به نام خدا

مقاله پزشکی قانونی دیجیتال (Digital Forensics)

آشنایی با پزشکی قانونی دیجیتال سناریو محور و مقدمه ای بر فرآیندها در Digital Forensic

ترجمه و گردآورنده: عباس باورصاد

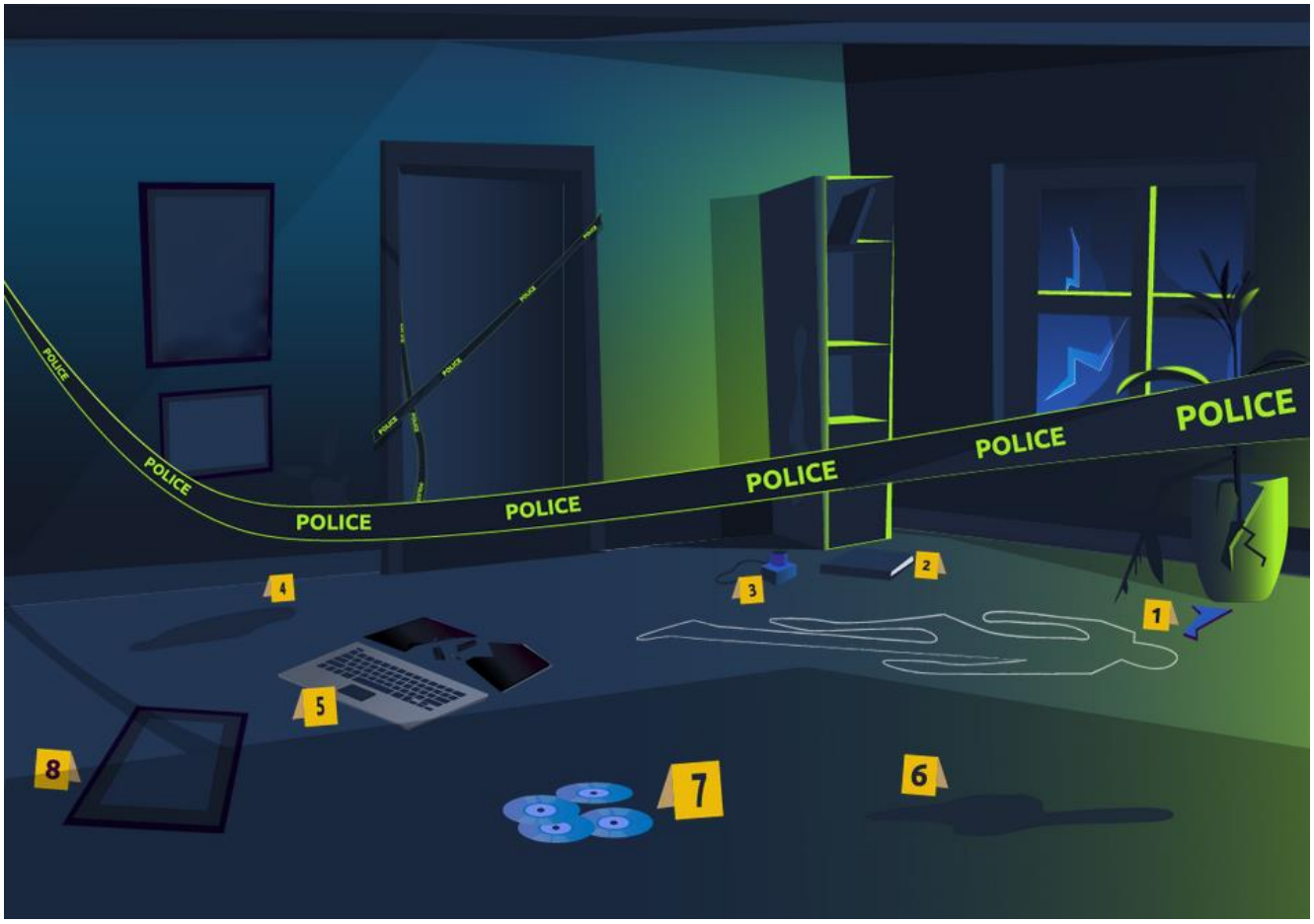
رشته تحصیلی: کارشناسی فناوری اطلاعات

استاد راهنما: عیسی جعفری

دانشگاه: جهاد دانشگاهی اهواز(علمی کاربردی)

