ادله الکترونیک با
Kali Linux

Digital Forensics with Kali Linux

Shiva V.N. Parasram

ترجمه: مهندس مهران تاجبخش

انتشارات پندار پارس

سرشناسه : پاراسرام، شیوا وی. ان.
Parasram, Shiva V.N.
عنوان و نام پدیدآور : ادله الکترونیک با Kali Linux/ [شیوا وی.ان پاراسرام] ؛ ترجمه مهران تاجبخش.
مشخصات نشر : تهران : پندار پارس ، ۱۳۹۷.
مشخصات ظاهری : ۲۰۲ ص.: مصور.
شابک : ۲۵۰۰۰۰ ریال978-600-8201-64-9:
وضعیت فهرست نویسی : فیپا
یادداشت : عنوان اصلی: DIGITAL FORENSICS WITH KALI LINUX, 2017.
موضوع : سیستم عامل لینوکس
موضوع : Linux
موضوع : نرم‌افزار کاربردی -- طراحی و توسعه
موضوع : Application software -- Development
شناسه افزوده : تاجبخش، مهران، ۱۳۴۷ -، مترجم
رده بندی کنگره : ۷۶/۷۶QA ۱۳۹۷ ۲پ۹۴س/
رده بندی دیویی : ۰۰۵/۴۳۲
شماره کتابشناسی ملی : ۵۲۳۷۱۲۸

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگرجنوبی، کوی رشتچی، شماره ۱۴، واحد ۱۶ **www.pendarepars.com**

تلفن: ۶۶۵۷۲۳۳۵ – تلفکس: ۶۶۹۲۶۵۷۸همراه: ۰۹۱۲۲۴۵۲۳۴۸ **info@pendarepars.com**

نام کتاب : **ادله الکترونیک با Kali Linux**

ناشر : **انتشارات پندار پارس**

تألیف : Shiva V.N. Parasram

ترجمه : **مهران تاجبخش**

چاپ نخست : **تیرماه ۹۷**

شمارگان : **۵۰۰ نسخه**

طرح جلد : **سارا یعسوبی**

چاپ، صحافی : **روز**

قیمت : **۲۵۰۰۰ تومان** **شابک : ۹-٦٤-۸۲۰۱-٦۰۰-۹۷۸**

تقدیم به رامتین، پسر عزیزم.

آینده متعلق به کسانی است که از امروز، خود را برای آن آماده می کنند.

فهرست

این کتاب برای چه کسانی است

مخاطبان این کتاب راهبران شبکه، سیستم و امنیت و همچنین مدیران امنیتی سازمان‌ها و ممیزان و مدیران فناوری اطلاعات و دانشجویان و محققان در حوزه امنیت و ادله الکترونیک و قانونی می‌باشند. در این کتاب با آخرین فناوری‌ها و روش‌های جمع‌آوری و بررسی ادله الکترونیک در فضای مجازی با استفاده از جدیدترین ابزارها و نرم‌افزارهای موجود آشنا خواهید شد.

پیش‌گفتار

امنیت در حوزه فناوری اطلاعات و فضای مجازی، گستره وسیعی را در بر می‌گیرد. استانداردها، روش‌ها و ابزارهای مورد استفاده در این حوزه را می‌توان به سه بخش، پیشگیری، عملیاتی و مقابله و برخورد تقسیم کرد. در بخش پیشگیری، از فناوری‌های مربوط به تست نفوذ استفاده می‌شود. در این بخش، هدف تست آسیب‌پذیری و قابلیت نفوذ به سیستم‌ها، ابزارها و نرم‌افزارهای مورد استفاده می‌باشد تا با شناسایی نقاط ضعف و آسیب‌پذیر، تا حدامکان آنها را برطرف کرده و یا کاهش دهیم. در بخش عملیاتی، به طور معمول ابزارها و فناوری‌های رصد و کنترل برخط سیستم و رخدادهای مربوط به آن مد نظر قرار دارند. هدف استفاده از این فناوری‌ها، محافظت سیستم در برابر حملات شناخته نشده و روز صفر می‌باشد و سرانجام در بخش مقابله با رخدادها و حملات، فناوری‌ها و ابزارهایی مورد استفاده قرار می‌گیرند که با استفاده از آنها، داده‌ها و اطلاعات به‌جا مانده از حمله و نفوذ و یا رخداد مورد نظر، جمع آوری، آنالیز و بررسی می‌شوند تا منشا و هدف حمله، عامل و میزان خسارات وارد شده مشخص شوند. این بخش همان فناوری ادله الکترونیک (Digital Forensics) می‌باشد.

فناوری ادله الکترونیک و موضوعات مربوط به آن چندان جدید نمی‌باشند و از دهه ۱۹۹۰ این فناوری برای نخستین بار مطرح شد، اما از سال ۲۰۰۰ میلادی به بعد، ایجاد انجمن‌ها و مؤسسات تخصصی در این حوزه و ورود سازمان‌ها و ارگان‌های انتضامی و قانونی به موضوع ادله الکترونیک، نشانه اهمیت و لزوم توجه به این بخش از امنیت فناوری اطلاعات و فضای مجازی است.

از آن زمان تاکنون، استانداردهای مختلفی در حوزه ادله الکترونیک و قانونی و بخش‌های مختلف آن، اعم از جمع آوری داده‌ها و اطلاعات، نگهداری آنها و بررسی و آنالیز و در نهایت تهیه گزارش ارائه شده‌اند.

مهمترین بخش در حوزه ادله الکترونیک، مربوط به آنالیز و بررسی تخصصی داده‌ها و شواهد جمع آوری شده از صحنه جرم است. این بخش، از پیچیدگی‌های مخصوص به‌خود برخوردار می‌باشد. مهمترین چالش پیش روی متخصص ادله الکترونیک در بخش آنالیز و بررسی شواهد و ادله به‌جای مانده، مربوط به شمار زیاد ابزارها، فناوری‌ها و نرم‌افزارهای مورد استفاده توسط کاربران، سیستم‌ها و شبکه‌های سازمان‌ها و همچنین عدم مستندسازی کامل و دقیق آنها می‌باشد.

هم اینک بسیاری از نرم افزارها و ابزارهای مورد استفاده، متن باز نبوده و مستندات دقیق و کاملی از ساختار داخلی و فرمت و قالب داده‌های مورد استفاده و چگونگی ارتباط بین بخش‌های مختلف آن، در دسترس نمی‌باشند، به‌همین دلیل متخصص ادله الکترونیک باید با استفاده از تجربه و ابزارهای تخصصی بررسی و آنالیز ادله الکترونیک، داده‌ها و شواهد مورد نیاز خود را از آنها استخراج کرده و نتیجه‌گیری‌های لازم از آنها را در قالب گزارش ارائه کند.

در کتاب سعی کرده‌ایم تا علاوه بر معرفی این فناوری، استانداردها، روش‌ها و ابزارهای مورد استفاده در این حوزه را معرفی کرده و به صورت عملی مراحل اجرای پرونده ادله الکترونیک را ارائه کنیم.

مطالعه این کتاب را به همه متخصصان حوزه امنیت اطلاعات و فضای مجازی و راهبران سیستم و امنیت شبکه سازمان‌ها توصیه می‌کنیم.

در باره مترجم

با بیش از ۲۶ سال سابقه تدریس در حوزه فناوری اطلاعات و شبکه در حدود ۱۰ سال است که به طور تخصصی در حوزه آموزش، مشاوره و اجرای پروژه‌های مربوط به امنیت شبکه و فضای مجازی و تست نفوذ و ادله الکترونیک و ارائه خدمات آموزش و مشاوره در حوزه پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISO27001) فعالیت دارد که حاصل آن مدارک بین المللی متعددی در حوزه شبکه، امنیت شبکه و تست نفوذ به شرح زیر می‌باشد:

Network+, CCNA, CCNP, CCNA Security, CCNP Security, Security+, CIW Security Professional, ISO27001 Lead Auditor, MCP - Microsoft Certified Professional (2016), MCT – Microsoft Certified Trainer

در صورت نیاز به برقراری ارتباط با وی می‌توانید از طریق رایانامه زیر اقدام نمایید:

info@mehrantajbakhsh.com

فصل نخست

مقدمه‌ای بر ادله الکترونیک

از ۱۳ سال پیش، یعنی زمانی که نخستین رایانه شخصی خود را داشتم، توجه خاصی به موضوع ادله الکترونیک پیدا کردم و همواره از خود سوال می‌کردم که چه اتفاقی برای فایل‌هایی که پاک می‌کنیم و یا آنها را بر روی فلاپی دیسک ۳/۵ اینچی جابجا می‌کنیم، می‌افتد.

