازل ۲
۵۰	قانون وطن‌پرستی و تنفیذ مجدد اختیارات مبارزه با تروریسم
۵۰	قانون ممنوعیت سرقت الکترونیکی: نت
۵۱	قانون جاسوسی اقتصادی

۵۲	قانون منع پورنوگرافی علیه کودکان (۲۰۰۵)
۵۲	قوانین پیشگیری از جرایم ناشی از نفرت (دشمنی)
۵۳	قانون سوءاستفاده و کلاهبرداری رایانه‌ای
۵۳	قانون کپی‌رایت در عصر دیجیتال
۵۴	قانون منع تصرف و سرقت هویت
۵۴	قانون حفاظت از کودکان در فضای سایبری
۵۴	قانون انواع کلاهبرداری اینترنتی (کلاهبرداری از طریق ارتباطات الکترونیکی)
۵۵	قانون حفاظت از زیرساخت‌های اطلاعات ملی
۵۵	قانون امنیت رایانه‌ای
۵۶	قانون حفظ حریم خصوصی ارتباطات الکترونیکی
۵۶	حسابرسی در مقایسه با تحقیقات سایبر فارنژیک
۶۰	جمع‌بندی

فصل ۲: ابزارها و برنامه‌های کاربردی سایبر فارنژیک

۶۳	مقدمه
۶۴	بررسی گستردگی محصولات
۶۵	ابزارهای سایبر فارنژیک
۶۷	خوب، بهتر، بهترین: کدام یک، ابزار مناسب در سازمان شما است؟
۷۱	بازنگری ابزار
۸۸	بهترین خرید یا پیشنهاد
۸۸	دیگر ابزارهای مناسب برای یک کارشناس
۸۹	نرم‌افزار ComputerCOP
۹۱	مجموعه نرم‌افزارهای Mares and Company
۹۴	اتحادیه فن‌آوری‌های جدید
۹۴	مجموعه برنامه‌های مربوط به پس از واقعه (واکنش به رویداد)
۹۶	وب‌سایت‌هایی برای کسب اطلاعات بیشتر در مورد ابزار و محصولات سایبر فارنژیک
۹۸	جمع‌بندی

فصل ۳: روش‌های پنهان‌سازی

۱۰۰	امحا (نابود سازی)
۱۰۱	رمزنگاری - شیوه‌ای قدیمی و پرکاربرد
۱۰۲	اشتراک‌گذاری اطلاعات سری
۱۰۳	انواع الگوریتم‌های رمزنگاری
۱۰۴	رمزنگاری کلید سری
۱۱۱	رمزنگاری کلید عمومی
۱۱۵	توابع هش - رمزنگاری به هم ریخته

۱۱۷	رمز نگاری؛ داستانی ناگفته
۱۱۸	کلاهبرداری (پنهان سازی اطلاعات شناسه)
۱۱۸	شناسه اینترنتی (IP) یا Internet Protocol
۱۱۹	اصول اولیه کنترل بر انتقال داده‌ها
۱۲۱	حملات سرقت چند مرحله‌ای
۱۲۲	پلی مورفیزیم
۱۲۴	پنهان نگاری
۱۲۷	بازگردانی فرایند پنهان نگاری
۱۲۹	مقابله با سایبر فارنزیک
۱۳۴	ضد سایبر فارنزیک: نگاهی از دیگر سو
۱۴۲	رمز گذاری برنامه‌های خط فرمان ویندوز ایکس‌پی
۱۴۳	شیوه‌های فریب دادن: پنهان کردن فایل‌ها و جستجو فایل‌های تبادلی
۱۴۴	فضای راکد فایل
۱۴۶	تغییر نام فایل‌ها
۱۴۷	ساختار فایل (پسوند فایل)
۱۵۲	تغییر ویژگی‌های فایل
۱۵۶	Ghosting
۱۵۸	فایل‌های فشرده
۱۶۴	دستکاری و تغییر فایل‌های سیستمی
۱۶۵	جدول تخصیص فایل
۱۶۷	فایل سیستم ان‌تی‌اف‌اس NTFS
۱۶۹	سختافزار ذخیره فایل و سازماندهی دیسک
۱۷۰	سکتورها و کلاسترها
۱۷۲	فضای راکد- فارنزیک نیروانا
۱۷۴	پنهان سازی داده‌ها در فضای راکد سیستمی، توسط ابزار Bmap
۱۷۶	پنهان سازی داده‌ها در سیستم ان‌تی‌اف‌اس
۱۷۸	روش‌های دیگر، برای پنهان کردن داده‌ها از چشم کارشناسان
۱۷۸	مناطق محافظت شده میزبان و پیکربندی
۱۷۹	پنهان سازی در فضای راکد فایل یا فضای خالی راکد
۱۸۰	ابزارهای مختلف پاکسازی
۱۸۲	نکات بیشتر در مورد ابزارهای پاکسازی اطلاعات
۱۸۴	روت‌کیت
۱۸۷	شنود؛ انتقال صدا از طریق شناسه اینترنتی (مکالمه اینترنتی)
۱۹۲	حصول اطمینان از ثبت گزارش‌های امنیتی، منطبق با زمان شبکه
۱۹۴	کشف زمان