فهرست

- **مقدمه ای بر پزشکی قانونی دیجیتال (Digital Forensics) :**

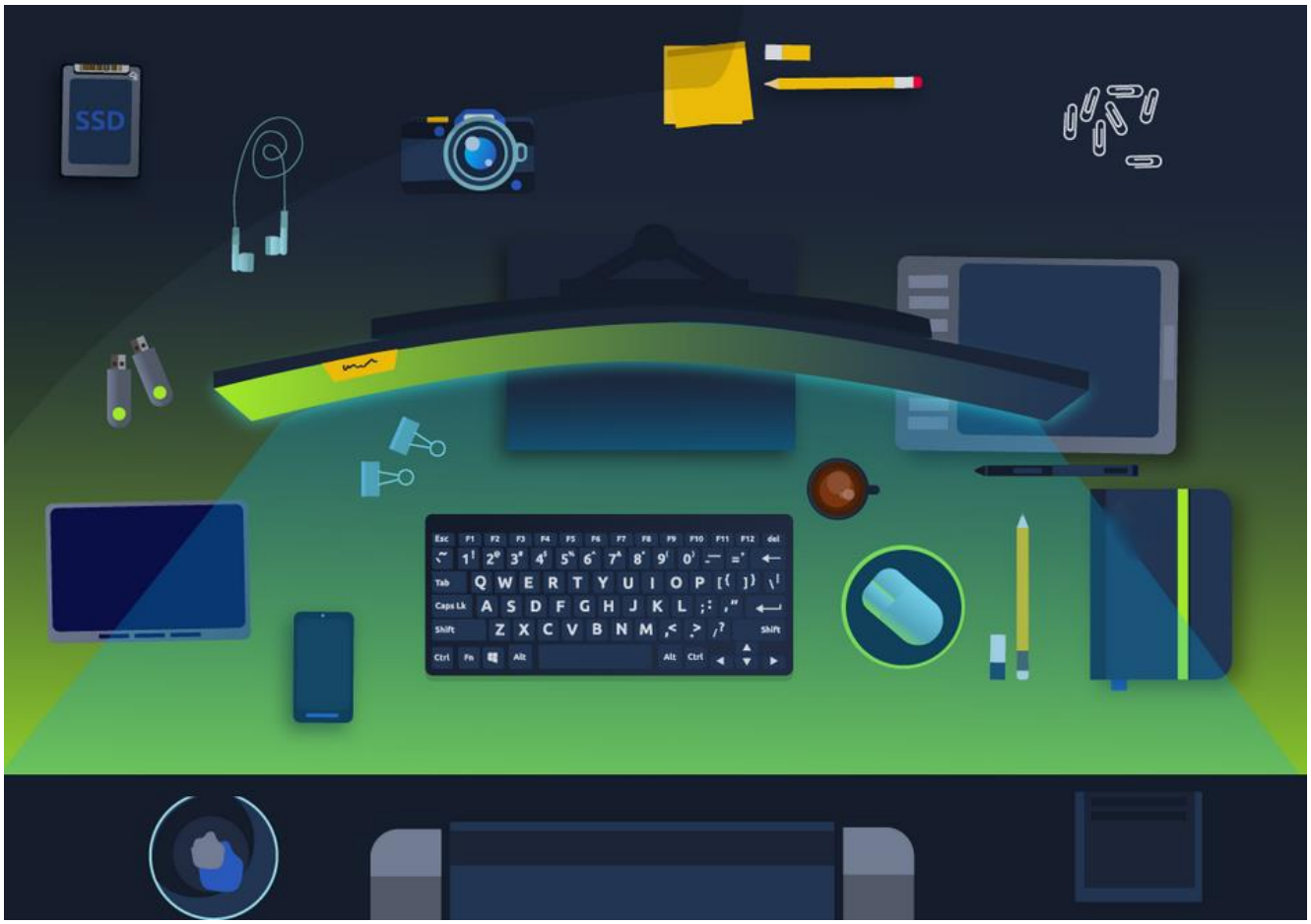


پزشکی قانونی کاربرد علم برای بررسی جرایم و اثبات حقایق است. با استفاده و گسترش سیستم‌های دیجیتال مانند رایانه‌ها و تلفن‌های هوشمند، شاخه جدیدی از پزشکی قانونی برای بررسی جرایم مرتبط متولد شد: پزشکی قانونی کامپیوتری **(Digital Forensics)** که بعداً به **پزشکی قانونی دیجیتال** تبدیل شد.

به سناریوی زیر فکر کنید. ماموران مجری قانون به صحنه جرم می رسند. با این حال، بخشی از این صحنه جرم شامل وسایل دیجیتال و رسانه ها می شود. دستگاه‌های دیجیتال شامل رایانه‌های رومیزی، لپ‌تاپ، دوربین‌های دیجیتال، پخش‌کننده‌های موسیقی و گوشی‌های هوشمند می‌شوند. رسانه های دیجیتال شامل سی دی، دی وی دی، درایو فلش مموری USB و حافظه خارجی است. چند سوال پیش می آید:

- **پلیس چگونه باید مدارک دیجیتالی مانند گوشی های هوشمند و لپ تاپ ها را جمع آوری کند؟ اگر رایانه و تلفن هوشمند در حال اجرا هستند، چه مراحلی باید رعایت شود؟**

- **چگونه مدارک دیجیتال را انتقال دهیم؟ آیا برای مثال، هنگام جابجایی رایانه‌ها، بهترین روش‌های خاصی وجود دارد که باید از آنها پیروی کرد؟**
- **چگونه شواهد دیجیتالی جمع آوری شده را تجزیه و تحلیل کنیم؟ فضای ذخیره سازی دستگاه های شخصی بین ده ها گیگابایت تا چند ترابایت است. چگونه می توان این را تحلیل کرد؟**



با فرض اینکه این کارمند در شکل بالا مشکوک است، می‌توانیم به سرعت دستگاه‌های دیجیتالی را ببینیم که ممکن است برای تحقیق جالب باشند. علاوه بر رایانه رومیزی، متوجه تبلت، تلفن هوشمند، دوربین دیجیتال و فلش مموری USB می شویم. هر یک از این دستگاه ها ممکن است حاوی مجموعه ای از اطلاعات باشد که می تواند به بررسی کمک کند .پردازش اینها به عنوان شواهد به پزشکی قانونی دیجیتال نیاز دارد.