پس از آن یاد گرفتم که هارددیسک‌ها و فلاپی دیسک‌ها توانایی نگهداری مادام العمر داده‌ها و اطلاعات دیجیتال ما را ندارند. ممکن است برای شما هم همین تجربه رخ داده باشد که برخی از فایل‌های‌تان پس از ذخیره‌سازی گم شده و یا از دست رفته باشند و امکان بازیابی و دسترسی مجدد به آنها را نداشته‌اید.

برای درک واقعیت رخدادهایی که بر روی فایل‌ها در هنگام ذخیره‌سازی و بازیابی و انتقال آنها می‌افتد، سراغ اینترنت رفته و در آنجا به دنبال پاسخی برای این سوالات گشتم. آن زمان به اندازه امروز اطلاعات مختلف در این بخش در کتاب‌ها و مقالات و مجلات مختلف در فضای مجازی وجود نداشت. اما به هر شکلی که بود توانستم اطلاعات کاملی در مورد سیستم‌های ذخیره‌سازی فایل‌ها و مکانیزم‌های ذخیره‌سازی اطلاعات بر روی دیسک و حافظه‌های مغناطیسی را بدست آورم.

در این زمان بود که با سیستم‌عامل لینوکس و توزیع‌های مختلف آن آشنا شدم و سعی کردم تا دلیل محبوبیت این سیستم‌عامل در عملیات بازیابی و بررسی ادله الکترونیک را پیدا کنم.

در این زمان دو توزیع لینوکس Auditor و Slax را دانلود کردم. البته در آن زمان به دلیل اینکه روندهای نصب ساده با رابط‌های کاربری گرافیکی نظیر آنچه که امروز آنها را مشاهده می‌کنیم، وجود نداشت، در نصب و فعال‌سازی این سیستم‌عامل با سختی‌ها و دشواری‌های زیادی روبرو شدم. در مورد این دو توزیع لینوکس، در فصل دوم بیشتر صحبت خواهم کرد.

با گذشت زمان، سعی کردم تا در مورد ابزارهایی که در سیستم‌عامل‌های مختلف نظیر ویندوز و مکینتاش و توزیع‌های مختلف لینوکس وجود دارند، تحقیق و بررسی کنم. با این‌کار متوجه شدم که ابزارهای متنوع‌تر و کامل‌تری برای استفاده در کاربردهای بررسی و تحقیق ادله الکترونیک در توزیع‌های مختلف لینوکس یافت می‌شوند. در میان توزیع‌های مختلف لینوکس، Kali یکی از توزیع‌هایی است که به‌طور مشخص برای چنین کاربردهایی طراحی و ارائه شده است و توسط کارشناسان موجود در این بخش مورد تأیید قرار گرفته است. پیش از اینکه در مورد این توزیع لینوکس صحبت کنیم، اجازه دهید تا در مورد تفاوت‌هایی که بین توزیع‌های مختلف لینوکس وجود دارد، توضیحاتی را ارائه کنم. در صورتی‌که سیستم‌عامل لینوکس را به عنوان یک نوشیدنی در نظر بگیرید، انواع مختلفی از آن می‌تواند تهیه و ارائه شود، مانند با شکر و یا بدون شکر و در رنگ‌های مختلف و یا اندازه‌های گوناگون. ورای ظاهر و تغییراتی که در آن ایجاد شده است، در همه انواع

آنها، اصل همان نوشیدنی است که در ابتدا داشتیم. در مورد سیستم‌عامل لینوکس نیز همان‌گونه است. وقتی در مورد توزیع‌های مختلف آن صحبت می‌کنیم، در واقع همگی دارای هسته اصلی مشابه و یکسانی می‌باشند که بر روی آن تغییراتی در رابط کاربری و ابزارها و نرم‌افزارهای موجود در آن داده شده است. از توزیع‌های مهم و پرکاربرد سیستم‌عامل لینوکس، می‌توانیم به مواردی چون RedHat و CentOS و Ubuntu و Mint و Knoppix و البته Kali اشاره کنیم. در مورد توزیع کالی در فصل دوم بیشتر صحبت خواهیم کرد.

در این کتاب سعی خواهیم کرد که به شکلی کاملا ساخت‌یافته به موضوع جمع‌آوری و بررسی ادله الکترونیک بپردازیم. در ابتدا سعی خواهیم کرد تا شما را با مفهوم ادله الکترونیک و موضوعات مربوط به آن آشنا کنیم و سپس به ابزارها و سیستم‌عامل‌هایی که در این حوزه مورد استفاده قرار می‌گیرند، خواهیم پرداخت و در ادامه به روش‌های جمع‌آوری و نگهداری و بررسی ادله الکترونیک می‌پردازیم.

اکنون از بیان مقدمه می‌گذریم و به موضوعاتی که در این فصل به آنها خواهیم پرداخت، اشاره می‌کنیم.

عناوینی که در این فصل در موضوع علم ادله الکترونیک ارائه می‌شوند، عبارتند از:

- ادله الکترونیک چیست؟
- روش‌های مورد استفاده در بررسی ادله الکترونیک.
- تاریخچه مختصری از ادله الکترونیک.
- نیاز به علم ادله الکترونیک با پیشرفت علم و فناوری
- ضد ادله الکترونیک: تهدیدهای ادله الکترونیک
- ابزارهای تجاری در حوزه جمع‌آوری و بررسی ادله الکترونیک
- ابزارهای متن باز
- سیستم‌عامل‌هایی که دارای ابزارهای داخلی جمع‌آوری و بررسی ادله الکترونیک می‌باشند.
- نیاز به استفاده از ابزارهای مختلف در بررسی ادله الکترونیک برای ایجاد توانایی و اعتمادپذیری بیشتر در روند عملیات.

ادله الکترونیک چیست؟

نخستین چیزی که در این فصل به آن می‌پردازم، تعریفی از علم ادله الکترونیک و کاربردها و رویه‌های موجود در آن می‌باشد، در کنار آن می‌توانید به تارنماها و وبلاگ‌ها و یا ویدیوهای مختلفی در این زمینه مراجعه کنید. به هر شکل برای شروع لازم است که تعریفی دقیق و کامل از فناوری ادله الکترونیک به عنوان یک علم که دارای مستندات دقیق و کاملی از روندها و روش‌های موجود برای شناسایی ادله و آثار الکترونیک موجود است را بدست آورید.

ادله الکترونیک در حوزه جمع‌آوری و نگهداری و مستندسازی و تحلیل و بررسی و تفسیر رخدادها و شواهد موجود در انواع مختلف رسانه در حوزه دیجیتال مورد استفاده قرار می‌گیرد. این موضوع تنها محدود به رایانه‌ها و لپ‌تاپ‌ها و تبلت‌ها و سیستم‌های همراه نمی‌شود و به بخش‌هایی نظیر انتقال داده‌ها در شبکه‌های خصوصی و عمومی نیز مربوط می‌شود.

در بیشتر موارد، علم ادله الکترونیک به موضوعاتی مانند کشف و بازیابی داده‌ها با استفاده از روش‌ها و ابزارهای مختلف مربوط می‌شود. بررسی و تحقیق ادله الکترونیک به موضوع‌های زیر می‌پردازد (البته تنها محدود به این موارد نمی‌شود):