۱۹۴	هماهنگی زمانی
۱۹۵	برقرار کردن امنیت زمانی
۱۹۵	اهمیت تنظیم زمان
۱۹۶	تنظیم ساعت مسیر یاب‌های سیسکو به وسیله پروتکل زمان شبکه
۱۹۹	نرم افزارهای مخرب مقیم در حافظه (Rootkits)
۲۰۱	روتکیت‌های سطح هسته
۲۰۱	هکر دِفندر Hacker Defender
۲۰۲	روتکیت‌های بایوس (نرم افزارهای مخرب مقیم در بایوس)
۲۰۳	هووکینگ Hooking
۲۰۴	هووکینگ رابط برنامه نویسی
۲۰۴	هووکینگ جدول آدرس‌های ورودی
۲۰۵	هووکینگ درون برنامه‌ای
۲۰۵	دستکاری مستقیم عناصر در هسته اصلی
۲۰۶	تصادم مقادیر هَش
۲۰۷	مهندسی اجتماعی
۲۰۹	جمع بندی
۲۱۱	فصل ۴: سخت افزار؛ سیستم پایه
۲۱۱	مقدمه
۲۱۲	رایانه‌ها
۲۱۵	منبع تغذیه
۲۱۷	دیسک سخت
۲۲۱	بُرد اصلی
۲۲۳	رایانه‌های همراه
۲۲۷	تبلت‌ها
۲۲۸	تجهیزات ذخیره سازی خارجی
۲۳۲	سرورها
۲۳۳	دستگاه‌های پخش موسیقی
۲۳۴	پی دی ای - منشی دیجیتال
۲۴۰	جمع بندی
۲۴۱	فصل ۵: نرم افزار، سیستم‌های عامل، ترافیک شبکه و برنامه‌های کاربردی
۲۴۱	مقدمه
۲۴۲	موسسه ملی استانداردها و فناوری
۲۴۳	به کارگیری داده‌های سیستم‌های عامل
۲۴۴	مبانی سیستم عامل