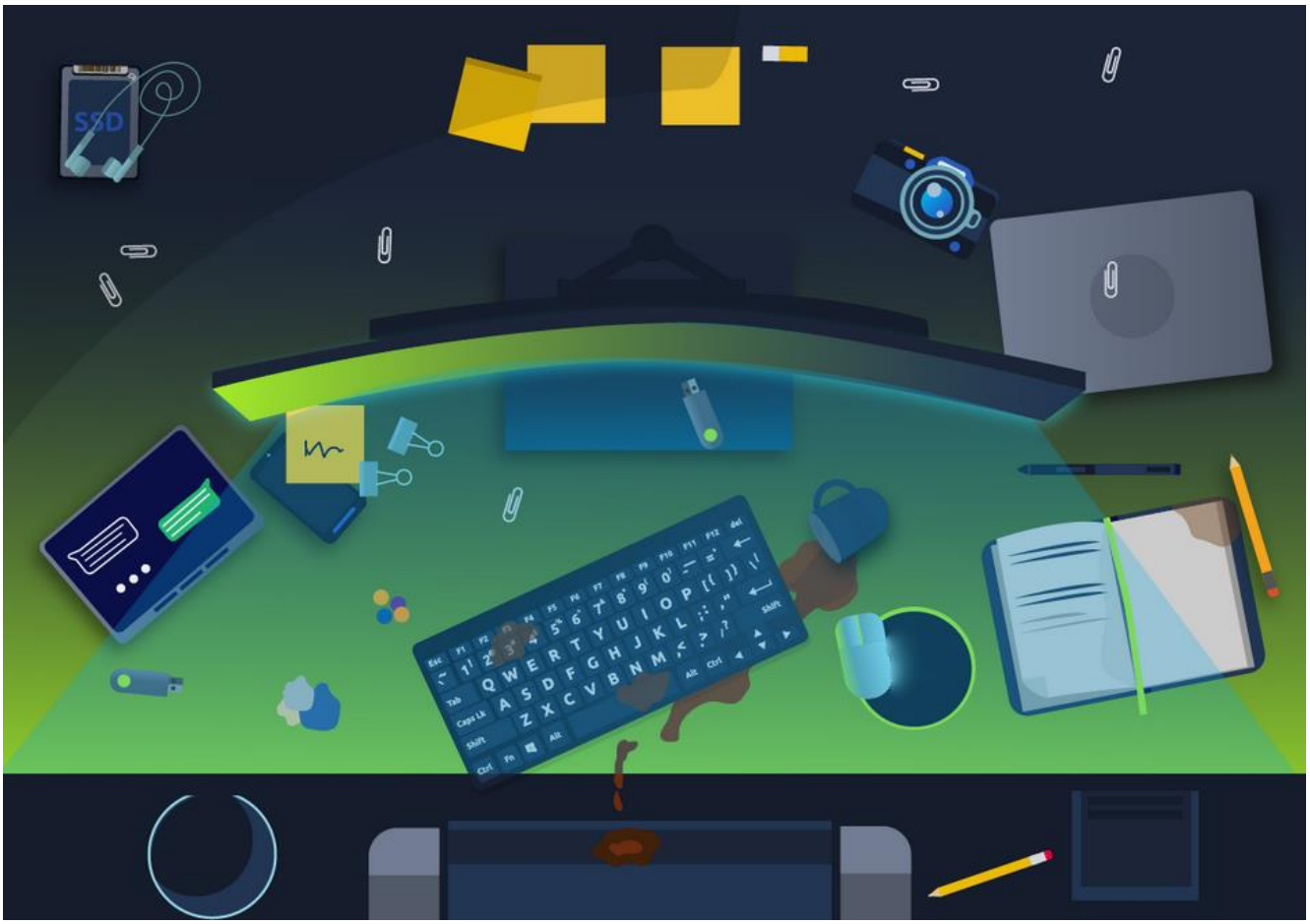
به طور رسمی تر، پزشکی قانونی دیجیتال کاربرد علم کامپیوتر برای بررسی شواهد دیجیتال برای اهداف قانونی است. پزشکی قانونی دیجیتال در دو نوع تحقیقات استفاده می شود:

۱- **تحقیقات بخش عمومی**(**Public-sector investigations**) به بررسی های انجام شده توسط دولت و سازمان های مجری قانون مراجعه کنید. آنها بخشی از یک جنایت یا تحقیقات مدنی خواهند بود.

۲- **تحقیقات بخش خصوصی**(**Private-sector investigations**) به تحقیقاتی اطلاق می شود که توسط نهادهای شرکتی با تعیین یک بازرس خصوصی، اعم از داخلی یا برون سپاری انجام می شود. آنها توسط نقض خط مشی شرکت ایجاد می شوند.