- **بازیابی داده (Data recovery):** بررسی و بازیابی داده‌ها که ممکن است حذف شده، تغییر داده شده و یا حتی مخفی شده باشند.
- **سرقت هویت (Identity theft):** بسیاری از فعالیت‌های مجرمانه، از استفاده غیر مجاز از کارت اعتباری تا ایجاد و استفاده غیرمجاز از پروفایل‌های شخصی غیر واقعی در شبکه‌های اجتماعی، همگی از مواردی هستند که در حوزه سرقت هویت قرار می‌گیرند.
- **تحقیق و بررسی در مورد بدافزارها و باج‌افزارها(Malware and ransomware investigations):** هم اینک باج افزارها با استفاده از بدافزارهایی مانند تروجان‌ها و کرم‌ها در شبکه‌ها و اینترنت منتشر می‌شوند و یکی از بزرگترین تهدیدها برای سازمان‌ها و شرکت‌ها محسوب می‌شوند.
- **بررسی تحقیق در ترافیک شبکه و اینترنت (Netwrok and Internet investigations):** در این حوزه ترافیک شبکه برای وجود تهدیدها و حمله‌هایی مانند DoS[1] و DDoS[2] بررسی و آنالیز می‌شود. این نوع حملات می‌توانند در شبکه‌های مختلف باعث از کارفتادن تجهیزات و عدم امکان دسترسی به فایل‌ها و نرم‌افزارهای کاربردی مختلف شوند.
- **بررسی ایمیل (Email investigations):** در این بخش اطلاعات مربوط به فرستنده ایمیل و محتوای ضمیمه آن و اطلاعات مربوط به موقعیت مکانی ارسال و یا دریافت آن مد نظر می‌باشند.
- **جاسوسی تجاری از شرکت‌ها (Corporate espionage):** امروزه بسیاری از شرکت‌ها از مستندسازی کاغذی چشم پوشی کرده و داده‌ها و اطلاعات خود را در رسانه‌های پیشرفته‌ای مانند فضاهای ابری نگهداری می‌کنند. در هر شرایطی امکان دارد که دسترسی‌های غیرمجاز به اطلاعات یابند و بر روی این اطلاعات حساس و مهم دسترسی‌های خراب‌کارانه و یا جاسوسی صورت گیرد.

---

[1] Denial of Services
[2] Distributed Denial of Services

- **بررسی و تحقیقات پورنوگرافی از کودکان (Child pornography investigations):** متاسفانه، در حال حاضر کودکان، هدف سوءاستفاده‌های جنسی مختلف در اینترنت و شبکه Deep Web می‌باشند. با استفاده از ابزارها و روش‌های دقیق و به‌روز در حوزه ادله الکترونیک می‌توانیم با بررسی ترافیک و تاریخچه مرورگرها و تراکنش‌های مالی و ایمیل‌های ثبت شده و تصاویر بدست آمده، منشا و روش انجام این جرائم را مشخص کنیم.

تاریخچه مختصری از ادله الکترونیک

هر چند علم بررسی صحنه جرم (پیدا کردن نخستین آثار انگشت و شواهد از صحنه جرم) علم جدیدی نیست و بیش از ۱۰۰ سال سابقه دارد، اما علم ادله الکترونیک که همین موضوع را در فضای دیجیتال بررسی می‌کند، علمی نوپا و جدید می‌باشد و عمر آن به زمانی که رایانه‌های شخصی در اوایل دهه ۸۰ ارائه شدند، مربوط می‌شود.

همانگونه که اشاره شد، علم ادله الکترونیک بسیار تازه و نوپا می‌باشد، اما باید در نظر داشته باشیدکه نخستین آزمایشگاه جرم شناسی علمی در سال ۱۹۳۲ توسط اف‌بی‌آی تأسیس شد.

نخستین ابزارهایی که برای بررسی ادله الکترونیک مورد استفاده قرار گرفتند، توسط اف‌بی‌آی در سال ۱۹۸٤ ارائه شدند و نخستین تیمی که مسئولیت بررسی ادله الکترونیک را بر عهده داشتند با نام CART[1] خوانده می‌شدند که توسط اف‌بی‌آی برای این منظور آموزش دیده بودند.

علم ادله الکترونیک و موضوعات مرتبط با آن در دهه ۱۹۹۰ رشد چشمگیری پیدا کردند، این تحول با کمک برخی از سازمان‌های قضایی و قانونی که وظیفه قانونگذاری در این حوزه را بر عهده داشتند، امکان‌پذیر شد.

یکی از نخستین کنفرانس‌هایی که در حوزه ادله الکترونیک برگزار شد، در سال ۱۹۹۳ توسط اف‌بی‌آی بود که عنوان آن "کنفرانس بین اللملی الزامات قانونی در حوزه رخدادهای رایانه‌ای"[2] بود و هدف از آن بررسی نیازها و الزام‌های قانونی در روند بررسی و جمع‌آوری ادله الکترونیکی و قانونی بود.

برای شکل‌گیری آیین نامه‌ها و قانون‌های مورد نیاز برای بررسی و جمع ادله الکترونیکی، سازمان‌ها و مؤسسات متعددی شکل گرفتند. به عنوان مثال، در سال ۱۹۹۸ مؤسسه SWGDE[3] توسط برخی از مدیران اف‌بی‌آی شکل گرفت. مؤسسه SWDGE برخی از مهمترین راه کارها و روش‌های بررسی و جمع‌آوری ادله الکترونیک که در ادامه این فصل به آنها اشاره خواهیم کرد را ارائه کرده‌اند. این مؤسسه با مؤسسات دیگری نیز ارتباط و همکاری داشته، که از آن جمله می‌توان به مؤسسه معتبر ASCLD[4] اشاره کرد که در سال ۱۹۷۳ ایجاد شده بود و وظیفه آن ارائه راه‌کارها و روش‌های بررسی علائم و نشانه‌های موجود در صحنه جرم می‌باشد.

---

[1] Computer Analysis and Response Team
[2] International Law Enforcement Conference on Computer Evidence
[3] Scientific Workgroup on Digital Evidence
[4] American Society of Crime Laboratory Directors

در اوایل دهه ۲۰۰۰ مؤسسه RCFL[1] توسط اف‌بی‌آی تاسیس گردید. در سال ۲۰۰۲ سازمان NPO[2] به عنوان سازمان مرکزی برای برنامه‌ریزی و مدیریت و پشتیبانی مؤسسه RCFL و سایر سازمان‌ها و ارگان‌های قضایی و قانونی تأسیس شد.

از آن پس در بسیاری از سازمان‌ها مانند FBI و CIA و NSA و GCHQ بخش ویژه‌ای برای بررسی و جمع‌آوری ادله الکترونیک ایجاد شد و همین امر باعث شد که ابزارها و فناوری‌های مورد استفاده در بخش جمع‌آوری و بررسی ادله الکترونیک به سرعت پیشرفت کنند و حوزه فعالیت این فناوری، از کامپیوترهای شخصی به اینترنت و حتی شبکه سیاه[3] نیز گسترش پیدا کند.

با پیشرفت فناوری ادله الکترونیک، ابزارهای مربوط به جمع‌آوری آنها نیز باید پیشرفت کنند تا بتوانند با جرائم پیشرفته فضای مجازی مقابله کنند و همچنین قابلیت بررسی و کشف و دسترسی به اطلاعات و داده‌های از دست رفته در صحنه جرم را فراهم کنند. در این مسیر، راه طولانی از فلاپی دیسک‌ها و دیسک‌های مغناطیسی و دسترسی به اینترنت از طریق خطوط تلفن و شماره گیری (Dialup) تا امروزه که زمان استفاده از حافظه‌های SD و اینترنت بر روی فیبر نوری با سرعت‌های گیگابیتی می‌باشد، طی شده است.

نیاز به علم ادله الکترونیک با پیشرفت فناوری

بسیاری از افراد با تجربه و دارای سابقه در حوزه فناوری اطلاعات، روزهایی را که در آنها از سیستم‌عامل‌های ویندوز ۹۵ و ویندوز 3.x و یا حتی DOS استفاده می‌کردیم به خاطر دارند. ساعت‌های هوشمند، ماشین‌های حساب و بسیاری از تجهیزات دارای قابلیت اینترنت اشیاء[4] (IoT) دارای سرعت‌ها و قابلیت‌های بسیار بیشتر و پیشرفته‌تری نسبت به آنچه که در آن روزها در رایانه‌ها وجود داشت و استفاده می‌شد، برخوردار می‌باشند. در سال ۱۹۹۵، دیسک‌های سخت مورد استفاده دارای فضاهایی بین ۴ گیگابایت تا ۱۰ گیگابایت بودند، اما اکنون استفاده از دیسک‌های سخت ۲ترابایتی به امری پیش پا افتاده و عادی تبدیل شده است.

انواع مختلفی از رسانه‌های ذخیره‌سازی اطلاعات، که امروزه مورد استفاده قرار می‌گیرند را در نظر بگیرید، مانند فلش دیسک‌ها و کارت‌های SD و انواع لوح‌های فشرده و دیسک‌های SSD، و آنها را با فلاپی دیسک‌هایی که قبلا مورد استفاده قرار می‌گرفتند و تنها ظرفیت ذخیره‌سازی ۱/۴ مگابایت اطلاعات را داشتند، مقایسه کنید، که با جزئیات بیشتر در ادامه این فصل شرح داده خواهند شد، اکنون با توجه به فناوری‌ها و تجهیزات موجود، نه تنها گزینه‌های بیشتری را برای ذخیره‌سازی اطلاعات و داده‌های‌مان در اختیار داریم، به همان اندازه نیز میزان تهدید در خرابی و از دست دادن اطلاعات نیز افزایش پیدا کرده است.

