مرکز تخصصی

آپا دانشگاه کردستان

معرفی مهم‌ترین ابزارهای جرم شناسی ویندوز

شماره سند: A96011

۱۳۹۶/۱۲/۰۶

www.cert.uok.ac.ir
apa@uok.ac.ir
087-33662932

فهرست مطالب

فصل ۱ : مقدمه‌ای بر جرم‌شناسی دیجیتال ۳

فصل ۲ : حافظه سیستم‌عامل ۶

Belkasoft Ram Capture ۷

DumpIt ۷

Belkasoft Evidence Center ۸

Volatility ۱۱

فصل ۳ : درایوهای سیستم عامل ۱۶

FTK Image Mounter ۱۶

Dc3dd ۲۱

Arsenal Image Mounter ۲۲

فصل ۴ : تجزیه و تحلیل نسخه های shadow ویندوز ۲۴

ShadowCopyView ۲۴

VSSADMIN و MKLINK ۲۷

Magnet AXIOM ۲۸

فصل ۵ : آنالیز رجیستری ۳۳

AXION ۳۳

RegRipper ۳۸

Registry Explorer ۳۹

FTK Registry Viewer ۴۱

فصل ۶ : Artifact های سیستم عامل ۴۵

سطل بازیافت ۴۶

Encase Forensic ۴۶

Rifiuti2 ..... ۴۹

Magnet Axiom ۵۰

رویدادهای ویندوز ۵۱

FullEventLogView ۵۱

Magnet Axiom ۵۲

EVTXtract recovery event ۵۴

فایل‌های LNK ۵۴

Encase forensic ۵۴

LECmd ۵۷

Link Parser ۵۹

فایل‌های Prefetch ۵۹
Magnet Axiom ۵۹
PECmd ۶۲
Prefetch Carver ۶۳

فصل ۷ : مرورگر وب ۶۴
تحلیل فایرفاکس با استفاده از BlackBag's Blacklight ۶۴
تحلیل گوگل کروم با استفاده از Magnet Axiom ۶۶
تحلیل مایکروسافت Edge با استفاده از Belkasoft Evidence Center ۶۸
Pagefile.sys ۷۲

فصل ۸ : ایمیل و پیام‌رسان ویندوز ۷۵
Intella ۷۵
Autopsy ۸۱
Magnet Axiom ۸۳
Belkasoft Evidence Center ۸۴
SkypeLogView ۸۵

فصل ۹ : ارزیابی ابزارهای معرفی شده ۸۷
مراجع ۹۱

فصل ۱ : مقدمه‌ای بر جرم‌شناسی دیجیتال

علم جرم‌شناسی رایانه‌ای (به عنوان شاخه ای از جرم شناسی دیجیتال) به شواهد و مدارک قانونی موجود در رایانه ها و محیطهای دیجیتالی ذخیره سازی اطلاعات می پردازد. هدف جرم شناسی دیجیتال ،ارائه توضیح پیرامون وضعیت فعلی یک ابزار دیجیتالی مثل سیستم کامپیوتر، رسانه ذخیره سازی یا یک سند الکترونیکی می باشد. گستره فعالیت یک تحلیل جرم شناسی، از بازیابی اطلاعات ساده تا بازسازی یک سری رویداد را دربرمی گیرد.

سنجش‌های خاصی برای انجام تحقیقات جرم شناسی وجود دارد که نتایج آن می تواند در دادگاه مورد استفاده قرار گیرد. هدف تکنیک های جرم شناسی رایانه‌ای، جستجو، حفظ و آنالیز اطلاعات موجود بر روی سیستم‌های کامپیوتری به منظور یافتن شواهد ومدارک احتمالی برای یک دادرسی است. بسیاری از تکنیکهایی که کارآگاهان از آنها در تحقیقات صحنه جرم استفاده می کنند دارای المثنی دیجیتالی هستند، اما تحقیقات کامپیوتری دارای برخی جنبه های منحصربفرد نیز می باشد. برای مثال، تنها باز کردن یک فایل کامپیوتری باعث تغییر آن می شود(کامپیوتر، زمان و تاریخ دسترسی به فایل را بر روی خود آن ثبت می کند).

اگر کارآگاهان یک کامپیوتر را توقیف نموده و سپس شروع به باز کردن فایلها نمایند، هیچ راهی وجود نخواهد داشت که مطمئن باشند چیزی را تغییر نداده اند. وکلای مدافع می توانند در هنگام رجوع پرونده به دادگاه به اعتبار این مدارک اعتراض نمایند.

بعضی از مردم معتقداند که استفاده از اطلاعات دیجیتال بعنوان شواهد و مدارک یک پرونده ایده چندان خوبی نیست اگر تغییر دادهای کامپیوتری تا این اندازه آسان است، چگونه می توان از آنها بعنوان یک مدرک قابل اعتماد استفاده کرد؟ بسیاری از کشورها ،استفاده از مدارک کامپیوتری در طول دادرسی‌ها را مجاز می دانند، اما اگر مدارک کامپیوتری در پرونده های آتی غیر قابل اعتماد به نظر برسند این وضعیت احتمالا تغییر خواهد کرد.

کامپیوترها دائما قدرت بیشتری پیدا می کنند، بنابراین حوزه جرم شناسی رایانه ای بایستی طور مستمر رشد و تکامل پیدا کند. در روزهای اولیه دوران کامپیوتر، این امکان برای یک کارآگاه تنها وجود داشت تا تمام فایلها را بررسی و دسته بندی نماید زیرا ظرفیت ذخیره سازی در آن زمان بسیار محدود بود.

امروزه با پیدایش درایوهای دیسکهای سختی که قادر به نگهداری چند ترابایت اطلاعات درایوهای دیسک سختی که قادر به نگهداری چند ترابایت اطلاعات هستند، اینکار به یک تلاش طاقت فرسا تبدیل می شود. کارآگاهان باید شیوه های جدیدی را برای جستجوی شواهد و مدارک پیدا کنند، بدون آنکه نیازی به تخصیص منابع بیش از حد به این فرآیند داشته باشند.

اما اصول جرم شناسی رایانه ای چیست؟ تیم تحقیق قادر به جستجوهای چه مواردی است وکجا به جستجوی این موارد می پردازد؟ در ادامه با بررسی پاسخ این پرسش‌ها می پردازیم.

۱-۱- مبانی جرم شناسی رایانه‌ای

Judd Robbins، یک دانشمند کامپیوتری و متخصص ارشد جرم شناسی رایانه ای، مراحلی که ماموران تحقیق باید برای بازیابی مدارک کامپیوتری دنبال نمایند را به ترتیب زیر فهرست می کند.

- ضبط سیستم کامپیوتری، برای تضمین اینکه تجهیزات و داده های آن در امنیت قرار دارند. این بدان معنی است که کارآگاهان باید مطمئن شوند که هیچ فرد غیرمجازی نمی تواند به کامپیوتر و ابزارهای ذخیره سازی مورد بحث تحقیقات، دسترسی پیدا کند. اگر سیستم کامپیوتری به اینترنت متصل است کارآگاهان باید این ارتباط را قطع نمایند.
- یافتن هر فایلی که بر روی سیستم کامپیوتری قرار دارد، شامل فایل‌های رمزنگاری شده، فایل‌هایی که با کلمه عبور محافظت شده‌اند، فایلهای مخفی و فایلهایی که حذف گردیده اما هنوز اطلاعاتی بر روی آنها نوشه نشده است. کارآگاهان باید از تمام فایلهای موجود بر روی سیستم، یک کپی تهیه کنند. این کپی، فایل‌های موجود بر روی درایو دیسک سخت کامپیوتر و یا سایر ابزارهای ذخیره سازی آن را در بر می گیرد. از آنجاییکه دسترسی به یک فایل می تواند آن را تغییر دهد، بسیار مهم است که

کارآگاهان در هنگام جستجو برای یافتن مدارک و شواهد تنها از کپی های فایلها استفاده نمایند. سیستم اصلی بایستی دست نخورده و محافظت شده باقی بماند.

- بازیابی اطلاعات حذف شده تا حد امکان با استفاده از نرم افزارهای کاربردی که داده های حذف شده را تشخیص داده و بازیابی می نمایند.
- آشکار نمودن محتوای تمام فایلهای مخفی با برنامه هایی که برای تشخیص وجود داده های مخفی طراحی شده اند.
- مزگشایی و دسترسی به فایلهای محافظت شده
- آنالیز نواحی خاص دیسکهای کامپیوتر، شامل بخشهایی که معمولا غیر قابل دسترسی هستند(در زبان کامپیوتری، فضای بلا استفاده بر روی درایو یک کامپیوتر را فضایUnallocated می نامند) این فضا می‌تواند حاوی فایل‌ها و یا قطعاتی از فایل‌هایی باشد که با پرونده مورد نظر ارتباط دارند.
- مستند سازی تمام مراحل فرآیند جستجو. برای کارآگاهان بسیار مهم است که اثبات کنند تحقیقات آنها تمام اطلاعات موجود را بر روی سیستم کامپیوتری را بدون تغییر و یا آسیب دیدگی حفظ کرده است. ممکن است یک فاصله چند ساله در بین فرآیند تحقیق و دادرسی وجود داشته باشد و بدون مستندسازی صحیح، مدارک قابل استفاده نخواهند بود.

Robbins معتقد است که مستندسازی بایستی نه تنها تمام فایل‌ها و داده‌های بازیابی شده از سیستم را در برگیرد، بلکه باید شامل یک گزارش در مورد چیدمان فیزیکی سیستم و اینکه آیا فایل‌هایی رمزگذاری یا مخفی شده بوده‌اند یا خیر نیز باشد.

- حتی زمانیکه تحقیقات به پایان می‌رسد ،وظیفه کاراگاهان تمام نشده است .ممکن است هنوز برای ارائه شهادت در دادگاه به حضور آنها نیاز باشد.

تمام این مراحل دارای اهمیت هستند اما اولین قدم بسیار تعیین کننده خواهد بود. اگر ماموران تحقیق نتوانند ثابت کنند که سیستم کامپیوتری را دست نخورده حفظ نموده اند، مدارکی که پیدا می کنند قابل قبول نخواهند بود. در روزهای آغازین عصر کامپیوتر، سیستم می‌توانست شامل یک PC و چند دیسک فلاپی باشد. امروزه یک سیستم می تواند شامل چندین کامپیوتر، دیسک، درایوهای Flash، درایوهای خارجی، تجهیزات جانبی و سرورهای وب باشد.

۱-۲- ابزارهای جرم‌شناسی

برنامه نویسان تعداد زیادی از نرم افزارهای کاربردی جرم شناسی رایانه ای را ایجاد کرده‌اند. برای بسیاری از دوایر پلیس، انتخاب ابزارها بودجه و تخصص موجود در این ادارات بستگی دارد.

تعدادی از ابزارها و برنامه های جرم شناسی رایانه ای که امکان تحقیقات کامپیوتری را بوجود می آورند، عبارتند از:

- نرم افزار تصویربرداری (Imaging) از دیسک که ساختار و محتوای یک درایو دیسک سخت را ضبط و بایگانی می نماید. با چنین نرم افزاری نه تنها امکان کپی برداری از اطلاعات داخل یک درایو وجود خواهد داشت بلکه حفظ سازماندهی فایلها و رابطه آنها با یکدیگر نیز امکانپذیر خواهد بود.
- ابزارهای سخت‌افزاری یا نرم افزاری Write که در درایوهای دیسک سخت را بصورت بیت به بیت کپی نموده و بازسازی می کنند هردو گروه ابزارهای سخت افزاری و نرم افزاری از تغییر اطلاعات موجود اجتناب می نمایند. بعضی از این ابزارها، ماموران تحقیق را ملزم می کنند که پیش از تهیه یک کپی، درایو دیسک سخت را از کامپیوتر متهم جدا نمایند.
- ابزارهای Hashing که درایوهای دیسک سخت اصلی را با کپی‌های تهیه شده مقایسه می‌کنند. این ابزارها، داده ها را آنالیز نموده و یک شماره منحصربفرد را به آن تخصیص می دهند. اگر اعداد هش بر روی یک درایو اصلی وکپی آن با یکدیگر انطباق داشته باشند کپی یک «تکرار» بی نقص از داده‌های اصلی است.

- ماموران تحقیق از برنامه های بازیابی برای جستجو و بازیابی داده های حذف شده استفاده می کنند. این برنامه‌ها، داده هایی که توسط کامپیوتر برای حذف علامت‌گذاری شده اما هنوز رونویسی نشده اند را مکان یابی می نماید. نتیجه این جستجو در بعضی از موارد یک فایل ناقص است که تجزیه و تحلیل آن دشوارتر خواهد بود.
- برنامه های مختلفی وجود دارند که برای حفظ اطلاعات داخل حافظه اصلی یک کامپیوتر طراحی شده اند. برخلاف اطلاعات موجود بر روی یک درایو دیسک سخت، داده های داخل RAM به محض خاموش شدن کامپیوتر از بین خواهند رفت. بدون نرم افزار، مناسب این اطلاعات به آسانی ازدست خواهند رفت.
- نرم افزارهای آنالیز که به بررسی تمام اطلاعات موجود بر روی یک درایو دیسک سخت پرداخته و محتویات خاصی را جستجو می کنند.

ازآنجایی که کامپیوترهای مدرن می‌توانند چندین گیگا بایت از اطلاعات را در خود نگهداری نمایند، جستجوی فایل‌های کامپیوتری بصورت دستی بسیار دشوار و وقتگیر خواهد بود. برای مثال، بعضی از برنامه های تحلیلگر به جستجو و ارزیابی کوکی های اینترنتی می پردازند که می توانند برای تشخیص فعالیتهای اینترنتی متهم به ماموران تحقیق کمک کنند. گروه دیگری از برنامه ها، به ماموران تحقیق اجازه می دهند تا مندرجات خاصی را جستجو نمایند که می توانند بر روی سیستم کامپیوتری متهم وجود داشته باشند.

در این گزارش سعی شده تا با استفاده از ابزارهای جرم‌شناسی به بررسی،تجزیه، تحلیل و دریافت اطلاعات از ویندوز پرداخت. موارد بررسی شده در این گزارش شامل حافظه سیستم عامل، درایوهای سیستم عامل، آنالیز رجیستری، سطل بازیافت، رویدادهای ویندوز، فایل های LNK، فایل‌های Prefetch، مرورگر وب و ایمیل و پیام رسان ویندوز می باشد. در فصول بعدی به تحلیل و بررسی هریک از این بخش ها با استفاده از ابزارهای جرم‌شناسی می پردازیم.

فصل ۲ : حافظه سیستم عامل

۲-۱- مقدمه

تجزیه و تحلیل حافظه یک زمینه نسبتا جدید اما به طور فزاینده ای است. یک تصویر حافظه را می توان به طور مشابه به عنوان یک تصویر فیزیکی بدست آورد، اما با استفاده از ابزار های مختلف، برخی از آنها در این بخش بحث خواهند شد. تصویر را می توان با استفاده از یکی از فرمت های مختلف ذخیره کرد، بسته به ابزار مورد استفاده برای بدست آوردن تصویر. هنگامی که یک محقق تصویر دارد، می توانند داده ها را درون آن تجزیه و تحلیل کنند.

یکی از چالش های اصلی مرتبط با جرم‌شناسی حافظه، حفظ اطلاعات است. اگر چه تنها گزینه شما در یک تحقیق مشخص ممکن است یک سیستم را خاموش کند و سپس داده ها را در آن تصویر کند، در واقع این امر تاثیری روی دیگر منابع داده های بالقوه ای که ممکن است بعدا مهم باشد را به اثبات برساند. بنابراین، بسیار مهم است که قبل از اینکه تصمیم بگیرید که کدام روش را انتخاب کنید، درک کامل از صحنه ای که در حال تحقیق و نیازهای خاص پرونده دارید، داشته باشید. هر بار که با یک سیستم ارتباط برقرار می کنید چیزی به سادگی با توجه به وجود آن تغییر می کند. با این حال، دستیابی به حافظه می تواند موجب به حداقل رساندن اثرات محقق بر روی داده های جمع آوری شده، از آنجایی که یک تصویر حافظه حافظه فرار را در یک زمان خاص نمونه می گیرد، بنابراین یک تصویر فوری ایجاد می شود که بعدا می تواند مورد تحلیل قرار گیرد.

در مواردی که یک محقق به یک صحنه می رسد برای پیدا کردن یک ماشین در حال حرکت، حافظه در سیستم در آن زمان فرار خواهد داشت. این بدان معنی است که اگر شما موفق به گرفتن تصویر حافظه پس از آن و در آنجا، شما می توانید یک عکس فوری از حافظه کامپیوتر در لحظه ای که شما آن را به دست آورد. این امر می تواند بسیار مفید باشد، به خصوص اگر یک مظنون به تازگی یک صحنه را فرار کرده یا در صحنه دستگیر شده است.

اگر میخواهید حافظه دائمی را به دست آورید، به طور کلی نیاز به مجوزهای اداری در رایانه دارید، مگر اینکه از سخت افزار استفاده کنید. یکی از این راه‌حل‌های سخت‌افزاری جذب حافظه فیزیکی CaptureGUARD است. این به یک داریور کوچک CaptureGUARD نیاز دارد که بر روی سیستم نصب شود و یک قالب حافظه را در قالب استاندارد WinDD ایجاد کند. شما می توانید یکی از این دستگاه‌ها را در شکل ۱-۱ ببینید.

شکل ۱-۱ : اکسپرس کارت

به عبارت دیگر، جرم شناسی یک زمینه پیچیده و پر حرارت است. قبل از تصمیم به استفاده از آن در یک موقعیت، باید درک کامل از مجموعه ابزارهایی که استفاده می کنید، و هر گونه تاثیر بالقوه ای که می توانید بر روی حافظه دائمی داشته باشید. با این حال، اگر شما موفق به گرفتن یک تصویر حافظه شوید، می تواند مقدار زیادی از اطلاعات مفید برای مورد شما فراهم می کند.

۲-۲- نسخه برداری و تجزیه و تحلیل حافظه ویندوز

- نسخه برداری از حافظه ویندوز با استفاده از Belkasoft RAM Capturer
- نسخه برداری از حافظه ویندوز با استفاده از DumpIt
- تجزیه و تحلیل تصویر حافظه ویندوز با استفاده از Belkasoft Evidence Center
- تجزیه و تحلیل تصویر حافظه ویندوز با استفاده از Volatility
- تغییرات در نسخه های ویندوز

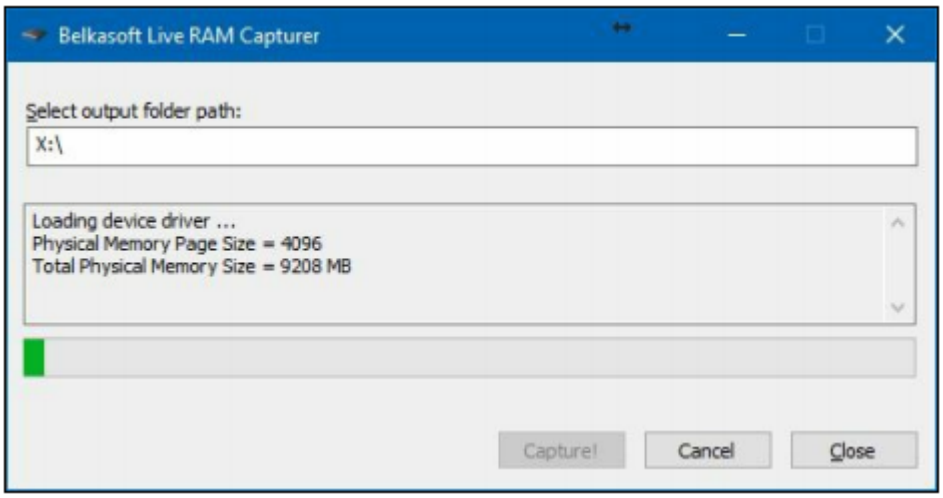
در ادامه هر یک از موارد فوق توضیح داده می‌شود.

۲-۲-۱- نسخه برداری از حافظه ویندوز با استفاده از Belkasoft RAM Capturer

Belkasoft RAM Capturer یک ابزار رایگان است که هر جرم‌شناس دیجیتال باید در کیت خود داشته باشد. این ابزاری کوچک و آسان برای استفاده است و توانایی به دست آوردن حافظه از سیستم‌های ویندوز، از جمله ویندوز ۱۰، حتی اگر آنها توسط یک سیستم فعال ضد دیباگ یا ضد دامپ محافظت می شود.

مراحل نسخه برداری از حافظه ویندوز با استفاده از Belkasoft Ram Capturer به شرح زیر است:

a. قبل از شروع نیاز به اطلاعاتی درباره اندازه حافظه فیزیکی می‌باشد.
b. مسیر پوشه خروجی را انتخاب نموده و باید مطمئن شد که درایو فلش است.
c. پس از آن بر روی دکمه Capture کلیک کنید.



شکل ۲-۱ : نسخه برداری از حافظه ویندوز با استفاده از Belkasoft RAM Capturer

در نتیجه، یک فایل با پسوند mem. مشابه با کل حافظه فیزیکی دریافت می‌کنید. به طور پیش فرض نام فایل، تاریخ دستیابی قرار داده شده، اما به شدت توصیه می‌شود که آن تغییر نام داده شود.

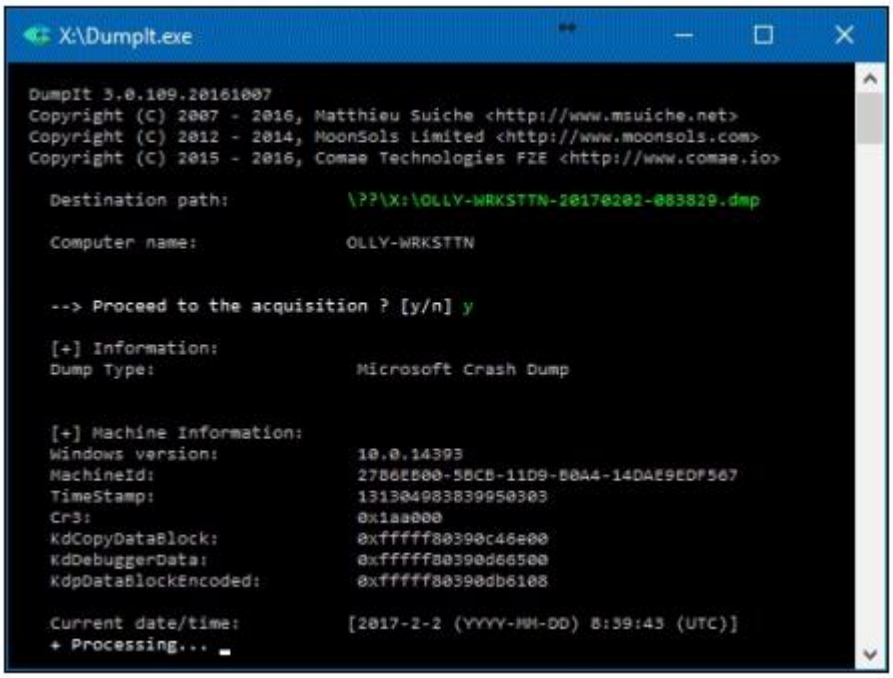
Belkasoft RAM Capturer با استفاده از درایورهای ۳۲ بیتی و ۶۴ بیتی در حالت هسته (نه در حالت کاربر مانند برخی از ابزارهای استخراج دیگر) عمل می کند. این ابزار کل حافظه فیزیکی، حتی اگر مورد حفاظت باشد، را استخراج می‌کند ، و آن را به یک فایل با فرمت mem. ذخیره می‌کند.

۲-۲-۲-استفاده از حافظه ویندوز با استفاده از DumpIt

DumpIt یک ابزار نسخه‌برداری حافظه از مجموعه ابزار Comet Memory Tool است. این ابزار ترکیبی از Win32dd و Win64dd در یک اجرا است. این ابزاری بسیار ساده برای استفاده است؛ حتی یک فرد غیر فنی می‌تواند از آن در شرایط اضطراری استفاده کند. DumpIt از تمام نسخه‌های جدید ویندوز پشتیبانی می‌کند، از XP تا ۱۰، هر دو ۳۲ و ۶۴ بیتی. همچنین این ابزار دارای یک ویژگی بسیار مهم است: پایگاه داده، دایرکتوری جدول و آدرس ساختار داده را در طول فرآیند استخراج نشان می دهد.

در این ابزار، ما نیازی به دانستن اینکه چه نوع سیستم عاملی استفاده می‌کنیم - ۳۲ یا ۶۴ بیتی- نداریم. همانطور که قبلا گفته شد، DumpIt یک همپوشانی از Win32dd و Win64dd در یک اجرا است. بنابراین، فقط دو مرحله دارد:

a. در سیستم هدف به درایو خارجی متصل شوید.
b. DumpIt را اجرا کرده و برای شروع فرایند y را تایپ کنید.



شکل ۲-۲ : نسخه برداری از حافظه ویندوز با استفاده از DumpIt

در نتیجه اجرا دو فایل دریافت می‌کنید: یک فایل با پسوند DMP و یک فایل با پسوند JSON. ابتدا، حافظه سیستم هدف با نام کامپیوتر، تاریخ و زمان (UTC) در نام فایل استخراج می‌شود. دوم، اطلاعات دامپ، شامل اطلاعات مهم از نقطه نظر قانونی است. این شامل اندازه فایل، نوع معماری سیستم(۳۲ بیتی یا ۶۴ بیتی)،KdCopyDataBlock ، KdDebuggerData، kdpDataBlockEncoded، هش sha256، و غیره است. اکنون، فایل DMP آماده است تا با نرم افزار جرم شناسی حافظه مورد نظر مورد تجزیه و تحلیل قرار گیرد.

به دلیل اینکه DumpIt ترکیبی از Win32dd و Win64dd است، به طور خودکار نوع معماری سیستم را تشخیص می دهد و یک نسخه حافظه و یک فایل در فرمت JSON با تمام اطلاعاتی که برای تجزیه و تحلیل بیشتر با ابزارهای قانونی جاسوسی مانند Volatility، Rekall، Belkasoft نیاز دارد، ایجاد می کند.

۲-۲-۳- تجزیه و تحلیل تصویر حافظه ویندوز با Belkasoft Evidence Center

مراحل تجزیه و تحلیل تصویر حافظه ویندوز با استفاده از Belkasoft Evidence Center:

a. برای انجام این کار، بر روی New در پنجره Open Case کلیک کنید. اکنون باید چند فیلدهای زیر پر شود:

Case name: معمولا ما از شماره کیس و سال برای نام پرونده ها استفاده می کنیم، اما این بار، چون با هدف تست ایجاد می شود، آن را Belkasoft Memory Forensics Test می نامیم.

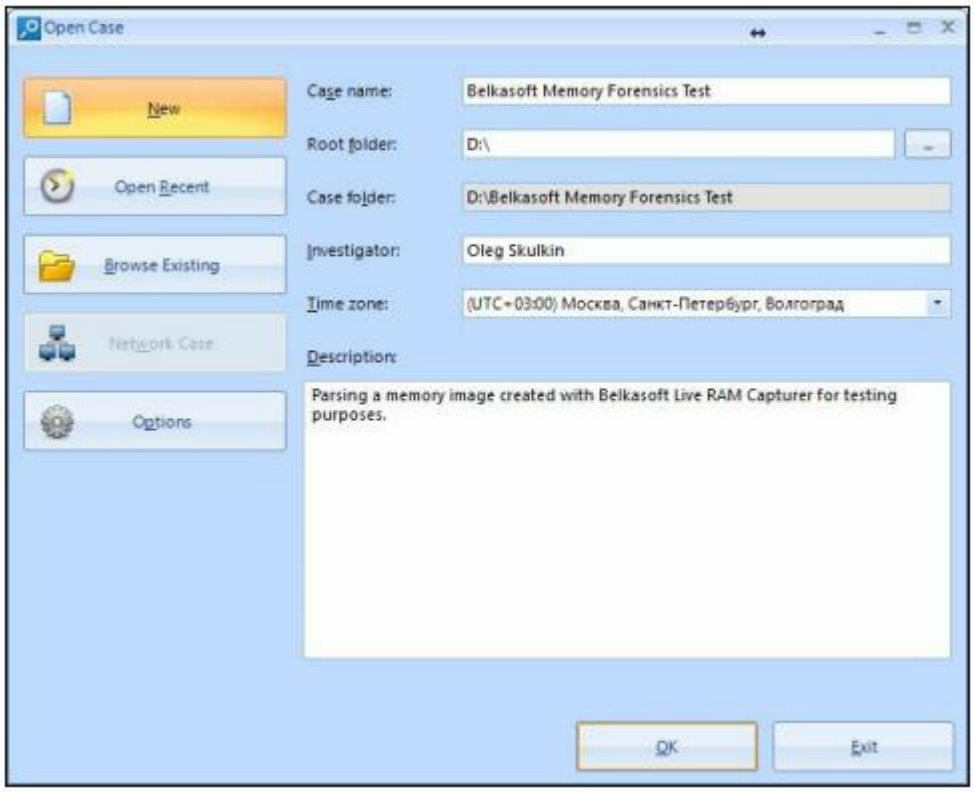
Root folder: در اینجا، باید پوشه ای را که اطلاعات کیس در آن قرار دارد انتخاب کنید.

Case folder: این فیلد به طور خودکار بر اساس دو فیلد قبلی پر شده است.

Investigator: نام خود را در این قسمت تایپ کنید.

Time zone: انتخاب منطقه زمانی مناسب بسیار مهم است. اگر قبلا آن را بدانید، آن را انتخاب کنید. اگر نه، بهتر است UTC را انتخاب کنید ۰۰:۰۰. در اینجا، از (UTC + 03:00) استفاده می شود.

Description: در اینجا می توانید توضیحی برای کیس خود بیان کنید. در اینجا از توضیح زیر استفاده نمده‌ایم: " تجزیه یک تصویر حافظه ایجاد شده توسط Belkasoft Live RAM Capturer برای اهداف تست"

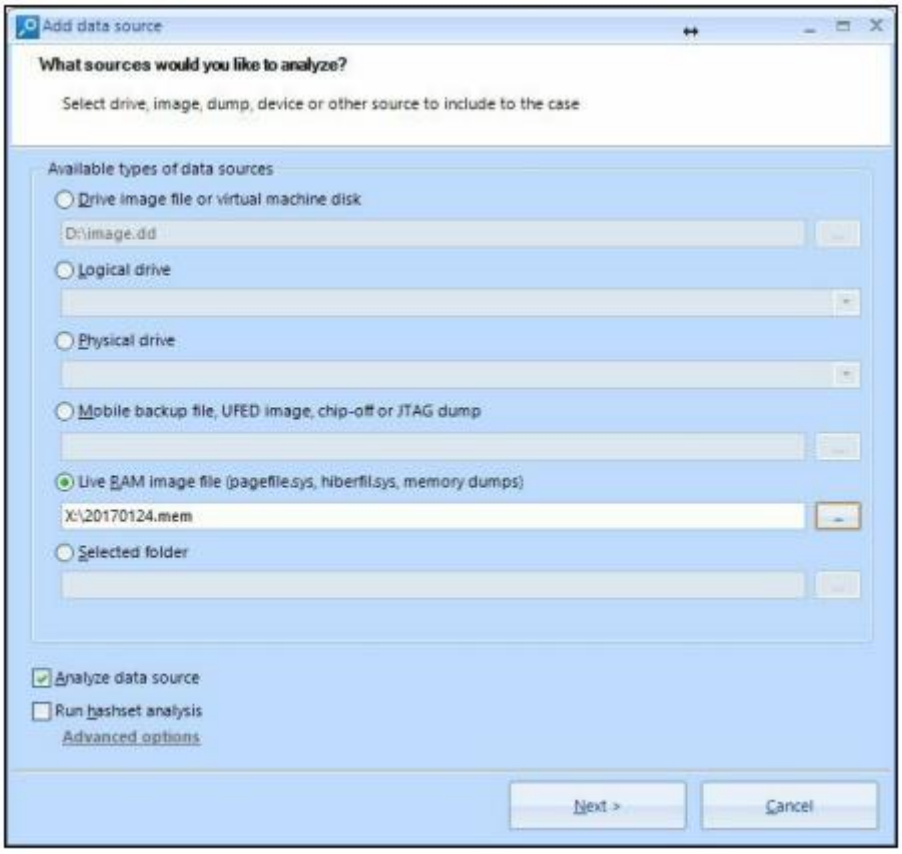


شکل ۲-۳ : باز کردن case

b. روی OK کلیک کنید و پنجره بعدی را مشاهده خواهید کرد - منبع داده را اضافه کنید.

Belkasoft Evidence Center از انواع مختلف منابع Evidence، از درایوهای فیزیکی و تصاویر درایو، پشتیبان گیری های موبایل و البته تصاویر حافظه، از جمله pagefile.sys و hiberfil.sys پشتیبانی می کند.

تصویری که در مرحله قبل از Belkasoft RAM Capturer بدست آمده را در اینجا به عنوان منبع داده انتخاب کنید.



شکل ۲-۴ : اضافه کردن تصویر حافظه قبلا به دست آمده به عنوان منبع داده در Belkasoft Evidence Center

c. برای انتخاب نوع داده هایی که می‌خواهید جستجو کنید روی Next کلیک کنید. برای اهداف تست، تمام انواع داده های موجود را انتخاب کردیم، اما شما می توانید آنهایی را که واقعا نیاز دارید انتخاب کنید تا زمان پردازش را کم کنید.

نکته: فراموش نکنید که به قسمت advance options بروید و BelkaCarving را فعال کنید - این به شما کمک می کند که داده های جداگانه را، به عنوان مثال، تصاویر را بازیابی کنید.

شکل ۲-۵ : انتخاب نوع داده در Belkasoft Evidence Center

d. حالا برای تجزیه و تحلیل تصویر حافظه آماده است- فقط روی Finish کلیک کنید.

شما می‌توانید از این ابزار برای بازیابی تاریخچه مرورگر در ابزارهای ناشناس مانند مرورگر Tor، که به طور گسترده ای در میان مجرمان استفاده می شود، و همچنین سایر مصنوعات دیجیتال مهم که ممکن است تنها در حافظه دائمی قرار بگیرند، استفاده کنید. این ابزاری برای تجزیه و تحلیل ساختار تصویر حافظه و استخراج اطلاعات موجوددر آن و قرار دادن آن در دسته های مربوطه است. گزینه های BelkaCarving ابزار را قادر می سازد داده‌های جداگانه‌ای (به عنوان مثال تصاویر) را بازسازی کند.

۲-۲-۴-تجزیه و تحلیل تصویر حافظه ویندوز با Volatility

Volatility Framework یک مجموعه منبع باز از ابزارهایی است که در پایتون برای استخراج آثار دیجیتالی از تصاویر حافظه نوشته شده است. برای نشان دادن توان نوآوری، تصمیم گرفتیم از یک تصویر حافظه از یک سیستم آلوده به بدافزار معروف استفاده کنیم(Stuxnet). با جمع آوری اطلاعات در مورد تصویر حافظه شروع می‌کنیم.

a. Cmd.exe را اجرا کنید.

b. دایرکتوری را به یک Volatility Standalone قابل اجرا تغییر دهید و از پلاگین imageinfo استفاده کنید.

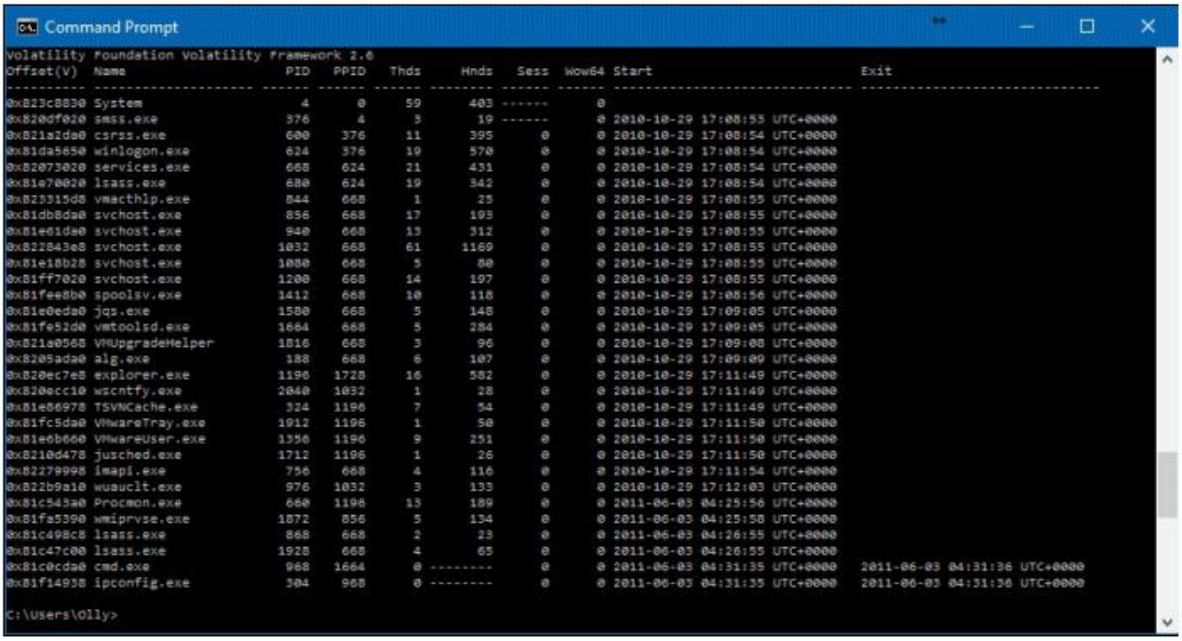
پلاگین imageinfo دو پروفایل پیشنهاد شده را باز می‌گرداند. ما می دانیم که این تصویر از یک سیستم در حال اجرا ویندوز XP با سرویس پک ۳ گرفته شده است، بنابراین مشخصات درست WinXPSP3x86 است.