۲۴۴	داده‌های پایدار (غیر فرار)
۲۴۸	مبانی پایه سیستم ورودی و خروجی (بایوس)
۲۴۹	داده‌های ناپایدار (فرار)
۲۵۲	جمع‌آوری داده‌های سیستم عامل
۲۵۲	جمع‌آوری داده‌های ناپایدار سیستم عامل
۲۵۳	انواع داده‌های ناپایدار سیستم عامل
۲۵۶	اولویت‌بندی جمع‌آوری داده‌ها
۲۵۷	جمع‌آوری داده‌های پایدار سیستم عامل
۲۶۱	تحلیل و بررسی داده‌های سیستم عامل
۲۶۳	توصیه‌هایی برای استفاده از داده‌هایی سیستم عامل
۲۶۳	استفاده از اطلاعات شبکه
۲۶۴	مبانی پروتکل کنترل انتقال اطلاعات یا پروتکل اینترنت
۲۶۵	اهمیت لایه‌ها در سایبر فارتیک شبکه
۲۶۶	منابع اطلاعاتی در ترافیک شبکه
۲۶۷	فایروال و مسیریاب‌ها
۲۶۸	ردیاب‌های بسته‌های اطلاعاتی و تحلیل‌گر پروتکل
۲۶۹	سیستم تشخیص نفوذ
۲۷۰	دسترسی از راه دور
۲۷۱	نرم‌افزار مدیریت رویدادهای امنیتی
۲۷۲	ابزارهای تحلیلی سایبر فارتیک در محیط شبکه
۲۷۳	سایر منابع
۲۷۴	جمع‌آوری داده‌های ترافیک شبکه
۲۷۵	بررسی و تحلیل داده‌های ترافیک شبکه
۲۷۶	شناسایی رویداد مورد نظر
۲۷۷	بررسی منابع مختلف اطلاعات
۲۷۹	ارزش منابع اطلاعاتی
۲۸۲	ابزارهای بررسی و تحلیل
۲۸۳	نتیجه‌گیری
۲۸۴	شناسایی مهاجم
۲۸۸	توصیه‌هایی برای استفاده از اطلاعات حاصل از ترافیک شبکه
۲۸۸	کارشناسان سایبر فارتیک باید:
۲۸۹	به‌کارگیری داده‌های برنامه‌های کاربردی
۲۹۰	اجزای نرم‌افزاری
۲۹۰	تنظیمات پیکربندی
۲۹۱	اعتبارسنجی (تایید اعتبار)

۲۹۲	فایل‌های ثبتي
۲۹۴	فایل‌های اطلاعاتي (داده‌اي)
۲۹۵	فایل‌های پشتیبان
۲۹۵	انواع برنامه‌ها (نرم‌افزارها)
۲۹۶	پست الکترونيكي (ایمیل)
۲۹۷	استفاده از وب
۲۹۹	ارتباطات تعاملی
۳۰۱	استفاده از اسناد
۳۰۱	برنامه‌های امنیتی
۳۰۲	ابزارهای پنهان‌سازی اطلاعات
۳۰۲	جمع‌آوری داده‌های برنامه‌ها
۳۰۴	بررسی و تحلیل داده‌های برنامه‌ها
۳۰۴	توصیه‌هایی برای کارشناسان سایبر فارنژیک
۳۰۵	جمع‌بندی

فصل ۶: رویه‌های اجرایی استاندارد؛ استانداردهای مورد نیاز آزمایشگاه سایبر فارنژیک

۳۰۷	مقدمه
۳۰۸	استانداردهای تعیین صلاحیت آزمایشگاه‌های سایبر فارنژیک معیار درجه‌بندی
۳۰۹	پرسشنامه بازبینی رویه‌های اجرایی استاندارد
۳۱۱	پرسشنامه کنترلی مدیر آزمایشگاه
۳۱۳	پرسشنامه کنترلی بازرس سایبر فارنژیک
۳۱۴	پرسشنامه کنترلی متخصص فنی یا دستیار
۳۱۶	پرسشنامه کنترل بودجه
۳۱۶	پرسشنامه آزمون و آموزش
۳۱۸	پرسشنامه کنترل مدارک یا شواهد
۳۱۹	پرسشنامه تضمین کیفیت
۳۲۲	پرسشنامه تجهیزات
۳۲۴	پرسشنامه ایمنی و سلامت
۳۲۵	پرسشنامه تجهیزات آزمایشگاهی
۳۲۹	جمع‌بندی

فصل ۷: اجرای تحقیق سایبر فارنژیک

۳۳۱	مقدمه
۳۳۱	ترسیم مسیر در تحقیق
۳۳۲	کنترل یا رسیدگی داخلی چیست؟
۳۳۴	تحقیقات سایبر فارنژیک و کنترل داخلی
۳۳۵	