با پیشرفت فناوری، شناخت عمیق‌تر از زبان‌های برنامه نویسی و امکانات و قابلیت‌های موجود در سیستم‌های عامل نیز بیشتر شده است و در این شرایط دانش استفاده و کاربرد تجهیزات الکترونیک و دیجیتال نیز افزایش یافته است. برخی افراد در استفاده از این فناوری‌ها و تجهیزات، از رابط‌های کاربری ساده و گرافیکی استفاده

---

[1] Regional Computer Forensics Laboratory
[2] National Program Office
[3] Dark Web
[4] Internet of Things

می‌کنند، در حالی که برخی کاربران حرفه‌ای‌تر ترجیح می‌دهند تا از رابط‌های کاربری ساده‌تر و غیرگرافیکی استفاده کنند. امروزه با توجه به ابزارهای مختلفی که در فضای مجازی و اینترنت یافت می‌شوند و دارای رابط‌های کاربری ساده و گرافیکی نیز می‌باشند، امکان مخفی کردن و خراب‌کاری در داده‌ها و اطلاعات بسیار ساده‌تر و سریع‌تر از پیش، قابل انجام می‌باشند.

مخفی کردن حجم زیادی از داده‌ها و اطلاعات در حال حاضر بسیار ساده‌تر از گذشته انجام می‌شود، دلیل آن سرعت بیشتر پردازشگرها به همراه حجم حافظه اصلی بیشتر مورد استفاده توسط آنها می‌باشد. همه این شواهد می‌توانند قانون مور[1] را تأیید کنند که وی در آن اشاره کرده است که در هر سال قدرت پردازش دوبار افزایش پیدا می‌کند.

البته در این میان نیز جنسن هوانگ[2]، مدیرعامل شرکت NVIDIA، بیان کرده است که قانون مور باید به جای استفاده از CPU، به استفاده از GPU تغییر کند، زیرا کارآیی و بازدهی GPUها امروزه، باعث شده است که در اغلب کاربردهای هوش مصنوعی از آنها استفاده شود. البته این گفته هوانگ را برایان کرزانیک[3] مدیرعامل شرکت اینتل نیز تکرار کرده است.

با توجه به همه مواردی که در بالا به آنها اشاره شد، اکنون می‌توانیم مشاهده کنیم که راه‌های متعددی برای ارتکاب جرائم رایانه‌ای در دسترس می‌باشند، که می‌توانند با استفاده از بدافزارها، باج افزارها و حملات DoS و DDoS و جاسوسی صنعتی و ایمیل‌های گول زننده و قلابی و سرقت هویت و سرقت داده‌ها و اطلاعات و انجام فعالیت‌های آنلاین مخرب اجرا شوند. بسیاری از این فعالیت‌ها به صورت نامحسوس و گمنام از طریق اینترنت انجام می‌شوند و این‌کار معمولا با مخفی کردن IP آدرس در شبکه‌های عمومی و اینترنت انجام می‌شوند، همین امر باعث می‌شود که عملیات بررسی و جمع‌آوری ادله و شواهد الکترونیک بسیار پیچیده‌تر و دشوارتر از گذشته شوند.

با توجه به حجم جرائم فضای مجازی و گسترش روزافزون آنها از جنبه تعداد و همچنین سطح فناوری و پیچیدگی آنها، ما را ملزم می‌کند که برای انجام عملیات بررسی و تحقیق درست و دقیق و سریع و کارآمد، سازمان‌هایی با تیم‌های تخصصی آموزش دیده و با در اختیار داشتن ابزارهای به‌روز و قابل اعتماد ایجاد کنیم.

علم ادله الکترونیک نه تنها برای رسانه‌های ذخیره‌سازی اطلاعات مورد استفاده قرار می‌گیرد بلکه در مورد ترافیک شبکه و اینترنت و دستگاه‌های موجود در شبکه اینترنت اشیا، و به طور کلی هر دستگاه و ابزاری که می‌تواند داده‌ها و اطلاعات را ذخیره کند و یا انتقال دهد، نیز به‌کار برده می‌شود. به همین دلیل در این فناوری ابزارها و نرم‌افزارهای مختلف و گوناگونی وجود دارند که با توجه به شرایط و موقعیت و نوع کاربرد می‌توانند مورد استفاده قرار گیرند.

---

[1] Moore Law (1970s)
[2] Jensen Huang
[3] Brian Krzanic

ابزارهای تجاری در زمینه ادله الکترونیک

هرچند که در این کتاب تمرکز بر روی ابزارهای موجود در سیستم‌عامل کالی لینوس می‌باشد، اما در این بخش برخی از معروفترین ابزارهای تجاری که در زمینه جمع‌آوری و بررسی و تحقیقات الکترونیک مورد استفاده قرار می‌گیرند را معرفی می‌کنیم. در زیر فهرست این ابزارها را به ترتیب الفبایی مشاهده می‌کنید:

- EnCase® Forensic: https://www.guidancesoftware.com/encase-forensic
- F-Response: https://www.f-response.com/
- Forensic Toolkit: http://accessdata.com/products-services/forensic-toolkit-ftk
- Helix Enterprise: http://www.e-fense.com/h3-enterprise.php
- Magnet Axiom: https://www.magnetforensics.com/computer-forensics/
- X-Ways Forensics: http://www.x-ways.net/forensics/index-m.html

اغلب این ابزارهای تجاری امکان استفاده از همه قابلیت‌های زیر را به همراه برخی از قابلیت‌های اختصاصی مربوط به خود در اختیارمان قرار می‌دهند:

- مسدود کردن ثبت اطلاعات
- کپی برداری بیت-به-بیت و یا جریان بیت[1] و نسخه‌برداری از دیسک و نسخه‌برداری از فضای ذخیره‌سازی به عنوان شاهد
- جمع‌آوری شواهد و ثبت رخدادها به صورت مورد تأیید برای ادله الکترونیک
- حفظ و نگهداری مشمولیت رخدادها و شواهد با استفاده از رمزنگاری hash
- بازیابی فایل‌های پاک شده و مخفی
- جمع‌آوری زنده و از راه دور شواهد و رخدادهای صحنه جرم
- بررسی اطلاعات موجود در حافظه اصلی و حافظه مجازی
- بارگذاری تصاویر از انواع و با قالب‌های مختلف
- امکان جستجو و فیلترینگ پیشرفته بر روی داده‌ها و شبه داده‌ها
- نشانه گذاری فایل‌ها و سکتورهای موجود بر روی فضای ذخیره‌سازی
- رمزگشایی hash و رمزهای عبور
- تولید خودکار گزارش تحقیق و بررسی ادله الکترونیک

اصلی‌ترین مزیت ابزارهای تجاری در زمینه ادله الکترونیک این است که معمولا عملیات مربوط به جمع‌آوری و بررسی ادله الکترونیک را به صورت خودکار و بسیار ساده انجام می‌دهند و معمولا از مجموعه‌ای از ابزارهای مختلف که در ارتباط با یکدیگر قرار گرفته‌اند، تشکیل شده‌اند که می‌توانند روند عملیات جمع‌آوری، نگهداری و بررسی و تهیه گزارش را از ابتدا تا انتها انجام دهند. مزیت دیگر امکان استفاده از پشتیبانی مربوط به هر یک از آنها در صورت خریداری لایسنس استفاده از هر یک از نسخه‌های آنها می‌باشد. گروهی که این نوع

[1] Bit-stream

ابزارها را تولید می‌کنند، همواره در حال تحقیق و بررسی و آزمایش ابزارهای خود می‌باشند تا با توجه به نیازها و آخرین روش‌های حمله، نفوذ، تهدید و ارتکاب جرم در فضای مجازی بتوانند به شکلی مناسب و قابل قبول مورد استفاده قرار گیرند.