حالا ما مشخصات درست را می دانیم، می توانیم آن را به عنوان یک سوئیچ برای جمع آوری اطلاعات در مورد فرایندهای در حال اجرا بر روی دستگاه آلوده استفاده کنیم.

```
volatility_2.6_win64_standalone.exe -f
X:stuxnet.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based
on KDBG
search...
Suggested Profile(s) : WinXPSP2x86,
WinXPSP3x86 (Instantiated    with WinXPSP2x86)
AS Layer1 : IA32PagedMemoryPae (Kernel AS)
AS Layer2 : FileAddressSpace (X:stuxnet.vmem)
PAE type : PAE
DTB : 0x319000L
KDBG : 0x80545ae0L
Number of Processors : 1
Image Type (Service Pack) : 3
KPCR for CPU 0 : 0xffdff000L
KUSER_SHARED_DATA : 0xffdf0000L
Image date and time : 2011-06-03 04:31:36 UTC+0000
Image local date and time : 2011-06-03 00:31:36
-0400
```

c. از پلاگین pslist استفاده کنید.

```
volatility_2.6_win64_standalone.exe -f X:stuxnet.vmem
--
profile=WinXPSP3x86 pslist
```



شکل۲-۶: خروجی پلاگین pslist

آیا چیزی مشکوک را می بینید؟ بله، سه نسخه از lsass.exe وجود دارد، و این یکی از علائم بدافزار Stuxnet است. به طور معمول، فقط یک فرآیند lsass.exe باید اجرا شود، بنابراین ما باید تعیین کنیم کدام دو بدافزار هستند.

d. به نشانگرهای زمانی در شکل ۲-۷ نگاه کنید. دو مورد از سه فرآیند در سال ۲۰۱۱ آغاز شد. حالا از پلاگین pstree استفاده کنید.

```
volatility_2.6_win64_standalone.exe -f
X:stuxnet.vmem --
profile=WinXPSP3x86 pstree
```

```
Command Prompt
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x823c8830:System                                      4      0     59    403 1970-01-01 00:00:00 UTC+0000
. 0x820df020:smss.exe                                 376      4      3     19 2010-10-29 17:08:53 UTC+0000
.. 0x821a2da0:csrss.exe                               600    376     11    395 2010-10-29 17:08:54 UTC+0000
.. 0x81da5650:winlogon.exe                            624    376     19    570 2010-10-29 17:08:54 UTC+0000
... 0x82073020:services.exe                           668    624     21    431 2010-10-29 17:08:54 UTC+0000
.... 0x81fe52d0:vmtoolsd.exe                         1664    668      5    284 2010-10-29 17:09:05 UTC+0000
..... 0x81c0cda0:cmd.exe                              968   1664      0 ------ 2011-06-03 04:31:35 UTC+0000
...... 0x81f14938:ipconfig.exe                        304    968      0 ------ 2011-06-03 04:31:35 UTC+0000
.... 0x822843e8:svchost.exe                          1032    668     61   1169 2010-10-29 17:08:55 UTC+0000
..... 0x822b9a10:wuauclt.exe                          976   1032      3    133 2010-10-29 17:12:03 UTC+0000
..... 0x820ecc10:wscntfy.exe                         2040   1032      1     28 2010-10-29 17:11:49 UTC+0000
.... 0x81e61da0:svchost.exe                           940    668     13    312 2010-10-29 17:08:55 UTC+0000
.... 0x81db8da0:svchost.exe                           856    668     17    193 2010-10-29 17:08:55 UTC+0000
..... 0x81fa5390:wmiprvse.exe                        1872    856      5    134 2011-06-03 04:25:58 UTC+0000
.... 0x821a0568:VMUpgradeHelper                      1816    668      3     96 2010-10-29 17:09:08 UTC+0000
.... 0x81fee8b0:spoolsv.exe                          1412    668     10    118 2010-10-29 17:08:56 UTC+0000
.... 0x81ff7020:svchost.exe                          1200    668     14    197 2010-10-29 17:08:55 UTC+0000
.... 0x81c47c00:lsass.exe                            1928    668      4     65 2011-06-03 04:26:55 UTC+0000
.... 0x81e18b28:svchost.exe                          1080    668      5     80 2010-10-29 17:08:55 UTC+0000
.... 0x8205ada0:alg.exe                               188    668      6    107 2010-10-29 17:09:09 UTC+0000
.... 0x823315d8:vmacthlp.exe                          844    668      1     25 2010-10-29 17:08:55 UTC+0000
.... 0x81e0eda0:jqs.exe                              1580    668      5    148 2010-10-29 17:09:05 UTC+0000
.... 0x81c498c8:lsass.exe                             868    668      2     23 2011-06-03 04:26:55 UTC+0000
.... 0x82279998:imapi.exe                             756    668      4    116 2010-10-29 17:11:54 UTC+0000
... 0x81e70020:lsass.exe                              680    624     19    342 2010-10-29 17:08:54 UTC+0000
 0x820ec7e8:explorer.exe                             1196   1728     16    582 2010-10-29 17:11:49 UTC+0000
. 0x81c543a0:Procmon.exe                              660   1196     13    189 2011-06-03 04:25:56 UTC+0000
. 0x81e86978:TSVNCache.exe                            324   1196      7     54 2010-10-29 17:11:49 UTC+0000
. 0x81e6b660:VMwareUser.exe                          1356   1196      9    251 2010-10-29 17:11:50 UTC+0000
. 0x8210d478:jusched.exe                             1712   1196      1     26 2010-10-29 17:11:50 UTC+0000
. 0x81fc5da0:VMwareTray.exe                          1912   1196      1     50 2010-10-29 17:11:50 UTC+0000

C:\Users\Olly>
```

شکل ۲-۷ : خروجی پلاگین pstree

فرایند مشکوک ما، lsass.exe، بصورت نرمال توسط winlogon.exe اجرا می‌شود.

e. به شکل زیر نگاه کنید. تنها یک lsass.exe توسط winlogon.exe آغاز شده است (با PID 680) ؛ دوتای دیگر توسط services.exe آغاز شده است! بنابراین، lsass.exe با PID های ۸۶۸ و ۱۹۲۸ می تواند مخرب باشند.

f. ما دو فرآیند پنهانی مخرب داریم. اجازه دهید DLL هایی که توسط این فرآیند ها با استفاده از پلاگین dlllist بارگذاری شده اند را بررسی کنیم:

```
volatility_2.6_win64_standalone.exe -f X:stuxnet.vmem
--
profile=WinXPSP3x86 -p 868
```

```
Command Prompt
Volatility Foundation Volatility Framework 2.6
**************************************************************************
lsass.exe pid:    868
Command line : "C:\WINDOWS\\system32\\lsass.exe"
Service Pack 3

Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x01000000     0x6000     0xffff C:\WINDOWS\system32\lsass.exe
0x7c900000    0xaf000     0xffff C:\WINDOWS\system32\ntdll.dll
0x7c800000    0xf6000     0xffff C:\WINDOWS\system32\kernel32.dll
0x77dd0000    0x9b000     0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000    0x92000     0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000    0x11000     0xffff C:\WINDOWS\system32\Secur32.dll
0x7e410000    0x91000     0xffff C:\WINDOWS\system32\USER32.dll
0x77f10000    0x49000     0xffff C:\WINDOWS\system32\GDI32.dll

C:\Users\Olly>
```

شکل ۲-۸ : خروجی پلاگین dlllist برای فرآیند مشکوک با PID 868

```
volatility_2.6_win64_standalone.exe -f X:stuxnet.vmem
profile=WinXPSP3x86 -p 1928
```

```
Command Prompt
Volatility Foundation Volatility Framework 2.6
**************************************************************************
lsass.exe pid:   1928
Command line : "C:\WINDOWS\\system32\\lsass.exe"
Service Pack 3

Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x01000000     0x6000     0xffff C:\WINDOWS\system32\lsass.exe
0x7c900000    0xaf000     0xffff C:\WINDOWS\system32\ntdll.dll
0x7c800000    0xf6000     0xffff C:\WINDOWS\system32\kernel32.dll
0x77dd0000    0x9b000     0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000    0x92000     0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000    0x11000     0xffff C:\WINDOWS\system32\Secur32.dll
0x7e410000    0x91000     0xffff C:\WINDOWS\system32\USER32.dll
0x77f10000    0x49000     0xffff C:\WINDOWS\system32\GDI32.dll
0x00870000   0x138000        0x1 C:\WINDOWS\system32\KERNEL32.DLL.ASLR.0360b7ab
0x76f20000    0x27000        0x2 C:\WINDOWS\system32\DNSAPI.dll
0x77c10000    0x58000       0x27 C:\WINDOWS\system32\msvcrt.dll
0x71ab0000    0x17000        0xa C:\WINDOWS\system32\WS2_32.dll
0x71aa0000     0x8000        0x8 C:\WINDOWS\system32\WS2HELP.dll
0x76d60000    0x19000        0x2 C:\WINDOWS\system32\IPHLPAPI.DLL
0x5b860000    0x55000        0x2 C:\WINDOWS\system32\NETAPI32.dll
0x774e0000   0x13d000        0x5 C:\WINDOWS\system32\ole32.dll
0x77120000    0x8b000        0x4 C:\WINDOWS\system32\OLEAUT32.dll
0x76bf0000     0xb000        0x2 C:\WINDOWS\system32\PSAPI.DLL
0x7c9c0000   0x817000        0x2 C:\WINDOWS\system32\SHELL32.dll
0x77f60000    0x76000        0x8 C:\WINDOWS\system32\SHLWAPI.dll
0x769c0000    0xb4000        0x2 C:\WINDOWS\system32\USERENV.dll
0x77c00000     0x8000        0x2 C:\WINDOWS\system32\VERSION.dll
0x771b0000    0xaa000        0x2 C:\WINDOWS\system32\WININET.dll
0x77a80000    0x95000        0x2 C:\WINDOWS\system32\CRYPT32.dll
0x77b20000    0x12000        0x2 C:\WINDOWS\system32\MSASN1.dll
0x71ad0000     0x9000        0x2 C:\WINDOWS\system32\WSOCK32.dll
0x773d0000   0x103000        0x2 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0
.2600.5512_x-ww_35d4ce83\comctl32.dll
0x5d090000    0x9a000        0x1 C:\WINDOWS\system32\comctl32.dll

C:\Users\Olly>_
```

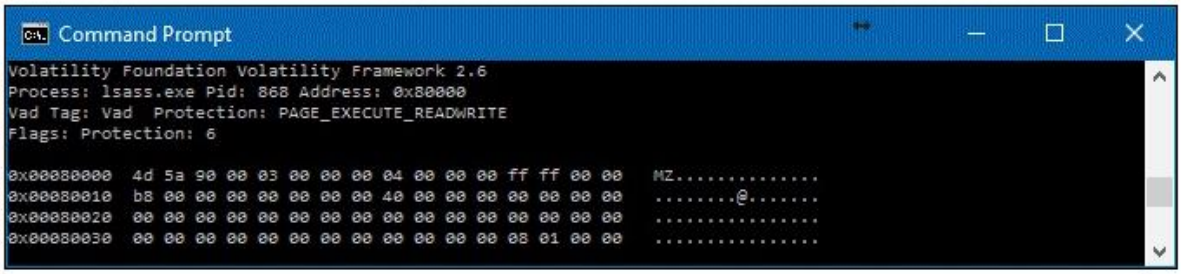
شکل ۲-۹ : خروجی پلاگین dlllist برای فرآیند مشکوک با PID 1928

g. به شکل بالا نگاه کنید. با توجه به توصیف تهدیدات Stuxnet در وب سایت F-Secure، یک فایل DLL رمزگذاری شده باید به یک فرایند تزریق شود و دارای این نام است: [normaldll].ASLR.[random]

h. حالا یکی دیگر از اثرات Stuxnet -KERNEL32.DLL.ASLR.0360b7ab پیدا کرده ایم.

یکی دیگر از پلاگین‌های Volatility بسیار مفید، falfind است. این افزونه به تست کنندگان دیجیتال قانونی کمک می کند تا کد / DLL های مخفی یا تزریقی را در حافظه مد کاربر پیدا کنند. این پلاگین را برای فرایند lsass.exe اجرا می‌کنیم.

```
volatility_2.6_win64_standalone.exe -f X:stuxnet.vmem
--
profile=WinXPSP3x86 malfind -p 868 --dump-dir
X:Stuxnet
```



شکل ۲-۱۰ : بخشی از پلاگین malfind برای فرآیند مشکوک با PID 868

همانطور که می بینید، از switch -dump-dir نیز استفاده کردیم تا DLL ها را به یک پوشه منتقل کنیم. پس از آن می توانیم، برای مثال، آنها را به VirusTotal آپلود کنیم. البته، بسیاری از آنها به عنوان مخرب شناخته شده اند. به عنوان مثال، فرایند 0x81c47c00.0x80000.dmp استخراج شده از lsass.exe با PID 1928 توسط Dr.Web Antivirus به عنوان Trojan.Stuxnet.1 شناسایی شده‌است.

در لیست زیر پلاگین های مورد استفاده در این دستورالعمل توضیح داده می‌شود.

- ✓ **Imageinfo**: این افزونه اطلاعاتی راجع به نسخه حافظه ای در حال تجزیه و تحلیل را جمع آوری می کند: سیستم عامل، پک سرویس، معماری سخت افزار، و همچنین اطلاعات مفید مانند آدرس DTB، آدرس KDBG، و زمان نشانه ایجاد نسخه کپی.
- ✓ **Pslist**: این پلاگین فرآیندهای سیستم را نشان می دهد، از جمله آفست، نام پروسه، شناسه پردازش، شناسه پروسه والد، تعداد نخ‌ها، تعداد دسته ها، تاریخ / ساعت زمانی شروع و خروج فرایند، Session ID.
- ✓ **Pstree**: این افزونه همانند pslist است، اما لیست فرایندها را در فرم درخت نشان می دهد. از indentation و دوره ها برای نشان دادن فرآیندهای فرزند استفاده می کند.
- ✓ **DllList**: این افزونه DLL هایی را که در فرآیند مورد نظر بارگذاری شده‌اند را نمایش می دهد.
- ✓ **Malfind**: این افزونه به تست کننده اجازه می‌دهد به شناسایی و استخراج کدهای مخفی یا تزریقی / DLL ها در حافظه مد کاربر برای اسکن و تجزیه و تحلیل بیشتر آنتی ویروس، بپردازد.

فصل ۳ : درایوهای سیستم عامل

ابزارهای اکتساب درایو ویندوز که در این فصل بررسی خواهیم کرد به صورت زیر است.

- **اکتساب درایو در فرمت E01 با FTK imager**
- **اکتساب درایو در فرمت RAW با dc3dd**
- **اکتساب نسخه های قانونی با Arsenal Image Mounter**

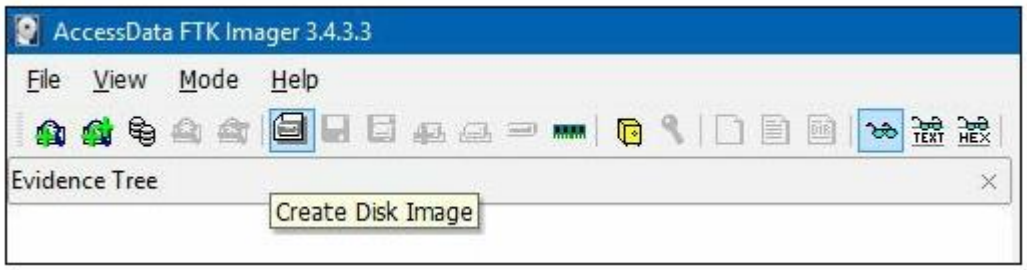
در ادامه هریک یک از این ابزارها به صورت مفصل بررسی خواهد شد.

۳-۱- اکتساب درایو در فرمت E01 با FTK

FTK Imager یک ابزار پیش نمایش نسخه برداری تصویری و داده ای توسط AccessData است که اجازه می دهد تا تست کننده نه تنها تصاویر قانونی در فرمت های مختلف از جمله RAW، SMART، E01 و AFF، ایجاد کند بلکه پیش نمایش منابع داده‌ها به روش قانونی sound را فراهم می‌کند. در اولین دستورالعمل، ما به شما نشان خواهیم داد که چگونه یک تصویر قانونی از هارد دیسک از یک سیستم ویندوز در فرمت E01 ایجاد کنید.

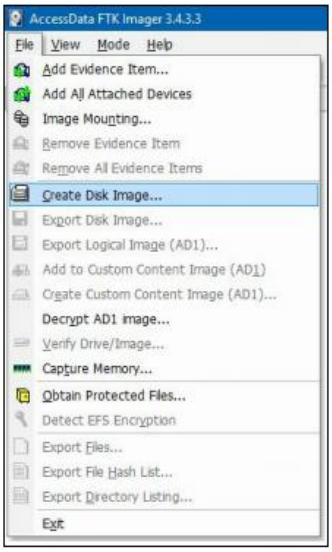
دو راه برای آغاز پردازش تصویر درایو وجود دارد:

a. استفاده از دکمه Create Disk Image در نوار ابزار



شکل ۳-۱ : دکمهCreate Disk Image در نوار ابزار

b. استفاده از گزینه Create Disk Image ... از منوی File



شکل ۳-۲ : گزینه Create Disk Image

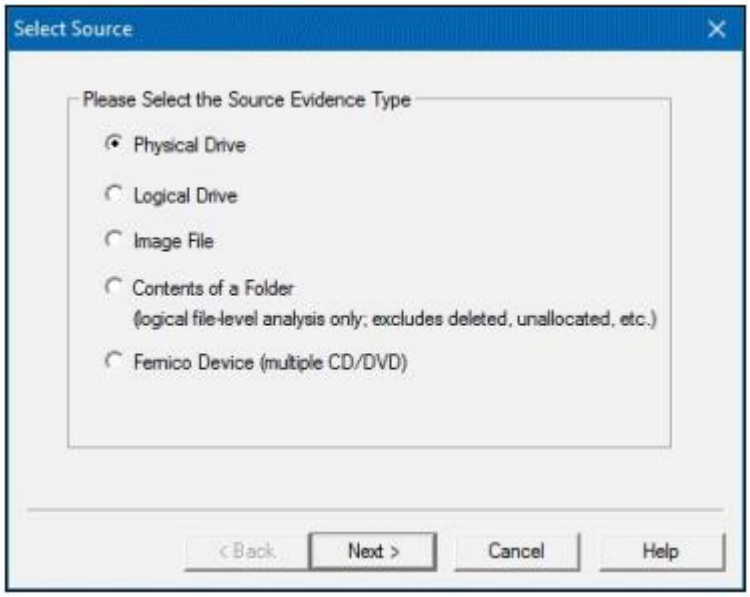
شما می توانید هر کدام را که ترجیح می دهید، انتخاب کنید.

اولین پنجره ای که می بینید انتخاب منبع است. در اینجا شما پنج گزینه دارید:

- ✓ **Physical drive**: این گزینه به شما اجازه می دهد یک درایو فیزیکی را به عنوان منبع انتخاب کنید، با تمام پارتیشن ها و فضای غیر اختصاص داده شده.
- ✓ **Logical drive**: این گزینه به شما اجازه می دهد یک درایو منطقی را به عنوان منبع انتخاب کنید، مثلا E: \ drive.
- ✓ **Image file**: این گزینه به شما اجازه می دهد یک فایل تصویری را به عنوان منبع انتخاب کنید، به عنوان مثال، تصویر جرم‌شناسی خود را از یک فرمت به دیگری تبدیل کنید.
- ✓ **Contents of tables**: این گزینه به شما اجازه می دهد یک پوشه را به عنوان منبع انتخاب کنید. مطمئنا، فایلهای حذف شده گنجانده نخواهند شد.
- ✓ **Fernico Device**: این گزینه امکان ذخیره سازی تصویر بر روی سی دی یا دی وی دی را فراهم می‌کند.

البته ما می خواهیم از کل درایو را نسخه برداری کنیم تا قادر به کار با داده های حذف شده و فضای غیر اختصاصی باشد، بنابراین:

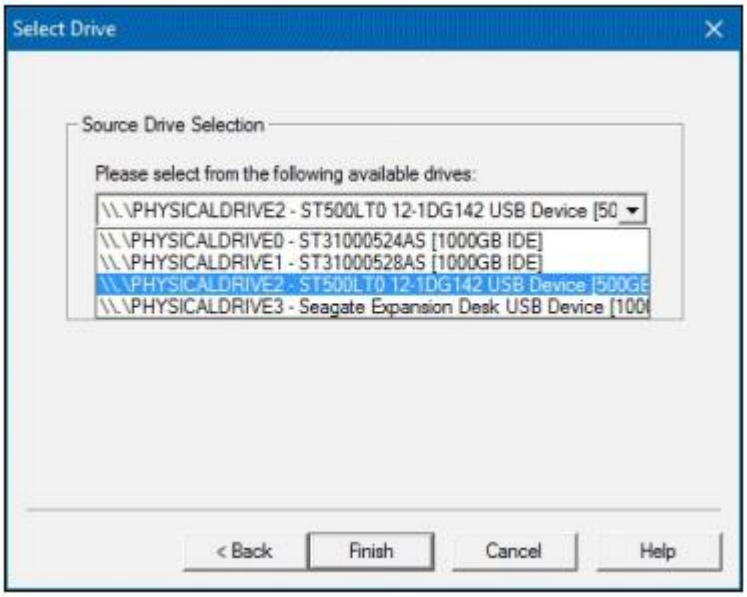
c. گزینه physical drive را انتخاب کنید.



شکل ۳-۳ : پنجره انتخاب منبع FTK Imager

d. روی Next کلیک کنید و در پنجره بعدی – Drive را انتخاب کنید.

e. حالا باید درایور منبع را از منوی کشویی انتخاب کنید، در مورد ما \\.\ PHYSICALDRIVE2.

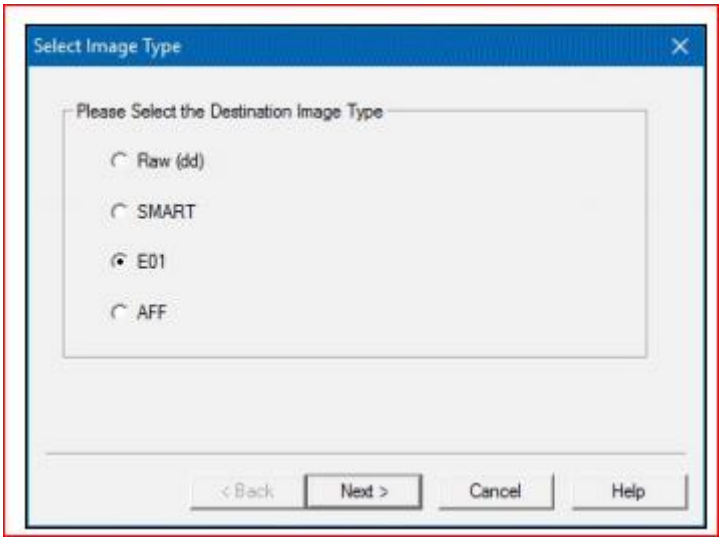


شکل ۳-۴ : پنجره انتخاب درایو در FTK Imager

f. حالا که منبع درایو انتخاب شده است، روی Finish کلیک کنید.

g. پنجره بعدی "ایجاد نسخه" است. به زودی به این پنجره بازخواهیم گشت، اما اکنون فقط روی Add کلیک کنید.

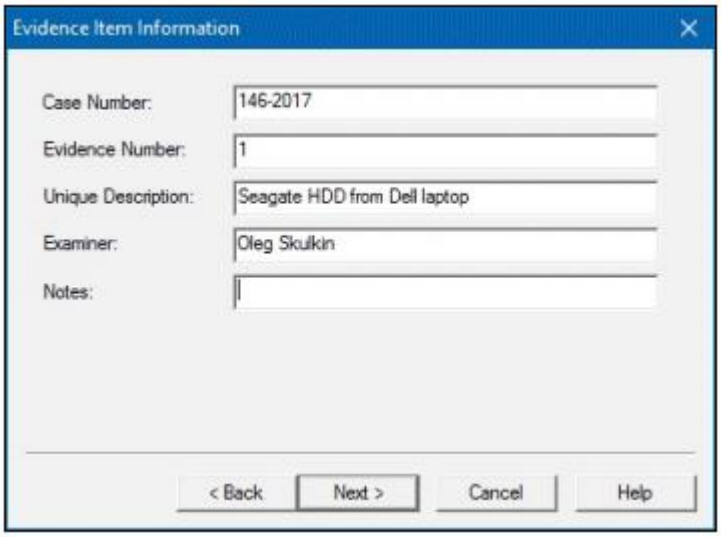
h. زمان انتخاب نوع تصویر مقصد است. در اینجا نسخه خود را در فرمت Evidance Encase ایجاد کرده، در اینجا E01 را انتخاب کنید.



شکل ۳-۵ : پنجره انتخاب نوع تصویر

i. روی Next کلیک کنید و پنجره Evidence Item Information را مشاهده خواهید کرد.

در اینجا، ما پنج فیلد برای پر کردن داریم: Case Number، Evidence Number، Unique Description، Examiner و Notes. تمام گزینه ها اختیاری هستند.



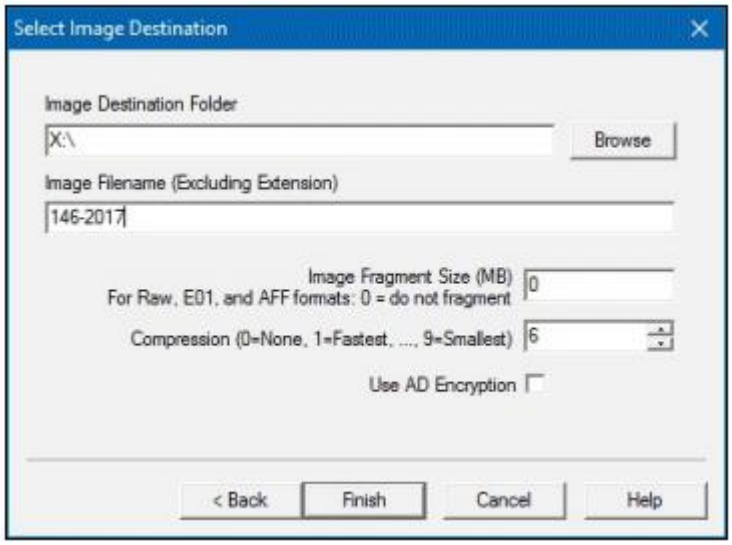
شکل ۳-۶ : پنجره Evidence Item Information

j. فیلدها را پر کنید یا اگر ترجیح می دهید آنرا رد کنید و سپس روی Next کلیک کنید.

k. حالا مقصد تصویر را انتخاب کنید. شما می توانید از دکمه Browse برای این کار استفاده کنید.

l. همچنین باید نام فایل تصویر را پر کنید.

اگر می خواهید نسخه تصویر قانونی خود را داشته باشید، اندازه قطعه (در مگابایت) را انتخاب کنید. فرمت E01 از فشرده سازی پشتیبانی می کند، بنابراین اگر می خواهید اندازه نسخه را کاهش دهید، می توانید از این ویژگی استفاده کنید. همانطور که در شکل زیر می بینید، ما ۶ را انتخاب کرده‌ایم و اگر می‌خواهید داده‌ها در تصویر کدگذاری شوند، از ویژگی Encryption AD استفاده کنید.

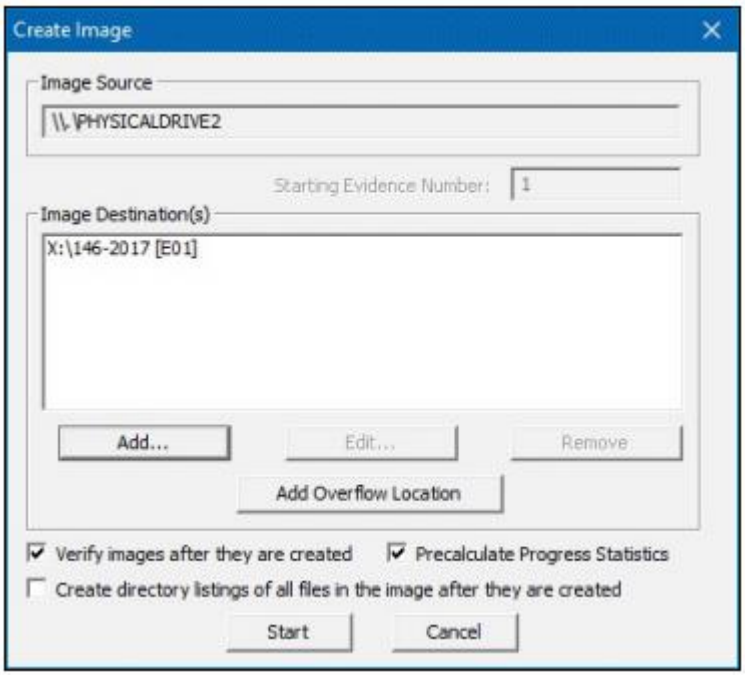


شکل ۳-۷ : پنجره تعیین آدرس مقصد

m. روی Finish کلیک کنید و پنجره ایجاد تصویر را دوباره خواهید دید.

n. به سه گزینه در پایین پنجره نگاه کنید.

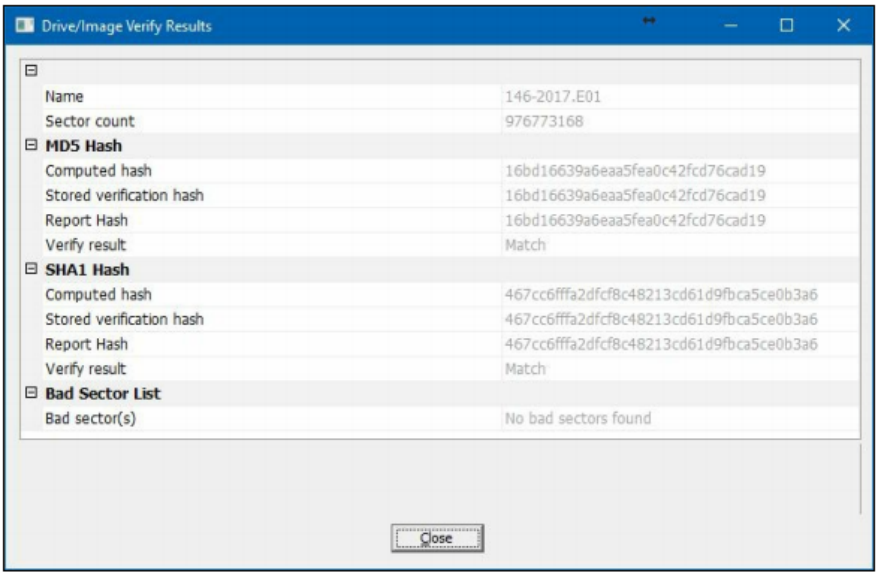
فرآیند تأیید بسیار مهم است، بنابراین اطمینان حاصل کنید که گزینه تأیید پس از ایجاد تصویر انتخاب شوند. این به شما کمک می کند تا مطمئن شوید که منبع و تصویر برابر هستند. گزینه Precalculated Progress Statistics نیز بسیار مفید است: به شما زمان تخمینی ورود در طول فرآیند imaging را نشان می دهد. آخرین گزینه فهرستی از تمام فایلهای تصویر را برای شما ایجاد میکند، اما البته، زمان نیاز دارد، پس فقط زمانیکه نیاز دارید از آن استفاده کنید.



شکل ۳-۸ : پنجره ایجاد تصویر در FTK imager

o. بر روی گزینه start کلیک کنید.

p. در نهایت، یک پنجره Drive/ImageVerifyResults را دریافت می کنید..



شکل ۳-۹ : پنجره نتایج FTK Imager Drive/Image

FTK Imager از درایو فیزیکی که شما انتخاب کرده اید به عنوان منبع استفاده می کند و یک تصویر بیت به بیت از آن را در قالب فایل Evidence File EnCase ایجاد می کند. در طول فرآیند تأیید، هش های MD5 و SHA1 از تصویر و منبع مقایسه می شوند.

۳-۲- اکتساب درایو در فرمت RAW با DC3DD

DC3DD یک نسخه پچ از نرم افزار GNU DD کلاسیک با برخی از ویژگی‌های جرم‌شناسی کامپیوتر است. برای مثال، هش با تعدادی الگوریتم مانند MD5، SHA-1، SHA-256 و SHA-512، نشان دهنده پیشرفت فرآیند کسب و غیره است. مراحل اکتساب درایو در قالب RAW با استفاده از DC3DD به شرح زیر است.

a. پنجره Command Prompt را باز کنید(شما می‌توانید از دستور cd برای انجام این کار استفاده کنید) ، دایرکتوری را به dc3dd.exe تغییر دهید و دستور زیر را تایپ کنید:

```
dc3dd.exe if=\\.\PHYSICALDRIVE2 of=X:\147-2017.dd hash=sha256
log=X:\147-2017.log
```

b. دکمه Enter را فشار دهید و فرایند اکتساب شروع خواهد شد.

بخش‌های مختلفی که در این بخش وجود دارند در ادامه توضیح داده می‌شود.

- ✓ **If:** مخفف فایل ورودی است در اصل، dd یک ابزار لینوکس بود، درایو فیزیکی ۲ را اینجا قرار می دهیم (این درایوی است که می خواهیم تصویر کنیم).
- ✓ **Of:** مخفف فایل خروجی است. در اینجا، شما باید مقصد تصویر خود را در فرمت RAW تایپ کنید. در مورد ما، این X: \ drive و فایل dd.۲۰۱۷-۱۴۷ است.
- ✓ **Hash:** همانطور که قبلا گفته شد، DC3DD از چهار الگوریتم هش پشتیبانی می کند: MD5، SHA-1، SHA-256 و SHA-512. ما SHA-256 را انتخاب کردیم، اما شما می توانید هریک از آنها را انتخاب کنید.
- ✓ **Log:** اینجا، شما باید مقصد را برای لاگ های مربوطه تایپ کنید. پس از اکتساب کامل، نسخه تصویر، تصویر هش و غیره در این فایل ذخیره می‌گردد.

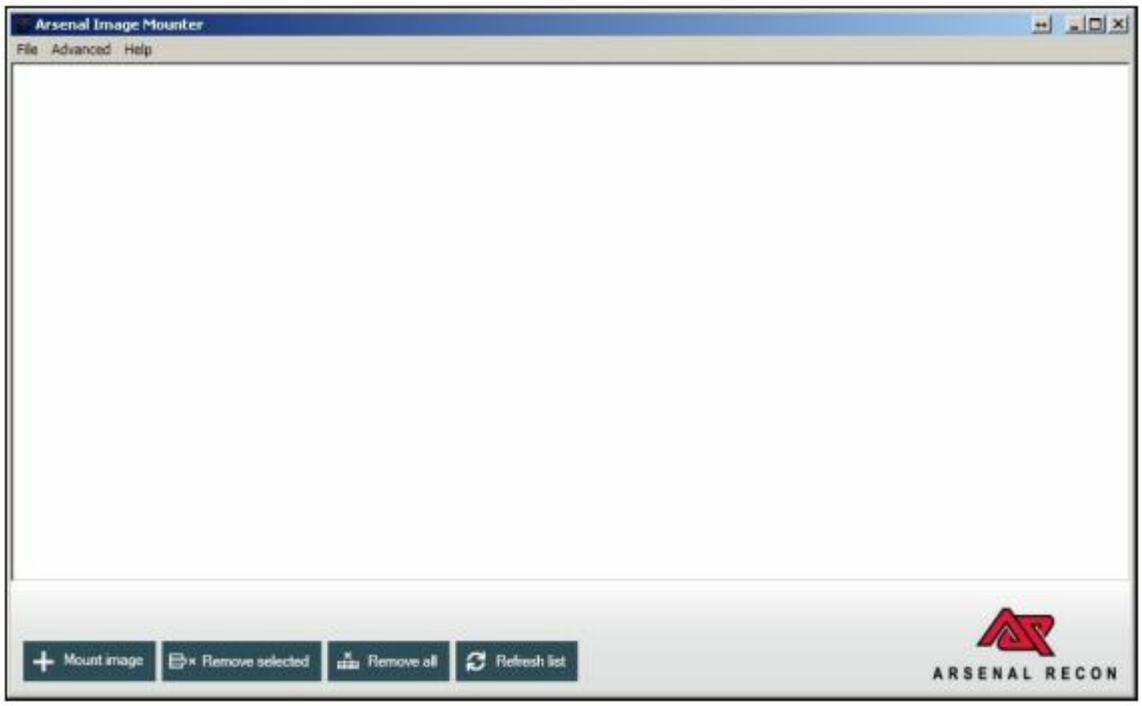
DC3DD یک تصویر بیت به بیت از درایو منبع را در قالب RAW ایجاد می کند، بنابراین اندازه تصویر همانند منبع خواهد بود و هش تصویر را با استفاده از الگوریتم انتخابی محاسبه می کند.

۳-۳- اکتساب نسخه های قانونی با Arsenal Image Mounter

Arsenal Image Mounter یک ابزار منبع باز است که توسط Arsenal Recon طراحی شده است. این ابزار می‌تواند یک تست دیجیتال قانونی برای نصب یک نسخه قانونی یا دیسک ماشین مجازی در ویندوز کمک کند. این ابزار از هر دو نسخه قانونی E01 (و EX01) و RAW پشتیبانی می‌کند، بنابراین شما می توانید آن را با هر یک از تصاویری که در دستور العمل های قبلی ایجاد شده است استفاده کنید.

مهم است که توجه داشته باشیم که Arsenal Image Mounter محتویات تصاویر دیسک را به عنوان دیسک های کامل کسب می کند. این ابزار از تمام فایل های سیستم شما که می توان بر روی درایوهای ویندوز یافت شود پشتیبانی می‌کند: NTFS، ReFS، FAT32 و exFAT .

دو راه برای انتخاب یک تصویر برای اکتساب در Arsenal Image Mounter وجود دارد. شما می توانید از منوی File (و Mount image ... را انتخاب کنید) یا بر روی دکمه Mount image همانطور که در شکل زیر می بینید، کلیک کنید.



شکل ۳-۱۰ : پنجره اصلی Arsenal Image Mounter

a. هنگامی که گزینه Mount image ... را از منوی File انتخاب می کنید یا روی دکمه Mount کلیک می‌کنید، پنجره بازشده بالا می آید - در اینجا باید یک تصویر را برای اکتساب انتخاب کنید.

b. پنجره بعدی که مشاهده می‌کنید ویژگی‌های Mount است.

شکل ۳-۱۱ : پنجره انتخاب گزینه های نصب در Arsenal Image Mounter

همانطور که می بینید، چند گزینه در اینجا وجود دارد.

- ✓ **Read only**: اگر این گزینه را انتخاب کنید، تصویر در حالت خواندن فقط نصب می شود، بنابراین عملیات نوشتن مجاز نیست.
- ✓ **Fake disk signature**: اگر امضای دیجیتال "تماما صفر" بر روی تصویر یافت شود، Arsenal Image Mounter یک امضا تصادفی دیسک را به ویندوز گزارش می دهد، به این معنی است که به درستی کسب شده است.
- ✓ **Write temporary**: اگر این گزینه را انتخاب کنید، تصویر در حالت خواندن و نوشتن نصب می شود، اما همه اصلاحات در فایل تصویر اصلی نیستند، بلکه در یک فایل متمایز موقت است.
- ✓ **Write original**: دوباره این گزینه تصویر را در حالت خواندن و نوشتن تنظیم می کند، اما این بار فایل تصویر اصلی تغییر خواهد کرد.
- ✓ **Sector size**: این گزینه به شما اجازه می دهد که اندازه سکتور را انتخاب کنید.

گزینه های مورد نیازتان را انتخاب کنید و روی OK کلیک کنید.

Arsenal Image Mounter تصاویر قانونی و یا دیسک های ماشین مجازی را به عنوان دیسک کامل در حالت خواندن یا خواندن و نوشتن نگه می دارد. بعدا یک محقق جرم شناسی دیجیتالی می تواند به نتایج خود حتی با ویندوز Explorer دسترسی پیدا کند.

فصل ۴ : تجزیه و تحلیل نسخه های ویندوز shadow

در این فصل به تجزیه و تحلیل اطلاعات موجود در shadow با استفاده از سه ابزار زیر خواهیم پرداخت.

- **مرور و کپی کردن فایل ها از VSC ها در یک سیستم با ShadowCopyView**
- **نصب VSC از تصاویر دیسک با VSSADMIN و MKLINK**
- **پردازش و تجزیه و تحلیل داده های VSC با Magnet AXIOM**

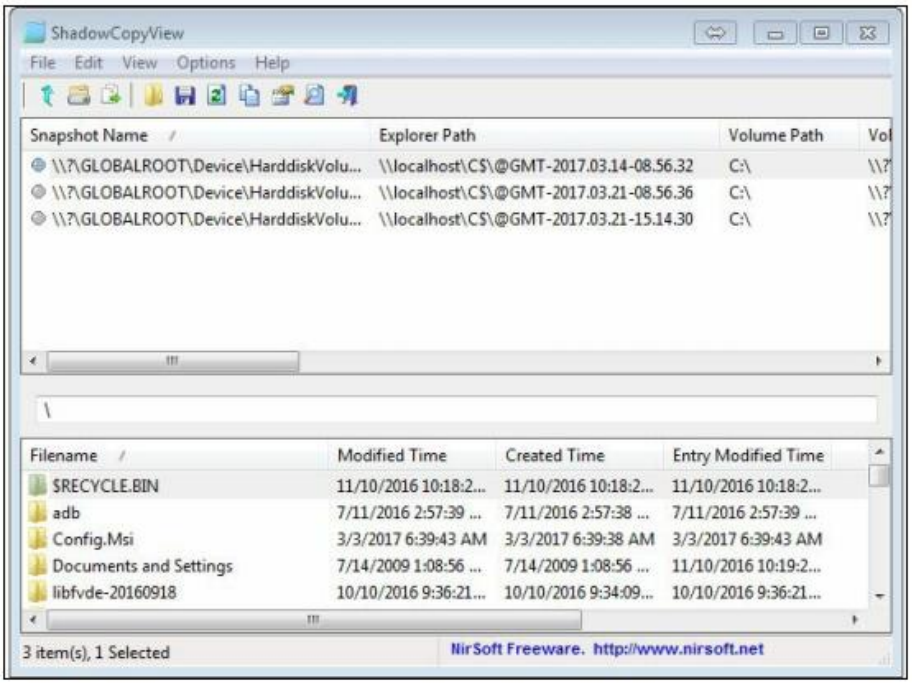
کپی سایه، همچنین به عنوان نسخه‌های سایه حجم شناخته می‌شود، کپی پشتیبان از فایل‌های ویندوز است که در طول دوره نرمال استفاده از یک ماشین در حال اجرا بر روی NTFS گرفته شده است. برای کاربر رایج کامپیوتری، نسخه های سایه ممکن است آشنا باشند، زیرا آنها چیزی است که امکان ایجاد پشتیبان گیری ویندوز را فراهم می‌کند.