۳۳۶	پرسشنامه کنترل داخلی
۳۳۷	جرایم رایانه‌ای: پرسشنامه واکنش به رویداد و فارنزیك دیجیتالی
۳۳۷	هدف
۳۳۸	پرسشنامه عمومی واکنش به رویداد
۳۳۹	خلاصه‌ای از فهرست مراحل واکنش به رویداد
۳۴۲	پرسشنامه اختصاصی واکنش به رویداد
۳۴۳	پرسشنامه واکنش به رویداد مزاحمت
۳۴۳	پرسشنامه واکنش به رویداد ایجاد اختلال در خدمات‌دهی
۳۴۴	پرسشنامه واکنش به رویداد رمز مخرب
۳۷۰	پرسشنامه واکنش به رویداد - ارتباطات زیانبار
۳۷۸	پرسشنامه واکنش به رویداد - سوءاستفاده از منابع
۳۸۶	پرسشنامه رویداد ویروسی
۳۸۶	پرسشنامه گزارش تهاجم ویروسی
۳۸۷	کشف تهاجم ویروس در خدمات‌دهنده شبکه
۳۸۹	شناسایی ویروس در ایستگاه کاری
۳۸۹	پرسشنامه سازمانی
۳۹۳	پرسشنامه پس از رویداد
۳۹۵	تأییدیه

فصل ۸: سایبر فارنزیك و حریم خصوصی...

۳۹۷	مقدمه
۳۹۷	قوانین مربوط به حفظ حریم خصوصی
۳۹۸	قوانین غیرمردون (عرفی) حفظ حریم خصوصی
۳۹۸	پرونده سازمان پخش اخبار استرالیا و شرکت لنا میتز
۳۹۹	حفظ حریم خصوصی: مداخله قانونی
۴۰۰	قانون مربوط به دسترسی به اطلاعات شخصی
۴۰۱	دسترسی به اطلاعات نگهداری‌شده توسط دولت
۴۰۲	دسترسی به اطلاعات غیردولتی توسط بخش خصوصی
۴۰۳	مسئولیت قانونی و حقوقی در مورد اشتباهات
۴۰۶	جمع‌بندی
۴۰۷	

فصل ۹: جعبه ابزار سایبر فارنزیك

۴۰۹	مقدمه
۴۰۹	آماده‌سازی برای موفقیت
۴۱۰	آداپتور دیسک‌سخت لپ‌تاپ به دیسک‌سخت با درگاه IDE
۴۱۱	کارت توسعه‌دهنده اسکازی SCSI 29160
۴۱۳	

- ۴۱۴ ادابتور رابط اسکازی؛ ادابتور سیستم‌های رایانه‌ای کوچک
- ۴۱۵ ادابتور رابط عریض AEC-7720WP اسکازی به IDE با قابلیت جلوگیری از نوشته شدن
- ۴۱۶ فهرست تجهیزات سازگار
- ۴۱۷ تجهیزات فایر وایر آی‌دی‌ای و ساتا
- ۴۱۸ فایر وایر ساتا
- ۴۱۹ خواندن یا نوشتن تجهیزات فایرفلای
- ۴۲۰ ادابتور دیسک‌سخت ZIF به آی‌دی‌ای
- ۴۲۱ ادابتور تبدیل تجهیزات ساتا به آی‌دی‌ای
- ۴۲۲ دیگر ابزارها و تجهیزات مورد نیاز و ضروری
- ۴۲۵ ادابتور ADP31 تبدیل اسکازی ۳ به اسکازی ۱
- ۴۲۶ ادابتور ADP32 تبدیل اسکازی ۳ به High Density
- ۴۲۶ دستگاه Fastbloc جلوگیری از نوشتن
- ۴۲۷ مجموعه سخت‌افزاری Logicube
- ۴۲۷ دستگاه سیار Ultra Block
- ۴۲۸ ادابتورها و تجهیزات مربوط به دستگاه بازی ایکس‌باکس ۳۶۰
- ۴۲۹ نرم افزار
- ۴۳۰ جمع‌بندی

فصل ۱۰: تجهیزات چندمنظوره دیجیتال

- ۴۳۱ مقدمه
- ۴۳۲ ارزیابی محصولات
- ۴۳۵ امنیت داده‌ها و شواهد الکترونیکی احتمالی
- ۴۳۷ مسایل و نگرانی‌ها
- ۴۴۰ کارکنان فنی
- ۴۴۱ چگونگی عملکرد فرایندها
- ۴۴۲ کاربرد فارنژیک
- ۴۴۳ دسترسی به تجهیزات چندمنظوره
- ۴۴۳ فرآیند بررسی
- ۴۴۴ بررسی گام به گام دیسک‌سخت تجهیزات چندمنظوره
- ۴۴۵ هیچ مطلق وجود ندارد
- ۴۴۷ جمع‌بندی