سیستم‌های عامل و ابزارهای متن باز ادله الکترونیک

علی‌رغم اینکه ابزارهای تجاری در حوزه ادله الکترونیک وجود دارند، بسیاری از ابزارها نیز در این حوزه به صورت متن باز بوده که می‌توانند توسط متخصصان و افراد آماتور برای جمع‌آوری، نگهداری و بررسی و تهیه گزارش ادله الکترونیک مورد استفاده قرار گیرند. اغلب این ابزارها در سیستم‌عامل لینوکس تعبیه شده‌اند و به صورت توزیع‌های خاص این سیستم‌عامل برای استفاده در زمینه ادله الکترونیک ارائه شده‌اند.

اصلی‌ترین پرسشی که در انتخاب ابزار مورد نظرمان مطرح می‌شود، این است که نوع تجاری و یا نوع متن باز را انتخاب کنیم. البته در شرایط کلی باید ورای نوع ابزار متن باز و یا تجاری، نتیجه یکسانی را در نهایت بدست آوریم، و البته در همه آنها نگهداری شواهد و ادله به طور صحیح و با حفظ تمامیت و مشمولیت در اولویت نخست قرار دارند.

بودجه مربوط به تهیه ابزارهای مورد نظر در اغلب موارد، عاملی تعیین کننده در انتخاب نوع ابزار تجاری می‌باشد (مانند اینکه ابزاری دقیق‌تر و سریع‌تر و با رابط کاربری کامل‌تر و راحت‌تری داشته باشد)، با توجه به شرایط مختلف، این ابزارهای تجاری در برخی موارد هزاران دلار ارزش دارند.

ابزارهای متن باز، رایگان بوده و بر اساس لایسنس‌های مختلفی که مربوط به این نوع نرم‌افزارها می‌باشند، ارائه می‌شوند و نباید صرفا به این خاطر که معمولا مورد پشتیبانی یک سازمان و یا تیم تخصصی خاصی قرار ندارند، از آنها استفاده نکنیم. بسیاری از ابزارهای متن باز بارها توسط انجمن‌ها و مؤسسات فعال در حوزه ادله الکترونیک مورد بررسی و آزمایش قرار گرفته‌اند و به خاطر اینکه دارای برنامه متن باز می‌باشند، بررسی‌های موشکافانه‌تری نیز بر روی آنها انجام شده است.

هر چند که تمرکزمان در این کتاب بر روی کالی لینوکس به عنوان توزیعی از سیستم‌عامل لینوکس که دارای ابزارهای مورد نیاز برای انجام همه عملیات مورد نیاز در یک پرونده ادله الکترونیک می‌باشد، اما توزیع‌های دیگری از این سیستم‌عامل نیز وجود دارند که می‌توانیم از آنها نیز در این زمینه استفاده کنیم.

هر یک از توزیع‌های لینوکس که در ادامه به آنها اشاره می‌کنیم به طور رایگان می‌توانند مورد استفاده قرار گیرند و می‌توانید آنها را از تارنماهای مختلفی تهیه کنید، اما به دلایل امنیتی لینک مستقیم مربوط به تارنمای اصلی آنها را ارائه می‌کنیم تا در صورت تمایل از آنها برای دریافت سیستم‌عامل مورد نظر اقدام کنید. سیستم‌عامل‌های ارائه شده در این بخش به ترتیب الفبایی می‌باشند:

توزیع DEFT[1]

توزیع لینوکس DEFT در دو نسخه کامل و خلاصه که به آن DEFT Zero گفته می‌شود، ارائه شده است. برای کاربردهای ادله الکترونیک معمولا ترجیح می دهیم که از نسخه کامل آن استفاده کنیم، زیرا نسخه خلاصه آنها عملیات ادله الکترونیک بر روی سیستم‌های همراه و همچنین کرک کردن رمزهای عبور را پشتیبانی نمی‌کند.

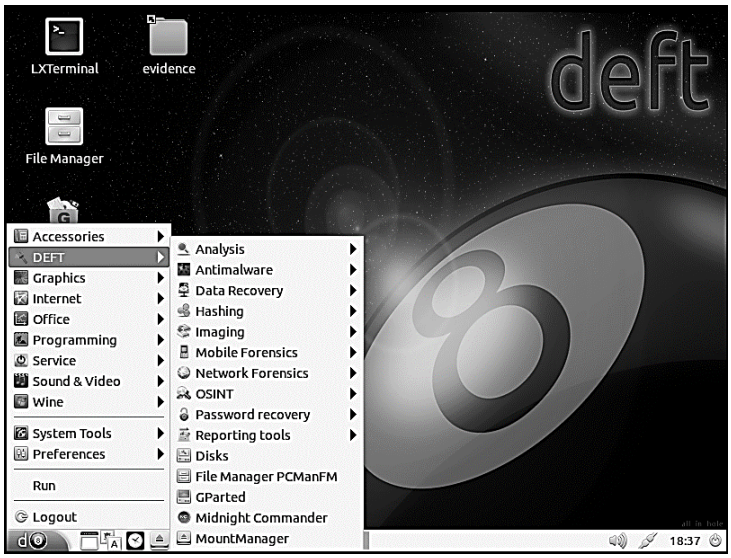
- **صفحه اصلی تارنما:** http://www.deftlinux.net/about/
- **مبتنی بر توزیع لینوکس :** Ubuntu Desktop
- **نوع توزیع:** ادله الکترونیک و ثبت رخدادها

همانند سایر توزیع‌های لینوکسی که در این بخش به آنها اشاره می‌کنیم، DEFT دارای صفحه رابط کاربری همانند شکل زیر می‌باشد، در این توزیع ابزارهایی برای بررسی ادله الکترونیک در مواردی که سیستم مورد نظر روشن بوده و امکان خاموش شدن را ندارد، وجود دارد و همچنین ابزارهایی برای بررسی محتوای جاری در حافظه اصلی و حافظه مجازی سیستم هدف، در آن پیش بینی شده است:

زمانی‌که با استفاده از لوح فشرده، حافظه فلش و یا رسانه‌های دیگر حاوی توزیع لینوکس DEFT سیستم مورد نظر را راه اندازی می‌کنید، صفحه‌ای حاوی گزینه‌های مختلفی به کاربر نشان داده می‌شود، یکی از این گزینه‌ها مربوط به نصب این توزیع از سیستم‌عامل لینوکس بر روی سیستم مورد نظر می‌باشد و یا اینکه می‌توانید آن را به صورت زنده و بدون نصب در سیستم هدف مورد استفاده قرار دهید. برای این‌کار کافی

[1] Digital Evidence and Forensics Toolkit

است که گزینه DEFT Linix 8 live را انتخاب کنید و با اینکار صفحه رابط کاربری آن همانند زیر بر روی صفحه باز می‌شود:



همانگونه که نشان داده شده است، ابزارهای مختلفی در زمینه ادله الکترونیک در گروه‌های مختلف در این توزیع در نظر گرفته شده‌اند، از جمله آنها می‌توانیم به انواع ضد بدافزار (Antimalware) و بازیابی داده (Data Recovery) و رمزنگاری (Hashing) و تصویربرداری (Imaging) و ادله الکترونیک سیستم همراه (Mobile Forensics) و ادله الکترونیک شبکه (Network Forensics) و بازیابی رمز عبور (Password Recovery) و ابزارهای تهیه گزارش (Reporting tools) اشاره کرد. در هر یک از گروه‌های بالا ابزارهای مختلفی وجود دارند که توسط تولیدکنندگان مختلفی تهیه شده‌اند و کاربر می‌تواند با توجه به نیاز از آنها استفاده کند.

