9th SASTech Symposium on Advances in & Science Technology (2014)
نهمین سمپوزیوم پیشرفت های علوم و تکنولوژی
مشهد- ۱۳ آذر- ۱۳۹۳
کمیسیون دوم: همایش ملی علوم و مهندسی کامپیوتر
بامحوریت
امنیت ملی و توسعه پایدار
برگزارکننده: موسسه آموزش عالی خاوران
www.khi.ac.ir

ردیابی دسترسی به فایل‌ها، با استفاده از داده‌های حفاظت شده سیستم عامل

آلا اکرامی فرد، الهه عباس زاده دربان ، مرضیه جوادیان نیک

۱- دانشجوی کارشناسی ارشد واحد بین الملل دانشگاه فردوسی مشهد

۲- دانشجوی کارشناسی ارشد واحد بین الملل دانشگاه فردوسی مشهد

۳- دانشجوی کارشناسی ارشد واحد بین الملل دانشگاه فردوسی مشهد

ekramifard@staff.um.ac.ir

خلاصه

در دنیای امروز که داده‌های تجاری با فرمت الکترونیکی ذخیره می‌شوند، بررسی یک تقلب بدون بررسی داده‌های الکترونیکی قابل تعقیب نیست. در اکثر موارد حقوقی، لازم است شواهد الکترونیکی توسط متخصص پزشکی قانونی کامپیوتر جمع‌آوری شوند. یکی از راه‌های شناسایی فایل‌هایی که اخیرا توسط کاربر باز شده‌اند، استفاده از Jump lists است. یکی از قابلیت‌های مهم Jump list که برای یک متخصص پزشکی قانونی کامپیوتر هم از اهمیت بسزایی برخوردار است، ثبت یک سری اطلاعات خاص در فایل‌های پنهان و حفاظت شده سیستمی است. با استناد به اطلاعات بدست آمده از این فایل‌های پنهان، می‌توان وجود یک کلاهبرداری را آشکار و ایجاد سندهای ساختگی و جعلی یا انجام دیگر فعالیت‌های غیر قانونی کامپیوتری را ردیابی کرد.

این مقاله با تشریح داده‌های پنهان و حفاظت شده سیستم‌عامل به بررسی اطلاعات مفید استخراج شده از آنها می‌پردازد. همچنین با بررسی سه نمونه از ابزارهای کاربری که در این زمینه وجود دارد، نحوه کار و میزان کارایی هر یک را بررسی می‌کند.

کلمات کلیدی : Jump list، Link File، داده های پنهان سیستم عامل

۱. مقدمه

ما در عصری زندگی می‌کنیم که سهولت استفاده از آخرین فن‌آوری‌های دیجیتال در جهان در حال افزایش است. کاربران اعم از کسانی که در خانه و یا اداره کار می‌کنند به کامپیوتر، اینترنت و دستگاه‌های دیجیتال برای انجام کارهای خود تکیه می‌کنند. امروزه با استفاده از رایانه و اینترنت اجرای بسیاری از کارها آسان شده است اما این سرعت و توانایی در انجام کارها راه را برای ارتکاب جرم هم باز گذاشته است.

حقوق کیفری نوین، امروزه با جرایم و مجرمان کامپیوتری رو به رو است؛ در حالی که ماهیت و ویژگی این دسته از جرایم به نحوی اساسی با جرایم سنتی تفاوت دارد.