فصل ۱۱: سایبر فارنژیک و قانون: ملاحظات حقوقی

- ۴۴۹ مقدمه
- ۴۵۰ اهداف
- ۴۵۰ مرزهای تعریف‌شده سایبر فارنژیک

۴۵۱	اطلاعات دیجیتالی
۴۵۲	شناسایی و تحلیل
۴۵۳	مشکل پیچیدگیِ فارنزیکِ دیجیتالی
۴۵۵	گسترش شواهد دیجیتالی
۴۵۵	فضای راکد
۴۵۶	فضای راکد حافظه رم
۴۵۷	فضای راکد درایو
۴۵۸	فایل‌های تبدیلی
۴۵۹	از قانون Frye تا قانون FER
۴۶۰	ماده چهارم، ارتباط و مرزهای آن
۴۶۱	تایید اعتبار (اعتبار سنجی)
۴۶۲	قانون شواهد اصیل
۴۶۲	ماده هفتم: نظرات و شهادت کارشناس
۴۶۴	تایید اعتبار با استفاده از قانون Daubert
۴۶۵	عوامل Daubert
۴۶۶	ثبت و ضبط (تصرف) و بازرسی رایانه
۴۶۷	حمله علوم ناخواسته
۴۶۹	زنجیره مراقبت از داده‌ها
۴۷۱	بی‌اعتبار ساختن شاهد (رد صلاحیت کارشناس سایبر فارنزیک)
۴۷۲	طرح کلی تحقیق
۴۷۶	اخذ مجوزهای مربوطه
۴۷۸	با چه کسی تماس خواهید گرفت؟
۴۷۸	مشاوران حقوقی برون‌سازمانی:
۴۸۰	ایمن‌سازی صحنه وقوع جرم الکترونیکی
۴۸۱	ضبط شواهد
۴۸۳	زنجیره شواهد
۴۸۵	الگوی زنجیره مراقبت از شواهد
۴۸۸	ضبط و توقیف رایانه
۴۸۹	مزایا و معایب قطع دستگاه
۴۹۲	جمع‌بندی

فصل ۱۲: سایبر فارنزیک و دگرگونی در بررسی اعمال مجرمانه

۴۹۳	مقدمه
۴۹۵	شواهد در قرن بیست و یکم
۴۹۶	تعریف جرایم رایانه‌ای
۴۹۸	جنبه‌های اقتصادی سایبر فارنزیک

- مشکلات عملی
شایستگی
دادرسی‌های هدفمند
برنامه‌ریزی برای پیگیری جرایم سایبری
تلاش‌های مشارکتی
توصیه‌ها
جمع‌بندی
- فصل ۱۳: داده‌های الکترونیکی و سایبر فارنزیک**
- عصر نوین اکتشاف
قوانین دادرسی مدنی - اصلاحیه‌های پیشنهادی
قوانین دولتی در مورد آیین‌های (دادرسی) مدنی؛ ۱ دسامبر ۲۰۰۶
آمادگی یا عدم آمادگی
جابه‌جایی هزینه‌ها
احتمال نیاز به داده‌های الکترونیکی، چقدر است؟
مدیریت اسناد چیست؟
مدیریت اسناد: مبانی
نگهداری همه‌چیز یا خیر!
برنامه‌ریزی برای نابودسازی اسناد
مدیریت اسناد - مهم اما فراموش شده
توجه خاص به جریان روزانه اسناد
استقرار یک برنامه مدیریت اسناد پویا
تأثیرات اصلاحیه‌های قوانین دادرسی مدنی بر خط‌مشی‌ها و شیوه‌های به کارگیری فناوری در سازمان‌ها
ارزیابی آمادگی سازمان: آیا آمادگی لازم برای کشف داده‌های الکترونیکی حاصل شده است؟
به خاطر داشته باشید تنها مسئله احتمالات مطرح نیست؛ بلکه زمان وقوع مطرح است.
فصل ۱۴: اطلاعاتی در زمینه سایبر فارنزیک؛ ارزیابی مدیریت
مقدمه
یکپارچگی نمونه آماری
تجزیه، تحلیل و بررسی یافته‌ها
جمع‌بندی
- فهرست اصطلاحات**
- پیوست (الف): پایگاه‌های اینترنتی مرتبط با سایبر فارنزیک**
پیوست (ب): سازمان‌های مرتبط با جرایم سایبری و فارنزیک