این برنامه می‌تواند برای افراد خبره جرم شناسی دیجیتال مفید باشد، به ویژه در مواردی که یک مظنون ممکن است شواهد را از دستگاه حذف کند. با بازگرداندن سیستم به حالت قبلی خود و یا با استفاده از ابزارهای قانونی برای کشف فایل هایی که در مکان های کپی سایه ذخیره می شوند، متخصصین جرم شناسی می توانند اطلاعاتی را که فرد در تلاش برای پنهان کردن آن است، کشف کنند.

۴-۱- مرور و کپی‌کردن فایل ها از VSCها با استفاده از ShadowCopyView

ShadowCopyView ابزار ساده ای است که توسط NirSoft طراحی شده است که آزمون گرهای دیجیتال را قادر می سازد تا نسخه‌های فوری توسط Windows Volume Shadow Copy Service ایجاد نمایند. این ابزار حتی از آخرین نسخه های ویندوز پشتیبانی می کند، و می تواند بر روی درایو usb مورد نظرشما ذخیره شود.

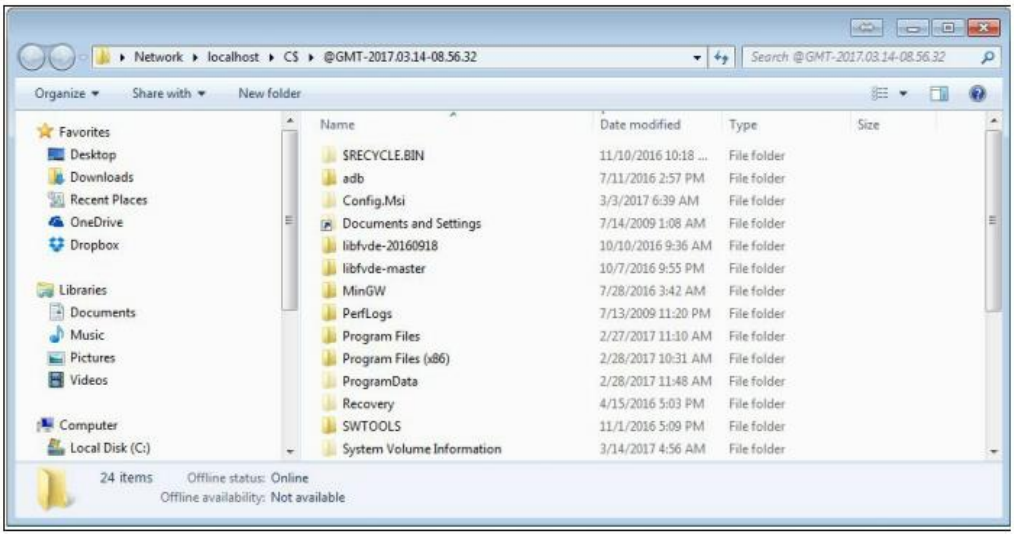
درایو فلش خود را به سیستم هدف وصل کنید. این ابزار به طور خودکار VSC های موجود را شناسایی می کند. همانطور که در شکل ۴-۱ می‌بینید در مورد ما سه VSC در دسترس وجود دارد.



شکل ۴-۱ : کپی‌های ایجاد شده توسط ShadowCopyView

پنجره اصلی ابزار شامل دو صفحه است. در قسمت اول اطلاعاتی درباره کدهای سایه شناسایی شده، از جمله نام، مسیر اکسپلورر، مسیر حجم، زمان ایجاد شده و غیره نمایش داده می شود. مسیر Explorer به این معنی است که شما می توانید کدهای سایه را در ویندوز اکسپلورر مرور کنید.

a. بر روی VSC که می خواهید در Explorer جستجو کنید، راست کلیک کرده و در «ویندوز اکسپلورر» گزینه open را انتخاب کنید، یا فقط F2 را فشار دهید.



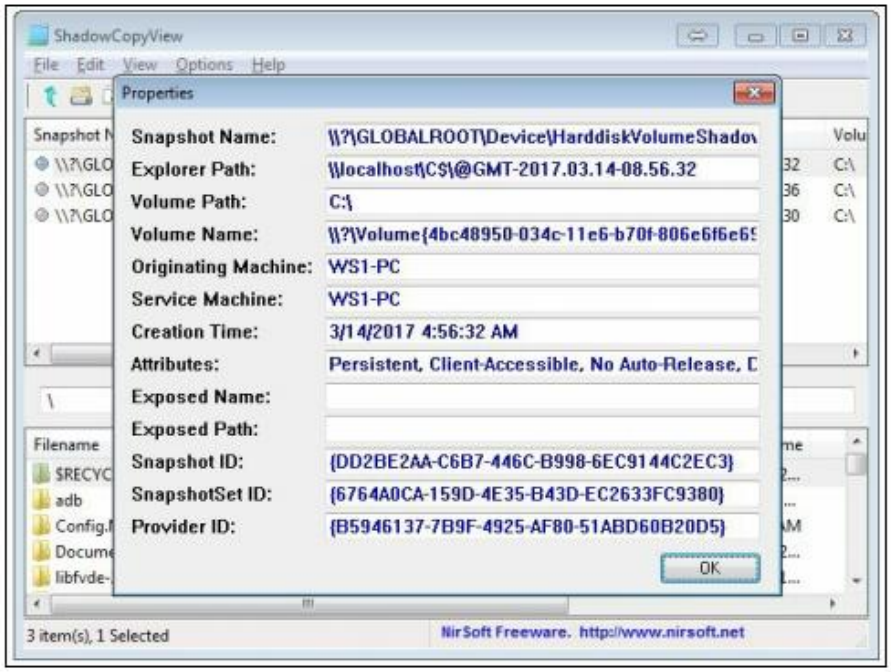
شکل ۴-۲ : باز کردن Volume Shadow Copy در ویندوز اکسپلورر

حالا، بیایید به ShadowCopyView بازگردیم، پنل دوم شما را قادر به براوز کدهای موجود در سایه می کند. با استفاده از این پنل، می توانید هر دو فایل و پوشه را اکسپورت کنید.

b. بر روی یک فایل یا پوشه کلیک راست کنید و گزینه Copy Selected Files To را انتخاب کنید یا فقط F8 را فشار دهید.

c. در این قسمت برخی از گزینه های مفید دیگری که می توانید استفاده کنید وجود دارد. به عنوان مثال، اگر برای زمان در UTC، زمان استاندارد را ترجیح می دهید، شما می توانید منطقه زمانی GMT را استفاده کنید. برای انجام این کار، به منوی options بروید و نمایش زمان GMT را انتخاب کنید.

d. همچنین اگر می‌خواهید لیست کامل ویژگی‌های یک کپی سایه را ببینید، می توانید بر روی آن راست کلیک کرده و گزینه Properties را انتخاب کنید یا فقط Alt + Enter را فشار دهید. حالا همه خواص را در یک پنجره (شکل ۴-۳) می‌بینید.



شکل ۴-۳ : لیست ویژگی های یک کپی shadow

و آخرین ویژگی بسیار مفیدی که بحث خواهیم کرد در مورد جستجوی کلید واژه است.

e. به Edit-Find بروید (یا Ctrl + F را فشار دهید) دراینجا مانند شکل ۴-۴ پنجره Find را مشاهده خواهید کرد.

شکل ۴-۴ : پنجره find در ShadowCopyView

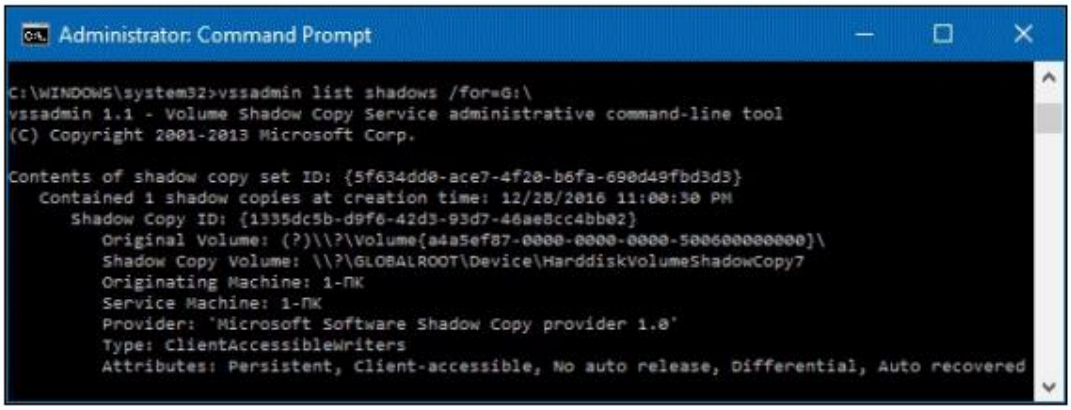
ShadowCopyView کپی های سایه ای موجود را تشخیص می دهد تا محقق جرم شناسی کامپیوتر آنها را از طریق ابزار و ویندوز اکسپلورر مرور کند و همچنین به آنها اجازه می دهد تا فایل ها و پوشه ها را جستجو و اکسپورت کنند.

۴-۲- نصب VSC از تصاویر دیسک با VSSADMIN و MKLINK

VSSADMIN یک ابزار خط فرمانی ویندوز است که قادر است کپی های حجم سایه را نمایش دهد. شما می توانید آن را نه تنها در یک سیستم عامل در حال اجرا، بلکه در تصاویر دیسک نیز استفاده کنید. در این دستورالعمل، ما به شما نشان خواهیم داد که چگونه این کار را انجام دهید. مراحل نصب VSC از تصاویر دیسک با استفاده از VSSADMIN و MKLINK به شرح زیر است:

a. ابتدا با Command Prompt شروع می‌کنیم (فراموش نکنید که آن را به عنوان Administrator اجرا کنید).

```
vssadmin list shadows /for=G:\
```

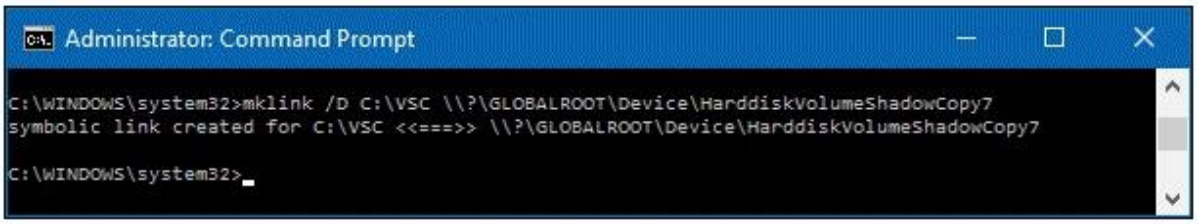


شکل ۴-۵ : خط فرمان برای شروع لیست VSSADMIN

قبلا تصویری ذخیره نموده ایم که شامل کپی سایه است.

b. مهمترین قسمت آن Shadow Copy Volume است، این تصویر در مسیر " \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7 " قرار دارد. اکنون آماده استفاده از MKLINK هستی تا کپی سایه ای که پیدا کردیم نصب شود. برای انجام این کار از دستور زیر استفاده کنید.

```
mklink /D C:\VSC \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7
```



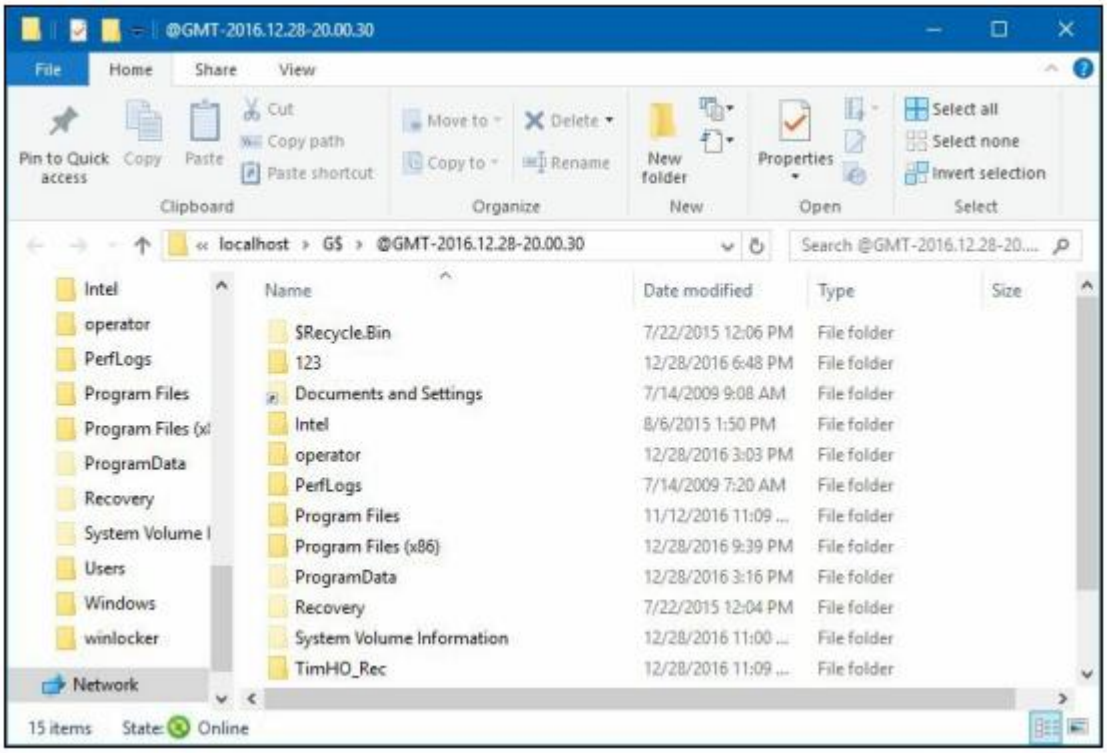
شکل ۴-۶ : خروجی برای دستور mklink /D C:\VSC \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7

MKLINK یک پوشه را ایجاد می‌کند (شما باید نام و محل آن را انتخاب کنید و آن را به عنوان بخشی از دستور تایپ کنید) و نسخه سایه آن را نصب می کند، بنابراین می توانید آن را مانند یک پوشه معمولی باز کنید.

c. راه دیگری برای استفاده از ویندوز اکسپلورر برای مرور VSC وجود دارد. ما باید مسیر VSC را در فرمت زیر دریافت کنیم:
\\ localhost \ G $ \ @ GMT-2016.12.28-20.00.30

بخش اول مسیر، \\ localhost \، همیشه یکسان است. بخش بعدی بستگی به درایو پارتیشن بوت دارد. در مورد ما این درایو G: \ است، بنابراین در مسیر آن G $ است. آخرین بخش بر اساس زمان ایجاد VSC است. شما می توانید آن را از خروجی VSSADMIN دریافت کنید، اما باید به GMT تبدیل شود. در حال حاضر فقط آن را به عنوان یک مسیر در ویندوز اکسپلورر تایپ کنید و مانند شکل زیر نسخه سایه برای بررسی در دسترس خواهد بود.

VSSADMIN کپی های حجم سایه را روی یک تصویر قانونی نصب می کند. MKLINK یک لینک نمادین را به کپی سایه ایجاد می کند، بنابراین یک جرم‌شناس دیجیتال می تواند آن را در ویندوز اکسپلورر مرور کند.



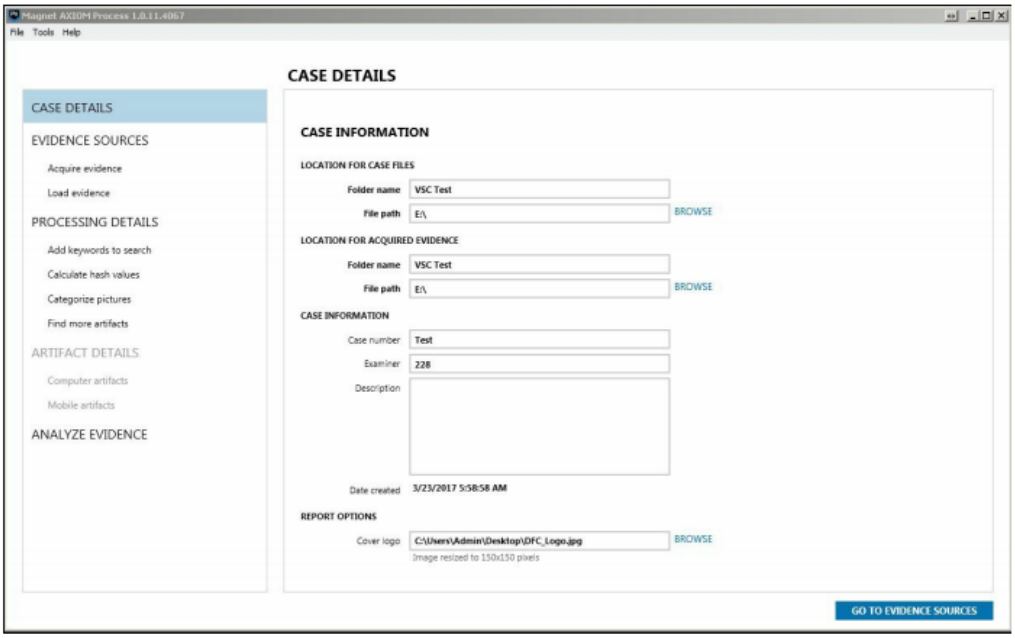
شکل ۴-۷ : یک Volume Shadow Copy در ویندوز اکسپلورر

۴-۳- پردازش و تجزیه و تحلیل داده های VSC با Magnet AXIOM

Magnet AXIOM یک ابزار جرم شناسی دیجیتال همه جانبه است که قادر به استخراج و پردازش داده ها از کامپیوتر و تلفن همراه است. این برنامه از بسیاری از نتایج جرم شناسی ویندوز پشتیبانی می کند، از جمله استخراج داده ها از نسخه های ویندوز سایه کپی. مراحل پردازش و تجزیه و تحلیل داده ها با استفاده از Magnet AXIOM به شرح زیر است:

a. فرایند Magnet AXIOM را شروع کنید.

b. همانطور که در شکل زیر مشخص است، اولین پنجره جزئیات CASE است.



شکل ۴-۸ : پنجره جزییات کیس در Magnet AXIOM

در اینجا، ما چهار بخش اصلی داریم:

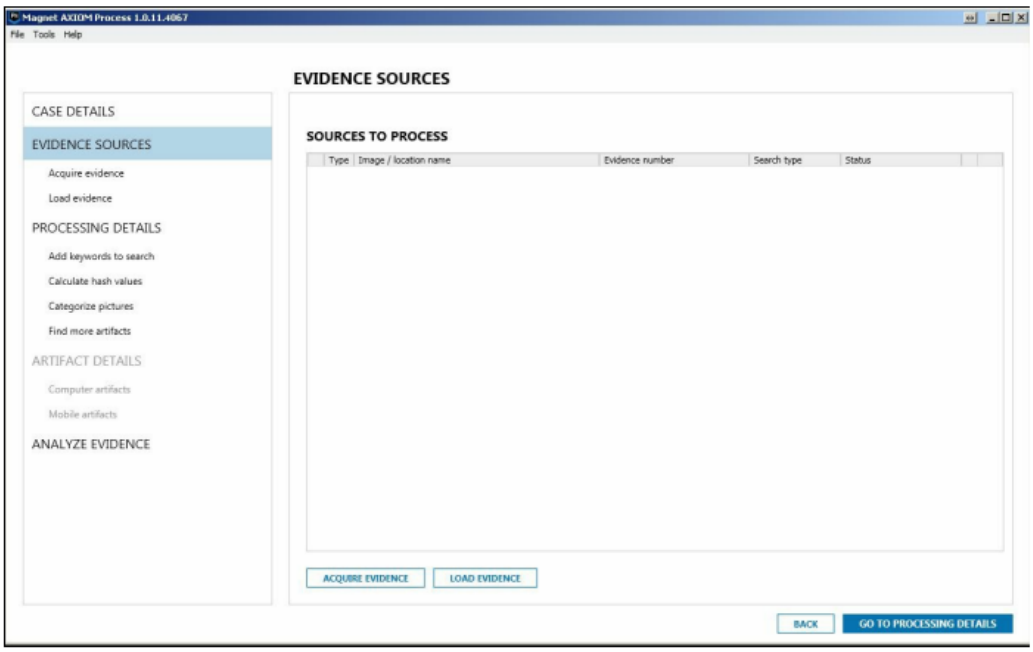
LOCATION FOR CASE FILES: در اینجا، باید نام پوشه و مسیر فایل را که در طول پردازش ایجاد می شود را انتخاب کنید.

LOCATION FOR ACQUIRED EVIDENCE: اگر قصد دارید درایو ها یا دستگاه های تلفن همراه را از طریق AXIOM بدست آورید، نام فایل و فولدر برای آنها را انتخاب کنید، یا فقط مسیر مشابه فایل های case را انتخاب کنید.

CASE INFORMATION: در این قسمت نام case، نام خود و توضیحات case را وارد کنید.

REPORT OPTIONS: اگر آرم یا لوگوی خود را دارید، می توانید آن را با کلیک بر روی فهرست انتخاب کنید. اطمینان حاصل کنید که تصویر مربع است، زیرا تا ۱۵۰ * ۱۵۰ پیکسل تغییر خواهد کرد.

c. پس از تکمیل تمامی فیلد ها، می توانید روی GO TO SOURCES EVIDENCE کلیک کنید. شما می توانید پنجره SOURCES EVIDENCE که در شکل ۴-۹ نشان داده شده است را ببینید.

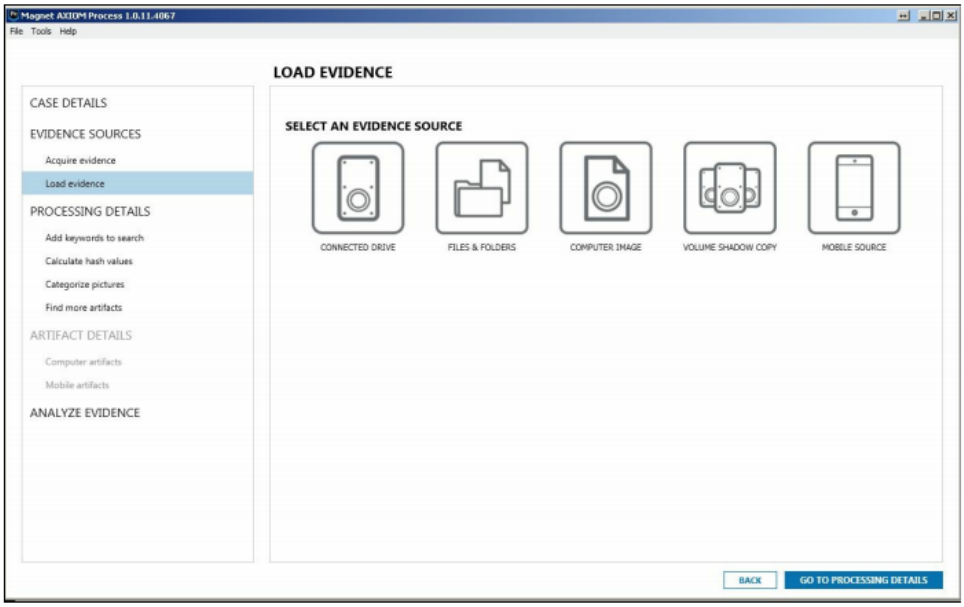


شکل ۴-۹ :پنجره Magnet AXIOM EVIDENCE SOURCES

در اینجا، ما دو گزینه داریم: ACQUIRE EVIDENCE و LOAD EVIDENCE.

d. ما قصد داریم از تصویری که قبلا بدست آورده ایم استفاده کنیم، بنابراین دکمه LOAD EVIDENCE را انتخاب می کنیم. شما می توانید از یکی از تصاویری که در دستورالعمل های قبلی بدست آورده‌اید استفاده کنید.

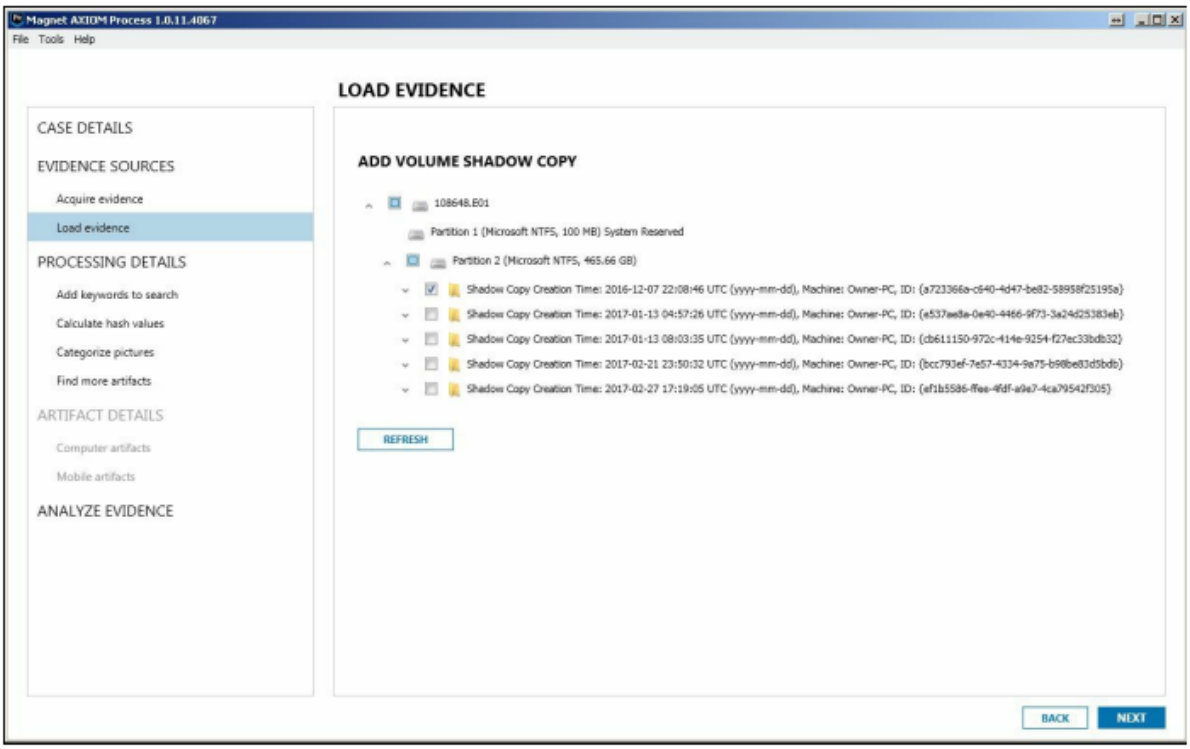
e. پنجره بعدی LOAD EVIDENCE است.



شکل ۴-۱۰ : پنجره Magnet AXIOM LOAD EVIDENCE

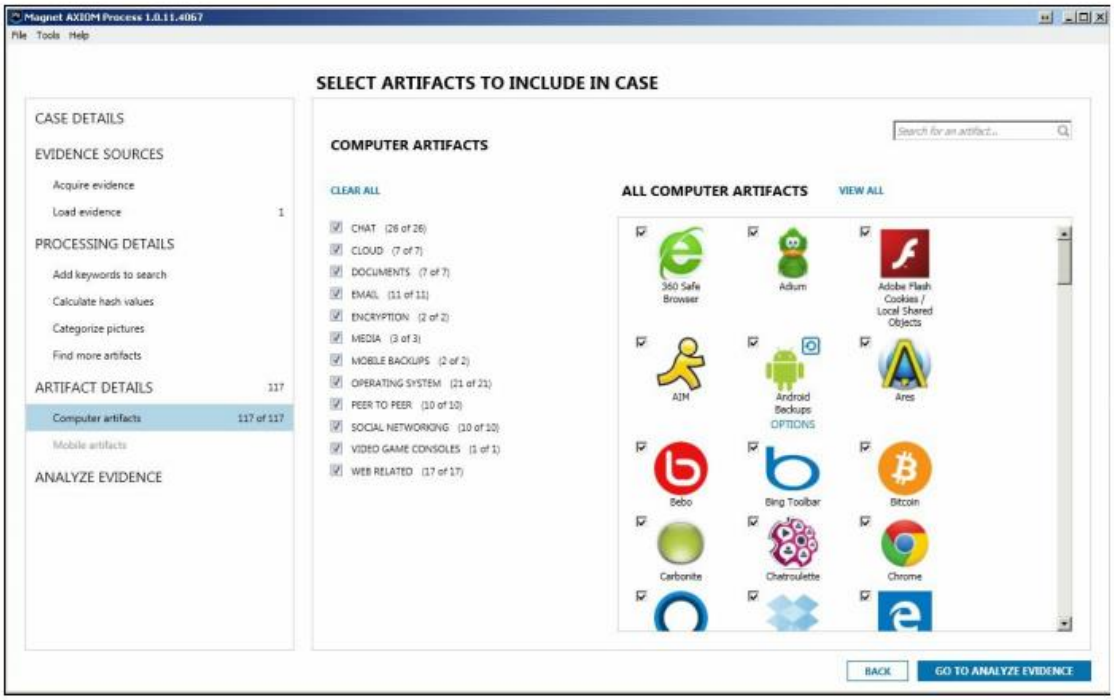
f. در اینجا، گزینه VOLUME COPY SHADOW وجود دارد. روی آن کلیک کنید و دو گزینه DRIVE و IMAGE نشان داده می شود.

g. همانطور که قبلا اشاره کردیم، ما قصد داریم از یک تصویر استفاده کنیم. هنگامی که شما آن را انتخاب می کنید، می توانید لیست کدهای سایه موجود در آن را ببینید.



شکل ۴-۱۱ : لیست olume Shadow Copies

h. شما می توانید یک یا چند نسخه سایه را انتخاب کرده و با کلیک بر روی NEXT به بخش جزئیات پردازش بروید. این بار ما این مرحله را رها کرده و به جزئیات دقیق نتایج می رویم (روی دکمه GO TO ARTIFATS DETAILS کلیک کنید).



شکل ۴-۱۲ : پنجره Magnet AXIOM SELECT ARTIFACTS TO INCLUDE IN CASE

i. برای اهداف تست، ما تمام آثار موجود را در این مورد گنجانده ایم. ابتدا روی دکمه GO TO ANALYZE EVIDENCE کلیک کنید و سپس بر روی دکمه ANALYZE EVIDENCE کلیک کنید. این شروع تست AXIOM Magnet خواهد بود.

j. پس از اتمام پردازش، نتایج را در Magnet AXIOM Exam مشاهده خواهید کرد.

Magnet AXIOMاسکن درایو یا یک تصویر برای کپی‌های Volume Shadowرا انجام داده و از آنها به عنوان منبع شواهد استفاده می کند. پس از آنکه تمام داده های موجود در نسخه های انتخاب شده سایه را پردازش کرد، با توجه به انتخاب های انجام شده توسط آزمونگر، عناصر قانونی را استخراج می‌کند.

فصل ۵ : آنالیز رجیستری

در این فصل به تجزیه و تحلیل رجیستری ویندوز با استفاده از ابزارهای زیر خواهیم پرداخت.

- **استخراج و مشاهده فایل‌های رجیستری ویندوز با Magnet AXIOM**
- **تجزیه فایل‌های رجیستری با RegRipper**
- **بازسازی فایل‌های رجیستری حذف شده با Registry Explorer**
- **تجزیه و تحلیل رجیستری با FTK Registry Viewer**

رجیستری ویندوز یکی از ثروتمندترین منابع مدارک دیجیتالی است. شما می توانید تعداد زیادی از اطلاعات مفیدی را هنگام بررسی دام و کدهای رجیستری پیدا کنید. اطلاعاتی مانند، تنظیمات کامپیوتر، صفحات اخیرا بازدید شده و اسناد باز شده، دستگاههای USB متصل شده و بسیاری از آیتم‌های دیگر. رجیستری ساختاری درختی دارد. هر درخت از کلیدهایی تشکیل شده و هر کلید ممکن است یک یا چند زیر کلید و مقادیر داشته باشد. بسیار مهم است که بدانید فایل‌های در کجای رجیستری ذخیره می شوند. شش فایل اول در C: \ Windows \ System32 \ config قرار دارد.

- ✓ COMPONENTS
- ✓ DEFAULT
- ✓ SAM
- ✓ SECURITY
- ✓ SOFTWARE
- ✓ SYSTEM

برای هر حساب کاربری دو فایل وجود دارد:

- ✓ NTUSER.DAT, located at C:\Users\%Username%\
- ✓ UsrClass.dat, located at C:\Users\%Username%\AppData\Local\Microsoft\Windows

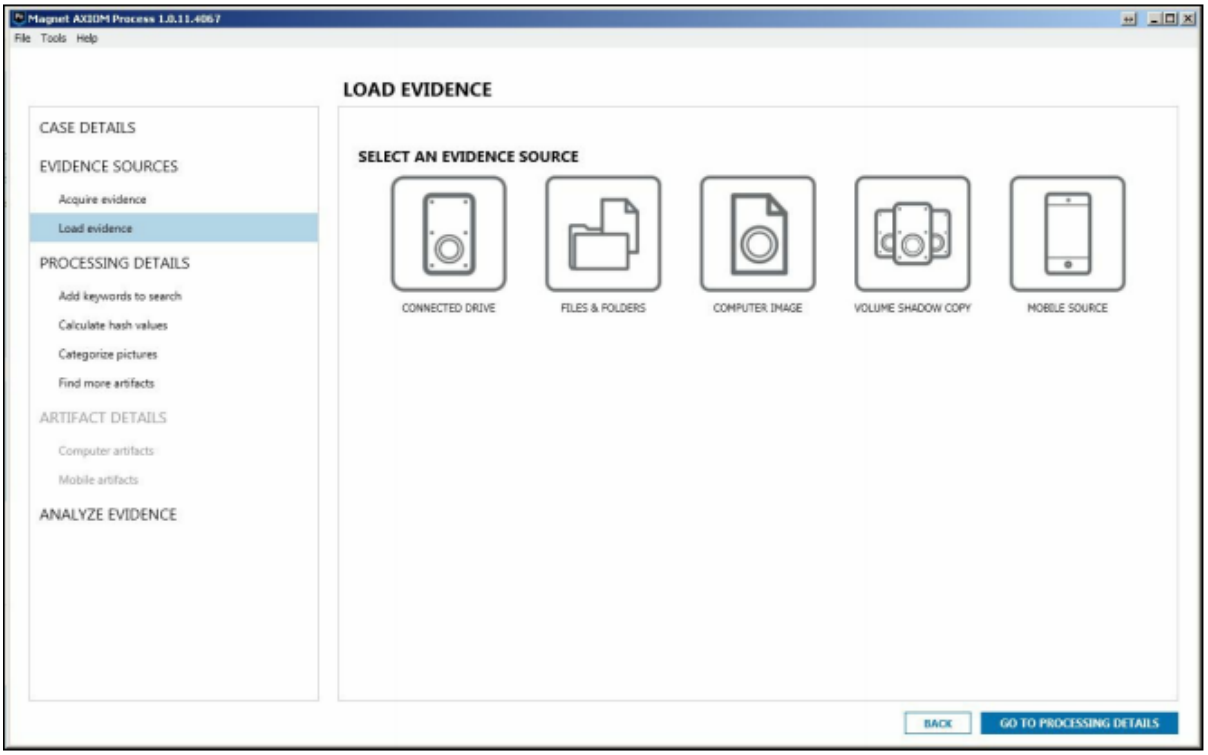
در این فصل ما به شما نحوه بررسی این فایل ها را با ابزارهای قانونی متن باز و نحوه بازیابی کلید های پاک شده، زیرکلید ها و ارزش ها را نشان خواهیم داد.

۵-۱- استخراج و مشاهده فایل های رجیستری ویندوز با Magnet AXIOM

قبلا تاحدودی درباره نحوه استفاده از Magnet AXIOM در استخراج و تجزیه و تحلیل داده ها از نسخه های سایه در تست جرم شناسی آشنا شده اید.اکنون شما یاد خواهید گرفت که برای پیشگیری از رجیستری ویندوز، چگونه از Magnet AXIOM، و به ویژه Component Registry Explorer استفاده کنید.

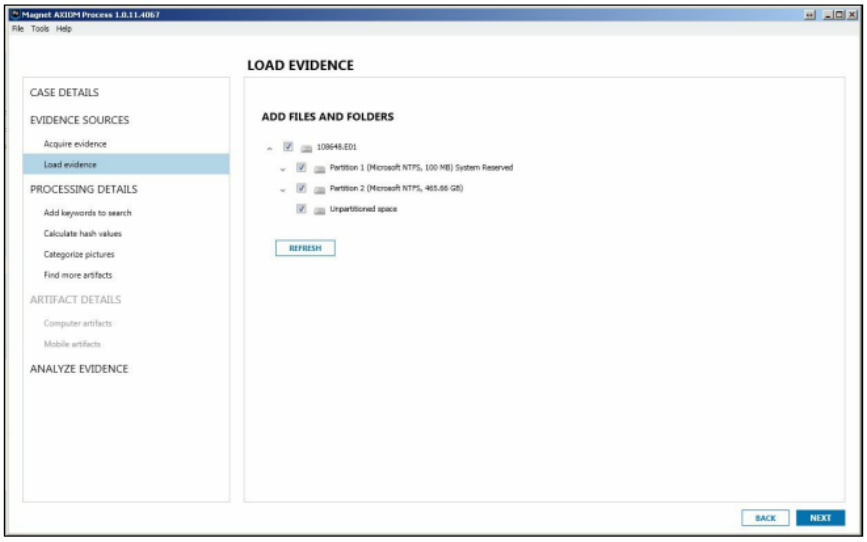
مراحل تجزیه و تحلیل رجیستری ویندوز با استفاده از Magnet AXIOM به شرح زیر است:

a. ابتدا یک case جدید ایجاد کنید. بعد از ایجاد و پرکردن تمام فیلدها، به منابع شواهد مراجعه کنید. روی دکمه Load evidence کلیک کنید و پنجره ی SELECT YOUR SOURCE SELECT، مانند شکل ۵-۱ را مشاهده خواهید کرد.



شکل ۵-۱ : پنجره Magnet AXIOM SELECT AN EVIDENCE SOURCE

b. این بار، گزینه انتخاب COMPUTER IMAGE را انتخاب کنید. باز هم می توانید از یکی از تصاویری که در دستورات قبلی بدست آورده اید استفاده کنید. فرمت های RAW و E01 پشتیبانی می شوند. با نگاهی به شکل ۵-۲، می توانیم ببینیم که تصویر ما شامل دو پارتیشن و یک فضای غیر مجزا است.



شکل ۵-۲ : پنجره Magnet AXIOM ADD FILES AND FOLDERS

c. می توانید فقط پارتیشن اصلی (پارتیشن ۲) را تیک بزنید، یا همه پارتیشن های موجود را انتخاب کنید. روی NEXT کلیک کنید تا مطابق شکل زیر به صفحه SELECT SEARCH TYPE وارد شوید.