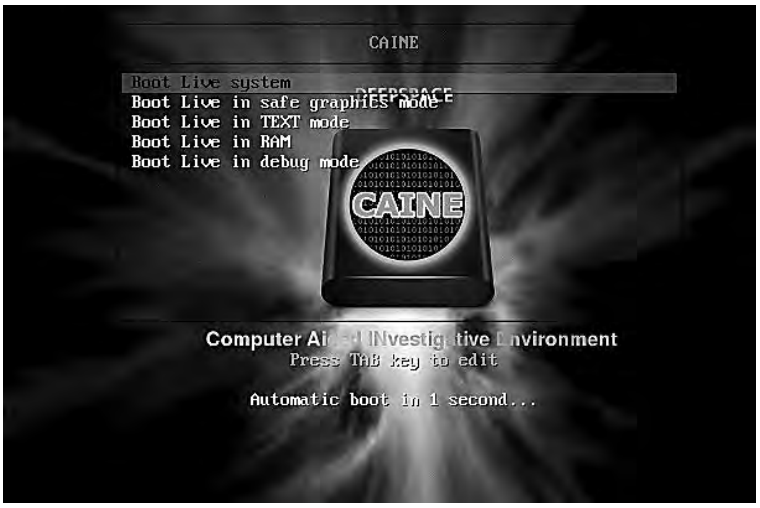
برای مشاهده فهرست کاملی از امکانات و قابلیت‌های پیش‌بینی شده در این توزیع لینوکس می‌توانید به لینک زیر مراجعه کنید:

http://www.deftlinux.net/package-list/

توزیع لینوکس CANE[1]

توزیع لینوکس CANE با قابلیت اجزای زنده با رابط کاربری گرافیکی و خط فرمان و همچنین در وضعیت امن (Safe mode) ارائه شده است، صفحه راه‌اندازی این توزیع لینوکس در زیر نشان داده شده است:

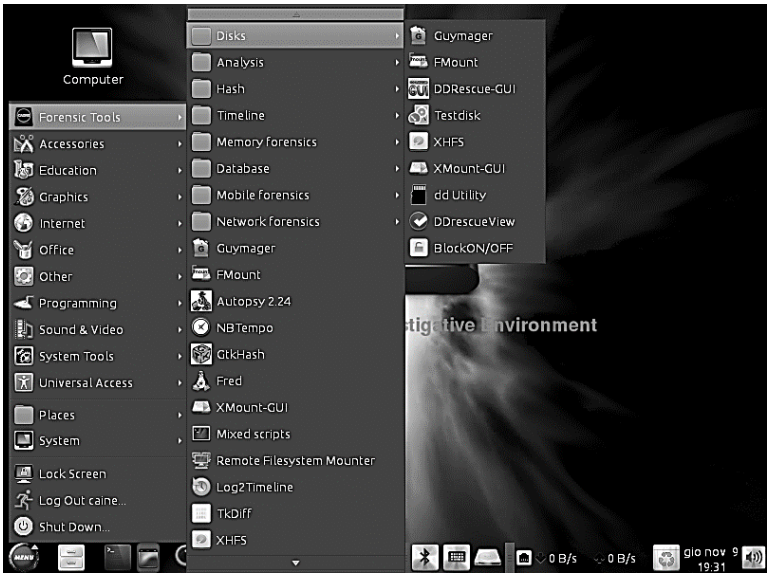
[1] Computer Aided INvestigative Environment



- **صفحه اصلی تارنما:** http://www.caine-live.net/
- **مبتنی بر:** GNU Linux.
- **نوع توزیع:** ادله الکترونیک و ثبت رخدادها

یکی از قابلیت‌های قابل اشاره در این توزیع لینوکس این است که به محض انتخاب شیوه راه‌اندازی آن می‌توانیم به راحتی ابزار مسدود کردن ثبت داده‌ها را در آن مشاهده کنیم. این ابزار با برچسب BlockON/OFF بر روی میز کار مشخص شده است، که در تصویر زیر نشان داده شده است. با فعال سازی این قابلیت، از ثبت هرگونه داده و اطلاعات توسط سیستم‌عامل CAINE بر روی سیستم هدف جلوگیری به‌عمل می‌آید:

ابزارهای ادله الکترونیک در نخستین منوی موجود در این توزیع لینوکس ارائه شده‌اند. همانند توزیع DEFT، این ابزارها در گروه‌های مختلفی ارائه شده‌اند که در تصویر زیر نشان داده شده‌اند که در بین آنها برخی از معروف‌ترین ابزارهای ادله الکترونیک متن باز نیز مشاهده می‌شوند. افزون بر این گروه‌ها، لینک‌های مستقیمی برای برخی از این ابزارهای معروف و شناخته شده در نظر گرفته شده است، مانند Guymager و Autopsy. این دو ابزار در فصل‌های آتی به طور کامل شرح داده می‌شوند:



فهرست کاملی از قابلیت‌ها و امکانات موجود در این توزیع لینوکس را می‌توانید در لینک زیر مشاهده کنید:

http://www.caine-live.net/page11/page11.html

توزیع کالی لینوکس[1]

سرانجام نوبت به محبوب‌ترین توزیع لینوکس در حوزه ادله الکترونیک می‌رسد. در مورد این توزیع، مراحل نصب و ابزارهای موجود و چگونگی استفاده از آنها در فصل‌های آتی شرح داده خواهند شد.

- **صفحه اصلی تارنما:** https://www.kali.org/
- **مبتنی بر:** Debian
- **نوع توزیع:** تست نفوذ، ادله و ضد ادله الکترونیک

این توزیع در ابتدا به عنوان ابزار تست نفوذ و بر اساس توزیع BackTrack ارائه شد، و در سال ۲۰۱۵ به عنوان توزیع کالی لینوکس معرفی شد. این ابزار قدرتمند دارای ابزارهای بی‌شماری برای انجام عملیات تست نفوذ

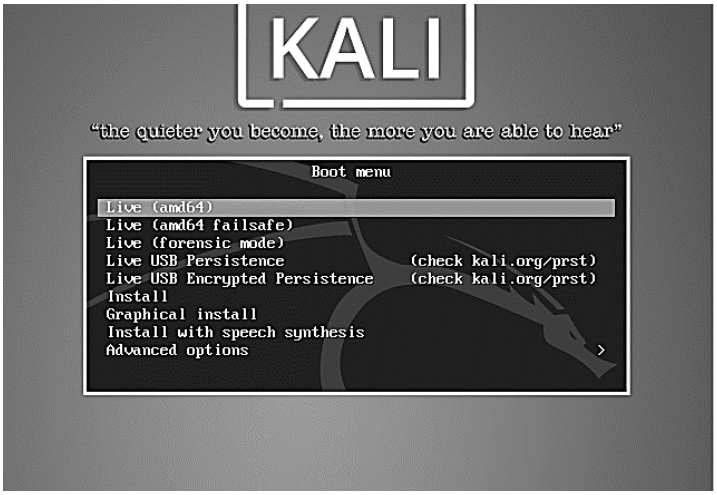
[1] KALI Linux

می‌باشد که می‌تواند در حوزه مختلف در این زمینه مورد استفاده متخصصان قرار گیرد. این توزیع لینوکس به عنوان ستاره‌ای در میان ابزارهای مختلف در زمینه تست نفوذ و هکر قانونمند در دوره CEH[1] مورد استفاده قرار می‌گیرد.

توزیع کالی لینوکس همانند سایر توزیع‌هایی که در بالاتر به آنها اشاره شد، می‌تواند به صورت زنده برای بررسی و جمع‌آوری ادله الکترونیک مورد استفاده قرار گیرد. این توزیع می‌تواند به عنوان یک سیستم‌عامل کامل بر روی دیسک سخت رایانه نصب شود و دارای امکانات و قابلیت‌های تولید نرم‌افزار و استفاده‌های سازمانی می‌باشد. در این توزیع لینوکس درایورهای متنوعی برای پشتیبانی انواع سخت افزارهای مختلف، کارت‌های گرافیکی و کارت‌های شبکه در نظر گرفته شده است. این توزیع لینوکس می‌تواند بر روی پردازنده‌هایی با معماری ٦٤/٣٢ بیتی نصب و مورد استفاده قرار گیرد. این توزیع لینوکس می‌تواند بر روی تلفن‌ها و تبلت‌های هوشمند مشخصی مانند Nexus و OnePlus نصب شود.