- پیوست (پ): فهرست مراکز آموزش سایبر فارنزیک ۶۰۹
- پیوست (ت): ۲۰ پرسش مهم در ارزیابی مدیریت ۶۱۵
- پیوست (د): معرفی روش‌های رمزنگاری ۶۱۷
- پیوست (ج): ابزارهای پنهان نگاری ۶۲۳
- پیوست (چ): منابع پیشنهادی و آموزشی سایبر فارنزیک ۶۲۹
- پیوست (ح): مکان‌یابی اطلاعات رجیستری ویندوز مورد کاربرد در سایبر فارنزیک ۶۳۳
- پیوست (خ): سرنام‌های واژگان به‌کار گرفته شده ۶۵۹

پیشگفتار

سایبر فارنزیک علمی است که از زمان ورود آن به جامعه ما مدت زیادی نمی‌گذرد و به همین دلیل جوانب ناشناخته آن هنوز برای ما فراتر از جنبه شناخته شده آن است. اما سایبر فارنزیک واقعا چیست؟ این کتاب دقیقاً به همین موضوع می‌پردازد و توضیحات متعددی برای تشریح این موضوع ارائه می‌دهد. اما آنچه در اینجا و در یک کلام می‌توان گفت این است که "سایبر فارنزیک علمی است نوین به منظور آموزش روش‌های شناسایی جرایم الکترونیکی و رایانه‌ای، جمع‌آوری و ارائه آن‌ها به مراجع قانونی". البته برای تحقق این مهم، مراحل و شرایط ویژه دیگری، لازم الاجرا هستند که این کتاب به همه آن‌ها می‌پردازد.

مانند هر فناوری سودآور دیگری، رایانه و عوامل مرتبط با آن در کنار سودمندی، مضراتی را نیز برای جامعه به همراه داشته‌اند و با توجه به قدرت، سرعت و میزان تاثیرگذاری رایانه بر جوامع امروزی این مضرات نیز به همین نسبت افزایش یافته‌اند. این عامل، نقطه شروعی برای شکل‌گیری دانش سایبر فارنزیک گردیده است.

اینکه جرم رایانه‌ای یا جرم دیجیتال شامل چه مواردی می‌تواند باشد موضوع گسترده‌ای است که درباره آن به تفصیل خواهیم خواند اما مطمئناً این مبحث به موارد ذکر شده محدود نمی‌شود و دامنه گسترده‌تری را در بر می‌گیرد؛ گرچه به محض شنیدن جرم رایانه‌ای ذهن بیشتر مردم به سمت سوءاستفاده‌های مالی منعطف می‌شود که بی‌دلیل هم نیست، زیرا بیش از نیمی از جرایم رایانه‌ای با هدف سوءاستفاده‌های مالی صورت می‌گیرد. اما جرایم رایانه‌ای موارد دیگری را نیز در بر می‌گیرند.

موضوع مهمی که توجه به آن اهمیت دارد و در این کتاب به آن پرداخته نشده است، موضوع تفکیک دانش سایبر فارنزیک از دانش‌های مرتبط و نزدیک به آن، مانند دانش برقراری امنیت یا راه‌های پیشگیری از وقوع جرایم این چنینی است. هرچند که در هنگام کسب دانش سایبر فارنزیک و مطالعه این کتاب چه به صورت مستقیم و چه به صورت مفهومی راه کارهایی برای ایمن‌سازی خواهید آموخت، اما دانش سایبر

فارنژیک ذاتاً از موضوع برقراری امنیت جداست. این دانش، در واقع سایبر فارنژیک به این موضوع می‌پردازد که اگر تحت هر شرایطی مجرم توانست از موانع امنیتی عبور کند و جرمی واقع شد، چه باید کرد و چه تصمیماتی باید گرفت؟ البته بدیهی است که کارشناسان امنیتی که با دانش سایبر فارنژیک آشنا هستند می‌توانند راه کارهای به مراتب بهتر و مناسب‌تری برای برقراری امنیت ارائه دهند.