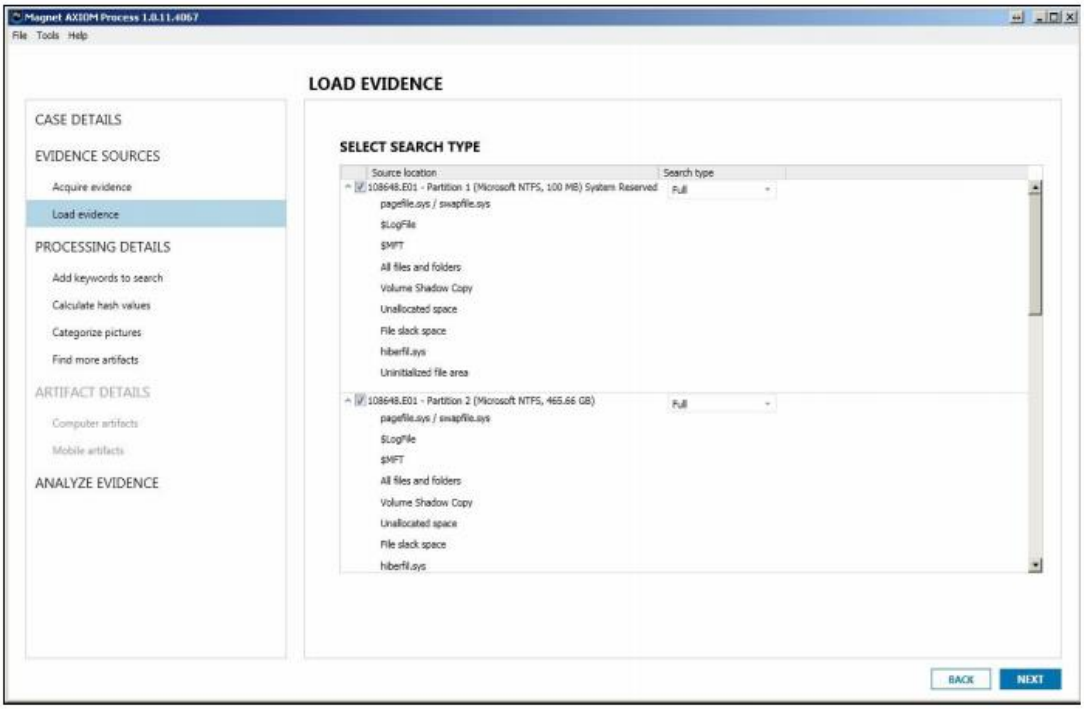
d. در فرآیند Magnet AXIOM چهار نوع جستجو وجود دارد:

Full: برای استخراج داده ها از تمام مکان ها شامل فضای غیر مجاز، کپی سایه ها و غیره.

Quick: برای استخراج داده ها از مناطق معمول استفاده می شود.

Sector level: این گزینه برای فایل سیستم‌های نامشخص یا خراب، و یا فرمت درایوهای بسیار مفید است.

Custom: این گزینه امکان انتخاب مکان ها را برای آزمونگر فراهم می کند. به عنوان مثال، اگر شما AXIOM را فقط برای فضایی غیر اختصاصی می خواهید، فقط می توانید این مکان را انتخاب کنید.



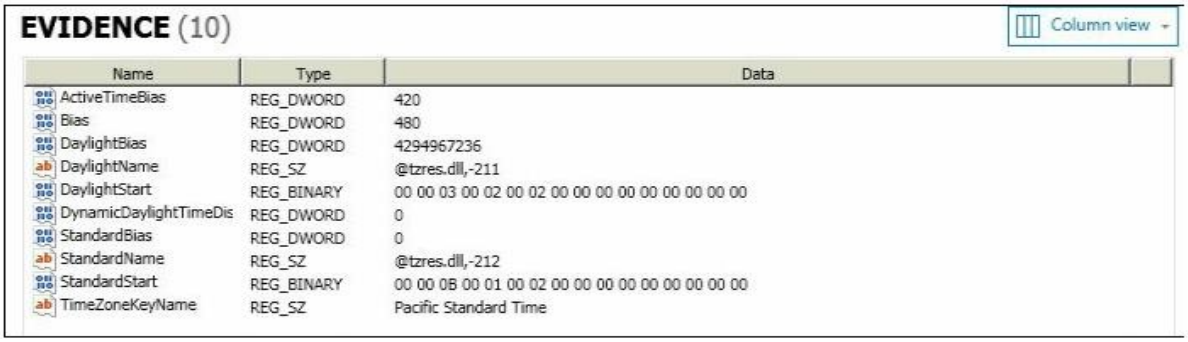
شکل ۵-۳ : پنجره Magnet AXIOM SELECT SEARCH TYPE

e. برای اهداف تست، شما می توانید تمام مکان ها را انتخاب کنید، اما برای پردازش آن زمان زیادی نیاز است. اگر شما نمی خواهید تغییراتی در این مرحله دهید، مستقیما به بخش تحلیلی ANALYZE بروید. روی دکمه ANALYZE EVIDENCE کلیک کنید و Magnet AXIOM Exam را نشان می دهد. هنگامی که پردازش منبع داده به پایان رسید، به منوی کشویی سمت چپ بروید، (مانند شکل زیر) و گزینه رجیستری را انتخاب کنید.

شکل ۵-۴ : پنل AXIOM Registry viewer's navigation

f. هنگام انتخاب این گزینه، می توان تمام فایل های موجود در رجیستری را در قسمت hive مشاهده کرد.

g. اگر بر روی علامت پلاس کنار یک فایل رجیستری کلیک کنید، می توانید محتویات آن را ببینید و همچنین مقادیر در پنل شواهد AXIOM Registry viewer را می توان دید.

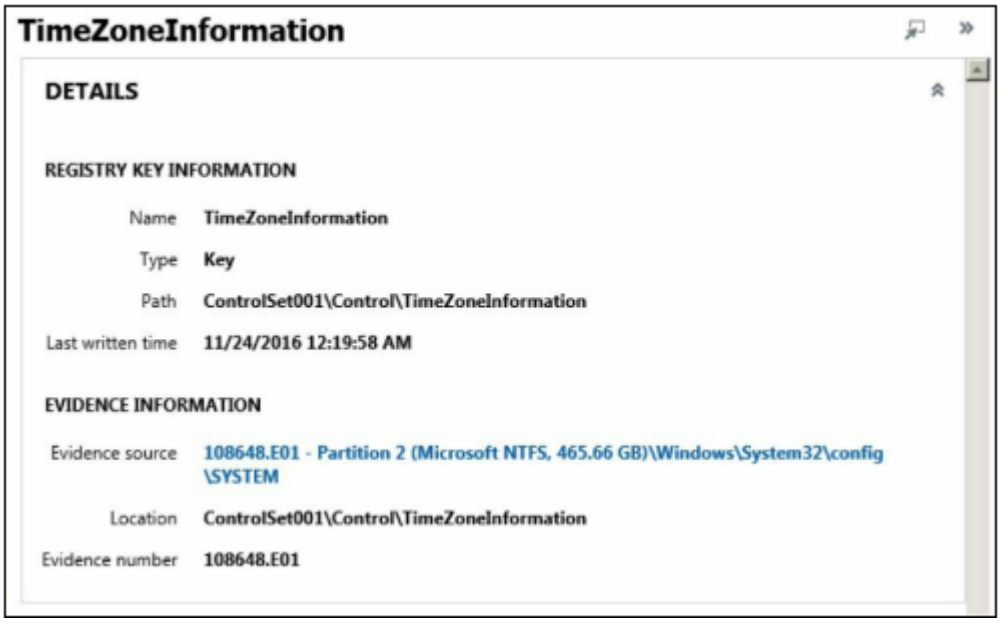


EVIDENCE (10) — Column view

Name	Type	Data
ActiveTimeBias	REG_DWORD	420
Bias	REG_DWORD	480
DaylightBias	REG_DWORD	4294967236
DaylightName	REG_SZ	@tzres.dll,-211
DaylightStart	REG_BINARY	00 00 03 00 02 00 02 00 00 00 00 00 00 00 00 00
DynamicDaylightTimeDis	REG_DWORD	0
StandardBias	REG_DWORD	0
StandardName	REG_SZ	@tzres.dll,-212
StandardStart	REG_BINARY	00 00 0B 00 01 00 02 00 00 00 00 00 00 00 00 00
TimeZoneKeyName	REG_SZ	Pacific Standard Time

شکل ۵-۵ : پنل شواهد AXIOM Registry viewer's

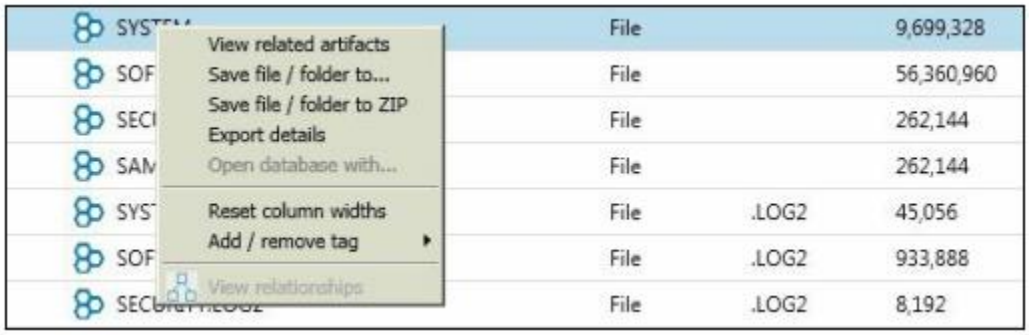
h. در شکل قبلی شما می توانید محتویات کلید TimeZoneInformation را ببینید. این کلید بسیار مهم است، زیرا به آزمونگرها کمک می کند تا منطقه زمانی مناسب را تشخیص دهند. اطلاعات بیشتر در مورد کلید مورد نظر شما و منبع آن را می توان در قسمت DETAILS مشاهده کرد که در شکل زیر نشان داده شده است.



شکل ۵-۶ : پنل جزییات AXIOM Registry

i. به Evidence source نگاه کنید. اگر روی لینک آبی کلیک کنید، مکان فایل رجیستری را باز می کند. حالا شما می توانید فایل رجیستری را اکسپورت کنید. برای انجام این کار، بر روی فایل راست کلیک کرده و گزینه Save file / folder to... را انتخاب کنید.

j. همچنین می توانید آیتم های AXIOM را به صورت خودکار در طول مرحله پردازش استخراج کنید. برای انجام این کار، روی فایل رجیستری راست کلیک کرده و بر روی View related artefacts از منوی زمینه کلیک کنید.



شکل ۵-۷ : اکسپورت کردن فایل رجیستری

هنگامی که فایل را اکسپورت کردید، می توانید آن را با ابزارهای دیگر تجزیه کنید. البته، Magnet AXIOM یک ابزار جرم شناسی بسیار قدرتمند است و داده های رجیستری زیادی را استخراج می کند، اما گاهی اوقات بهتر است که آنها را با برخی از ابزارهای دیگر، مانند RegRipper، تجزیه کنید. ما به شما نحوه انجام این کار را در دستورالعمل بعدی نشان خواهیم داد.

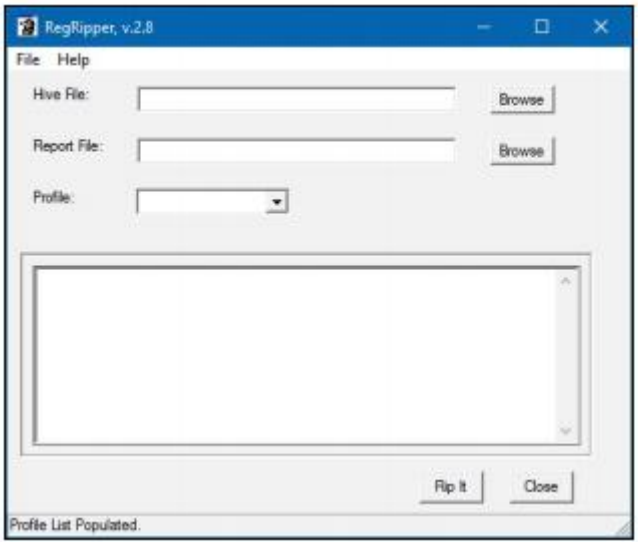
Magnet AXIOM فایلهای رجیستری موجود را جمع آوری می‌کند تا یک آزمونگر جرم شناسی بتواند آنها را به صورت دستی تجزیه و تحلیل کند یا آنها را برای تجزیه با ابزارهای دیگر ایجاد کند. همچنین، AXIOM بسیاری از نتایج قانونی این فایل ها را به صورت خودکار استخراج می کند، بنابراین یک آزمونگر میتواند نتایج را در صفحه شواهد Magnet AXIOM Exam بررسی کند.

۵-۲- تجزیه فایل‌های رجیستری با RegRipper

RegRipper ابزار جرم شناسی ویندوز منبع باز است که توسط هارلان کارو، نویسنده سری تحلیل های جرم شناسی ویندوز ارائه شده است. این ابزار با زبان Perl نوشته شده است و دارای بسیاری از پلاگین های مفید است. همچنین، آزمون‌گرهای جرم شناسی می توانند با کد نویسی در پرل، پلاگین‌های مورد نیاز خود را ایجاد کنند.

مراحل تجزیه فایل های رجیستری با RegRipper:

a. با نحوه اکسپورت کردن فایل های رجیستری از تصاویر دیسک آشنا شده اید. اکنون که شما یک فایلبرای تجزیه با RegRipper دارید. ابتدا rr.exe را اجرا کنیدو یک پنجره مانند شکل بالا باز خواهد شد.



شکل ۵-۸ : پنجره اصلی RegRipper

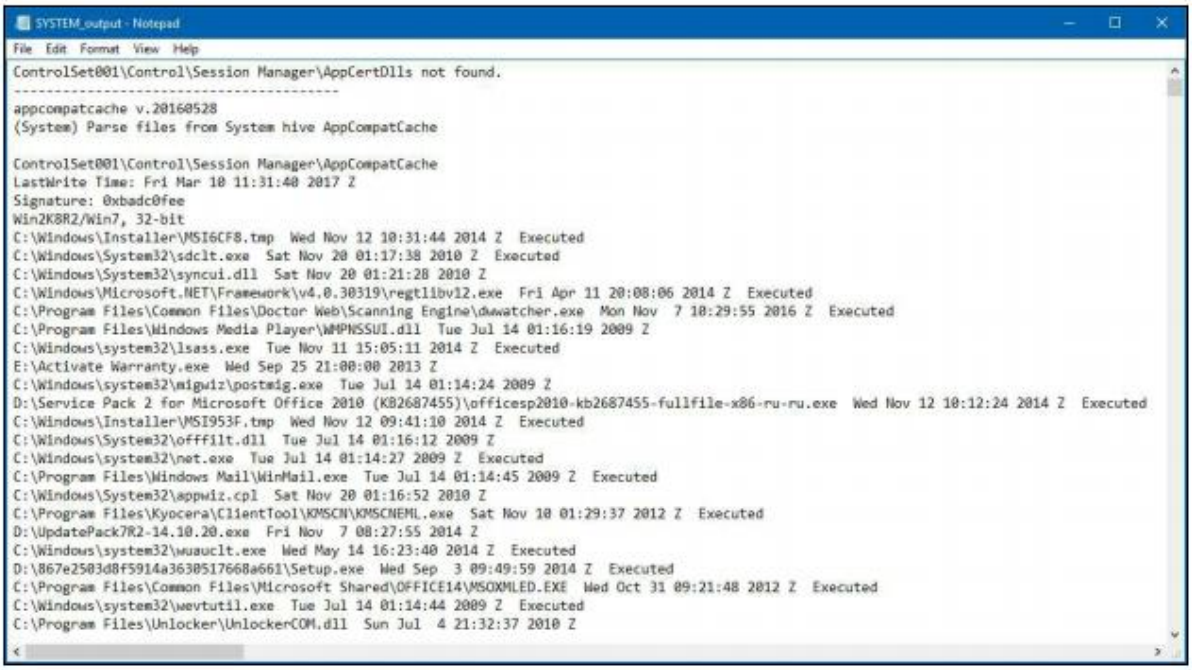
در اینجا سه فیلد وجود دارد:

Hive File: از دکمه Browse استفاده کنید و هایو (رجیستری) که قبلا اکسپورت کرده اید را انتخاب کنید.

Report File: از دکمه Browse استفاده کنید و فایل خروجی را برای ذخیره انتخاب کنید (برای سادگی فایل TXT انتخاب شود).

Profile: پروفایل مناسب برای تجزیه را از منوی کشویی انتخاب کنید. ما از فایل SYSTEM به عنوان منبع استفاده می کنیم، بنابراین پروفایل انتخابی انتخابی ما سیستم است.

b. بعد از انتخاب فایل ها و مشخصات مناسب، می توانید روی دکمه Rip It کلیک کنید. به محض اینکه پردازش تمام شد، آماده تجزیه و تحلیل خروجی است.



شکل ۵-۹ : خروجی RegRipper

اگر پایین فایل خروجی را مشاهده کنید، خواهید دید که اطلاعات مهم زیادی از نقطه نظر جرم‌شناسی وجود دارد مانند دستگاه های USB متصل شده، پیکربندی EventLog، دستگاه های نصب شده، اتصالات شبکه و غیره.

RegRipper با استفاده از پروفایل انتخاب شده توسط یک متخصص جرم شناسی، و با بکارگیری ماژول های پرل، داده ها را از فایل هایو (رجیستری) استخراج می کند، و خروجی را در فایلی با پسوند TXT ذخیره می کند.

۵-۳- بازسازی آیتم‌های رجیستری حذف شده با Registry Explorer

Registry Explorer یکی دیگر از ابزارهای جرم شناسی رجیستری ویندوز است. یکی از ویژگی های بسیار مفید این ابزار قابلیت آن برای بازیابی رکوردهای حذف شده است.

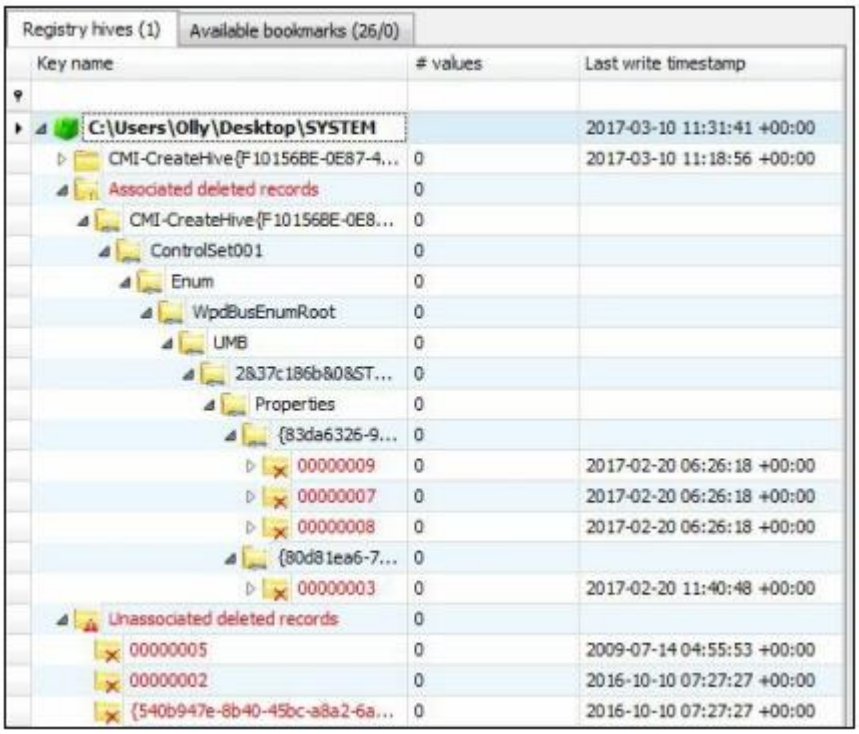
مراحل بازیابی اطلاعات حذف شده رجیستری با استفاده از رجیستری به شرح زیر است:

a. برنامه RegistryExplorer.exe را اجرا کنید، به قسمت Options بروید و مطمئن شوید که گزینه Recover deleted keys / values فعال شده است.

شکل ۵-۱۰ : گزینه حذف کلید/مقدار در Registry Explorer Recover

حالا می‌توانید یک فایل هایو برای پردازش را انتخاب کنید. برای انجام این کار، به File - Load offline hive بروید، یا فقط Alt + 1 را فشار دهید.

b. اکنون می توانید محتویات فایل hive خود را در سیستم مورد نظر فهرست کنید، از جمله رکوردهای حذف شده مرتبط و غیر مرتبط.



شکل ۵-۱۱ : رکوردهای حذف شده مرتبط و غیر مرتبط

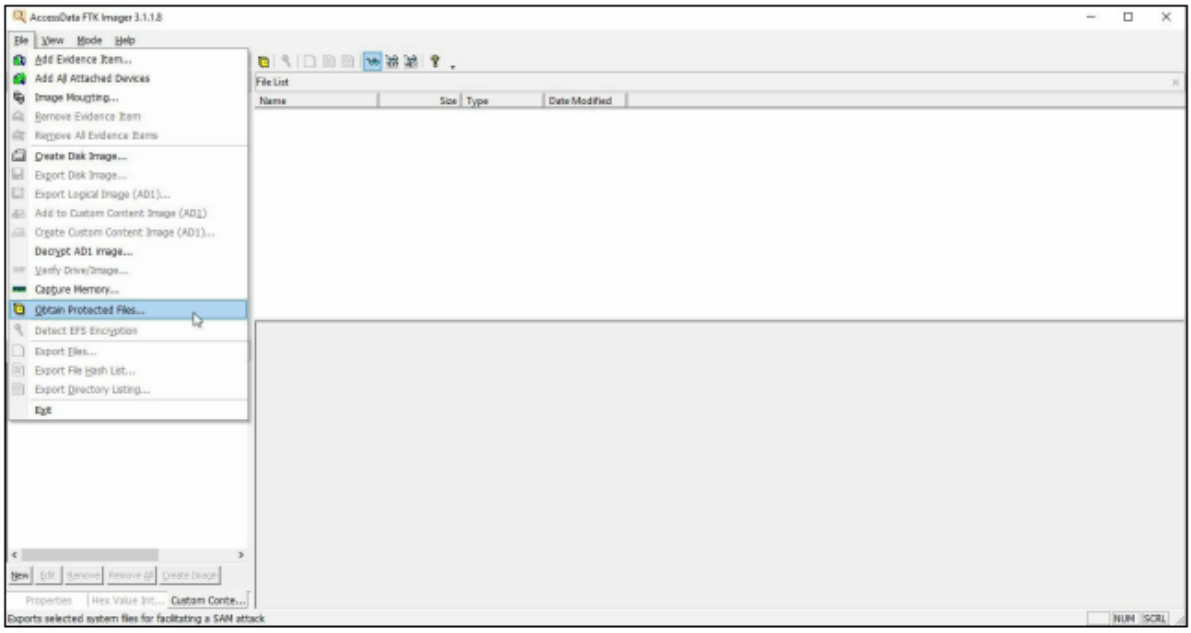
تفاوت بین پرونده های مرتبط و غیر مرتبط این است که گروه اول هنوز با کلید در رجیستری فعال همراه است.Registry Explorer فایل hive انتخاب شده را پردازش کرده و به طور خودکار رکوردهای حذف شده را (مرتبط و غیر مرتبط)، بازیابی می کند. پس از اتمام پردازش، یک آزمونگر می تواند داده های موجود را ببیند.

۴-۵- تجزیه و تحلیل رجیستری با FTK Registry Viewer

FTK Registry Viewer در دسته محصولات AccessData موجود است یا می‌توان به صورت جداگانه نیز دانلود شود. این ابزار به کاربران اجازه می دهد تا بتوانند محتویات رجیستری بر روی یک ماشین ویندوز را مشاهده کنند.

هنگامی که Registry Viewer نصب شد، بر روی آیکون دوبار کلیک کنید تا برنامه باز شود. FTK Imager را نیز همزمان باز کنید.

a. در Imager، به قسمت File > برای دریافت فایل های محافظت شده بروید.



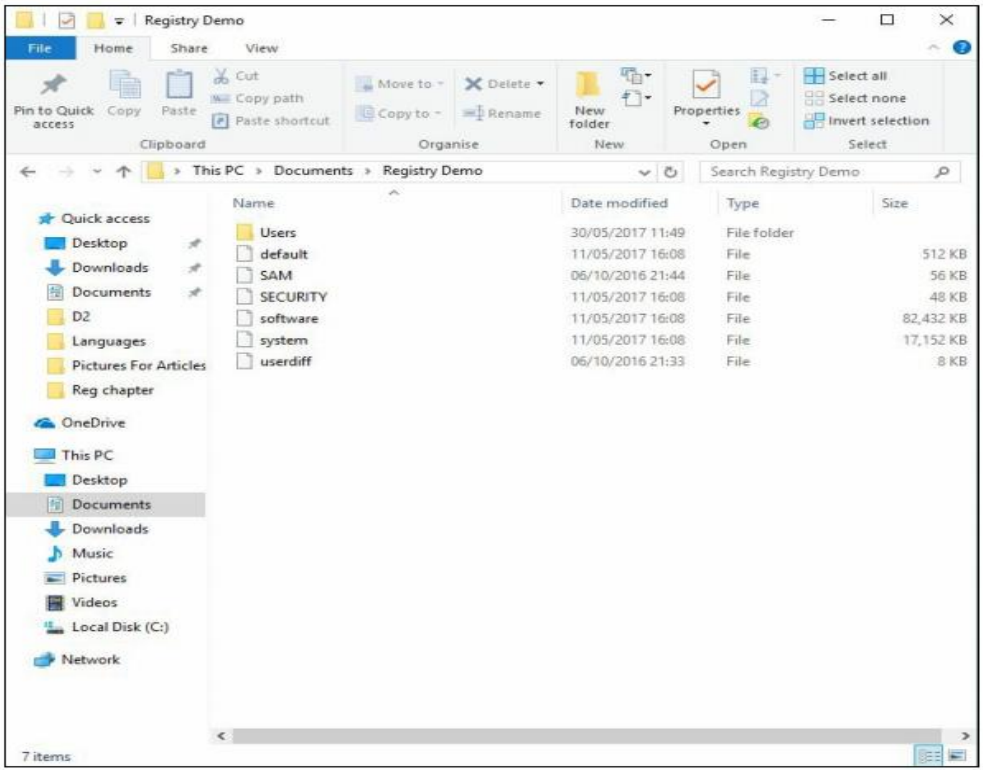
شکل ۵-۱۲ :دریافت فایل های محافظت شده

b. در پنجره کوچکی که ظاهر می شود، یک فولدر مقصد برای فایل های خود را انتخاب کنید.

شکل ۵-۱۳ : انتخاب پوشه مقصد

c. اطمینان حاصل کنید که بازیابی رمز عبور و تمامی فایل های رجیستری را از زیر نوار پوشه مقصد انتخاب کرده اید، در غیر این صورت فقط یک نسخه از نتایج حذف شده را دریافت خواهید کرد. روی OK کلیک کنید.

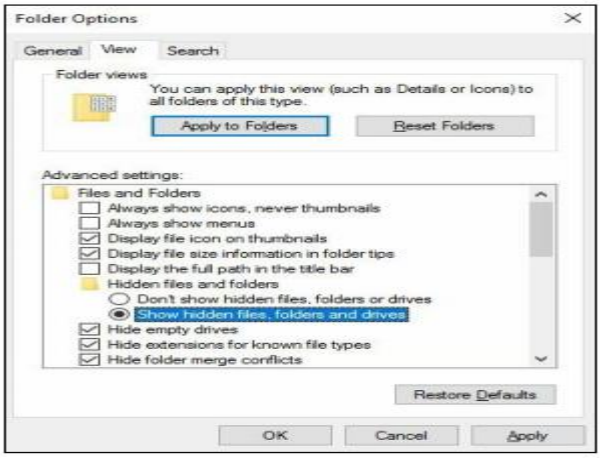
اجرا و دریافت نتایج ممکن است کمی طول بکشد، و در چند ثانیه اول ممکن است به نظر برسد چیزی اتفاق نمی افتد. شما می توانید بررسی کنید که آیا فرایند با باز کردن پوشه در مسیر فایل که پیشتر تعیین کرده اید، به اتمام رسیده است.



شکل ۵-۱۴ : پوشه آلوده

d. روی فایل کلیک کنید و سپس پوشه و گزینه های جستجو را تغییر دهید. سپس یک پنجره کوچک را باز خواهد شد. بر روی زبانه View کلیک کرده و گزینه Show hidden files, folders and drives را فعال کنید. بر روی Apply کلیک کرده و ok را بزنید.

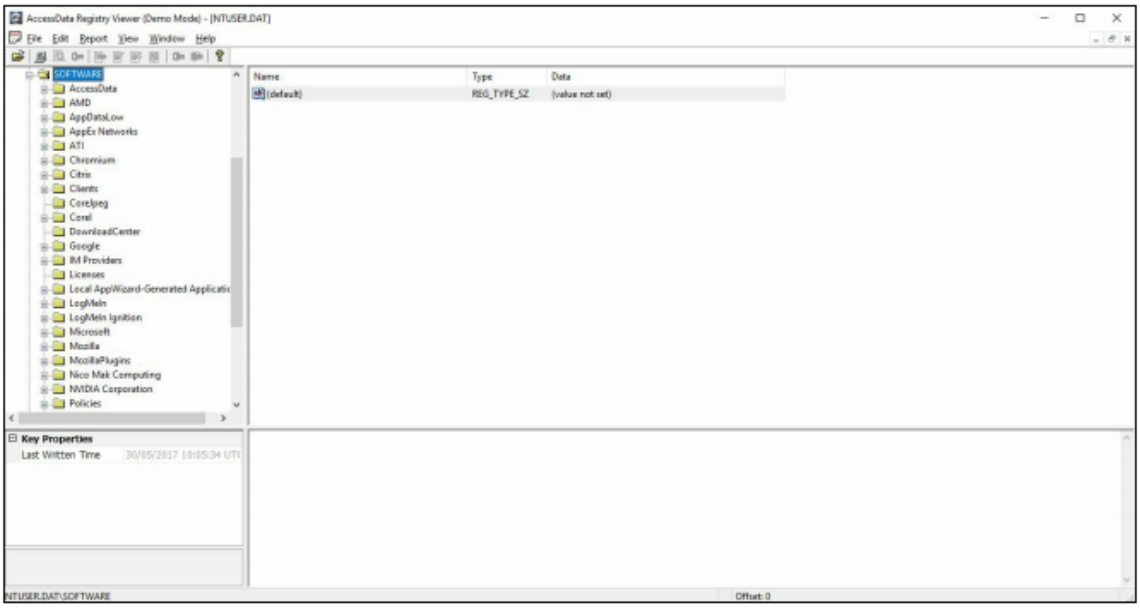
حالا می توانیم داده هایی را که از رجیستری با استفاده از Registry Viewer جمع آوری شده مشاهده کنید.



شکل ۵-۱۵ : نمایش فایل‌های مخفی

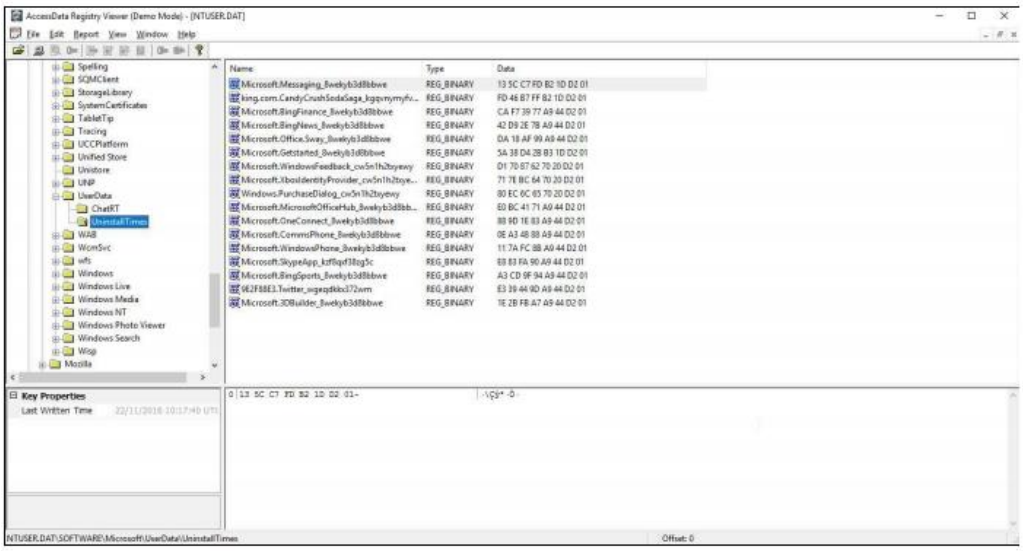
e. برای انجام این کار، Registry Viewer را باز کنید و روی File> Open کلیک کنید، سپس به پوشه ای که فایل های رجیستری را در آن ذخیره کرده اید، پیدا کنید و یکی از آن ها را NTUSER.DAT علامت گذاری کنید.سپس این فایل را باز کنید.

منوی SOFTWARE به شما یک لیست طولانی خوب از تمام بخش های نرم افزاری که در دستگاه مورد نظر نصب شده‌است را می‌دهد.



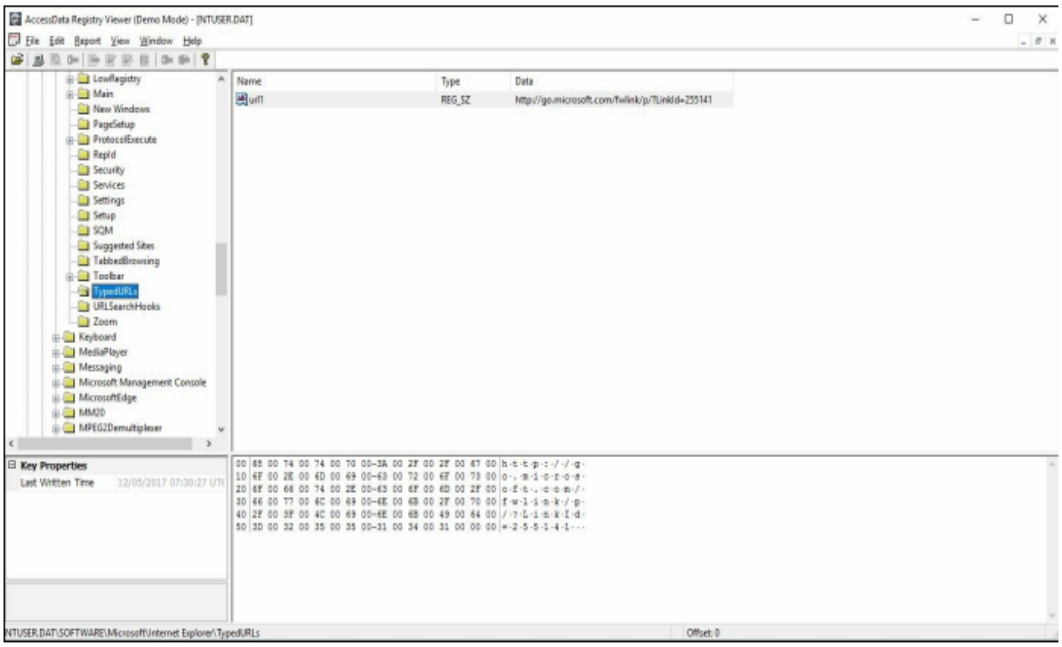
شکل ۵-۱۶ : نرم افزار نصب شده بر روی سیستم

f. شما می توانید برنامه های حذف شده و زمان حذف آنها را در NTUSER.DAT \ SOFTWARE \ Microsoft \ UserData \ UninstallTimes ببینید.



شکل ۵-۱۷ : زمان حذف

g. تحت NTUSER.DAT \ SOFTWARE \ Microsoft \ InternetExplorer \ TypedURLs، شما می توانید آدرس‌های هر سایتی را که در اینترنت اکسپلورر مشاهده کرده اید، ببینید.



شکل ۵-۱۸ : سایت های بازدید شده در internet explorer

در NTUSER.DAT \ Software \ Microsoft \ Internet Explorer \ IntelliForms، می توانید داده هایی را از فرم هایی که بصورت اتوماتیک تکمیل شده اند،(مانند نام های کاربری و گذرواژه‌ها) مشاهده کنید.

Registry Viewer فایل های رجیستری را از یک دستگاه یا یک تصویر جرم شناسی جمع آوری می کند، و امکان بررسی دستی با FTK یا Imager را می دهد.

فصل ۶ : artifacte های سیستم عامل

در این فصل به تجزیه و تحلیل artifacte های سیستم عامل ویندوز خواهیم پرداخت. لیست artifacte های مورد بررسی در زیر آمده‌است.

- **تجزیه و تحلیل محتوای سطل بازیافت با EnCase Forensic**
- **تجزیه و تحلیل محتوای سطل بازیافت با Rifiuti2**
- **تجزیه و تحلیل محتوای سطل بازیافت با Magnet AXIOM**
- **تجزیه و تحلیل گزارش رویداد (Event log) با FullEventLogView**
- **تجزیه و تحلیل گزارش رویداد با Magnet AXIOM**
- **بازیابی گزارش رویداد با EVTXtract**
- **تجزیه و تحلیل فایل LNK با EnCase Forensic**
- **تجزیه و تحلیل فایل LNK با LECmd**
- **تجزیه و تحلیل فایل LNK با Link Parser**
- **تجزیه و تحلیل فایل Prefetch با Magnet AXIOM**
- **تجزیه فایل Prefetch با PECmd**
- **بازیابی فایل Prefetch با Windows Prefetch Carver**

مقدمه

برخی از ویژگی های سیستم عامل ویندوز تعداد زیادی آثار ارزشمند را تولید می‌کنند که به عنوان بخشی از مدارک دیجیتال استفاده می شود. رایج ترین منابع این آثار عبارتند از: سطل بازیافت، رجیستری ویندوز، فایل‌های LNK و فایل‌های Prefetch.

سطل بازیافت حاوی فایل‌ها و پوشه‌هایی است که توسط کاربر حذف شده است. در واقع، این فایل‌ها از سیستم فایل حذف نشده‌اند، فقط از محل اصلی خود به سطل بازیافت منتقل می‌شود.

دو فرمت از سطل بازیافت وجود دارد: ۱) فرمت Recycler (ویندوز ۲۰۰۰، XP) – در این فرمت فایل ها در C:\Recycler\%SID% \ ذخیره می شوند و فراداده آنها در فایل INFO2 ذخیره می شود. ۲) فرمت $Recycle.Bin – در این فرمت فایل ها در C:\$Recycle.Bin\%SID% \ در فایل $R ذخیره می شود، و فراداده آنها در فایل های $L ذخیره می شود.