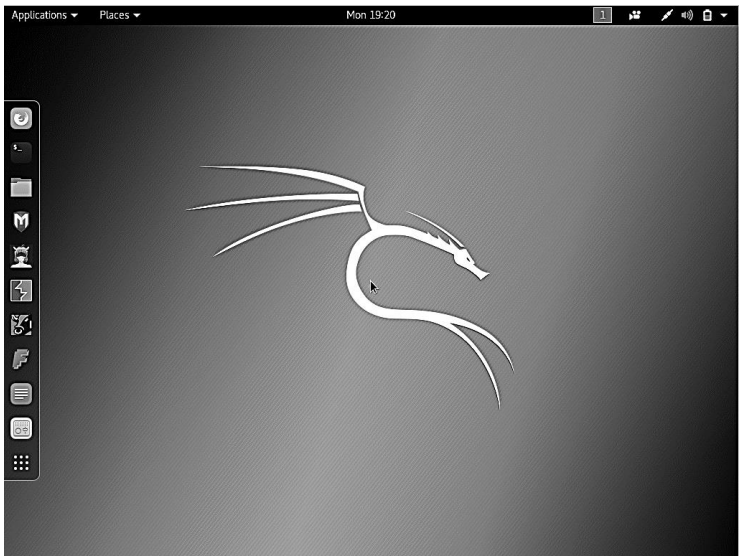
افزون بر گزینه‌های متنوعی که در هنگام راه اندازی این توزیع لینوکس در اختیارمان می‌باشد، امکان انتخاب راه‌اندازی به صورت زنده (forensic mode) نیز در آن پیش بینی شده است، در این شرایط هیچ داده‌ای از جانب این توزیع بر روی سیستم هدف و مورد بررسی ثبت نمی‌شود. افزون بر این امکان بارگذاری خودکار هر نوع حافظه فلش و رسانه ذخیره‌سازی اطلاعات را نیز در سیستم مورد نظر غیر فعال می‌کند. همه این موارد برای حفظ تمامیت و مشمولیت سیستم مورد نظر برای بررسی ادله و شواهد الکترونیک موجود در آن انجام می‌شوند.

پس از راه اندازی این توزیع لینوکس از روی لوح فشرده و یا حافظه فلش، نخستین صفحه‌ای که روی صفحه نمایش ظاهر می‌شود، گزینه‌های مختلفی مبنی بر راه‌اندازی آن به صورت زنده و یا نصب بر روی دیسک سخت سیستم مورد نظر را دربر می‌گیرد. برای استفاده از آن در زمینه ادله الکترونیک، گزینه سوم یعنی forensic mode را انتخاب می‌کنیم، در شکل زیر نشان داده شده است:

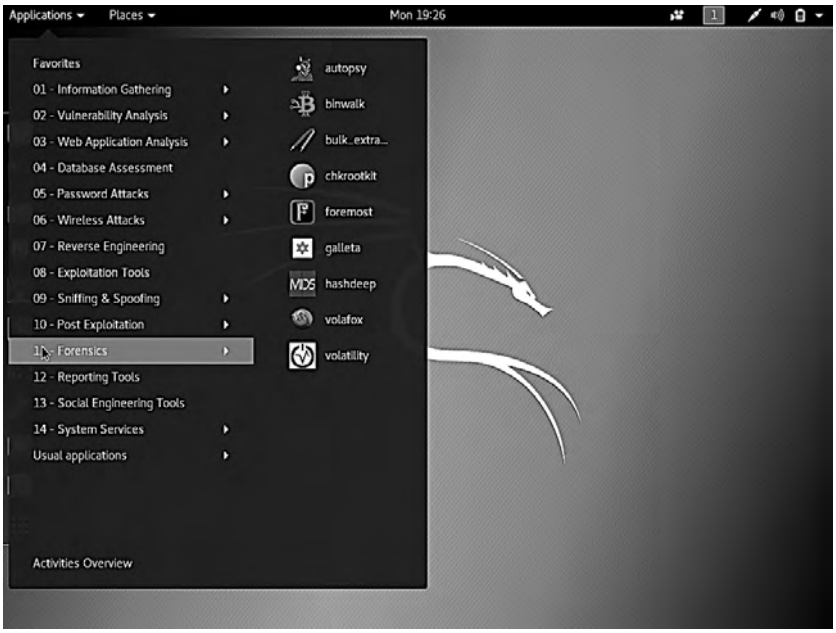


[1] Certified Ethical Hacking (Ec-Council)

زمانی که کالی را به صورت زنده (forensic mode) راه‌اندازی می‌کنید، کاربر همانند شرایط عادی رابط کاربری گرافیکی و میزکار آن را مشاهده خواهد کرد، در شکل زیر نشان داده شده است:



منوی کالی را با کلیک بر روی عبارت Application در گوشه بالا و سمت راست صفحه میزکار، باز می‌کنید. با این کار منوی مربوط به ابزارهای ادله الکترونیک موجود در آن به صورت گروه بندی شده نمایش داده می‌شوند، در زیر نمونه‌ای از این ابزارها که در فصل‌های آتی به آنها خواهیم پرداخت، نشان داده شده است:



باید توجه داشته باشید که ابزارهای موجود در توزیع کالی لینوکس، در آنچه که در تصویر بالا نشان داده شده خلاصه نمی‌شود. برخی از ابزارهای دیگر در این توزیع وجود دارند که امکان دسترسی به آنها از طریق خط فرمان پیش بینی شده است که در ادامه کتاب به آنها اشاره خواهیم کرد.

در صورتی‌که کالی را در حالت زنده (forensic mode) راه‌اندازی کنید، افزون بر اینکه هیچ نوع داده‌ای را در حافظه اصلی سیستم هدف بازنویسی نمی‌کند، از ثبت هر نوع داده و اطلاعات در حافظه مجازی swap file نیز جلوگیری می‌کند. به این ترتیب همه اطلاعات و شواهد موجود در سیستم هدف به‌صورت دست نخورده باقی خواهند ماند.

در تصویر زیر روشی دیگر برای دسترسی به منوی ابزارهای ادله الکترونیک موجود در کالی نشان داده شده است. در این روش کافی است که بر روی نمایه مربوط به آن در منوی کنار صفحه کلیک کنید :

برای مشاهده فهرستی کامل از امکانات و قابلیت‌های موجود در توزیع کالی لینوکس کافی است که بر روی لینک زیر کلیک کنید:

https://tools.kali.org/tools-listing

در بین سه توزیع لینوکس که به آنها اشاره کردیم و در زمینه ادله الکترونیک مورد استفاده قرار می‌گیرند، کالی می‌تواند به‌صورت زنده مورد استفاده قرار گرفته و دارای همه امکانات و قابلیت‌های مربوط به یک سیستم‌عامل کامل نیز می‌باشد، مانند ویندوز و مک و اندروید. با توجه به اینکه کالی لینوکس می‌تواند بر روی دیسک سخت نصب شود، ابزارهای موجود در آن می‌توانند از طریق اینترنت به‌روز رسانده شوند و امکان دسترسی دائمی و در مواقع مورد نیاز و در هر لحظه برای متخصصان امنیت و فناوری اطلاعات فراهم می‌باشد.

با استفاده از سیستم‌عامل‌هایی که در آنها ابزارهای ادله الکترونیک به صورت متن باز پیش بینی شده اند، مانند کالی، محدوده وسیعی از ابزارها در اختیارمان قرار می‌گیرند. برای انجام یک کار می‌توانیم از ابزارهای مختلف و متنوعی استفاده کنیم. این قابلیت بسیار خوبی است که می‌توانیم برای رسیدن به اعتماد بیشتر، نتیجه بدست آمده از یک ابزار را با ابزارهای دیگر مقایسه کنیم.

استفاده از چند ابزار در بررسی ادله الکترونیک

حفاظت از شواهد و ادله، یکی از مهمترین بخش‌های تحقیقات ادله الکترونیک می‌باشد. با استفاده از ابزارهای تجاری و متن باز می‌توانیم به نتایج یکسانی در روند تحقیقات و ادله الکترونیک دست پیدا کنیم. البته با توجه به اهمیت بررسی ادله و شواهد، همواره بهترین توصیه این است که از بیش از یک ابزار برای انجام بررسی و آنالیز شواهد و ادله استفاده کنیم و سپس نتایج بدست آمده از آنها را با یکدیگر مقایسه کنیم تا مطمئن شویم که نتیجه بدست آمده از آنها یکسان می‌باشند.

یکی دیگر از دلایلی که توصیه می‌شود از بیش از یک ابزار در بررسی ادله الکترونیک استفاده کنیم، مسئله هزینه است. با توجه به اینکه ابزارهای تجاری معمولا با توجه به شرایطی که در تهیه و ارائه و نیز خدمات پشتیبانی آنها وجود دارد، گران قیمت می‌باشند، با امکان استفاده از چند ابزار برای انجام مراحل تحقیق و بررسی می‌توانیم در صورت عدم برخورداری از بودجه مناسب برای استفاده از ابزارهای تجاری، از انواع متن باز آنها برای این‌کار استفاده کنیم.