برای به سرانجام رساندن پرونده‌ای با موضوع جرم رایانه‌ای به دانش‌های گسترده‌ای از قبیل آشنایی با رایانه، تجهیزات سخت‌افزاری، نرم‌افزار، الکترونیک، زبان انگلیسی، شِم کارآگاهی و عوامل متعدد دیگری نیاز است. در کنار این عوامل از آنجا که در نهایت این پرونده‌ها باید به مراجع قانونی ارائه شوند، اطلاع و حتی تسلط بر مسایل حقوقی و قانونی بسیار مهم و حتی الزامی است. چه بسیار پرونده‌هایی که با وجود تشخیص درست و کارشناسی صحیح، به دلیل لغزش یا کوتاهی در مراعات مسایل و تبعات حقوقی به سرانجام نرسیده‌اند. در متن این کتاب به تعدادی از چنین پرونده‌هایی اشاره شده است. با این توضیحات در می‌یابیم که این دانش بسیار و گسترده و نیازمند به همسویی با پیشرفت‌های روزانه فناوری است. کارشناسان این دانش، شخص ایده‌آل برای این حرفه را فردی متخصص در رشته رایانه می‌دانند که در این راستا، دانش سایبر فارنژیک رایانه را نیز کسب کرده، با مسایل حقوقی آشنا باشد و در کنار این عوامل روحیه کارآگاهی نیز داشته باشد.

شایان ذکر است که در کشورهای اروپایی و ایالات متحده چنین فعالیت‌هایی عمدتاً توسط بخش خصوصی و دانشگاه‌ها که در عین حال ارتباط رسمی با بخش دولتی یا پلیس را دارند انجام می‌شود. مطلب دیگری که توضیح آن ضرورت دارد، موضوع دو دستگی تالیف کتاب است که ممکن است تا حدودی در متن ترجمه شده نیز به چشم بخورد، هر چند که اینجانب تلاش کرده‌ام آن را به حداقل برسانم. در واقع متن اصلی کتاب توسط دو تن از کارشناسان رشته سایبر فارنژیک تالیف شده است که هرچند از نظر فنی پربار است اما به دلیل اینکه هیچکدام از این دو نفر زبان مادری‌شان انگلیسی نبوده، مشکلاتی را متوجه متن کرده‌اند و متأسفانه آن را در معرض ویراستاری ادبی قرار نداده‌اند! بنابراین چنانچه تلاش مترجم برای یکسان‌سازی، کاستی‌هایی دارد پیشاپیش از شما عذرخواهی می‌کنم. ضمناً لازم به ذکر می‌دانم که در ترجمه عبارات بنا را بر رعایت امانت گذاشته‌ام تا اهمیت موضوع و شیوه بیان از دیدگاه مولفین حفظ شود و حتی المقدور نکته ظریفی حذف نگردد.

البته شما خواننده عزیز باید در نظر داشته باشید که دانش رایانه و موضوعات مرتبط با آن از زمان تالیف و ترجمه تا انتشار این کتاب، دائماً در حال تغییر و توسعه بوده و خواهد بود، پس جرایم رایانه‌ای و پیرو آن سایبر فارنژیک نیز گسترده‌تر شده و نیازمند به روزرسانی دانش کارشناس است.

نکته بعدی مربوط به زیرنویس‌های کتاب است که هیچکدام مربوط به متن اصلی نیست و همگی توسط مترجم و به جهت درک بهتر مطالب ارائه شده است. خواهشمندم همه آن‌ها را مطالعه کرده تا متن اصلی را بهتر متوجه شوید. در مورد اصطلاحات به کار رفته در کتاب نیز باید گفت که تا حد ممکن تلاش شده

است از واژه‌های جایگزین و در عین حال رایج و قابل فهم استفاده شود. به همین دلیل گاهی از اصطلاحات اصلی که کاملاً رایج و معنا دار هستند به جای معادل نامانوس آن‌ها استفاده شده است. در پایان توصیه می‌کنم مطالب کتاب را حتماً به همین ترتیبی که توسط نویسندگان نگارش و ترجمه شده است مطالعه نمایید تا یکپارچگی مطالب حفظ شود.

با تشکر
امیر توکلی

www.ketab.ir