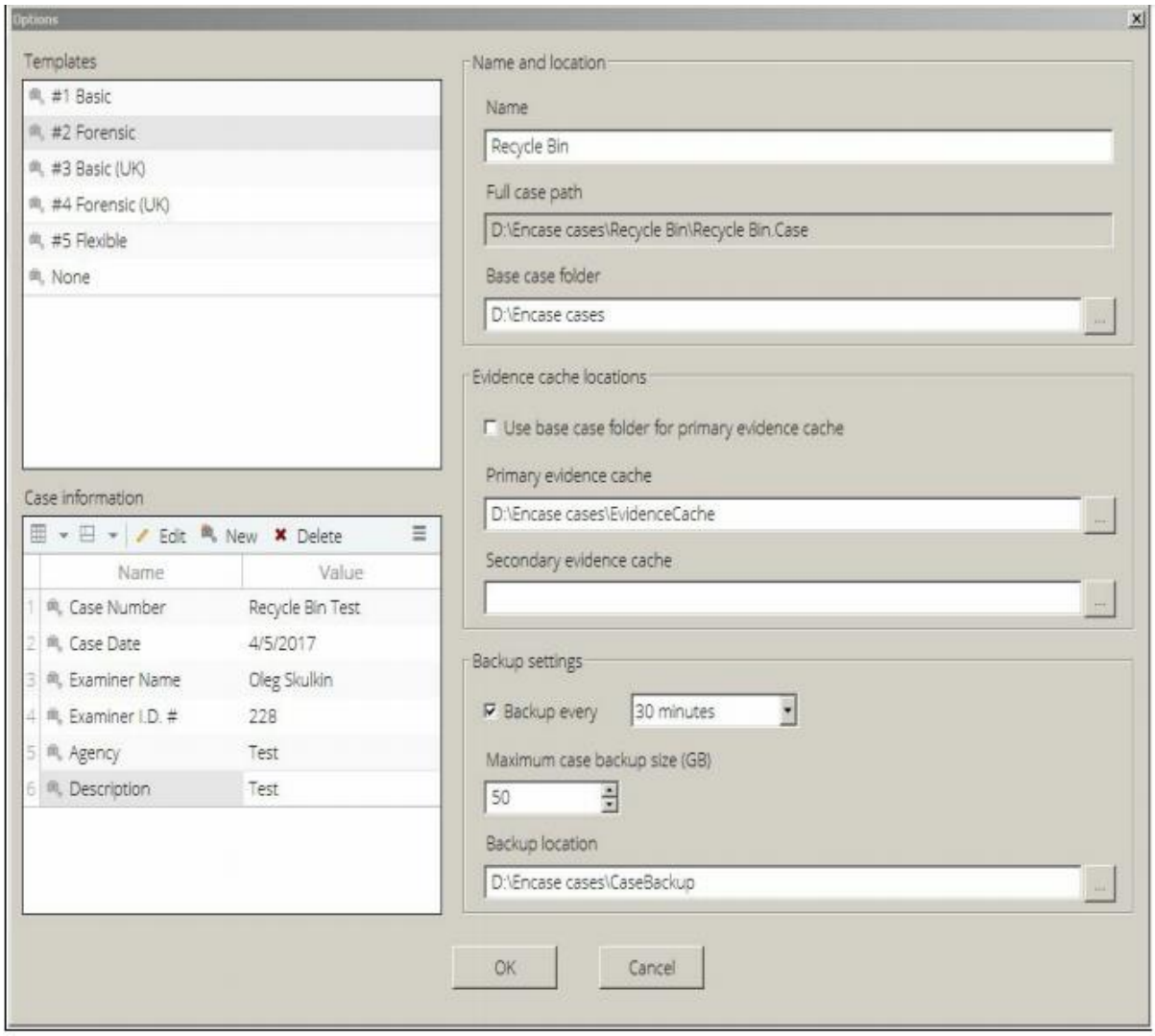
همانطور که از نام آن قابل حدس است، Windows Event Logs اطلاعات مربوط به لاگ های مختلف سیستم را جمع آوری می کند. ویندوز ۲۰۰۰، XP و ۲۰۰۳ (به جز نسخه سرور) این لاگ ها را در سه فایل "program، system و security " ذخیره می کند. این فایل ها را می توان در مسیر C:\Windows\system32\config پیدا کرد. در ویندوز ویستا، فرمت لاگ ها به XML تغییر کرده است. این فایل های EVTX را می توان در زیرشاخه C:\Windows\System32\Winevt\Logs پیدا کرد. فایل های LNK و یا فایل های میانبر ویندوز با سایر فایل ها (برنامه ها، اسناد و غیره) قابل دسترسی هستند. این فایل ها در سراسر سیستم یافت می شوند و می توانند به یک متخصص جرم شناسی دیجیتال در کشف برخی از فعالیت های مشکوک، از جمله فایل هایی که اخیرا استفاده شده اند، برنامه های کاربردی و ... کمک کنند.

فایل های Prefetch را می توان در مسیر C:\Windows\Prefetch پیدا کرد. این فایل حاوی اطلاعات ارزشمند در مورد برنامه های کاربردی مورد استفاده، از جمله تعداد دفعات اجرا، تاریخ و زمان آخرین اجرا و غیره هستند.

۶-۱- تجزیه و تحلیل محتوای سطل بازیافت با استفاده از EnCase Forensic

EnCase یک ابزار حرفه ای جرم شناسی دیجیتال شناخته شده می‌باشد که توسط Guidance Software تهیه شده است. این ابزار تمام چرخه عمر تحقیق را از جمع آوری تا گزارش پشتیبانی می‌کند. علاوه براین، با زبان اسکریپتی توکار - EnScript – طراحی شده‌است به طوری که کاربران می‌توانند اسکریپت‌های خود را برای حل مسائل دیجیتالی جرم‌شناسی بنویسند. مراحل تجزیه و تحلیل محتویات سطل بازیافت در Encase Forensics به شرح زیر است:

a. با ایجاد یک case جدید شروع می کنیم. برای انجام این کار، روی New Case در سمت چپ کلیک کرده تا پنجره case option ظاهر شود.



شکل ۶-۱ : case options

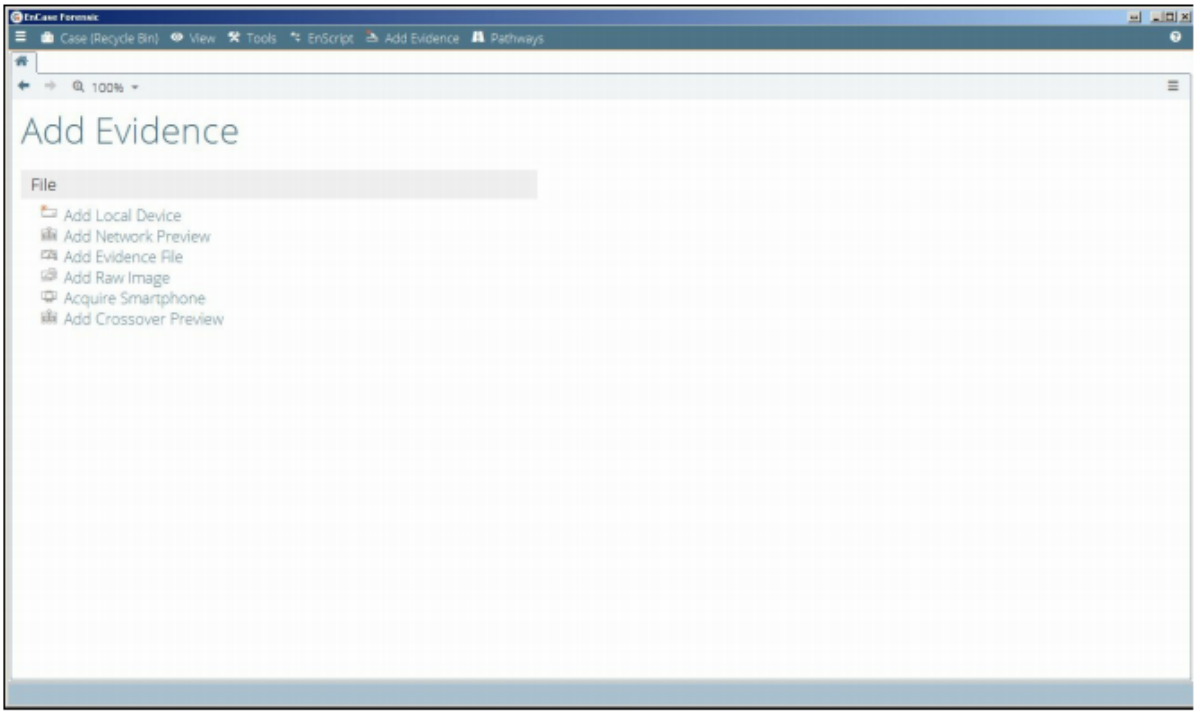
b. از قسمت information case شروع کنید. در اینجا، ما ۶ فیلد برای پر کردن داریم: شماره case، تاریخ case، نام آزمونگر، آی دی آزمونگر.، آژانس و شرح. همه فیلدها "خود توضیحی" هستند، بنابراین فقط آنها را پر کنید.

c. به قسمت name و location بروید. نام و شماره case خود را در فیلد اول تایپ کنید و پوشه case اصلی را انتخاب کنید (جایی که case در آنجا ذخیره شده). فیلد مسیر case به طور خودکار پر خواهد شد.

d. به مکان کش شواهد بروید. شما می توانید از همان پوشه برای ذخیره کش استفاده کنید، یا یک یا دو پوشه را برای ذخیره آن انتخاب کنید.

e. در نهایت، اگر می‌خواهید case شما پشتیبان‌گیری شود، گزینه Backup every را تیک بزنید و مقدار آن را انتخاب کنید. انتخاب پوشه پشتیبان و حداکثر اندازه نسخه پشتیبان را فراموش نکنید. درنهایت روی OK کلیک کنید.

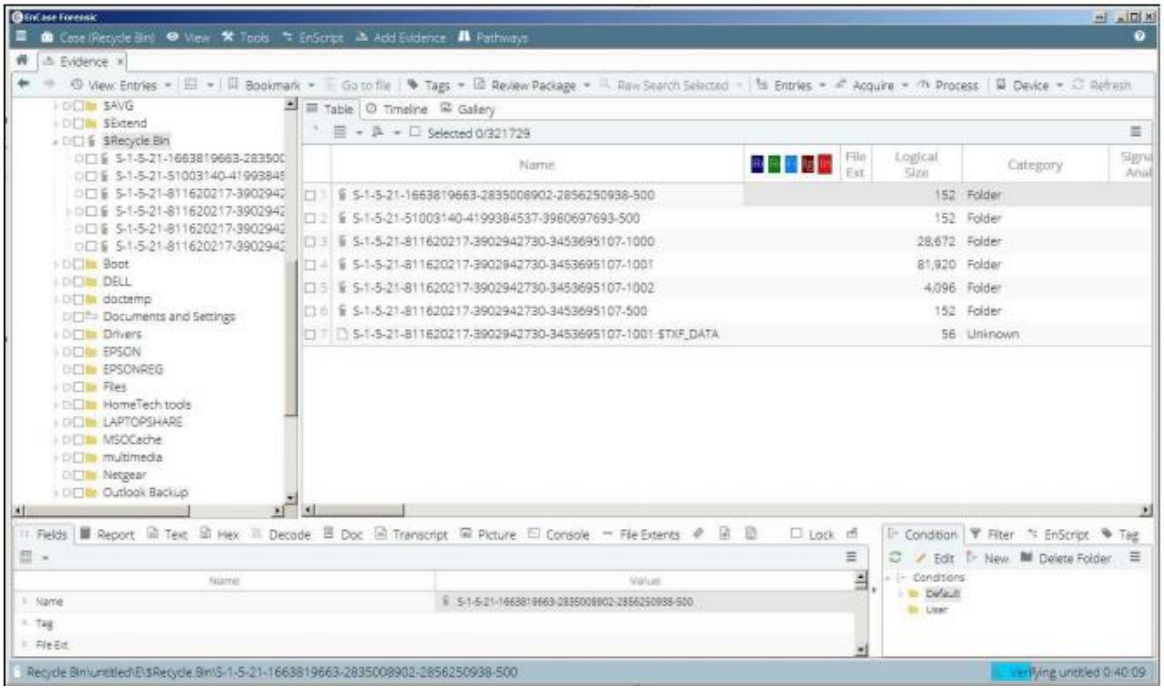
f. حالا شما یک پنجره با اطلاعات case خود می‌بینید، اکنون می‌توانید یک تصویر جرم شناسی را اضافه کنید. برای انجام این کار، روی لینک Add Evidence File در سمت چپ کلیک کنید.



شکل ۶-۲ : اضافه کردن شواهد

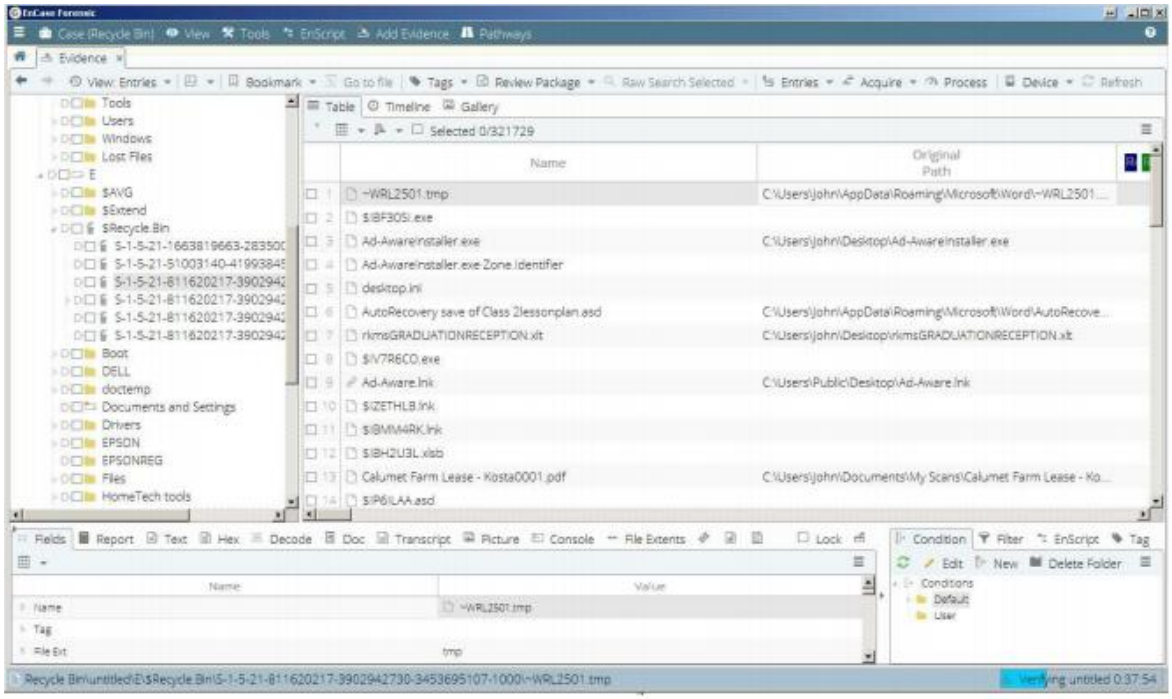
همانطور که در تصویر ۶-۲ می بینید، ۶ گزینه برای منبع شواهد وجود دارد: شما می توانید دستگاه محلی (فراموش نکنید که از writeblocker استفاده کنید)، یک منبع شواهد از راه دور، تصویر E01 یا RAW و غیره را اضافه کنید.

g. اکنون فایل شواهد را مشاهده می‌کنید. برای دیدن محتویات روی نام آن کلیک کنید. ممکن است برای تجزیه داده‌ها کمی وقت لازم باشد. پس از پایان تجزیه داده ها، به فولدر Recycle bin بروید.



شکل ۶-۳ : محتوای فولدر recycle bin

همانطور که در شکل قبلی مشاهده می کنید، یک لیست از شناسه های امنیتی کاربر (SID) وجود دارد. این لیست می تواند به یک آزمونگر در تعیین اینکه کاربر کدام فایل ها را در سطل آشغال قرار داده است، کمک کند.



شکل ۶-۴ : محتوای فولدر بدست آمده

EnCase محتویات Recycle Bin را برای شما به صورت خودکار پردازش می کند. همچنین، مقدار اطلاعات ارزشمند زیادی شامل نام فایل اصلی، مسیر اصلی آن، تاریخ و زمان حذف، و غیره را جمع آوری می‌کند.

۶-۲- تجزیه و تحلیل محتوای سطل بازیافت با استفاده از Rifiuti2

Rifiuti2 یک ابزار منبع باز است که یک آزمونگر جرم شناسی را قادر به تجزیه و تحلیل محتوای سطل بازیافت ویندوز می‌کند. این ابزار اطلاعات مهمی مانند تاریخ و زمان حذف فایل بازیافتی، مسیر اصلی آن و غیره را نشان می دهد. Rifiuti2 از فرمت‌های بازیافت در تمام نسخه‌های ویندوز، قدیمی (از ویندوز ۹۵) تا جدید (تا ویندوز ۱۰) پشتیبانی می‌کند. این ابزار از تمام نسخه‌های محلی ویندوز نیز پشتیبانی می کند.

هر کاربر پوشه خاص خود را در سطل آشغال دارد. به خاطر داشته باشید، در دستور قبلی (EnCase) چندین پوشه وجود داشت. برای استفاده از Rifiuti2، ابتدا باید یکی از این پوشه ها را اکسپورت کنید. ابزارهای زیادی وجود دارد که قادر به انجام این کار هستند، مانند Autopsy، FTK Imager و Magnet AXIOM.

هنگامی که این پوشه را اکسپورت کردید، Command Prompt ویندوز را اجرا کنید. اگر از یک سیستم ۳۲ بیتی استفاده می کنید، به پوشه x32 بروید؛ اگر سیستم ۶۴ بیتی دارید، به پوشه x64 بروید. در هر دو پوشه، شما دو فایل اجرایی ویندوز را پیدا کنید: rifiuti.exe و rifiuti-vista.exe. اگر پوشه خود را در ویندوز XP اکسپورت کردید، از rifiuti.exe استفاده کنید، در غیر این صورت (در ویستا) از rifiuti-vista.exe استفاده کنید.

```
rifiuti-vista.exe S-1-5-21-3736901549-408126705-1870357071-1001 >
rec_bin.txt
```

همانطور که می بینید، خروجی را در فایلی با فرمت TXT قرار می‌دهیم. محتویات آن را می‌توان در شکل ۶-۵ مشاهده کرد.

```
rec_bin - Notepad
File  Edit  Format  View  Help
Recycle bin path: 'S-1-5-21-3736901549-408126705-1870357071-1001'
Version: 2

Index    Deleted Time     Size     Path
$IL1E3HH.exe     2017-01-09 10:26:29     419840  C:\Program Files (x86)\mpck\Q8XA1S.exe
$IU9JTLX.exe     2017-01-09 10:26:37     1277952 C:\Program Files (x86)\mpck\uninstaller.exe
$IQS2WIG         2017-01-10 08:14:11     24      C:\Program Files (x86)\1cv8
$IXZT6RG         2017-01-10 08:14:29     763     C:\ProgramData\1C
$I3BY4LB         2017-01-10 08:18:12     2665025 C:\Users\Дмитрий\AppData\Local\1C
$I5CVINC         2017-01-10 08:18:20     8218    C:\Users\Дмитрий\AppData\Roaming\1C
$I0QH9M9         2017-01-10 08:18:31     21858   C:\Users\Дмитрий\AppData\Local\Temp\00019247
$IE4BXN1         2017-01-10 08:18:31     0       C:\Users\Дмитрий\AppData\Local\Temp\00019273
$IICH743         2017-01-10 08:18:31     0       C:\Users\Дмитрий\AppData\Local\Temp\00019270
$IPQY63S         2017-01-10 08:18:31     0       C:\Users\Дмитрий\AppData\Local\Temp\00019276
$IVZQSES         2017-01-10 08:18:31     2071552 C:\Users\Дмитрий\AppData\Local\Temp\00019283
$I2NXHHX         2017-01-10 08:18:32     0       C:\Users\Дмитрий\AppData\Local\Temp\00019453
$I323YQH         2017-01-10 08:18:32     0       C:\Users\Дмитрий\AppData\Local\Temp\00019381
$I5ATG1G         2017-01-10 08:18:32     0       C:\Users\Дмитрий\AppData\Local\Temp\00019384
$I773CME         2017-01-10 08:18:32     9174264 C:\Users\Дмитрий\AppData\Local\Temp\58471F6C-DF08-48F1-A37E-3A1A02A1EE12
$I9P9ISF         2017-01-10 08:18:32     0       C:\Users\Дмитрий\AppData\Local\Temp\00019420
$IC2TSAM         2017-01-10 08:18:32     9174264 C:\Users\Дмитрий\AppData\Local\Temp\6246106C-F26A-43AD-8EFA-93638F54182A
$IC52GM7         2017-01-10 08:18:32     9174264 C:\Users\Дмитрий\AppData\Local\Temp\87963D83-FA16-4A39-BE15-CBDF053B0BFB
$IDPVXUM         2017-01-10 08:18:32     14614528        C:\Users\Дмитрий\AppData\Local\Temp\00019462
$IDV7HEV         2017-01-10 08:18:32     0       C:\Users\Дмитрий\AppData\Local\Temp\00019378
$IE4X0DX         2017-01-10 08:18:32     1143104 C:\Users\Дмитрий\AppData\Local\Temp\00019293
$IE8WY6M         2017-01-10 08:18:32     8466117 C:\Users\Дмитрий\AppData\Local\Temp\1989603921
$IH52BML         2017-01-10 08:18:32     9174264 C:\Users\Дмитрий\AppData\Local\Temp\5478223C-5235-4F6D-8998-8943879BFF8A
$IKLTALX         2017-01-10 08:18:32     5223968 C:\Users\Дмитрий\AppData\Local\Temp\00019289
$IMMRA9B         2017-01-10 08:18:32     9174264 C:\Users\Дмитрий\AppData\Local\Temp\537350E0-AE88-47D0-B1A2-2A1E916A1094
$IMYC6XH         2017-01-10 08:18:32     1650917 C:\Users\Дмитрий\AppData\Local\Temp\14840068621co
$INMM2OL         2017-01-10 08:18:32     3078592 C:\Users\Дмитрий\AppData\Local\Temp\A5FBF58F-811D-483A-BDD0-F7BBE071D730
```

شکل ۶-۵ : خروجی Rifiuti2

اگر یک پوشه از یک سیستم ویندوز قبل از ویستا داشته باشید، می‌توانید از rifiuti.exe استفاده کنید که محتوای فایل INFO2 را تجزیه و تحلیل می‌کند و اطلاعات مربوط به محتویات سطل بازیافت کاربر را مشخص می کند.

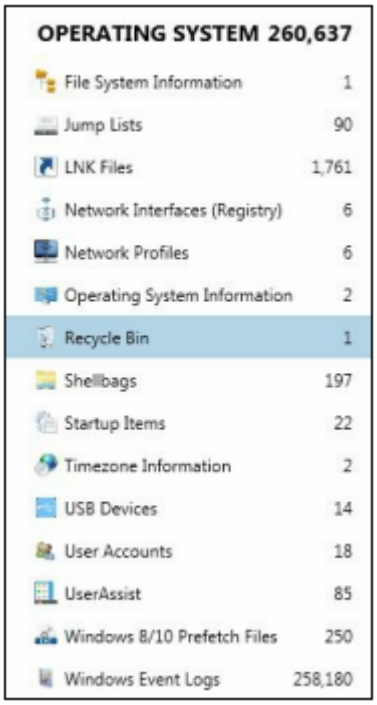
اگر یک پوشه از سیستم ویندوز ویستا یا بعد از آن دارید، از rifiuti-vista.exe استفاده کنید که فایل‌های ایندکس ($I) را تجزیه کند و اطلاعات مربوط به فایل‌های بازیافت شده، مسیرهای اصلی، نام، اندازه و تاریخ و زمان حذف آن را تجزیه و تحلیل کند.

۶-۳- تجزیه و تحلیل محتوای سطل بازیافت با Magnet AXIOM

Magnet AXIOM از تمامی آثار سیستم عامل ویندوز معمولی از قبیل سطل بازیافت پشتیبانی می‌کند. در این دستورالعمل، نحوه استفاده از این ابزار برای تجزیه و تحلیل فایل‌هایی که بصورت مشکوکی حذف شده‌اند، بیان می‌شود.

مراحل تجزیه و تحلیل محتوای بازیافت با Magnet AXIOM به شرح زیر است.

a. هنگامی که تصویر جرم‌شناسی پردازش می‌شود، به قسمت AXIOM Examine's artifact types بروید و به OPERATING SYSTEM بروید.



شکل ۶-۷ : لیست Operating system artifacts

b. همانطور که می بینید، در اینجا بسیاری از آیتم های مختلف سیستم عامل ، از جمله سطل بازیافت وجود دارد. در اینجا، تنها یک فایل مشکوک وجود دارد. در شکل زیر قابل مشاهده است.

File Name	Deleted Date/Time	User Security Identifier	Original Path	Type	Current...	File Siz...
TeamViewer 9.lnk	3/29/2017 12:14:58 AM	S-1-5-21-2250098342-4205279653-4187590567-1000	C:\Users\Public\Desktop\TeamViewer 9.lnk	File	$RIVPSZD.lnk	1199

شکل ۶-۸ : محتوای Recycle Bin

c. بنابراین، یک فایل مشکوک LNK برای برنامه TeamViewer در Recycle Bin داریم. این برنامه برای دسترسی از راه دور استفاده میشود. همچنین اطلاعات مربوط به تاریخ و زمان حذف فایل، شناسه امنیتی کاربری که آن را حذف کرده و مسیر فایل اصلی – تمام مواردی که ممکن است برای تحقیقات مورد نیاز باشد پیدا می‌کند.

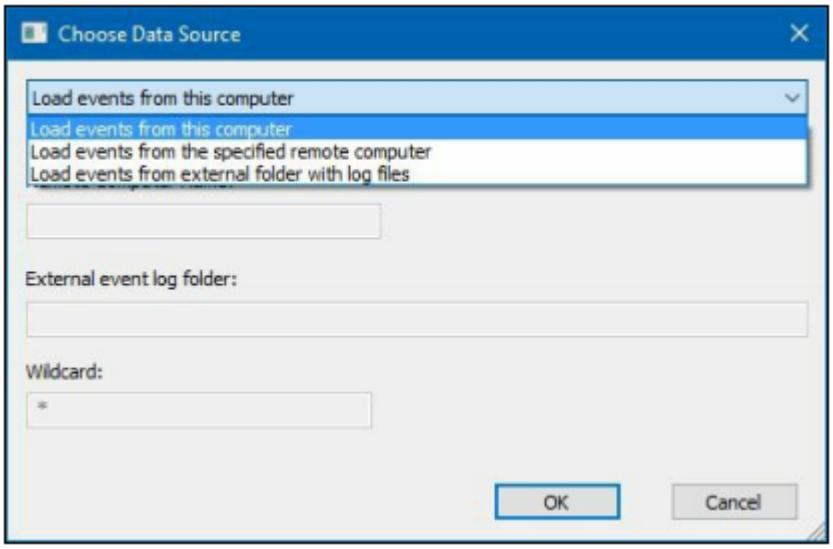
۶-۴- تجزیه و تحلیل گزارش رویداد (Event log) با FullEventLogView

FullEventLogView یکی دیگر از ابزارهای مفید NirSoft است، که قادر به تجزیه ویندوز ۷، ۸، ۱۰، و همچنین لاگ‌های رویداد ویندوز می‌باشد. یک آزمونگر جرم‌شناسی می‌تواند از آن برای مشاهده هر دو لاگ رویداد محلی و فایل‌های EVTX که در٪ SystemRoot٪ \ Windows \ System32 \ winevt \ Logs یافت می‌شود، استفاده کند.

مراحل تحلیل لاگ رویداد با FullEventLogView به شرح زیر است:

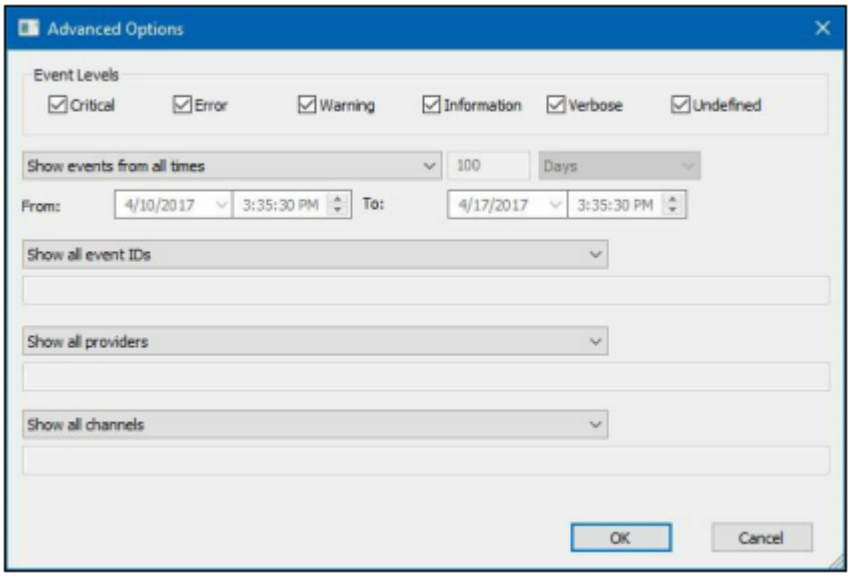
a. در ابتدا منبع داده را انتخاب کنید. برای انجام این کار، به File بروید - Data Source را انتخاب کنید (یا F7 را فشار دهید). همانطور که در شکل زیر می بینید ، سه گزینه در دسترس وجود دارد:

- بارگیری لاگ‌ها از رایانه ای که در حال استفاده از آن هستید.
- بارگیری لاگ‌ها از یک کامپیوتر از راه دور
- بارگیری لاگ‌ها از پوشه ای که قبلا اکسپورت کرده اید (به عنوان مثال از یک تصویر جرم‌شناسی)



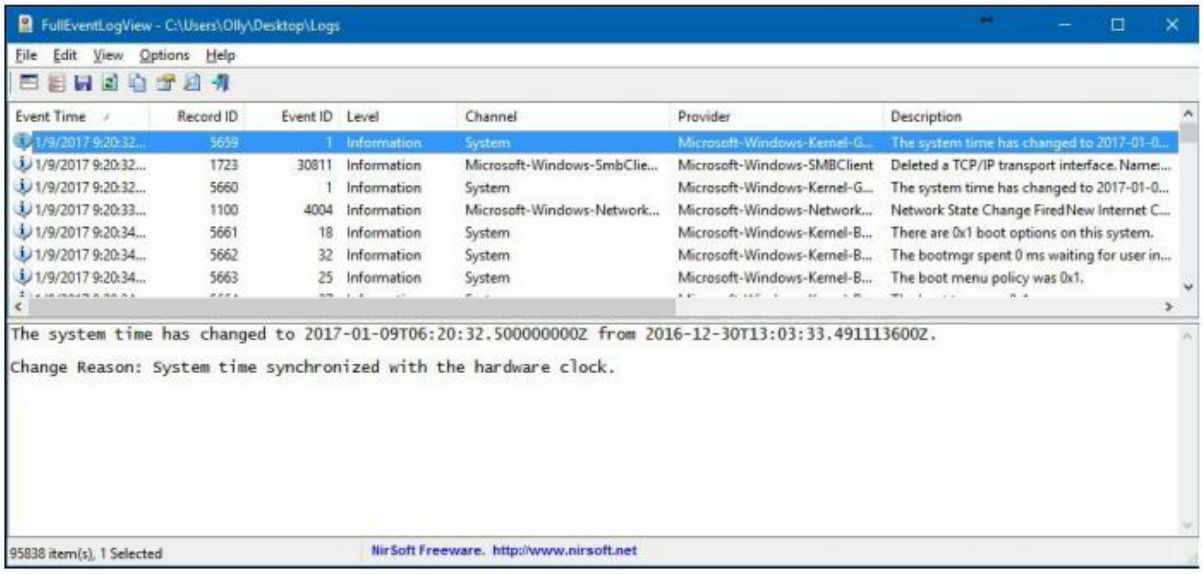
شکل ۶-۹ : انتخاب منبع داده در FullEventLogView

b. به طور پیش فرض، FullEventLogView رویدادها را فقط از ۷ روز گذشته نشان می‌دهد. اگر به یک دوره طولانی‌تر نیاز دارید، به Options بروید - گزینه advance را کلیک کنید (یا F9)، و Show Events را all times انتخاب کنید. همچنین می‌توان یک بازه زمانی برای نمایش انتخاب کرد (هم با زمان محلی وهم با GMT)، و حتی می‌توان رویدادهای ضبط شده را طبق سطح، شناسه رویداد، ارائه دهنده یا کانال فیلتر کرد.



شکل ۶-۱۰ : گزینه option در FullEventLogView

c. هنگامی که تمام فیلترهای مورد نیاز را اعمال و منبع داده انتخاب شد، تمام ورودی های رویداد موجود را در پنجره اصلی FullEventLogView مشاهده خواهید کرد.



شکل ۶-۱۱ : لیست لاگ‌های رویداد استخراج شده از یک فولدر

d. یک آزمونگر می‌تواند لاگ‌ها را با هر ستونی مرتب کند. همچنین میتوانید از طریق لاگ‌ها جستجو کنید: به Edit-Find بروید یا فقط Ctrl + F را فشار دهید.

بسته به منبع داده، FullEventLogView رویدادها را از کامپیوتر محلی، یک کامپیوتر از راه دور یا یک پوشه نشان می دهد و آزمونگرهای جرم شناسی را قادر می سازد تا آنها را مرتب کند و یا از طریق کلمات کلیدی آنها جستجو کند.

۶-۵- تجزیه و تحلیل گزارش رویداد با Magnet AXIOM

در اینجا با استفاده از Magnet AXIOM به کشف برخی از شایع ترین آثار قانونی سیستم عامل ویندوز می‌پردازیم. در این دستورالعمل، نحوه استفاده از این ابزار و تهیه گزارش های رویداد ویندوز آموزش داده می‌شود.

مراحل تحلیل گزارش رویداد با استفاده از Magnet AXIOM به شرح زیر است:

a. کیس‌هایی را که در مرحله تجزیه و تحلیل جرم‌شناسی سطل بازیافت استفاده کردید، باز کنید و دوباره لیست آثار سیستم OPERATING SYSTEM را باز کنید، اما اکنون Event Log را انتخاب کنید.

شکل ۶-۱۲ : لیست آثار سیستم عامل

b. همانطور که در شکل می بینید، تعداد زیادی از لاگ‌های رویداد وجود دارد. برای تجزیه و تحلیل ساده تر می توانید آنها را مرتب کنید. به عنوان مثال می‌توان از ستون Date / Time Created برای مرتب کردن گزارش‌های رویداد بر اساس زمان ایجاد، استفاده کرد. جزییات نتایج در شکل زیر قابل مشاهده است.

Event ID	Security User ID	Created Date/T...	Event Description Summary	Level	Keywords	Provider Name
23	LocalSystem	7/14/2009 4:56:45 AM	Remote Desktop Services: Session logoff succeeded.	Information	0x1000000000000000	Microsoft-Windows-TerminalServices-Lo
101	LocalSystem	7/14/2009 4:56:45 AM	Windows Defender state updated.	Information	0x4000000000000000	Microsoft-Windows-Windows Defender
1002	LocalService	7/14/2009 4:56:45 AM	The Windows Resource Exhaustion Detector stopped.	Information	0x4000000010000000	Microsoft-Windows-Resource-Exhaustio
5320	LocalSystem	10/19/2010 3:15:20 AM	Checking for Group Policy client extensions that are...	Information	0x4000000000000000	Microsoft-Windows-GroupPolicy
5320	LocalSystem	10/19/2010 3:15:20 AM	Checking for Group Policy client extensions that are...	Information	0x4000000000000000	Microsoft-Windows-GroupPolicy
5320	LocalSystem	10/19/2010 3:15:20 AM	Checking for Group Policy client extensions that are...	Information	0x4000000000000000	Microsoft-Windows-GroupPolicy
5321	LocalSystem	10/19/2010 3:15:20 AM	A previous instance of the Group Policy Client Servic...	Information	0x4000000000000000	Microsoft-Windows-GroupPolicy
4001	LocalService	10/19/2010 3:15:25 AM		Information	0x4000200000000000	Microsoft-Windows-NetworkProfile
10000	LocalService	10/19/2010 3:15:25 AM		Information	0x4000200000000000	Microsoft-Windows-NetworkProfile
4002	LocalService	10/19/2010 3:15:26 AM		Information	0x4001200000000000	Microsoft-Windows-NetworkProfile
10000	LocalService	10/19/2010 3:15:26 AM		Information	0x4000200000000000	Microsoft-Windows-NetworkProfile
10001	LocalService	10/19/2010 3:15:40 AM		Information	0x4000200000000000	Microsoft-Windows-NetworkProfile
4001	LocalService	10/19/2010 3:15:45 AM		Information	0x4000200000000000	Microsoft-Windows-NetworkProfile
10000	LocalService	10/19/2010 3:15:45 AM		Information	0x4000200000000000	Microsoft-Windows-NetworkProfile
4002	LocalService	10/19/2010 3:15:46 AM		Information	0x4001200000000000	Microsoft-Windows-NetworkProfile
10000	LocalService	10/19/2010 3:15:46 AM		Information	0x4000200000000000	Microsoft-Windows-NetworkProfile
1006	LocalService	10/19/2010 3:15:57 AM	Router Advertisement settings have been changed...	Information	0x8000000000000000	Microsoft-Windows-DHCPv6-Client
1017	LocalSystem	10/19/2010 3:16:03 AM	A device will not be used for a ReadyBoost cache be...	Information	0x8000000000004000	Microsoft-Windows-ReadyBoost
1015	LocalSystem	10/19/2010 3:16:13 AM	Summary of ReadyBoot Performance.	Information	0x8000000000002000	Microsoft-Windows-ReadyBoost
1016	LocalSystem	10/19/2010 3:16:14 AM	Boot plan calculation completed.	Information	0x8000000000002000	Microsoft-Windows-ReadyBoost
306	LocalSystem	10/19/2010 3:17:25 AM	The BITS service loaded the job list from disk.		0x4000000000000000	Microsoft-Windows-Bits-Client

شکل ۶-۱۳ : رکوردهای لاگ های رویداد ذخیره شده

البته، می‌توان از ستون های دیگر نیز برای مرتب‌سازی لاگ‌ها، مانند شناسه رویداد و یا شرح رویداد خلاصه استفاده کرد، که بستگی به شرایط خاص case دارد.

۶-۶- بازیابی گزارش رویداد با استفاده از EVTXtract

شما قبلا با اکسپورت کردن، مرتب‌سازی و جستجو از طریق لاگ‌های رویداد ویندوز، آشنا شدید. اکنون نحوه بازیابی آثار لاگ رویداد حذف شده یا خراب شرح داده می‌شود. خوشبختانه، یک ابزار منبع باز با نام EVTXtract نوشته شده توسط ویلی بالنتین وجود دارد که قادر به حل این مشکل است. این ابزار می تواند قطعات EVTX را نه تنها از تصاویر RAW، بلکه از فضای غیرمجاز و دامپ حافظه نیز بازیابی کند.

اول از همه، باید منبع case را مشخص کرد. در اینجا سه گزینه وجود دارد. ۱) یک تصویر دیسک در فرمت RAW، ۲) یک دامپ حافظه یا ۳) یک فضای غیر اختصاصی. تصاویر دیجیتال RAW و تصاویر حافظه دامپ را در دستورالعمل‌های قبلی ایجاد نمودیم، اما فضای غیر اختصاص داده شده چیست؟ قبلا با نحوه کار با Autopsy آشنا شدید و حتی برخی از داده ها را از یک پارتیشن NTFS بازیابی کردیم. از این ابزار برای استخراج فضای غیر مجاز برای یک فایل جداگانه می‌توان استفاده کرد. برای انجام این کار، به قسمت منابع داده بروید، بر روی پارتیشنی که می خواهید فضای غیر اختصاص داده شده را از آن اکسپورت کنید، راست کلیک کنید، و Extract Unallocated Space را انتخاب کنید. هنگامی که فضای غیر اختصاصی استخراج می‌شود، می‌توان از این فایل به عنوان منبع برای EVTXtract استفاده کرد. برای شروع روند بازیابی، از دستور زیر استفاده کنید.

```
evtxtract.exe image.raw > output.xml
```

فراموش نکنید که image.raw را به فایل انتخابی خود تغییر دهید. پس از اتمام فرایند، می‌توان از طریق فایل خروجی، تجزیه و تحلیل و جستجو انجام داد.