اکنون پرسش این است، چگونه ابزار مورد نظر را انتخاب کنیم؟

انجام بررسی و تحقیقات ادله الکترونیک معمولا نیازمند صرف زمان زیاد است، بنابراین معمولا سعی می‌کنیم تا در بررسی ادله، از نسخه‌های کپی متعددی از شواهد و ادله الکترونیک استفاده کنیم. بنابراین می‌توانیم همزمان از چندین ابزار به طور موازی در بررسی و تحقیقات بر روی شواهد مشابه استفاده کنیم. بنابراین در حالی‌که معمولا ترجیح می‌دهیم از ابزارهایی استفاده کنیم که دارای سرعت اجرای سریع‌تری می‌باشند، اما باید به قابلیت اطمینان و دقت آنها نیز توجه داشته باشیم.

انستیتو ملی استاندارد و فناوری (NIST)[1] برنامه‌ای به نام CFTT[2] را ارائه کرده است که با استفاده از آن استانداردی برای تست و آزمایش کیفیت و صحت ارائه پاسخ توسط ابزارهای مختلف مورد استفاده در بررسی ادله الکترونیک را ارائه کرده است. برخی از ابزارها بر اساس قابلیت‌های‌شان انتخاب می‌شوند و در بخش تست در گروه‌های مخصوص به خود مانند ابزارهای نسخه‌برداری، ابزارهای استخراج داده و ابزارهای بازیابی داده‌ها و اطلاعات طبقه‌بندی شده‌اند. برای این ابزارها روش‌ها و رویه‌های مشخصی برای تست صحت و درستی عملکرد طراحی و در معرض استفاده عموم قرار داده شده است.

---

[1] National Institute of standard and Technology
[2] Computer Forensics Tool Testing

اطلاعات بیشتر در مورد این برنامه را می‌توانید در لینک زیر مشاهده کنید:

https://www.cftt.nist.gov/disk_imaging.htm

گزارش مربوط به تست اعتبارسنجی و صحت عملکرد ابزارهای مورد استفاده در این کتاب را می‌توانید در لینک زیر مشاهده کنید.

https://www.dhs.gov/science-and-technology/nist-cftt-reports

یکی دیگر از دلایلی که ما را ملزم می‌کند تا از چندین ابزار به طور همزمان در بررسی‌های ادله الکترونیک استفاده کنیم، حفظ تمامیت و مشمولت نتایج و یافته‌های بدست آمده در حین آزمایش‌ها می‌باشد. استفاده از چندین ابزار در بررسی‌های ادله الکترونیک در بخش‌های سوم و چهارم این کتاب ارائه شده‌اند.

ضد ادله الکترونیک: تهدید برای ادله الکترونیک

همچنان که همواره سعی می‌کنیم تا روند انجام عملیات جمع‌آوری، نگهداری و بررسی ادله الکترونیک را هر چه ساده‌تر کنیم، اما همواره با شرایطی مواجه می‌شویم که انجام عملیات بررسی و تحقیقات ادله الکترونیک را با دشواری و استرس زیاد همراه می‌کنند. افراد معمولا تمایل دارند تا اطلاعات خود را مخفی کنند، ردپاهای خود را از بین ببرند و آنهایی که معمولا مرتکب جرائم می‌شوند و یا در انجام آنها همکاری و مشاورت می‌کنند معمولا سعی می‌کنند تا به گونه‌ای عمل کنند تا انجام تحقیقات و بررسی‌های ادله الکترونیک را دشوارتر و یا در مواردی غیرممکن سازند.

اخیرا در فضای مجازی شاهد اجرای حملات سایبری متعددی بوده‌ایم، به‌ویژه از سال ۲۰۱۱ به بعد. بسیاری از این حملات از جانب افراد و گروه‌های هکری ناشناخته، مانند LulzSec و Anonymous و Lizard Squad بوده‌اند که اغلب با هدف و منظورهای مشخصی اقدام به عملیات مجرمانه خود کرده و نگرانی زیادی از بابت دست‌گیر شدن و زندانی شدن نیز نداشتند. برخی از این حملات منجر به بروز اختلال و خرابی در شبکه‌ها و اختلال در فعالیت سازمان‌های مختلف و در نتیجه ایجاد میلیون‌ها دلار خسارت به صورت مستقیم و غیر مستقیم شده‌اند.

اجرای این حملات و انتشار عمومی آنها باعث شده است که بسیاری از افراد و گروه‌های جدید بتوانند از اشتباهات و نقاط ضعف، حملات آنها را شناسایی کنند. وجود شبکه‌های اجتماعی و کانال‌های ارتباطی مخفی باعث شده است که این افراد مجرم و خراب‌کار بتوانند سریع‌تر و راحت‌تر با یکدیگر ارتباط برقرار کنند. با توجه به اینکه سعی بر این است که دسترسی و استفاده از اینترنت و شبکه وب روز به روز ساده‌تر شود، مشاهده می‌کنیم که ارائه دهندگان اینترنت در ارائه خدمات اینترنت بی‌سیم از طریق نقاط دسترسی رایگان در نقاط مختلف شهر با یکدیگر رقابت می‌کنند.

در نتیجه امروزه تقریبا در هر کافی شاپ و مرکز عمومی مشاهده می‌کنیم که به‌راحتی با استفاده از یک تلفن هوشمند و یا تبلت می‌توانیم بدون تأیید هویت و ارائه اطلاعات شخصی به اینترنت دسترسی داشته باشیم.

همین امر باعث می‌شود که هکرها و مجرمان فضای مجازی بتوانند براحتی و بدون شناسایی، محتواهای مجرمانه خود را ارسال و یا دریافت کنند و یا ایمیل‌های خراب‌کارانه و یا گول زننده خود را به صورت ناشناس در شبکه منتشر کنند.

رمزنگاری

افزون بر موارد فوق، امکان دسترسی به ابزارهایی با رابط کاربری آسان به منظور مخفی کردن اطلاعات قابل شناسایی عمومی [1](PII)، و یا مخفی کردن هر نوع اطلاعاتی که بتواند در مشخص کردن فرد مجرم در فضای مجازی کمک کند، نیز از دیگر چالش‌های بررسی و تحقیق در حوزه ادله الکترونیک می‌باشند. ابزارهایی که برای رمزنگاری اطلاعات و یا گمنامی استفاده می‌شوند، مانند آنهایی که می‌توانند IP آدرس‌ها را مخفی کنند، امروزه به‌سادگی برای هر کسی در دسترس می‌باشند و روزبه‌روز نحوه استفاده و رابط کاربری آنها ساده‌تر می‌شوند.

باید به این نکته نیز توجه شود که نقاط دسترس وای‌فای نیز می‌توانند خود عاملی برای تهدید و خطر برای استفاده کننده از آن باشند، زیر آنها می‌توانند به راحتی برای دسترسی غیرمجاز و نسخه‌برداری از ترافیک کاربران تنظیم و پیکربندی شوند، به طور مثال با استفاده از آنها می‌توان به راحتی به نام کاربری و رمزعبور و اطلاعات شناسایی عمومی کاربران (PII)، دسترسی پیدا کرد.

عملیات رمزنگاری منجر به حفظ محرمانگی بین طرفین انتقال ترافیک می‌شود و استفاده از این فناوری بسیار شبیه به استفاده از قفل و کلید برای امن نگه‌داشتن محل نگهداری اطلاعات شخصی و خصوصی می‌باشد. برای اینکه قفل بتواند باز شود، باید از کلید مناسب برای آن استفاده شود. در فضای دیجیتال نیز اطلاعات رمزنگاری می‌شود و برای باز کردن آنها باید از کلید رمزگشایی مناسب آن استفاده شود. البته روشی دیگر برای استفاده از فناوری رمزنگاری وجود دارد که در آن اطلاعات با استفاده از یک کلید، رمزنگاری می‌شود و با استفاده از کلید دیگر می‌توانیم اطلاعات رمزشده را رمزگشایی کنیم. دو نوع از ابزارهای بسیار معروف در این فناوری عبارتند از TrueCrypt و VeraCrypt.

با استفاده از این دو ابزار می‌توانیم اطلاعات خود را با پیشرفته‌ترین روش‌ها، رمزنگاری کنیم و آنها را به بهترین شکل محرمانه نگهداریم. از جمله چالش‌های موجود در فناوری ادله الکترونیک این است که چگونه بتوانیم کلید مناسب برای رمزگشایی چنین اطلاعات رمزنگاری شده‌ای را پیدا کنیم.

این دو ابزار افزون بر فایل‌ها قادرند تا پوشه‌ها و پارتیشن‌ها و تمام فضای ذخیره‌سازی اطلاعات را نیز رمزنگاری کنند.

[1] Publicly Indentifiable Information