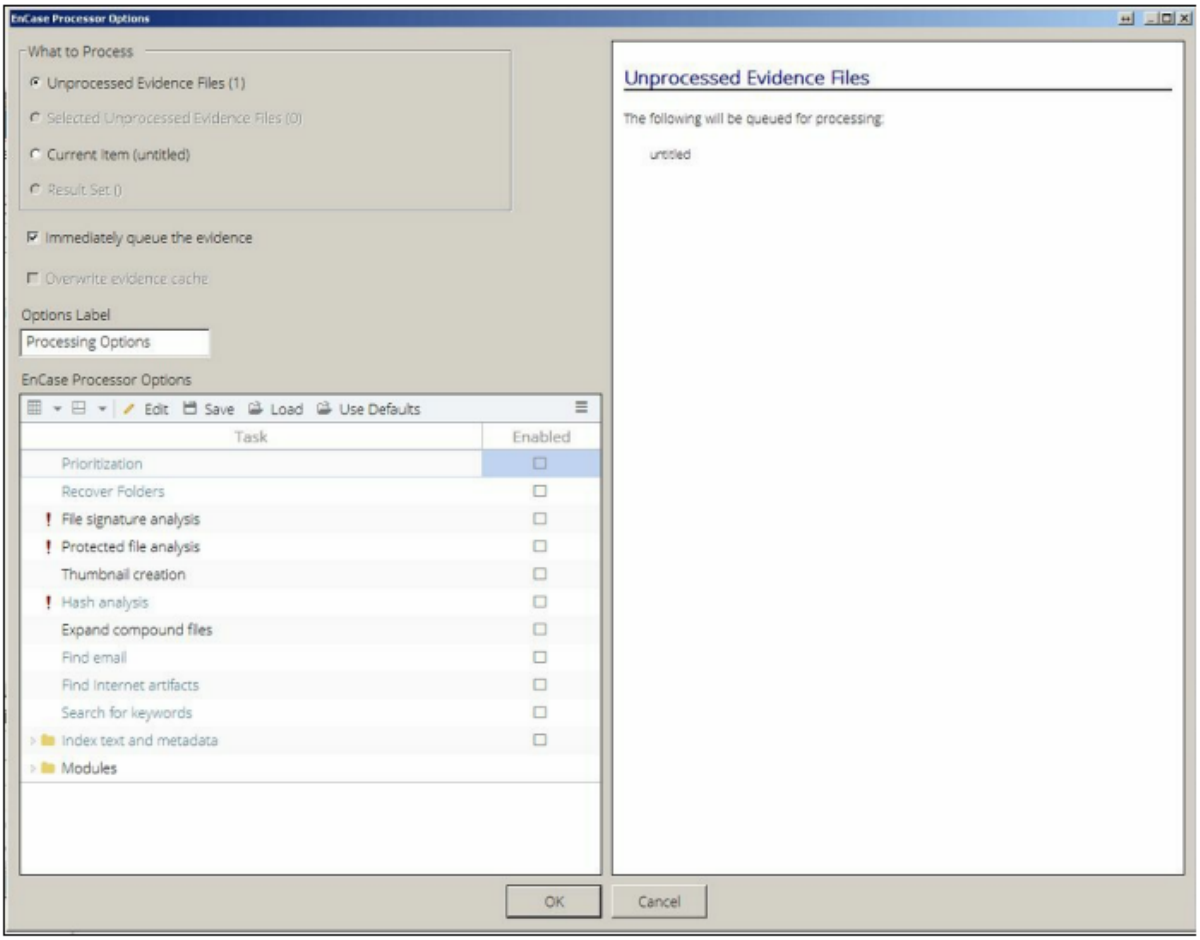
۶-۷- تجزیه و تحلیل فایل LNK با EnCase Forensic

قبلا با نحوه ایجاد یک case جدید آشنا شدید، فایل‌های شواهد را اضافه کنید، و محتویات سطل بازیافت ویندوز را با EnCase Forensic بررسی کنید. اکنون وقت آن رسیده است که با Evidence EnCase Processor و مخصوصا Parser Artifact Windows آشنا شوید. این

ماژول یک آزمونگر جرم شناسی را قادر می سازد به صورت خودکار به تجزیه و تحلیل آثار جرم شناسی ویندوز، از جمله فایل های LNK بپردازد.

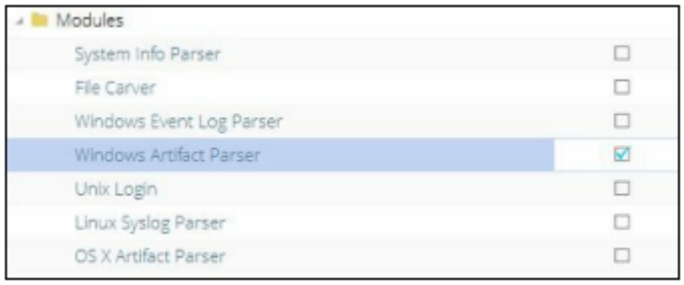
مراحل تجزیه و تحلیل فایل های LNK به شرح زیر است:

a. هنگامی که یک پرونده جدید ایجاد کردید و یک آیتم مدرک اضافه کردید، به قسمتProcess Evidence – Process بروید. سپس، پنجره EnCase Processor Options را مشاهده خواهید کرد.



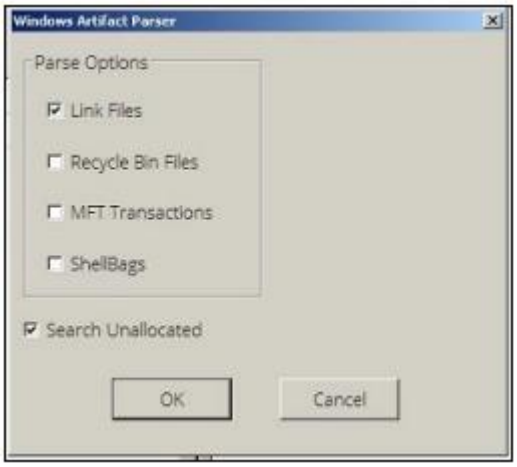
شکل ۶-۱۴ : پنجره EnCase Processor Options .

b. همانطور که مشخص است، در اینجا گزینه‌های بسیار زیادی وجود دارد: شما می توانید پوشه ها را بازیابی کنید، ایمیل را بیابید، آثار اینترنت را بیابید و غیره. اکنون، به پوشه ماژول رفته و محتویات آن مطابق شکل ۶-۱۵ قابل مشاهده است.



شکل ۶-۱۶ : محتوای فولدر Modules

c. در اینجا گزینه Parser Artifact Windows را انتخاب می‌کنیم. اگر روی نام آن کلیک کنید، گزینه های موجود در شکل ۶-۱۷ را می بینید.

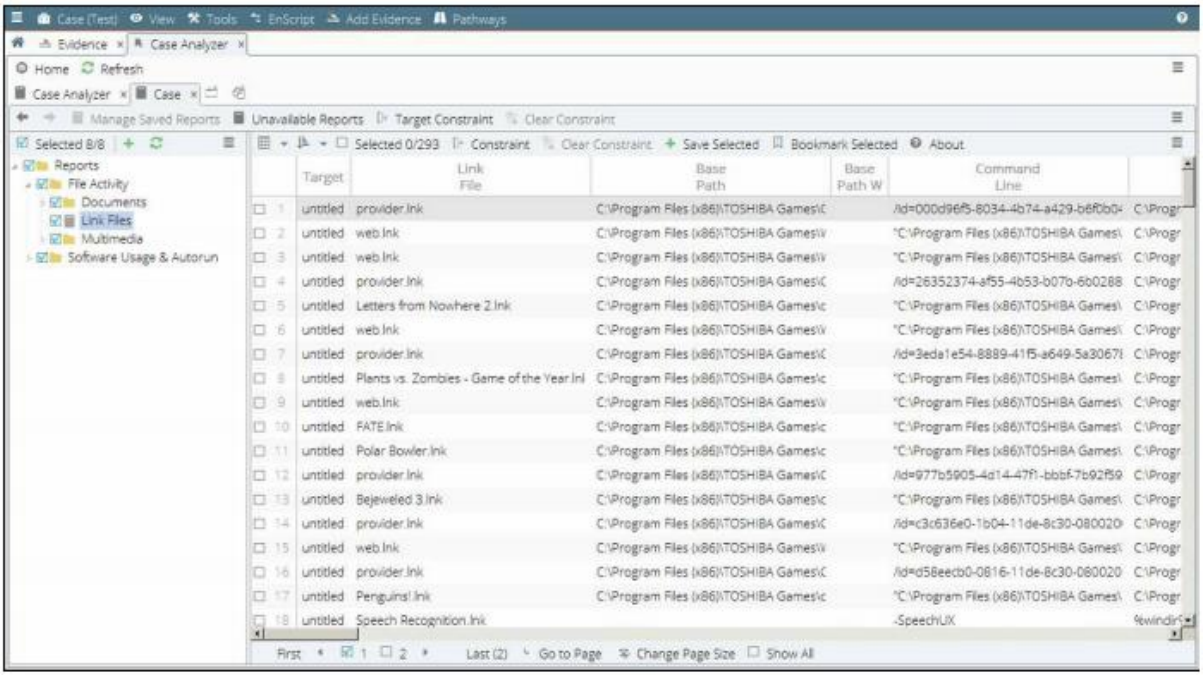


شکل ۶-۱۷ : پنجره گزینه‌های Windows Artifact Parser

d. این ماژول قادر است اطلاعاتی را درباره فایل‌های link، فایل های بازیافتی (اگر آنها را در گزارش می‌خواهید، مطمئن شوید که این گزینه فعال است)، تراکنش MFT و ShellBags و پرونده‌هایی که از فضای غیراختصاصی نسخه‌برداری شده اند (اگر شما گزینه Unallocated را انتخاب کنید) بازگرداند.

e. در این گام به تجزیه فایل‌های LNK می‌پردازیم، گزینه Link Files را انتخاب کنید (فراموش نکنید که جستجو Unallocated را فعال کنید).

f. پس از اتمام پردازش، به قسمت Analyzer Case – EnScript بروید. در اینجا، می‌توان تمام فایل‌های موجود در LNK را با فراداده های استخراج شده توسط Windows Artifact Parser پیدا کنید. نتایج بیشتر در شکل ۶-۱۸ آمده است.



شکل ۶-۱۸ : فایل های Parsed LNK

Windows Artifact Parser در نسخه افزوده شده به پرونده، جستجو کرده و اطلاعاتی از جمله فضای غیر اختصاصی، از فایل‌های LNK آن پیدا می‌کند. پس از اتمام فرایند، آزمونگر می‌تواند به تجزیه و تحلیل، نشانه‌گذاری و اضافه‌کردن این اطلاعات به گزارش خود بپردازد.

۶-۸- تجزیه و تحلیل فایل LNK با LECmd

LECmd یکی دیگر از ابزارهای جرم‌شناسی رایگان و متن باز ویندوز است که توسط Zimmerman نوشته شده‌است. این ابزار فایل ها را واقعا سریع پردازش می‌کند و می‌تواند برای تجزیه و تحلیل فایل‌های LNK تک و پوشه هایی که حاوی آنها باشد استفاده شود. همچنین دارای طیف وسیعی از گزینه های اکسپورت از جمله CSV و XML است.

مراحل تجزیه و تحلیل فایل LNK با LECmd بصورت زیر است.

a. همانطور که قبلا گفتیم، LECmd می‌تواند فایل‌ها و پوشه‌های تک فرایندی را پردازش کند. اگر می‌خواهید اطلاعات را از یک فایل جداگانه بگیرید، از کلید f- استفاده کنید؛ اگر هدف شما یک دایرکتوری باشد، از کلید d- استفاده کنید. اگر فقط به فایلهای LNK مربوط به درایوهای قابل حذف اشاره دارید، میتوانید از کلید r- استفاده کنید. گزینه های دیگر را می توان در شکل زیر مشاهده کرد.

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Admin>C:\Users\Admin\Downloads\LECmd\LECmd.exe

LECmd version 0.9.6.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/LECmd

        d                 Directory to recursively process. Either this or -f is r
equired
        f                 File to process. Either this or -d is required
        q                 Only show the filename being processed vs all output. Us
eful to speed up exporting to json and/or csv

        r                 Only process lnk files pointing to removable drives
        all               Process all files in directory vs. only files matching *
.lnk

        csv               Directory to save CSV (tab separated) formatted results
to. Be sure to include the full path in double quotes
        xml               Directory to save XML formatted results to. Be sure to i
nclude the full path in double quotes
        html              Directory to save xhtml formatted results to. Be sure to
 include the full path in double quotes
        json              Directory to save json representation to. Use --pretty f
or a more human readable layout
        pretty            When exporting to json, use a more human readable layout


        nid               Suppress Target ID list details from being displayed. De
fault is false.
        neb               Suppress Extra blocks information from being displayed.
Default is false.

        dt                The custom date/time format to use when displaying time
stamps. See https://goo.gl/CNVq0k for options. Default is: yyyy-MM-dd HH:mm:ss
        np                Display higher precision for time stamps. Default is fal
se
```

شکل ۶-۱۹ : گزینه های LECmd

b. برای اجرای LECmd در یک فایل یا پوشه روی یک تصویرجرم شناسی، ابتدا باید آن را نصب کنید. به عنوان مثال در پارتیشن اصلی N:\ نصب می‌کنیم. در اینجا از پوشه Roaming استفاده کردیم و خروجی را در فایلی با فرمت xhtml ذخیره نموده ایم. برای انجام این کار، از دستور زیر استفاده کنید.

```
LECmd.exe -d "N:\Users\NP\AppData\Roaming" -xhtml
"C:\Users\Admin\Desktop\test.html
```

c. بخشی از خروجی با فرمت xhtml را در شکل ۶-۲۰ قابل مشاهده است.

```
N:\Users\NP\AppData\Roaming\Microsoft\Office\Recent\LacyMilletCL.LNK
    Source Created:  2016-07-28 13:43:04
    Source Modified: 2016-08-04 17:58:23
    Source Accessed: 2016-08-04 17:58:23
    Target Created:  2016-07-28 13:43:03
    Target Modified: 2016-08-04 17:58:22
    Target Accessed: 2016-08-04 17:58:22
    File Size: 25088 (bytes)
    Relative Path: ..\..\..\..\Desktop\LacyMilletCL.doc
    Working Directory:
    File Attributes: FileAttributeArchive
    Header Flags: HasTargetIdList, HasLinkInfo, HasRelativePath, IsUnicode
    Drive Type: Fixed storage media (Hard drive)
8E19DC20 OS
    Local Path: C:\Users\
    Common Path: NP\Desktop\LacyMilletCL.doc
    Arguments:
    TargetID Absolute Path: My Computer\C:\Users\NP\Desktop\LacyMilletCL.doc
    Target $MFT Entry Number: 0x173C6
    Target $MFT Sequence Number: 0x28
    MachineID: np-pc
    Machine MAC Address: 5c:a0:c5:6d:aa:b9
    MAC Vendor: (Unknown vendor) (vendor not included in source .lnk file, auto-resolved by LECmd for end-user upon parsing)
    Tracker Created On: 2016-07-14 08:23:35
    Extra Blocks Present: KnownFolderDataBlock, PropertyStoreDataBlock, TrackerDataBaseBlock
```

شکل ۶-۲۰ : بخشی از خروجی LECmd

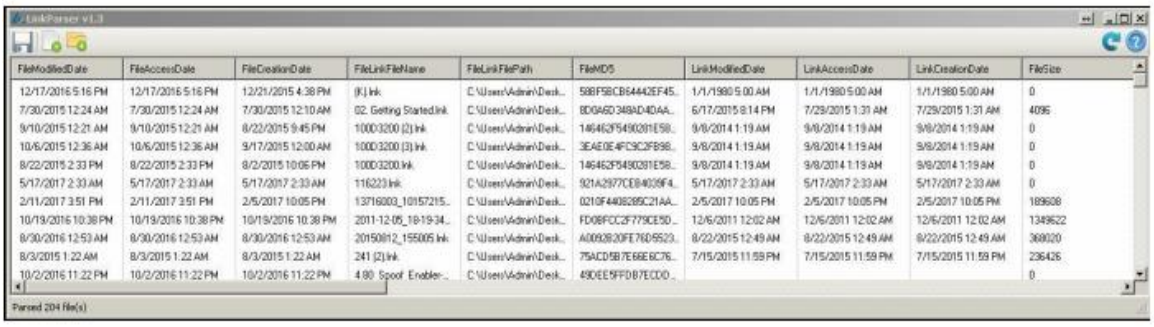
d. همانطور که در شکل قبلی مشخص است، LECmd مقدار زیادی اطلاعات از فایل‌های LNK استخراج می کند.

بطور خلاصه LECmd یک پوشه یا یک فایل را پیمایش کرده، اطلاعات را از فایل‌های LNK در دسترس استخراج و خروجی را به فرمت انتخاب شده توسط آزمونگر ذخیره می کند.

۶-۹- تجزیه و تحلیل فایل LNK با Link Parser

Link Parser یک ابزار رایگان دیگر است که می تواند توسط آزمونگرهای جرم‌شناسی برای فایل‌های LNK استفاده شود. این ابزار توسط Discovery توسعه داده شده است، و قادر به تجزیه یک فایل LNK تک، چندین فایل انتخاب شده، و یا بصورت بازگشتی به بیش از یک پوشه و یا تصویراست.

برنامه LinkParser.exe را اجرا کنید، روی آیکون folder کلیک کنید، و یک پوشه با فایل های LNK که میخواهید این ابزار آنها را تجزیه کند، انتخاب کنید. در اینجا C: \ Users {username} \ AppData \ Roaming \ Microsoft \ Windows \ Recent – انتخاب شده است. این پوشه حاوی پرونده‌هایی است که اخیرا استفاده شده است و با استفاده از FTK Imager از یک تصویر جرم‌شناسی اکسپورت کرده‌ایم. Link Parser داده هایی را از ۲۰۴ فایل LNK استخراج کرده است.



شکل ۶-۲۱ : خروجی Link Parser

Link Parser مقدار زیادی داده از فایل های LNK را استخراج می کند - بیش از ۳۰ ویژگی، از جمله شماره سریال، Volume Label، Volume ID و غیره.

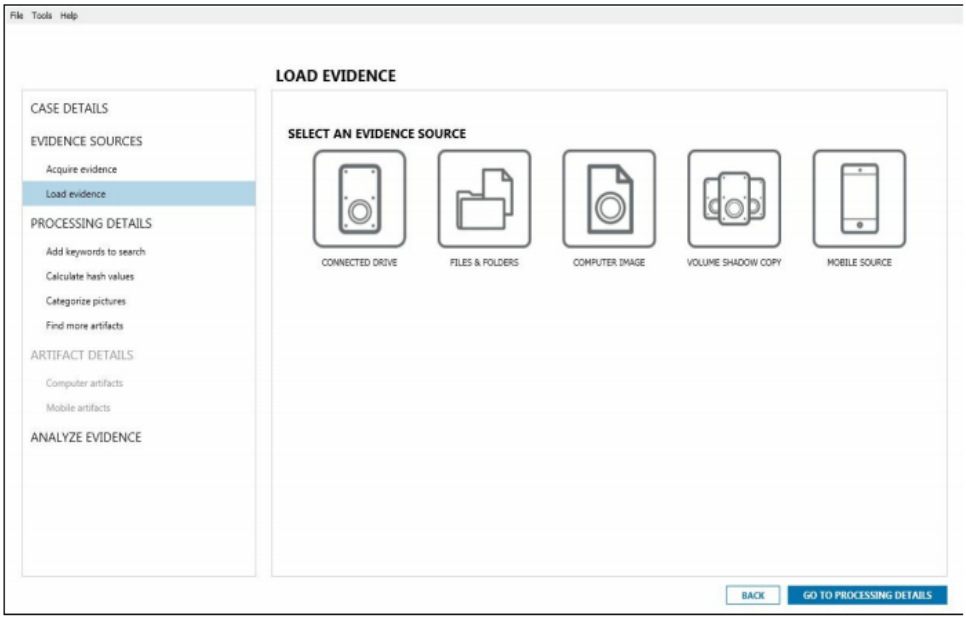
تمام ویژگی های تجزیه شده را می توان به راحتی به CSV اکسپورت کرد. برای انجام این کار، روی نماد فلاپی دیسک کلیک کنید، Export file name را انتخاب کنید و یک مکان را انتخاب کنید. سپس، به راحتی می توانید داده های استخراج شده را به برنامه های کاربردی موردنظرتان وارد کنید.

۶-۱۰- تجزیه و تحلیل فایل Prefetch با استفاده از Magnet AXIOM

اگر دستورالعمل های این کتاب را دنبال کرده باشید، می‌دانید که Magnet AXIOM چیست، و حتی آن را برای تجزیه و تحلیل جرم شناسی برخی از آثار ویندوز استفاده کرده اید. در اینجا قصد داریم به نشان دهیم که چگونه در تجزیه و تحلیل آثار مختلف سیستم عامل از این ابزار استفاده کنید.

مراحل تجزیه و تحلیل فایل Prefetch با استفاده از Magnet AXIOM در زیر شرح داده شده‌است.

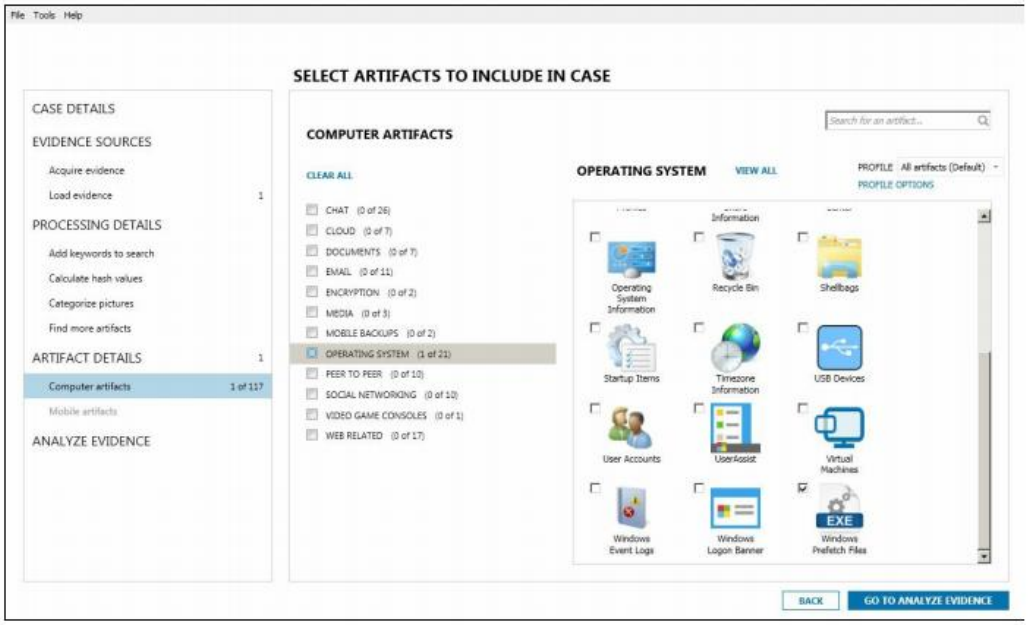
a. ابتدا یک پرونده جدید ایجاد کنید و به Load evidence بروید. در اینجا پنج گزینه وجود دارد: CONNECTED DRIVE، FILES & FOLDERS، COMPUTER IMAGE، VOLUME SHADOW COPY و MOBILE DEVICES.



شکل ۶-۲۲ : قسمت Load evidence

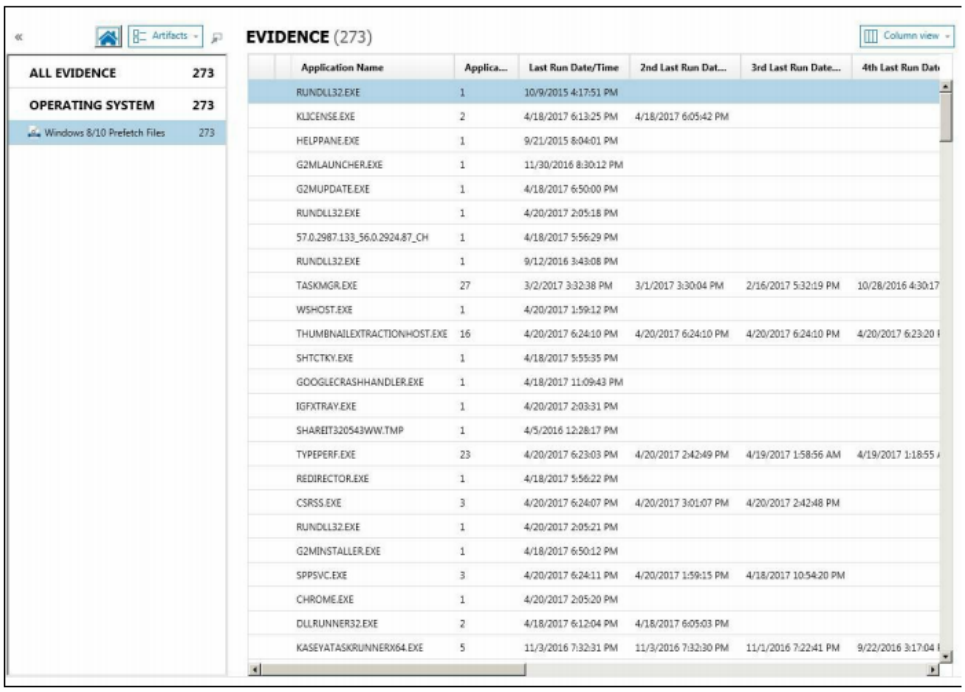
b. همانطور که قبلا ذکر شد، می توانید از یک تصویر جرم شناسی یا یک پوشه با فایل‌های prefetch، که قبلا اکسپورت شده استفاده کنید. اگر گزینه اول را ترجیح می دهید، COMPUTER IMAGE را انتخاب کنید اگر دوم، FILES & FOLDERS را انتخاب کنید. در اینجا، با کمک مرورگر پوشه AXIOM انتخاب شده است.

c. به قسمت artifact details رفته و آثار مورد نظر خود را از لیست انتخاب کنید. روی دکمه CUSTOMIZE COMPUTER ARTIFACTS کلیک کرده، سپس CLEAR ALL را بزنید، به OPERATING SYSTEM رفته و گزینه Prefetch Files Windows را علامت بزنید.



شکل ۶-۲۳ : انتخاب آثار برای یک پرونده

d. اکنون می‌توانیم شواهد را تحلیل کنیم. در اینجا یک پوشه با فایل‌های prefetch انتخاب کردیم، بنابراین خیلی زود می توان نتایج تجزیه را در AXIOM Exam مشاهده کرد. پس از پایان مرحله پردازش، می‌توان به مشاهده و تجزیه و تحلیل نتایج پرداخت.



شکل ۶-۲۴ : نتایج Prefetch files

در اینجا می‌توان تعداد اجراهای هر برنامه و همچنین برچسب‌های زمانی تا هشت برنامه اخیر را دریافت کرد. Magnet AXIOM جستجویی برای فایل های prefetch و استخراج اطلاعات در مورد تعداد دفعات اجرا و برچسب‌های زمانی تا هشت اجرای اخیر است.

۶-۱۱- تجزیه فایل Prefetch با PECmd

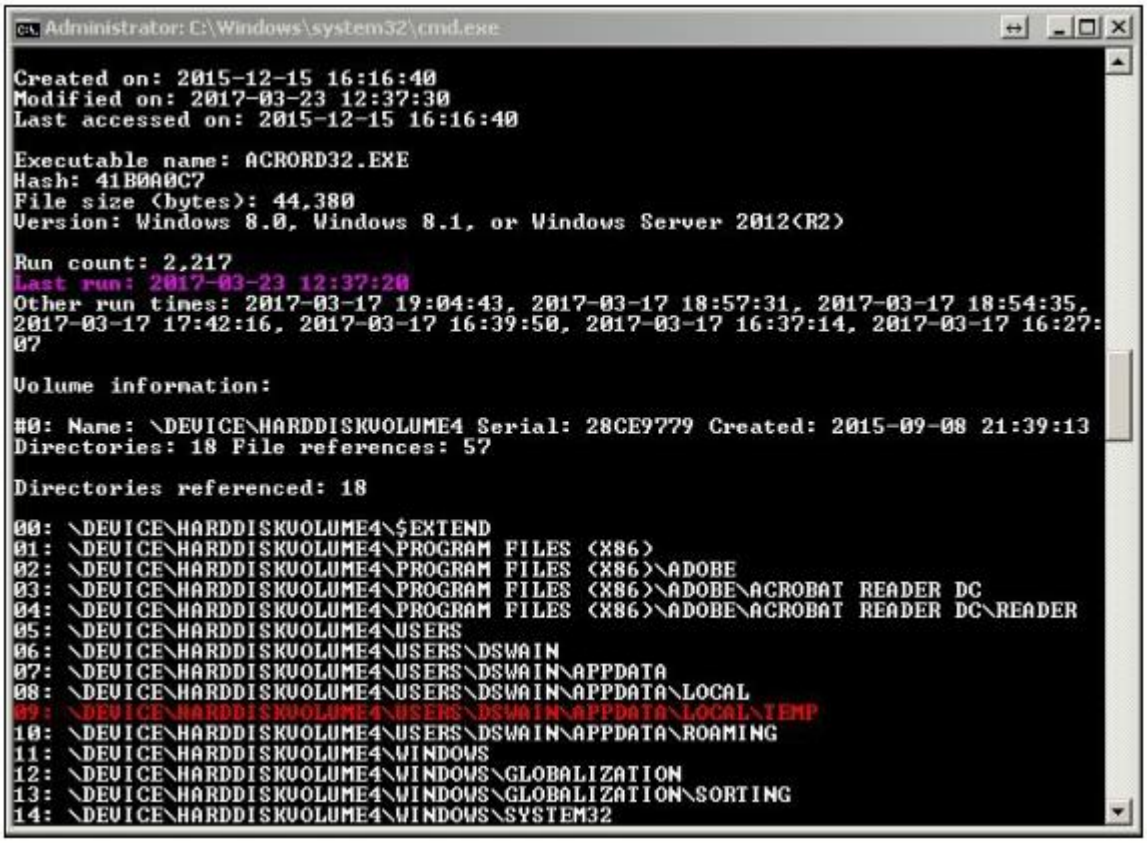
اگر برخی از فایل های prefetch مشکوک را پیدا کرده‌اید و می‌خواهید تجزیه و تحلیل عمیق روی آنها انجام دهید، یک ابزار دیگر با نام PECmd توسط Zimmerman ارائه شده که می تواند در این زمینه به شما کمک کند. PECmd یک ابزار خط فرمانی رایگان و سریع است که قادر به تجزیه فایل های prefetch ویندوز است. در این دستورالعمل، امکان کسب اطلاعات با ارزشی از فایل های prefetch را فراهم می کنیم.

مراحل پردازش و تجزیه فایل prefetch با PECmd به شرح زیر است.

a. با استفاده از Command Prompt ویندوز، دایرکتوری را به همان جایی که مجموعه برنامه را از پک خارج کرده اید تغییر دهید و دستور زیر را اجرا کنید.

```
PECmd.exe -f C:\Users\Admin\Desktop\Prefetch\ACRORD32.EXE-41B0A0C7.pf
```

خروجی مختصر در شکل زیر قابل مشاهده است.



شکل ۶-۲۵ : خروجی PECmd

همانطور که در شکل قبلی مشخص است، می‌توان نام اجرا، تعداد دفعات اجرا، زمان‌بندی هشت اجرای گذشته و حتی فهرست دایرکتوری ها و مراجع فایل را بدست آوریم.

b. همچنین می توان همه فایل‌ها را در یک دایرکتوری به طور مجزا تجزیه کرد. برای انجام این کار باید از دستور زیر استفاده کرد.

```
PECmd.exe -d C:\Users\Admin\Desktop\Prefetch\
```

این ابزار، کوچک اما واقعا قدرتمند است و برای استفاده در تجزیه و تحلیل فایل Prefetch ویندوز در جرم شناسی ویندوز بسیار توصیه می شود. PECmd اطلاعات موجود در یک فایل prefetch یا چند فایل prefetch را در یک پوشه مشخص شده توسط کاربر استخراج می کند. این اطلاعات شامل تعداد کل اجرا، برچسب زمانی برای اجرای اخیر، راهنماها و مراجع فایل و غیره است.

۶-۱۲- بازیابی فایل Prefetch با Windows Prefetch Carver

اگر میخواهید فایلهای Prefetch ویندوز را از داده‌های باینری دلخواه خود جدا کنید، برای شما یک ابزار با نام Windows Prefetch Carver وجود دارد که توسط Adam Witt ارائه شده‌است. برای مثال می توان از آن برای جدا کردن(بریدن) prefetch از یک فضای غیر اختصاصی درایو یا یک تصویر حافظه استفاده کرد. در این دستور ما به شما نحوه استفاده از آن را نشان خواهیم داد.

مراحل بازیابی فایل prefetch با Windows Prefetch Carver به شرح زیر است:

a. برای این دستور، ما یک تصویر حافظه در ویندوز ۷ استفاده کردیم. نام این تصویر joshua1.vmem است - شما می توانید لینک دانلود برای این تصویر حافظه را نیز مشاهده کنید. حالا دستور زیر را تایپ کنید:

```
prefetch-carve.py -f joshua1.vmem -o output.txt
```

به عنوان نتیجه، یک فایل خروجی با داده های جدا شده دریافت خواهید کرد.

```
2013-03-23 02:06:43.592936 | WMIPRVSE.EXE-1628051c | run_count: 2
2013-03-23 02:07:34.168224 | CONHOST.EXE-1f3e9d7e | run_count: 7
2013-03-23 02:06:46.744143 | VSSVC.EXE-b8afc319 | run_count: 1
2013-03-23 02:07:34.277426 | TASKHOST.EXE-7238f31d | run_count: 5
2013-03-23 02:06:43.405735 | WMIADAP.EXE-f8dfdfa2 | run_count: 1
2013-03-23 02:06:52.796951 | DRVINST.EXE-4cb4314a | run_count: 14
2013-03-23 02:06:45.854940 | NOTEPAD.EXE-d8414f97 | run_count: 1
2013-03-23 02:07:34.152624 | SC.EXE-945d79ae | run_count: 1
2013-03-23 01:57:31.976156 | SVCHOST.EXE-9efc97f2 | run_count: 1
2013-03-23 02:07:34.152624 | SC.EXE-945d79ae | run_count: 1
2013-03-23 02:06:46.931341 | SVCHOST.EXE-7cfedea3 | run_count: 1
2013-03-23 02:07:08.334579 | WUAUCLT.EXE-70318591 | run_count: 2
2013-03-23 02:07:08.240978 | WUSETUPV.EXE-c61614f3 | run_count: 1
```

شکل ۶-۲۶ : خروجی Windows Prefetch Carver

b. همانطور که می بینید،این ابزار ۱۳ رکورد را جدا کرده است: نشانگرهای زمانی، نام فایل ها و تعداد اجراها، ارائه شده است. چند فرمت خروجی، از جمله CSV و mactime پشتیبانی می شود.

Windows Prefetch Carver قسمتی از داده های باینری منتخب را اسکن می کند و عناصر آرایه ای از فایل های Prefetch ویندوز را از جمله برچسب های زمان بندی، نام فایل ها و شمارش های اجرا، برمیگرداند.

فصل ۷ : مرورگر وب

در این فصل به تجزیه و تحلیل مرورگرهای وب با استفاده از ابزارهای زیر خواهیم پرداخت.

- تحلیل مرورگر فایرفاکس با BlackBag's BlackLight
- تحلیل گوگل کروم با استفاده از Magnet AXIOM
- مرورگر اینترنت مایکروسافت و تحلیل Microsoft Edge با Belkasoft Evidence Center
- استخراج داده های مرورگر وب از طریق Pagefile.sys

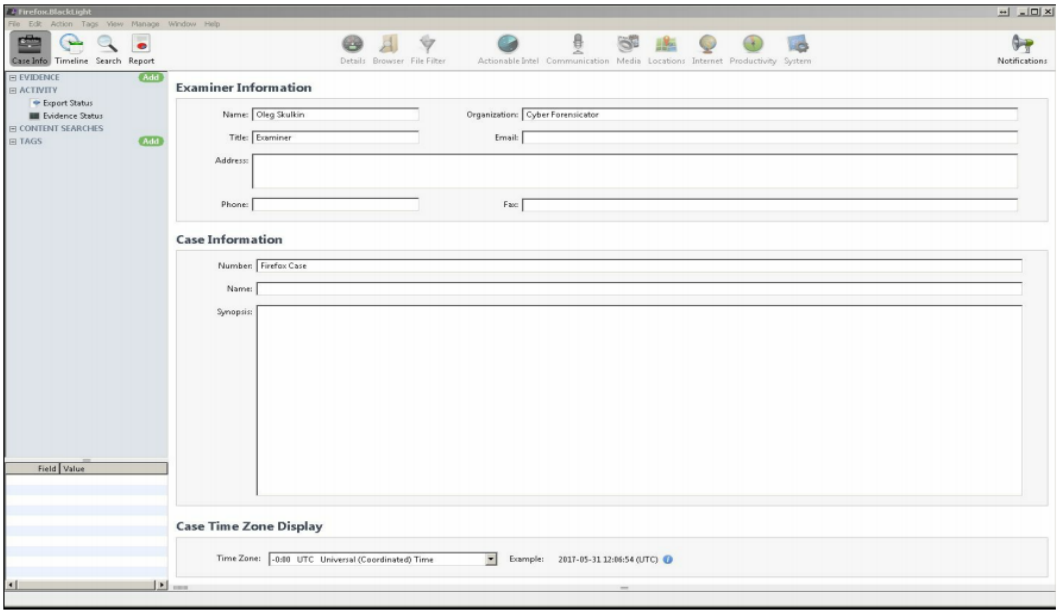
هریک از این ابزارها به صورت مفصل شرح داده خواهد شد.

۷-۱- تحلیل مرورگر فایرفاکس با BlackBag's BlackLight

BlackBag's BlackLight یک ابزار دیجیتال بسیار قدرتمند است که معمولا برای سیستم عامل Mac OS X مورد استفاده است اما سیستم عامل مک تنها سیستم عاملی نیست که از آن پیشتبانی میکند. میتوان از آن برای سیستم عامل های Android ، IOS و ویندوز نیز استفاده کرد. علاوه بر این، میتوان از BlackLight برای ایستگاه های کاری در سیستم عامل های ویندوز و مکینتاش استفاده کرد به این معنی که میتوان بر روی سیستم عامل مک تجزیه و تحلیلی از تصاویر جرم شناسی ویندوز انجام داد. برای این مورد چگونگی کار BlackLight در موزیلا فایرفاکس نشان داده شده است.

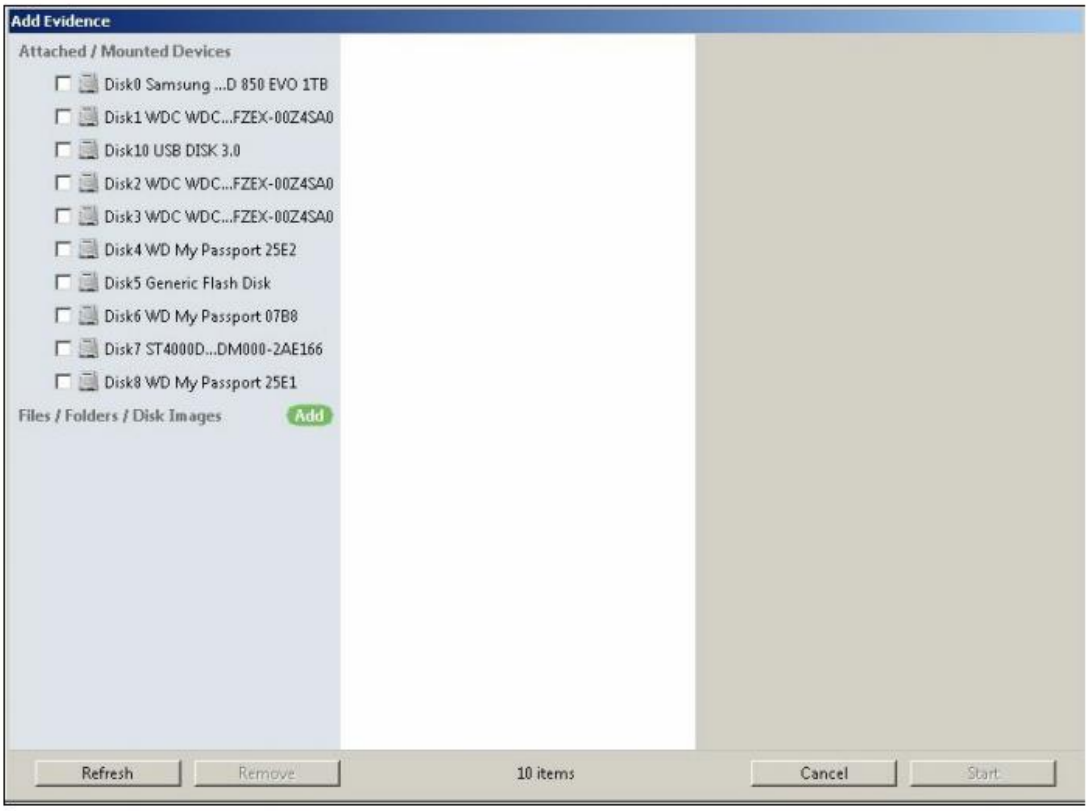
مراحل تجزیه و تحلیل ها با استفاده از موزیلا فایرفاکس به صورت زیر است :

a. ابتدا BlackLight را باز کرده و نمونه جدید ساخته میشود. برای این انجام این کار، به منوی فایل رفته و new case را زده و یا بر روی NEW کلیک کرده و محل مورد نظر را انتخاب کنید. هنگامی که آن مورد را ذخیره کردید، میتوانید فیلدهای ضروری را پر کرده و منطقه زمانی مناسب را انتخاب کنید، به صورتی که در شکل نشان داده شده است.



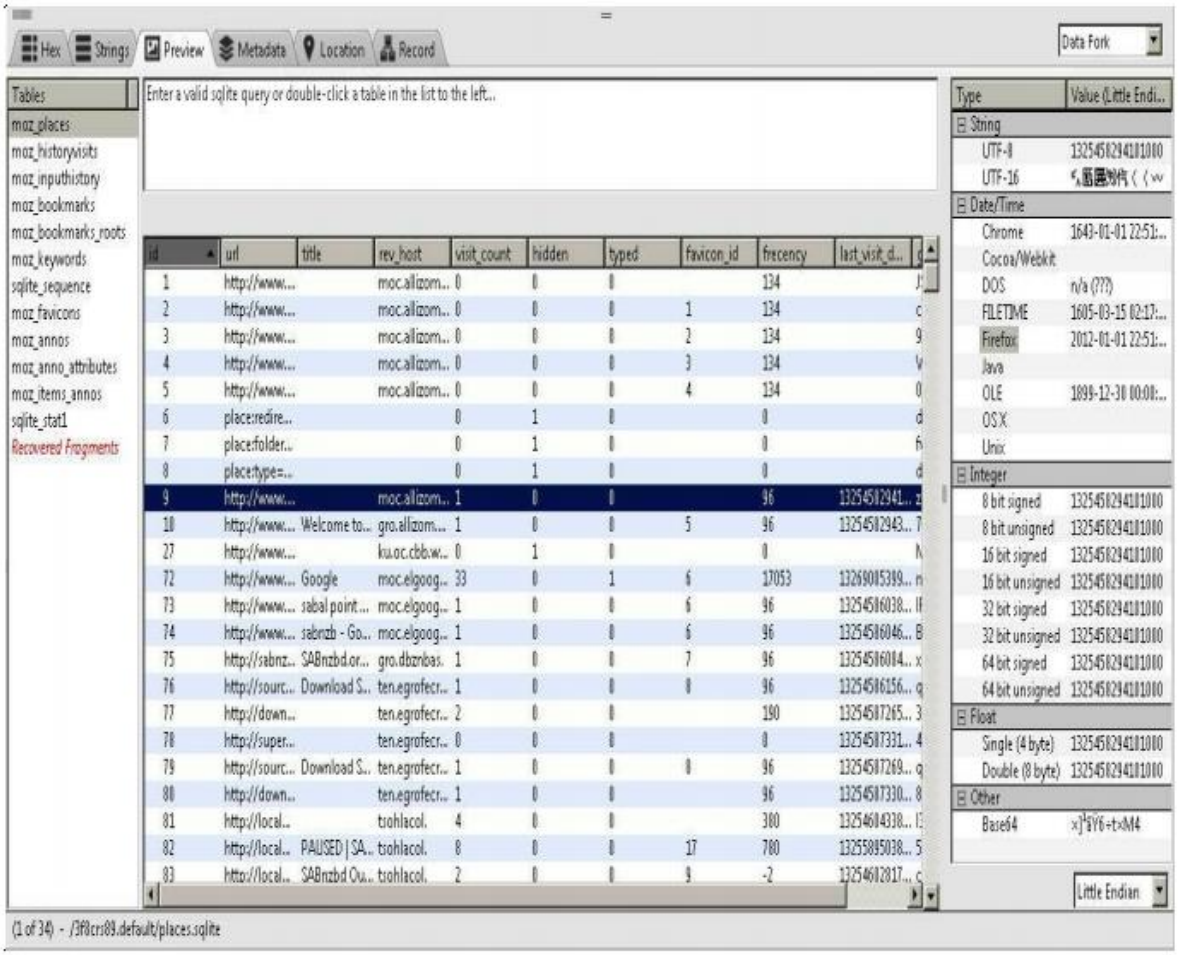
شکل ۷-۱ : جزئیات case

b. حال آماده اضافه کردن مدارک هستیم. بر روی دکمه سبز رنگ add در مقابل مدارک کلیک کنید. حال که ما پروفایل مربوط به فایرفاکس را در یک پوشه export کردیم، بر روی دکمه سبز رنگ add باز هم کلیک کرده سپس دکمه Add folder را زده و پوشه ای برای فایل های export شده را انتخاب میکنیم.



شکل ۷-۲ : اضافه کردن مدارک

c. هنگامی که داده ها پردازش شدند، شما باید داده های استخراج شده را tab اینترنت پیدا کنید. اگر برای دلایلی این tab دارای محتوای مورد انتظار نبود، شما میتوانید به صورت دستی Firefox SQLite database را تحلیل کنید- BlackLight دارای یک درگاه قدرتمند SQLite browser است، از آن برای تحلیل مرورگرها استفاده کنید- یک SQLite database شامل اطلاعاتی در مورد تاریخچه های مشکوک مرورگر است. به تب preview رفته و پایگاه‌داده را انتخاب کنید. از ویژگی‌های پیش‌نمایش با استفاده از مرورگر BlackLight SQLite استفاده کنید.



شکل ۷-۳ : تحلیل دستی 'places.sqlite' SQLite database

d. ویژگی های تاریخ وزمان. آیا متوجه جدول بازیابی بخش ها شده اید؟ این موارد میتواند به یک متخصص برای بازیابی داده های حذف شده کمک کند که در این مورد ما رکورد های تاریخچه حذف شده نشان داده شده است.

تحلیل پایگاه داده BlackLight و استخراج داده های موجود (شامل داده های حذف شده) برای بررسی های بیشتر، شامل تاریخچه، بوکمارکها، دانلودها، فرم های داده ای، کوکی ها و امثال این موارد بوده است. همچنین یک مرورگر SQLite ساخته شده ما را قادر میسازد که تحلیل ها بر روی پایگاه داده را به صورت دستی نیز انجام دهیم.

۷-۲- تحلیل گوگل کروم با استفاده از Magnet AXIOM

گوگل کروم یکی دیگر از مرورگرهای بسیار مشهور است. شما میتوانید Artifact های آن را برای تست های جرم شناسی پیدا کنید، نه فقط در سیستم های ویندوز بلکه در مکینتاش، لینوکس و حتی پلتفرم های موبایلی نیز موجود است. با کمک این دستورالعمل ها شما میتوانید یاد بگیرید که چگونه گوگل کروم را با استفاده از Magnet AXIOM تجریه و تحلیل کنید.

یک نمونه از AXIOM ایجاد کرده و از پوشه ای که سورس مدارک در آنجا export میشود استفاده کنید و مطمئن شوید که گوگل کروم در لیست نتایج انتخاب شده است. به محض اینکه همه این مراحل انجام شد ابزار تحلیل مدارک را اجرا کنید. این زمان زیادی نمیگیرد اما شما نتایج مفیدی از جرم شناسی را بدست خواهید آورد. نتایج استخراج شده در مورد مثال ما در شکل زیر نشان داده شده است.

Chrome Autofill	186
Chrome Autofill Profiles	2
Chrome Bookmarks	191
Chrome Cache Records	30,750
Chrome Cookies	2,903
Chrome Current Session	17
Chrome Current Tabs	15
Chrome Downloads	144
Chrome FavIcons	2,539
Chrome Keyword Search Terms	81
Chrome Last Session	10
Chrome Last Tabs	4
Chrome Logins	17
Chrome Shortcuts	15
Chrome Sync Accounts	2
Chrome Sync Data	711
Chrome Top Sites	31
Chrome Web History	6,050
Chrome Web Visits	4,870
Chrome/360 Safe Browser Carved Session/Tabs	137
Chrome/360 Safe Browser/Opera Carved Web History	1,948

شکل ۷-۴ : نتایج استخراج شده از تحلیل گوگل کروم با استفاده از Magnet AXIOM

همانطور که در شکل بالا میبینید نتایجی بسیاری وجود دارد. بیایید کمی عمیق تر بررسی کنیم.

Chrome autofill profile: پروفایلی که کروم به صورت خودکار پر میکند.

Chrome bookmarks: صفحاتی که توسط کاربر بوکمارک میشوند.

Chrome cache records: فایل های دانلود شده با مرورگر که برای سرعت بخشیدن به بار شدن صفحات استفاده میشود. این میتواند شامل عکس‌ها، html ، javascript و امثال این‌ها باشد.

Chrome cookies: فایل کوچکی که شامل اطلاعاتی در مورد وب سایت های دیده شده توسط کاربر است.

Chrome current session: اطلاعاتی در مورد session حال حاضر است.

Chrome download: فایل های دانلود شده توسط گوگل کروم در اینجا قرار دارد.

Chrome favIcons: شامل favIcons که در آدرس بار کروم می آید.

Chrome keyword search terms: کلمات کلیدی زده شده توسط کاربر است.

Chrome last session: اطلاعاتی در خصوص آخرین session است.

Chrome last tab: آخرین tab که در session باز شده است.

Chrome logins: اطلاعات لاگین ذخیره شده توسط کروم کاربران است.

Chrome shortcuts: shortcutهایی که توسط کاربر در urlها زده شده است.

Chrome sync accounts: حساب کاربری که برای همگام سازی با فضای ابری مورد استفاده است.

Chrome sync data: داده های همگام سازی شده با فضای ابری است.

Chrome top site: وب سایت های که نرخ دیده شدن بالایی داشته اند.

Chrome web history: وب سایت هایی که کاربر آنها را دیده است

Chrome web visits: وب سایت هایی که کاربر آنها را دیده است (همه موارد)

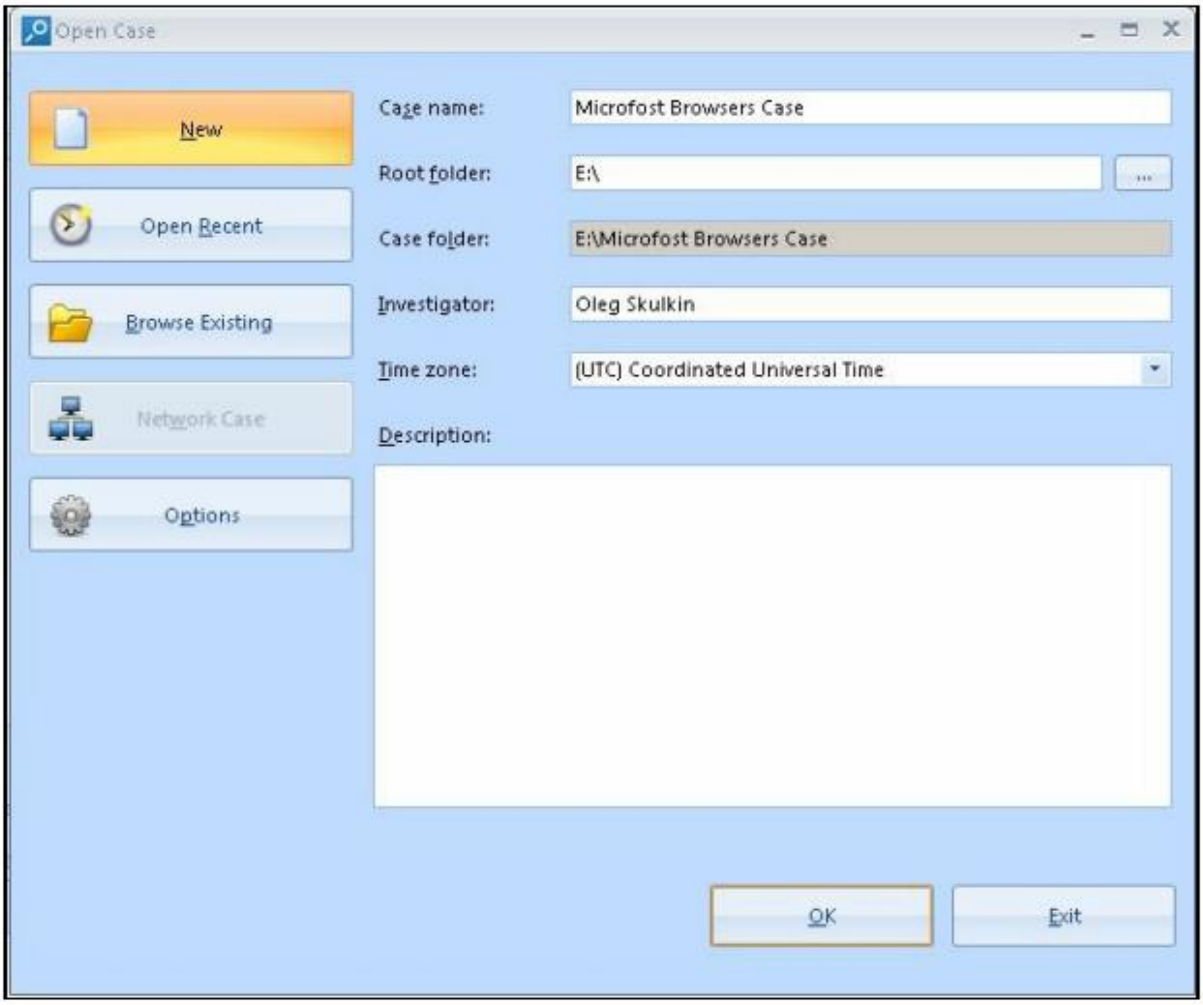
همچنین AXIOM از فنون carving برای بازیابی داده های حذف شده از پایگاه داده کروم استفاده میکند. Magnet AXIOM از نتایج گوگل کروم از قبیل جرم شناسی عکس ها، درایوها، پوشه ها و یا فایل های مشخص شده با تست کننده های دیجیتال جرم شناسی، جستجو و تحلیل انجام میدهد. نتایج تحلیل شده به دسته های مختلفی برای بررسی جرم شناسی راحت تر، تقسیم میشوند.

۷-۳- مرورگر اینترنت مایکروسافت و تحلیل Microsoft Edge با Belkasoft Evidence Center

امیدواریم شما Belkasoft Evidence Center را به لیست ابزارهای جرم شناسی ویندوزتان اضافه کرده باشید. همانطور که میدانید این ابزار میتواند برای carve data out of memory dumps شما را کمک کند. همچنین این تنهخا کارش کمک به شما در حل مشکلات نیست. این ابزار پیشتبانی قوی برای هزاران سیستم عامل ویندوز با مرورگرهای وب متفاوت برای بررسی جرم شناسی دارد. در این دستورالعمل، ما به شما نشان میدهیم که این ابزار به چه شکل برای Microsoft Internet Explorer و Microsoft Edge برای تحلیل جرم شناسی کاربرد دارد. مراحل تست در ادامه شرح داده شده‌است.

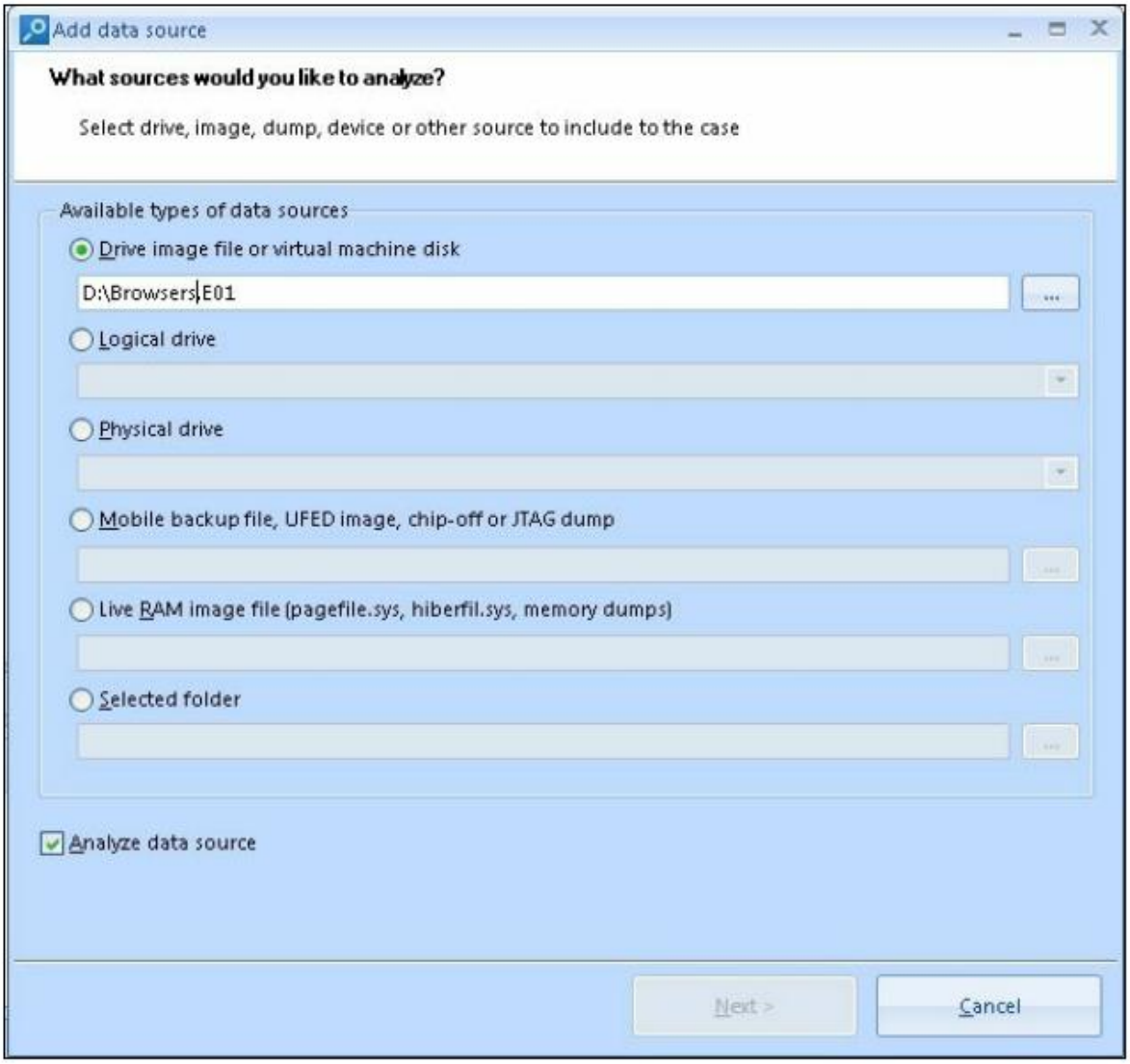
مراحل تحلیل Microsoft Edge و تحلیل Microsoft Internet Explorer با استفاده از Belkasoft Evidence Center به صورت زیر است.

a. ابتدا باید یک نمونه جدید ساخته شود. اطلاعات مربوط به نمونه را پر کرده و پوشه ریشه را انتخاب کنید (پوشه نمونه خودکار ایجاد میگردد) و و مطمئن شوید که منطقه زمانی را در منوی مورد نظر به شکل صحیح انتخاب کرده اید. اگر بخواهید میتوانید توضیحات اضافه تر در مورد نمونه ها را اضافه کنید.



شکل ۷-۵ : ایجاد یک حساب کاربری در Belkasoft Evidence Center

b. اکنون زمان انتخاب منبع داده است. همانطور که در ادامه میبینید ما دارای چند گزینه هستیم. در این مورد ما تصویر درایو را انتخاب میکینم. ما یک تصویر آزمایشی به نام Browsers.E01 انتخاب میکنیم. اگر شما یک تصویر از درایو در ویندوز ۱۰ بسازید، میتوانید از آن برای این دستورالعمل استفاده کنید در غیر اینصورت چنین سیستمی پیدا کنید و دانش خود را در این خصوص افزایش دهید. همچنین شما میتوانید یک ماشین مجازی ویندوز ۱۰ بسازید و از درایو مجازی آن استفاده کنید – چنین درایوهایی نیز با ابزار Belkasoft Evidence Center قابل پشتیبانی است.



شکل ۷-۶ : اضافه کردن منبع داده در Belkasoft Evidence Center

c. در این زمان نتایج جرم شناسی را که میخواهیم برای آن جستجو کنیم را انتخاب میکنیم. ابتدا بر روی گزینه هیچکدام برای عدم انتخاب همه انواع داده کلیک میکنیم. حال به مرورگر مراجعه میکنیم، به پایین صفحه در سمت چپ ویندوز می آیم و گزینه Edge و سپس Internet Explorer را انتخاب میکنیم. فراموش نکنید برای استخراج داده های بیشتر گزینه های دیگر را نیز تیک بزنید.

شکل ۷-۷ : انتخاب فرمت داده ها در Belkasoft Evidence Center

در این عکس پردازش انجام شده است که میتوانید نتیجه آن را در شکل ۷-۸ ببینید.

شکل ۷-۸ : Overview tab

اگر شما خواهان تحلیل و آنالیز عمیق‌تر بر روی تاریخچه مرورگر هستید، متوجه خواهید شد که باید تمامی موارد در Internet Explorer باید تیک زده شوند. به این دلیل که هردوی Internet Explorer و Edge رکوردهای تاریخچه‌ها را در یک پایگاه داده ذخیره می‌کنند که آدرس آن به صورت زیر است.

C:\Users\%USERNAME%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat

همچنین شما میتوانید بخش url تایپ شده را در شکل قبلی ببینید. این url به صورت مستقیم توسط کاربر در قسمت آدرس مرورگر تایپ شده است و در رجستری ذخیره شده است. میتوانید اطلاعات بیشتری در مورد جرم شناسی ریجستری را در فصل ۶ و تحلیل ریجستری ویندوز را یاد بگیرید. ابزار Belkasoft Evidence Center مبتنی بر همه فایل ها و پوشه ها و داده موجود استخراج شده در مرورگر وب عملیات انجام میدهد. اگر بررسی عمیق مدنظر باشد داده ها از فضای اختصاص داده نشده نیز استخراج میشود.

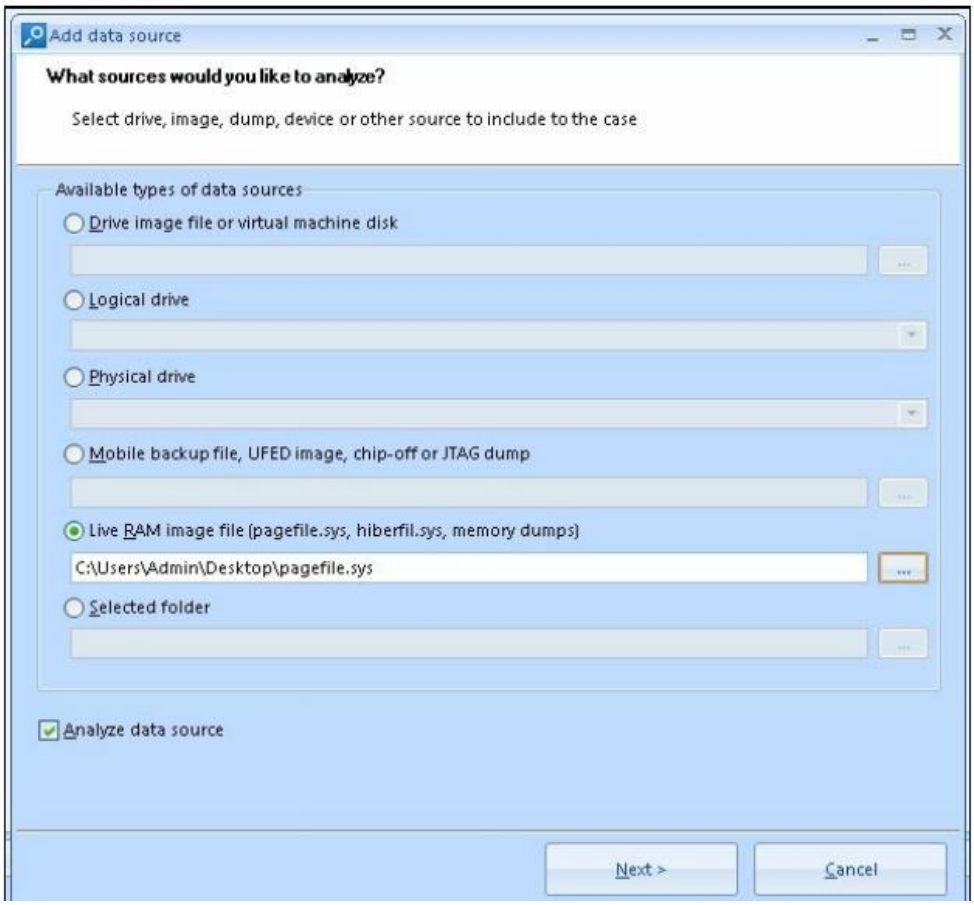
۷-۴- استخراج داده های مرورگر وب از طریق Pagefile.sys

شما میدانید که میتوانید بسیاری اطلاعات از نتایج جرم شناسی از طریق memory dump را به دست آورید. اما نکات بیشتری وجود دارد که اینکه شما میتوانید اطلاعات و نتایج بسیاری را به دست آورید حتی بدون انجام memory dump . فایل هایی بر روی درایو وجود دارد که شامل بخش هایی از حافظه است. این فایل ها Pagefile.sys، swapfile.sys و hiberfile.sys هستند که در ریشه سیستم در C:\ قرار داده شده اند. در این دستورالعمل ما به شما آموزش میدهیم که چگونه داده ها را از مرورگرهای وب از طریق Pagefile.sys با ابزار Belkasoft Evidence Center استخراج کنید.

مراحل استخراج داده از مرورگر وب در Pagefile.sys در ادامه توضیح داده شده است :

a. شروع با ایجاد یک نمونه جدید در Belkasoft Evidence Center است که میدانید چطور آن را ایجاد کنید. سپس فایل Pagefile.sys را که قبلا از منبع مدارک استخراج نموده‌اید، اضافه کنید.

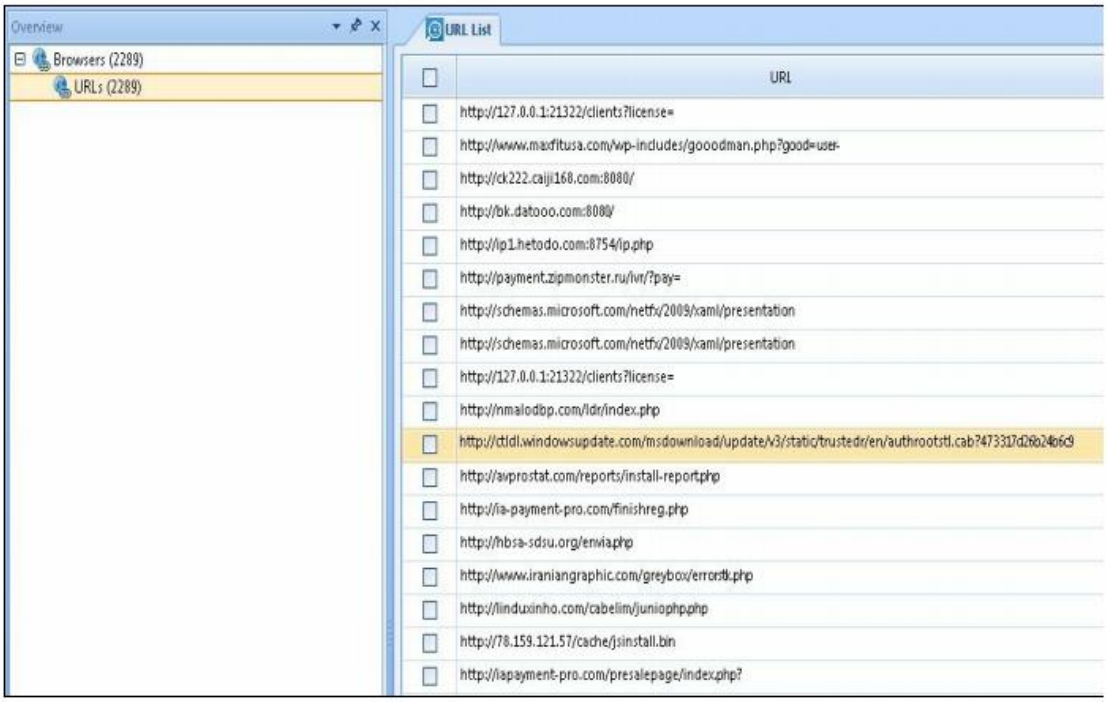
b. طبق برنامه ریزی که برای استخراج داده از مرورگر وب در یک سیستم ویندوز، باید انواع فرمت داده انتخاب شود که در شکل ۷-۹ نشان داده شده است.



شکل ۷-۹: اضافه کردن Pagefile.sys از منبع مدارک

c. گزینه پایان را انتخاب کرده و پردازش آغاز خواهد شد. یک فاز پردازش تمام میشود سپس به تب نتایج رفته و آن را چک کنید.

شکل ۷-۱۰ : انتخاب فرمت داده



شکل ۷-۱۱ : نتایج پردازش

همانطور که در شکل قبل مشاهده می‌شود ۲۲۸۹ url از pagefile.sys استخراج شده‌است. می‌توان همین کار را با دو فایل دیگر (swapfile.sys و hiberfile.sys) نیز انجام داد.

ابزار Belkasoft Evidence Center از طریق Pagefile.sys و استخراج رکوردها از داده های موجود مرورگر وب آن را انجام میدهد. اگر متخصص جرم شناسی دیجیتال فرمت های داده ای بیشتری را نیز انتخاب کند میتواند داده های بیشتری شامل عکس ها، پیام ها، ایمیل ها و مواردی دیگر اینچینی نیز استخراج کند.

فصل ۸ : ایمیل و پیام‌رسان ویندوز

در این فصل به تجزیه و تحلیل اطلاعات ایمیل و پیام‌رسان ویندوز با استفاده از ابزارهای زیر خواهیم پرداخت.

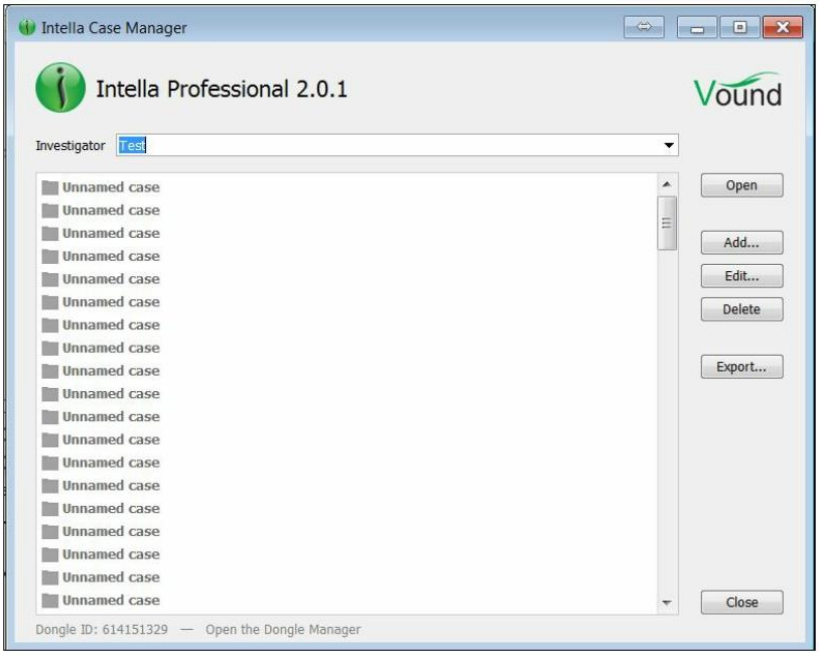
- **Outlook mailbox parsing with Intella**
- **تجزیه صندوق پستی Thunderbird با Autopsy**
- **جرم‌شناسی اسکایپ با ابزار Belkasoft Evidence Center**
- **تجزیه و تحلیل ایمیل با Magnet AXIOM**
- **جرم شناسی اسکایپ با SkypeLogView**

در ادامه هریک از این ابزارها به صورت مفصل تشریح خواهند شد.

۸-۱- Outlook mailbox parsing with Intella

ابزار Intella یک ابزار بسیار قدرتمند در زمینه جرم‌شناسی و کاوش با قابلیت های پردازش، جستجو و تحلیل اطلاعات ذخیره شده الکترونیکی (ESI) است. یکی از ویژگی‌های آن تحلیل بصری است. این ویژگی می‌تواند به متخصصین برای درک بهتر ESI و روابط custodian کمک کند. در این دستورالعمل ما به شما چگونگی تجزیه و تحلیل Outlook mailbox با این ابزار را آموزش خواهیم داد. ترتیب مراحل اجرا به صورت زیر می‌باشد.

a. ابتدا باید یک نمونه جدید ایجاد کرد. برای این کار ابزار Intella را اجرا و نام خود را وارد کرده (برای این نمونه ما Test را انتخاب کرده‌ایم) و سپس بر روی دکمه Add کلیک شود.

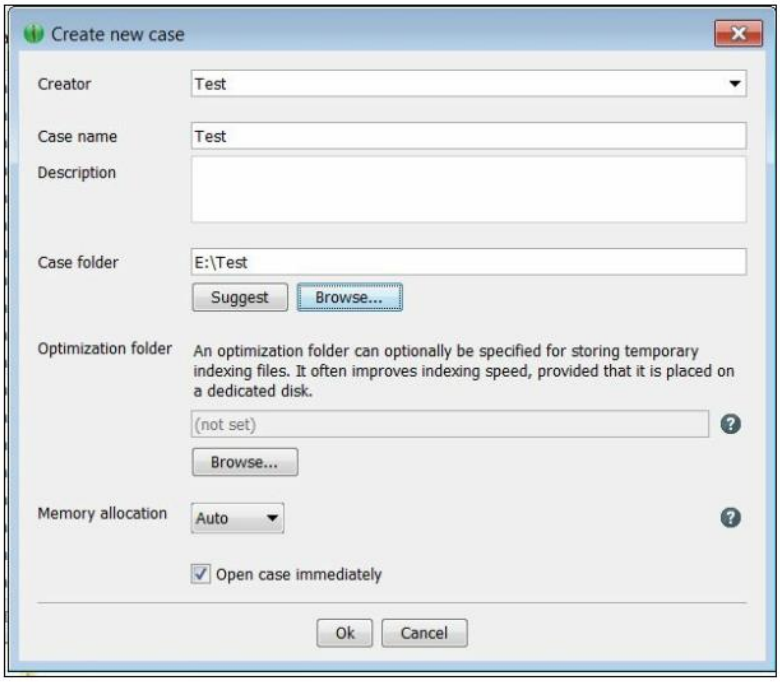


شکل ۸-۱ : اضافه کردن یک نمونه جدید

b. با استفاده از پنجره add یک متخصص میتواند یک نمونه جدید ایجاد کند، یک نمونه را به اشتراک بگذارد، یا نمونه ای که قبلا ایجاد شده را اضافه کند.

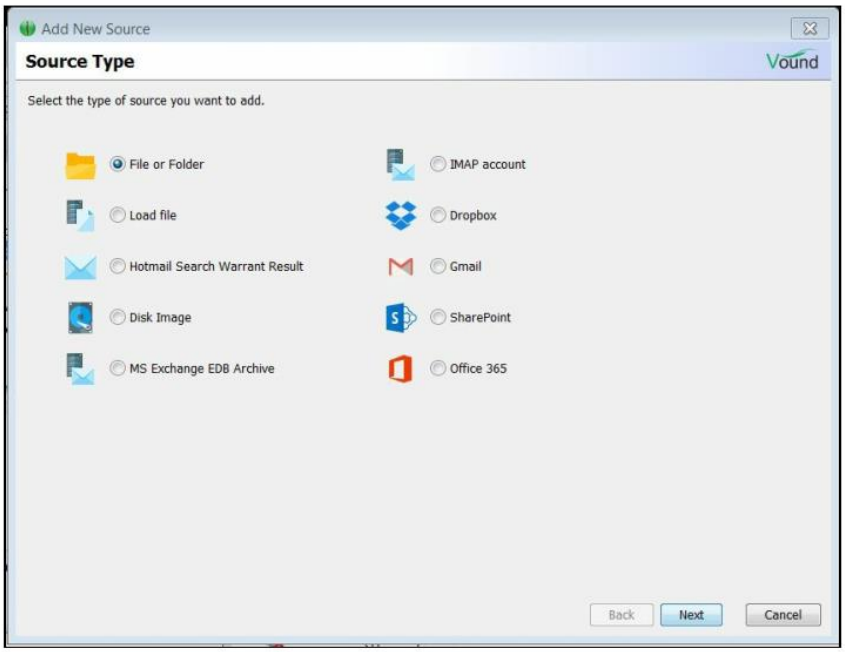
شکل ۸-۲ : پنجره اضافه کردن یک مورد

c. ابتدا باید یک نمونه جدید با استفاده از گزینه Create a new case ایجاد کرد. اکنون چند فیلد وجود دارد که باید آن را پر کنید. همچنین میتوانید یک پوشه را برای ذخیره سازی فایل‌های اندیس موقت انتخاب کرد که این می‌تواند باعث افزایش سرعت اندیس‌گذاری شود.



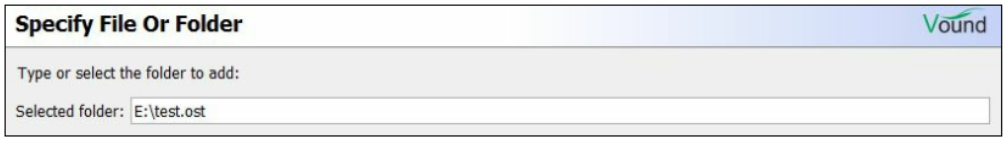
شکل ۸-۳ : ایجاد یک نمونه جدید

d. اکنون باید منبع مدارک را انتخاب کرد. در اینجا از فایل های OST استفاده نموده ایم، سپس فایل یا پوشه موردنظر را مطابق شکل زیر انتخاب می‌کنیم.



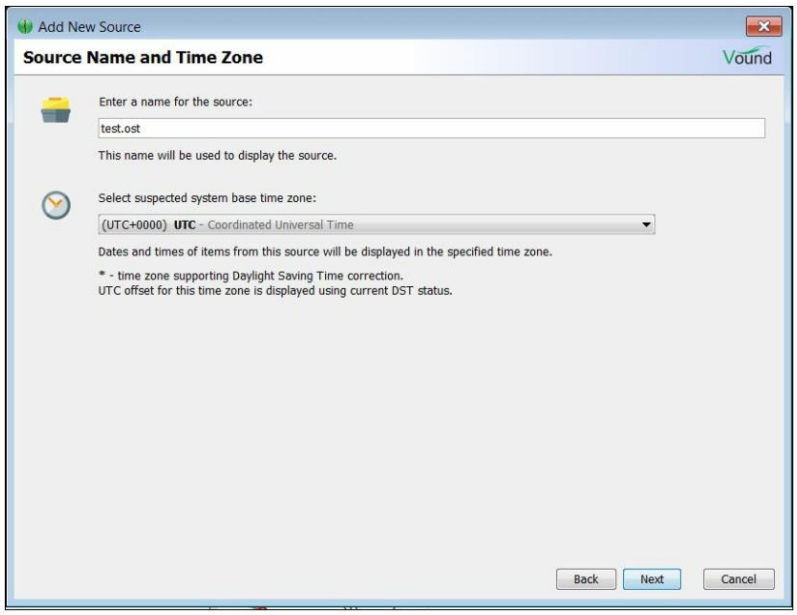
شکل ۸-۴ : اضافه کردن یک منبع جدید

e. در نمونه ما، فایل با نام test.ost و در ریشه E:\drive قرار داده شده است که می‌توان آن را در شکل ۸-۵ دید.



شکل ۸-۵ : اضافه کردن یک فایل برای پردازش

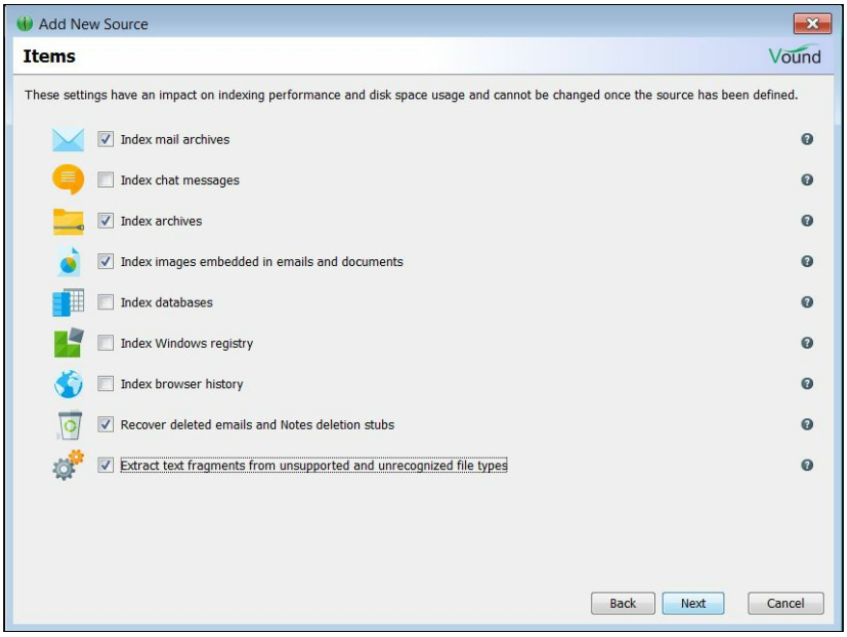
f. در این مرحله، باید منطقه زمانی صحیح را انتخاب کرد یا اگر می خواهید منطقه زمانی نامعین باشد گزینه UTC را انتخاب کنید.



شکل ۸-۶ : انتخاب نام منبع و منطقه زمانی

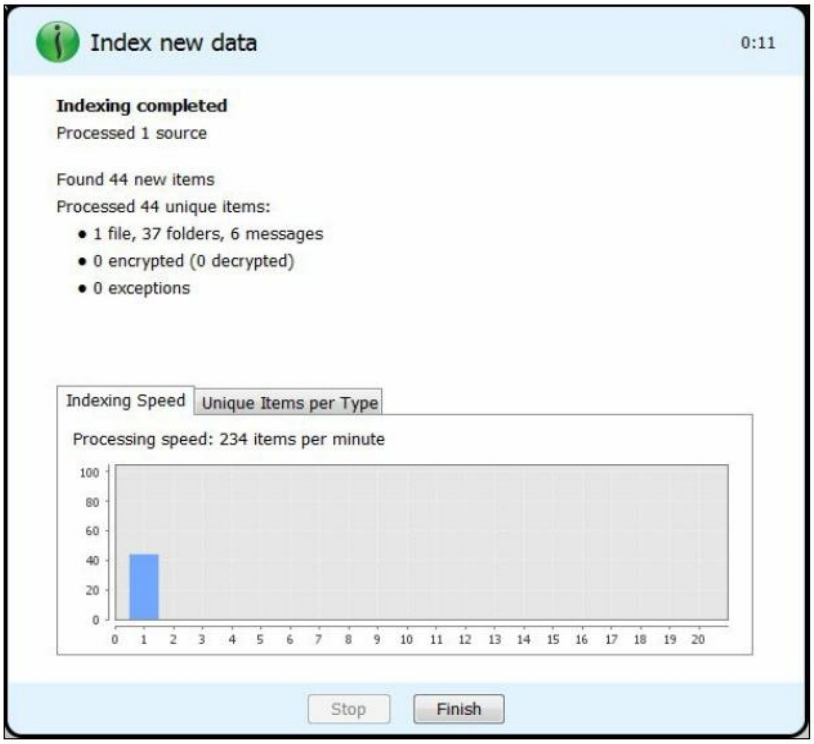
g. حال باید آیتم هایی که می‌خواهید پردازش شوند را انتخاب کنید. آیتم‌هایی که در اینجا انتخاب شده است بصورت زیر می باشد.

- آرشیو ایمیل : ما آن را در Outlook mailbox پردازش میکنیم که این بسیاردارای اهمیت است.
- آرشیو : که میتواند به ایمیل ها پیوست شوند.
- عکس های درون ایمیل ها و داکیومنت ها
- ایمیل های حذف شده
- بخش های متنی از فرمت های پشتیبانی نشده و ناشناس



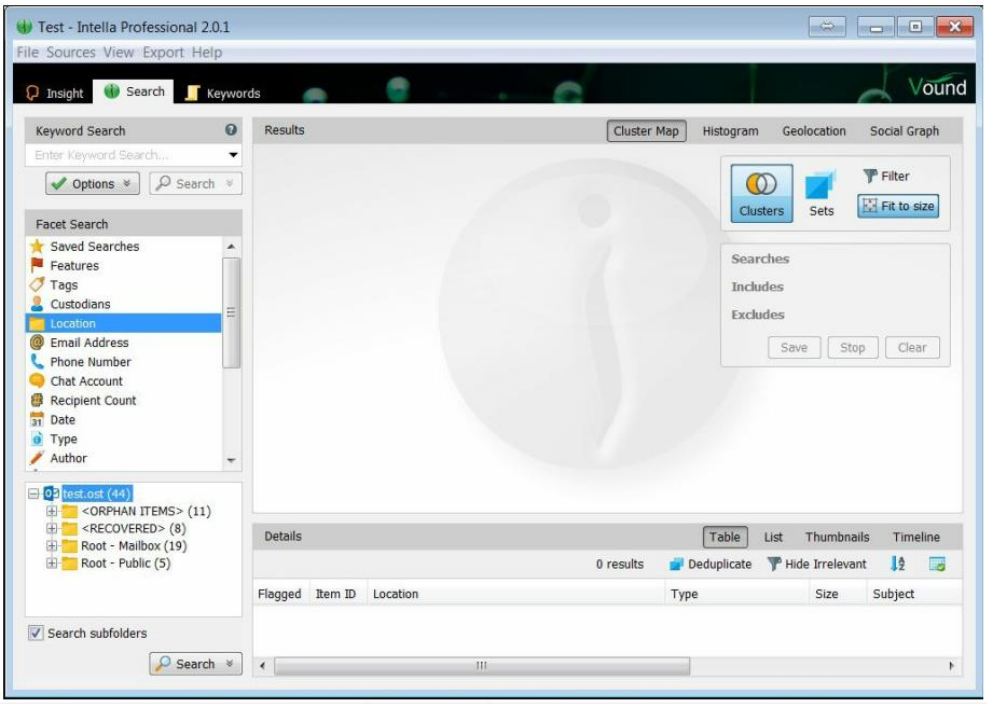
شکل ۸-۹ : انتخاب آیتم ها برای پردازش

h. می‌توان پنجره های بعدی را نادیده گرفت و پردازش مدارک را شروع کرد. وقتی اندیس‌گذاری کامل شود، می‌توان خلاصه کلی را مشاهده کرد.



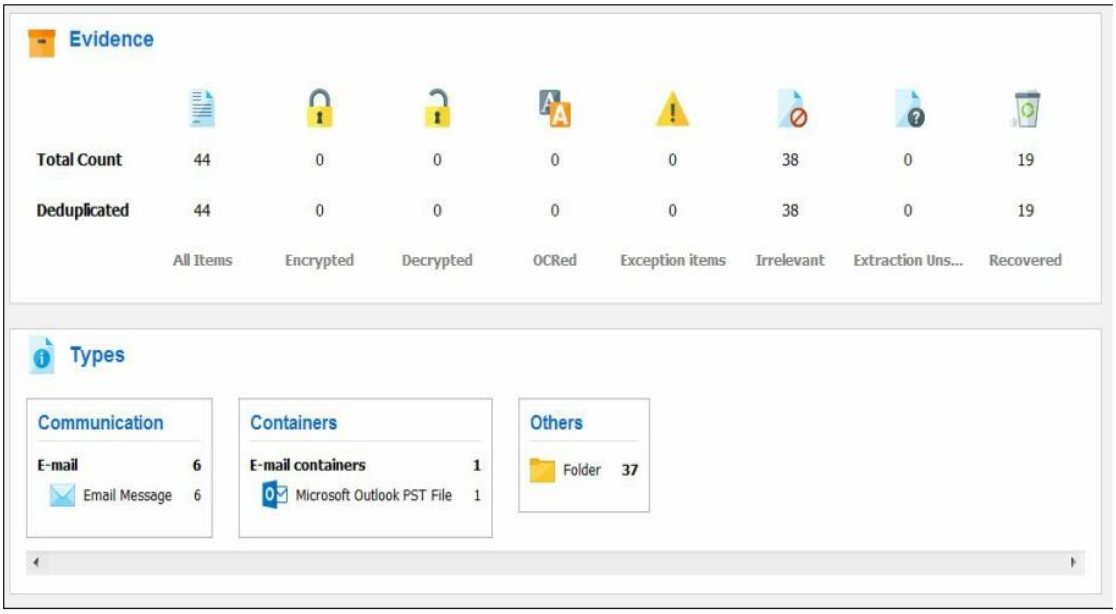
شکل ۸-۱۰ : اندیس گذاری منبع مدارک

i. با انتخاب finish به صفحه اصلی برمی‌گردید که داری سه تب است.



شکل ۸-۱۱ : تب سرچ ابزار intella

j. همانطور که میبینید در اینجا ۴۴ آیتم داریم، که ۱۹ مورد آن فایل های بازیابی شده هستند. اکنون میتوان اندیس داده ها را با استفاده از کلمات کلیدی متفاوت و ابعاد مختلف جستجو کرد مانند آدرس ایمیل، شماره تلفن، مولف، تاریخ فرمت و امثال آن. همچنین ما می‌توانیم در این تب نقشه خوشه ای، هیستوگرام و گراف های اجتماعی ایجاد کرد به صورتیکه بسیار مفید باشند.

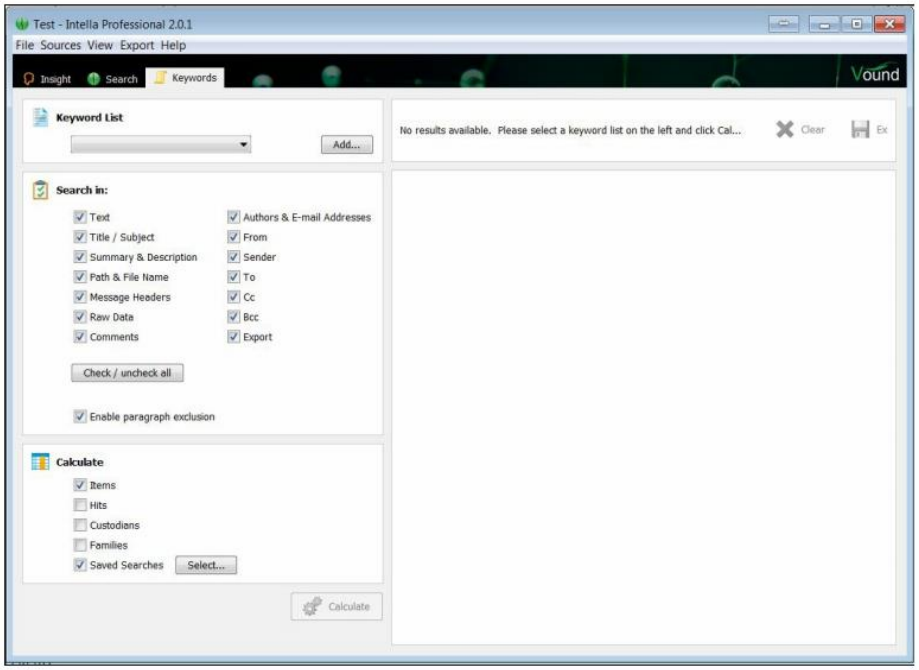


شکل ۸-۱۲: تب insight در ابزار intella

k. اکنون به تب Insight رفته و به صورت شکل زیر عمل کنید.

در اینجا خلاصه کلی در مورد مدارک ارائه شده است. به عنوان مثال، ابزار Intella به ما نشان می‌دهد که چگونه با Microsoft Outlook ارتباط برقرار کنیم، اکنون ۱۹ سند بازیابی شده داریم، ۶ پیام ایمیل داریم و در کل ۴۴ آیتم موجود است.

I. حال آخرین تب که keywords است را چک می‌نماییم.



شکل ۸-۱۳ : تب Keywords در ابزار Intella

ابتدا برای صرفه‌جویی در زمان از این تب برای اضافه کردن کلمات کلیدی سفارشی استفاده کنید. همچنین می‌توان چگونگی جستجوی خود را انتخاب کرد. به عنوان مثال، اگر شما بخواهید برای یک کلمه کلیدی خاص با موضوع خاصی جستجو کنید، میتوانید همه انتخاب ها را ابتدا از حالت انتخاب خارج کنید و فقط موضوع مورد نظر خود را انتخاب کنید.

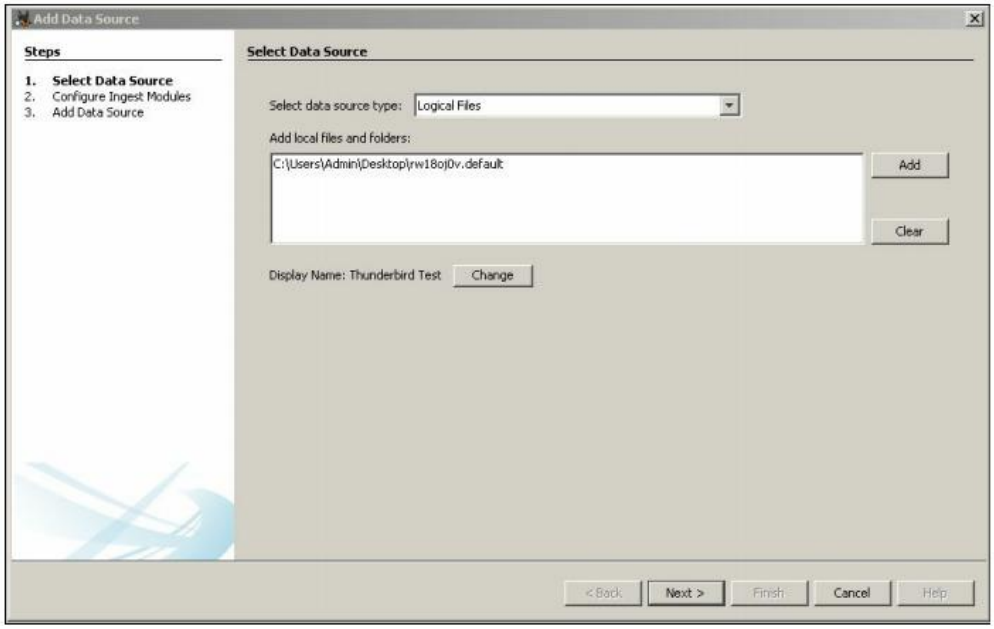
ابزار Intella منابع مدارک مورد نظر را ایندکس می‌کند و متخصصین جرم شناسی کامپیوتر را قادر می‌سازد که در بین داده‌های ایندکس شده جستجو انجام گیرد. همچنین این ابزار برای ایجاد cluster maps, histograms, social graphs و امثال آن کاربرد دارد.

۸-۲- تجزیه صندوق پستی Thunderbird با Autopsy

Thunderbird یک سرویس ایمیل پست الکترونیکی رایگان از موزیلا و توسعه دهندگان مرورگر فایرفاکس است. اگر کاربری از Outlook استفاده نمی کند، احتمالا از Thunderbird استفاده می کند. در این دستورالعمل، با نحوه استخراج داده ها از فایل های Thunderbird MBOX را با پلت فرم جرم شناسی دیجیتال رایگان و منبع باز Autopsy آشنا خواهید شد.

می توان روند اجرا را با پیروی از مراحل زیر آغاز کنیم.

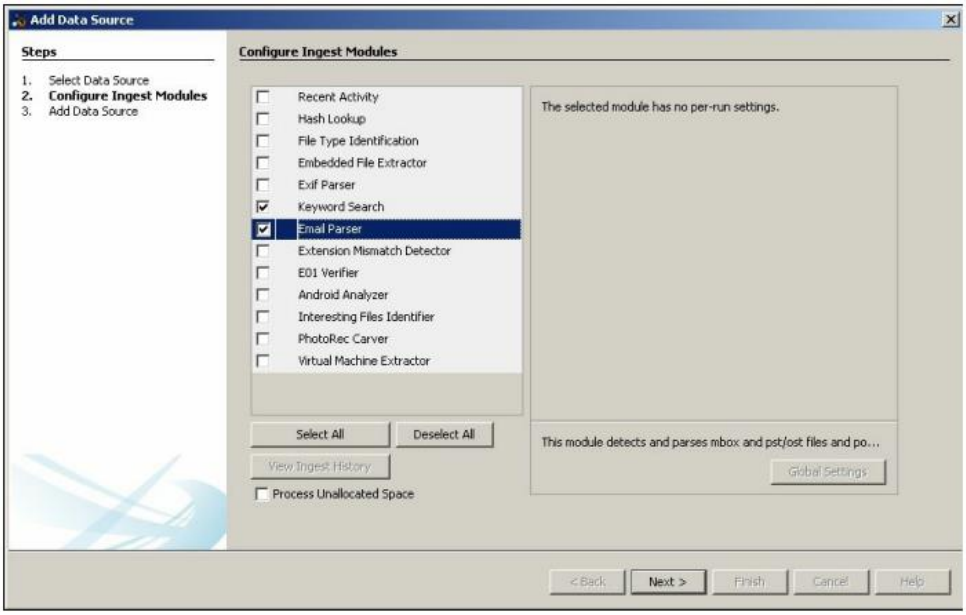
a. با ایجاد یک پرونده جدید و پر کردن جزئیات آن، شروع کنید. قصد داریم از یک پوشه پروفایل Thunderbird به عنوان منبع استفاده کنیم، بنابراین در پنجره Source Data Source، فایلهای Logical را انتخاب می کنیم.



شکل ۸-۱۴ : انتخاب منبع داده در Autopsy

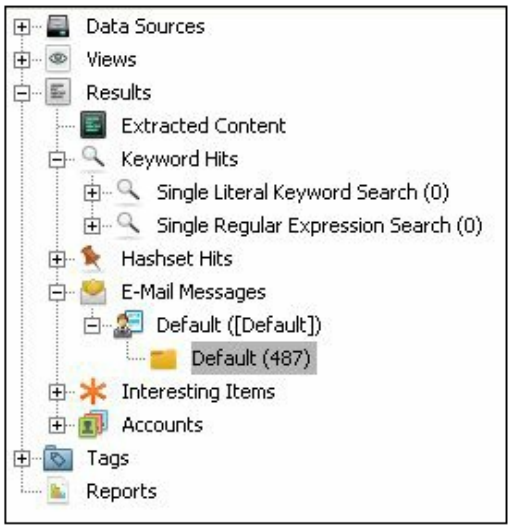
همچنین می توانید نام نمایشگر برای منبع شواهد خود انتخاب کنید. توجه کنید که آن را Thunderbird Test بنامید.

b. حالا Ingest Modules را انتخاب کنید. ما به شدت توصیه می کنیم همیشه Keyword Search module را انتخاب کنید. البته، مطمئن شوید که Parser Email علامت گذاری شده است.



شکل ۸-۱۵ : پیکربندی ingest modules در Autopsy

c. هنگامی که منبع داده شما پردازش می شود، می‌توانید نتایج را تجزیه و تحلیل کنید. برای این کار به قسمت پیام های ایمیل در سمت چپ رجوع کنید.



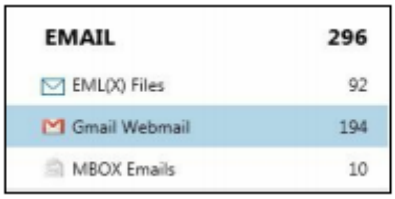
شکل ۸-۱۶ : پیام‌های ایمیل تجزیه شده

همانطور که می بینید، ۴۸۷ پیام ایمیل توسط Autopsy استخراج شده اند. در سمت راست می‌توانید همه چیزهایی را که برای تجزیه و تحلیل نیاز دارید مانند فرستنده، گیرنده، بدنه پیام، نشانگرهای زمانی و غیره پیدا کنید.

۸-۳- تجزیه و تحلیل ایمیل با Magnet AXIOM

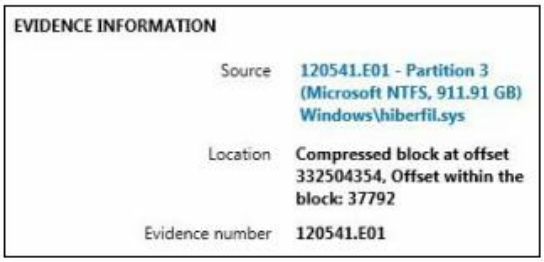
در این دستورالعمل، بانحوه بازیابی ایمیل وب با ابزار جرم شناسی دیجیتال Magnet AXIOM آشنا خواهید شد. فرایند شناسایی با اجرای مراحل زیر تکمیل می‌شود.

a. پردازش منبع داده با AXIOM Process ؛ باید شامل pagefile.sys و hiberfil.sys باشد و مطمئن شوید که آیتم های پست الکترونیکی بررسی می شوند. پس از پایان مرحله پردازش، به AXIOM Exam بروید و به بخش EMAIL نگاه کنید. در اینجا از آثار ایمیل استخراج شده، از جمله پست الکترونیکی، در مورد Gmail را خواهید یافت.



شکل ۸-۱۷ : آثار استخراج شده از ایمیل

b. همانطور که می بینید، ۱۹۴ آثار Gmail استخراج شده‌اند. ابتدا منبع اولین اثر را بررسی می‌کنیم. روی artifact کلیک کنید و بخش EVIDENCE INFORMATION را بررسی کنید.



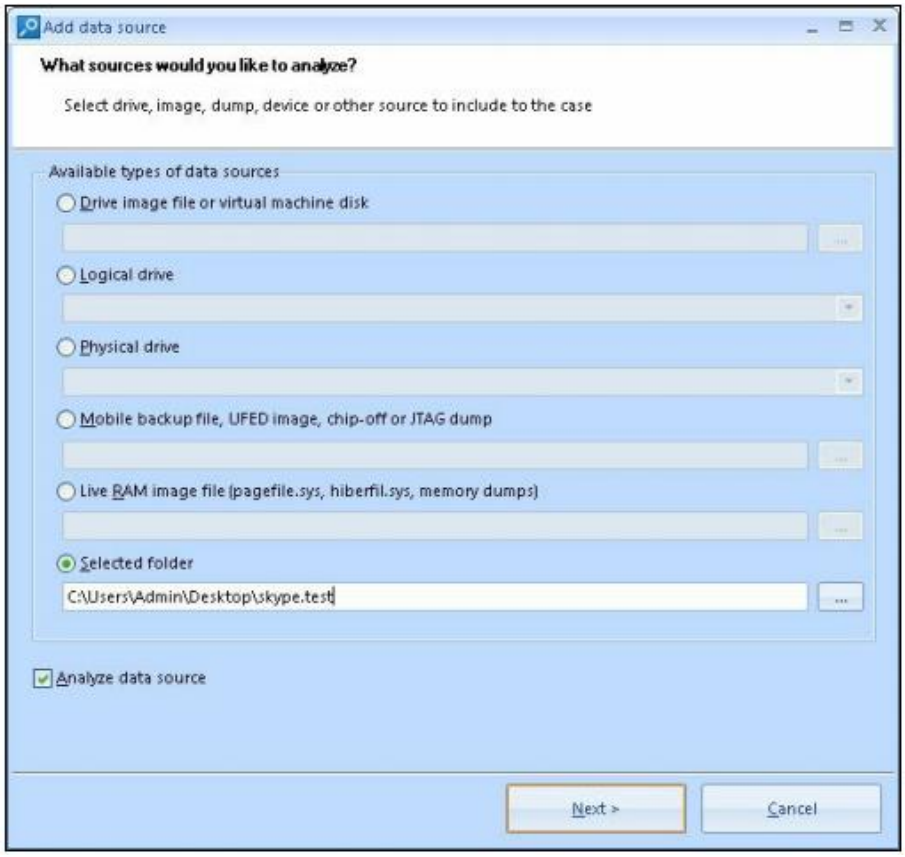
شکل ۸-۱۸ : اطلاعات Artifact

در شکل قبل خواهید دید که این آثار از hiberfil.sys استخراج شده است. همچنین آدرس‌هایی را مشاهده می کنید که برای مستندسازی بسیار مهم هستند.

۸-۴- جرم‌شناسی اسکایپ با ابزار Belkasoft Evidence Center

در سیستم‌های ویندوز مدرن اسکایپ به طور پیش فرض نصب شده است، بنابراین برای بررسی جرم شناسی ویندوز بسیار مهم است که اطلاعات کاربر را از این برنامه استخراج کنید. این تست می تواند تماس ها، پیام ها، انتقال و یا دریافت فایل ها، و غیره را ارائه دهد. در این دستورالعمل، به شما نشان خواهیم داد که چگونه این آثار با ارزش را با Belkasoft Evidence Center تجزیه کنید. مراحل انجام تست در زیر آورده شده است :

a. یک پرونده جدید ایجاد کنید و پوشه پروفایلی که پیش از آن به عنوان منبع داده اکسپورت شده است را اضافه کنید. از گزینه Selected folder استفاده کنید.



شکل ۸-۱۹ : اضافه کردن منبع داده ای در Belkasoft Evidence Center

b. نوع داده درست را انتخاب کنید. در اینجا یک پوشه پروفایل اسکایپ داریم، بنابراین به Chats بروید، Skype را پیدا کنید و آن را تیک بزنید. روی Finish کلیک کنید و برای تجزیه و تحلیل داده ها کمی منتظر بمانید.

شکل ۸-۲۰ : انتخاب نوع داده در Belkasoft Evidence Center

هنگامی که داده‌ها پردازش می شوند، می توانید با تب‌های Overview یا Case Explorer برای تحلیل داده های استخراج شده، از جمله تماس ها، پیام ها (از جمله صدا)، تصاویر و غیره، کار کنید. لازم است بدانید که Belkasoft Evidence Center پیام های حذف شده از پایگاه داده اسکایپ (main.db) را نیز استخراج می کند و فایل های chatsync را تحلیل می کند که ممکن است شامل پیام هایی باشند که در پایگاه داده اصلی موجود نیستند.

۸-۵- جرم شناسی اسکایپ با SkypeLogView

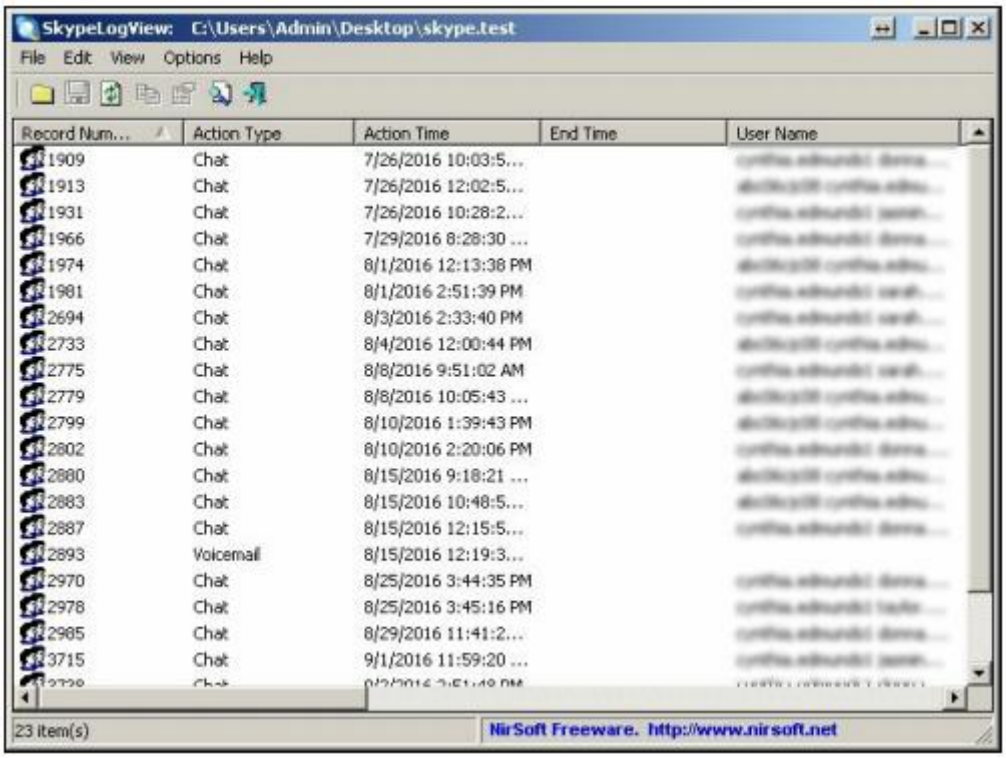
ابزارهای رایگان و متن باز گوناگونی برای جرم شناسی اسکایپ وجود دارد و یکی از آنها SkypeLogView است که توسط NirSoft نوشته شده است. شما قبلا با برخی از ابزارهای NirSoft آشنا شدید و در این دستورالعمل با نحوه استفاده از SkypeLogView برای اسکایپ آشنا خواهید شد.

برای انجام تست با ابزار SkypeLogView مراحل زیر باید انجام داده شود:

a. برنامه را اجرا کنید؛ یک پنجره منبع داده باز می‌شود.

شکل ۸-۲۱ : اضافه کردن منبع داده در SkypeLogView

b. روی OK کلیک کنید.



شکل ۸-۲۲ : اجرای SkypeLogView

c. می توانید داده های استخراج شده را با استفاده از ستون های مختلف مرتب کنید. اگر می خواهید نشانگر زمانی در GMT نمایش داده شود، به Options بروید و Show Time in GMT را فعال کنید.

d. در نهایت شما می توانید یک گزارش HTML ایجاد کنید. برای انجام این کار به View بروید و HTML Report را فعال کنید.

SkypeLogView با استفاده از پوشه‌ای که آزمونگر انتخاب می‌کند به استخراج آرشیوهای اسکایپ ، مانند چت، پست صوتی، تماس و غیره می‌پردازد. همچنین یک آزمونگر می تواند یک گزارش HTML برای آثار انتخاب شده کاربر ایجاد کند.

فصل ۹ : بررسی ویژگی‌های کاربردی ابزارهای جرم‌شناسی ویندوز

لازم بر آن است تا ابزارهای جرم‌شناسی معرفی شده در فصول قبل مورد تحلیل و بررسی قرار گیرد. در این فصل سعی بر ان شده تا این ابزارها بر اساس دارا بودن ویژگی‌های کاربردی و گرافیکی مورد بررسی قرار گیرد. در هر بخش چندین ابزار معرفی شد که در اینجا به مقایسه آنها خواهیم پرداخت. مقایسه ابزارهای هر بخش به صورت جداگانه و در قالب جدولی انجام گرفته‌است.

در جدول ۹-۱ ابزارهای جرم‌شناسی حافظه ویندوز مورد بررسی قرار گرفته‌است.

جدول ۹-۱ مقایسه ابزارهای جرم‌شناسی حافظه ویندوز

نام ابزار	گزارش‌دهی (Reporting)	گرافیکی (GUI)	خط فرمانی (CLI)	فیلترگذاری (Filtering)	ماژولار (Modular)	رایگان (Free)	کاربرپسند (User Friendly)	پذیرش آرگومان (Adding Argument)
Belkasoft Ram Capture	×	✓	×	×	×	✓	✓	×
DumpIt	×	×	✓	✓	✓	✓	×	✓
Belkasoft Evidence Center	✓	✓	×	✓	×	×	✓	×
Volatility	×	×	✓	✓	✓	✓	×	✓

در جدول ۹-۲ ابزارهای جرم‌شناسی درایوهای ویندوز را مورد بررسی و مقایسه قرار داده‌ایم.

جدول ۹-۲ مقایسه ابزارهای جرم‌شناسی درایوهای ویندوز

نام ابزار	گزارش‌دهی (Reporting)	گرافیکی (GUI)	خط فرمانی (CLI)	فیلترگذاری (Filtering)	ماژولار (Modular)	رایگان (Free)	کاربرپسند (User Friendly)	پذیرش آرگومان (Adding Arguman)
FTK Image Mounter	×	✓	×	×	×	✓	✓	×
Dc3dd	×	✓	✓	✓	✓	✓	✓	✓
Arsenal Image Mounter	✓	✓	×	×	×	✓	✓	×

در جدول ۹-۳ ابزارهای جرم‌شناسی تجزیه و تحلیل نسخه‌های shadow ویندوز را مورد بررسی قرار داده‌ایم.

جدول ۹-۳ مقایسه ابزارهای جرم‌شناسی نسخه‌های shadow ویندوز

نام ابزار	گزارش‌دهی (Reporting)	گرافیکی (GUI)	خط فرمانی (CLI)	فیلترگذاری (Filtering)	ماژولار (Modular)	رایگان (Free)	کاربرپسند (User Friendly)	پذیرش آرگومان (Adding Arguman)
ShadowCopyView	×	✓	×	×	×	✓	✓	×
MKLINK	×	×	✓	✓	×	✓	×	✓
Magnet AXIOM	✓	✓	×	✓	✓	×	✓	×

در جدول ۹-۴ ابزارهای جرم‌شناسی آنالیز رجیستری مورد بررسی قرار گرفته‌است.

جدول ۹-۴ مقایسه ابزارهای جرم‌شناسی آنالیز رجیستری

نام ابزار	گزارش‌دهی (Reporting)	گرافیکی (GUI)	خط فرمانی (CLI)	فیلترگذاری (Filtering)	ماژولار (Modular)	رایگان (Free)	کاربرپسند (User Friendly)	پذیرش آرگومان (Adding Arguman)
AXION	✓	✓	×	✓	✓	×	✓	×
RegRipper	×	✓	×	×	×	✓	✓	×
Registry Explorer	×	✓	×	✓	×	✓	✓	×
FTK Registry Viewer	✓	✓	×	✓	×	✓	✓	×

در جداول ۹-۵ ، ۹-۶، ۹-۷، ۹-۸، ابزارهای جرم‌شناسی Artifacteهای سیستم عامل مورد بررسی قرار گرفته‌است. جدول ۹-۵ مقایسه ابزارهای آنالیز سطل بازیافت ویندوز را نشان می‌دهد. جدول ۹-۶ مقایسه ابزارهای آنالیز رویدادهای ویندوز ویندوز را نشان می‌دهد. در جدول ۹-۷ ابزارهای آنالیز فایل‌های LNK ویندوز مورد بررسی قرار گرفته‌است. جدول ۹-۸ مقایسه ابزارهای جرم‌شناسی تجزیه و تحلیل فایل‌های Prefetch ویندوز را نشان می‌دهد.

جدول ۹-۵ مقایسه ابزارهای جرم‌شناسی آنالیز سطل بازیافت ویندوز

نام ابزار	گزارش‌دهی (Reporting)	گرافیکی (GUI)	خط فرمانی (CLI)	فیلترگذاری (Filtering)	ماژولار (Modular)	رایگان (Free)	کاربرپسند (User Friendly)	پذیرش آرگومان (Adding Arguman)
Encase Forensic	×	✓	×	✓	×	✓	✓	×
Rifiuti2	×	×	✓	✓	×	✓	×	✓
Magnet Axiom	✓	✓	×	✓	✓	×	✓	×

جدول ۹-۶ مقایسه ابزارهای جرم‌شناسی آنالیز رویدادهای ویندوز

نام ابزار	گزارش‌دهی (Reporting)	گرافیکی (GUI)	خط فرمانی (CLI)	فیلترگذاری (Filtering)	ماژولار (Modular)	رایگان (Free)	کاربرپسند (User Friendly)	پذیرش آرگومان (Adding Arguman)
FullEventLogView	×	✓	×	✓	×	✓	✓	×
Magnet Axiom	✓	✓	×	✓	✓	×	✓	×
EVTXtract recovery event	×	×	✓	✓	✓	✓	×	✓

جدول ۹-۷ مقایسه ابزارهای جرم‌شناسی آنالیز فایل‌های LNK ویندوز

نام ابزار	گزارش‌دهی (Reporting)	گرافیکی (GUI)	خط فرمانی (CLI)	فیلترگذاری (Filtering)	ماژولار (Modular)	رایگان (Free)	کاربرپسند (User Friendly)	پذیرش آرگومان (Adding Arguman)
Encase forensic	×	✓	×	✓	×	✓	✓	×
LECmd	×	×	✓	✓	✓	✓	×	✓
Link Parser	×	✓	×	✓	×	✓	✓	×

جدول ۹-۸ مقایسه ابزارهای جرم‌شناسی آنالیز فایل‌های Prefetch ویندوز

نام ابزار	گزارش‌دهی (Reporting)	گرافیکی (GUI)	خط فرمانی (CLI)	فیلترگذاری (Filtering)	ماژولار (Modular)	رایگان (Free)	کاربرپسند (User Friendly)	پذیرش آرگومان (Adding Arguman)
Magnet Axiom	✓	✓	×	✓	✓	×	✓	×
LECmd	×	×	✓	✓	✓	✓	×	✓
Prefetch Carver	×	✓	×	×	×	✓	✓	×

در جدول ۹-۹ ابزارهای جرم‌شناسی آنالیز مرورگر وب مورد بررسی قرار گرفته‌است.

جدول ۹-۹ مقایسه ابزارهای جرم‌شناسی آنالیز مرورگر وب

نام ابزار	گزارش‌دهی (Reporting)	گرافیکی (GUI)	خط فرمانی (CLI)	فیلترگذاری (Filtering)	ماژولار (Modular)	رایگان (Free)	کاربرپسند (User Friendly)	پذیرش آرگومان (Adding Arguman)
فایرفاکس: BlackBag's Blacklight	✓	✓	×	✓	✓	×	✓	×
گوگل کروم: Magnet Axiom	×	✓	×	✓	✓	×	✓	×
Belkasoft Evidence Center	×	✓	×	✓	✓	×	✓	×

در جدول ۹-۱۰ ابزارهای جرم‌شناسی آنالیز ایمیل و پیام‌رسان ویندوز مورد بررسی قرار گرفته‌است.

جدول ۹-۱۰مقایسه ابزارهای جرم‌شناسی آنالیز آنالیز ایمیل و پیام‌رسان ویندوز

نام ابزار	گزارش‌دهی (Reporting)	گرافیکی (GUI)	خط فرمانی (CLI)	فیلترگذاری (Filtering)	ماژولار (Modular)	رایگان (Free)	کاربرپسند (User Friendly)	پذیرش آرگومان (Adding Arguman)
Intella	×	✓	×	✓	✓	✓	✓	×
Autopsy	×	✓	×	✓	✓	✓	✓	×
Magnet Axiom	×	✓	×	✓	×	×	✓	×
Belkasoft Evidence Center	✓	✓	×	✓	×	×	✓	×
SkypeLogView	×	✓	×	✓	×	✓	✓	×

مراجع

[1] Skulkin, O., & de Courcier, S. (2017). Windows Forensics Cookbook.

[2]https://cert.eccouncil.org/computer-hacking-forensic-investigator.html

[3]https://digital-forensics.sans.org/community/downloads

[4]http://sectools.org/tag/forensics/

[5]https://tools.kali.org/forensics/

[6]https://tools.pentestbox.org/

[7]https://www.cftt.nist.gov/