چه تحقیق در مورد جرم و چه نقض خط مشی شرکت، بخشی از شواهد مربوط به دستگاه های دیجیتال و رسانه های دیجیتال است. اینجاست که پزشکی قانونی دیجیتال وارد بازی می شود و سعی می کند آنچه را که اتفاق افتاده است مشخص کند. **بدون محققین پزشکی قانونی دیجیتال آموزش دیده، پردازش هر مدرک دیجیتالی به درستی امکان پذیر نخواهد بود.**

- **فرآیند پزشکی قانونی دیجیتال (Digital Forensics Process):**



به عنوان یک **محقق پزشکی قانونی دیجیتال**، شما به صحنه ای شبیه به آنچه در تصویر بالا نشان داده شده است می رسید. شما به عنوان یک محقق پزشکی قانونی دیجیتال چه باید بکنید؟ پس از اخذ مجوز قانونی مناسب، طرح اولیه به شرح زیر است:

۱- شواهد را به دست آورید: دستگاه های دیجیتالی مانند لپ تاپ، دستگاه های ذخیره سازی و دوربین های دیجیتال را جمع آوری کنید. (توجه داشته باشید که لپ‌تاپ‌ها و رایانه‌ها در صورت روشن بودن نیاز به کنترل خاصی دارند، اما این خارج از محدوده این اتاق است).
۲- ایجاد یک زنجیره نگهداری: هدف این است که اطمینان حاصل شود که فقط بازرسان مجاز، به شواهد دسترسی داشته باشند و هیچ کس نتواند در آن دستکاری کند.
۳- شواهد را در یک ظرف امن قرار دهید: می‌خواهید مطمئن شوید که شواهد آسیب نمی‌بینند. در مورد گوشی های هوشمند، می خواهید مطمئن شوید که آنها نمی توانند به شبکه دسترسی داشته باشند، بنابراین از راه دور پاک نمی شوند.
۴- شواهد را به آزمایشگاه پزشکی قانونی دیجیتال خود منتقل کنید.

- **در آزمایشگاه، روند به شرح زیر است:**

۱- شواهد دیجیتالی را از ظرف امن بازیابی کنید.
۲- یک کپی پزشکی قانونی از شواهد ایجاد کنید: نسخه پزشکی قانونی به نرم افزار پیشرفته نیاز دارد تا از تغییر داده های اصلی جلوگیری شود.
۳- شواهد دیجیتال را به ظرف امن برگردانید: شما روی کپی کار خواهید کرد. اگر به کپی آسیب وارد کنید، همیشه می توانید یک نسخه جدید ایجاد کنید.
۴- پردازش کپی را در ایستگاه کاری پزشکی قانونی خود شروع کنید.

****مراحل بالا از کتاب Guide to Computer Forensics and Investigations, 6th Edition برگرفته شده است****

به طور کلی، به گفته مدیر سابق **آزمایشگاه پزشکی قانونی دفاعی**(**Defense Computer Forensics Laboratory**)، کن زاتیکو، پزشکی قانونی دیجیتال شامل موارد زیر است:

- **مرجع جستجوی مناسب**(**Proper search authority**): بازرسان نمی توانند بدون اختیار قانونی مناسب شروع به کار کنند.
- **زنجیره نگهداری**(**Chain of custody**): این برای پیگیری اینکه چه کسی مدارک را در هر زمانی نگه داشته است ضروری است.
- **اعتبارسنجی با ریاضیات**(**Validation with mathematics**): با استفاده از نوع خاصی از تابع ریاضی به نام تابع هش، می‌توانیم تأیید کنیم که فایلی تغییر نکرده است.
- **استفاده از ابزارهای معتبر**(**Use of validated tools**): ابزارهای مورد استفاده در پزشکی قانونی دیجیتال باید اعتبارسنجی شوند تا اطمینان حاصل شود که درست کار می کنند. به عنوان مثال، اگر تصویری از یک دیسک ایجاد می کنید، می خواهید مطمئن شوید که تصویر پزشکی قانونی با داده های روی دیسک یکسان است.
- **تکرارپذیری**(**Repeatability**): یافته‌های پزشکی قانونی دیجیتال تا زمانی که مهارت‌ها و ابزار مناسب در دسترس باشد، قابل بازتولید هستند.
- **گزارش**(**Reporting**): تحقیقات پزشکی قانونی دیجیتال با گزارشی به پایان می رسد که شواهد مربوط به پرونده کشف شده را نشان می دهد.

• مثال عملی پزشکی قانونی دیجیتال:

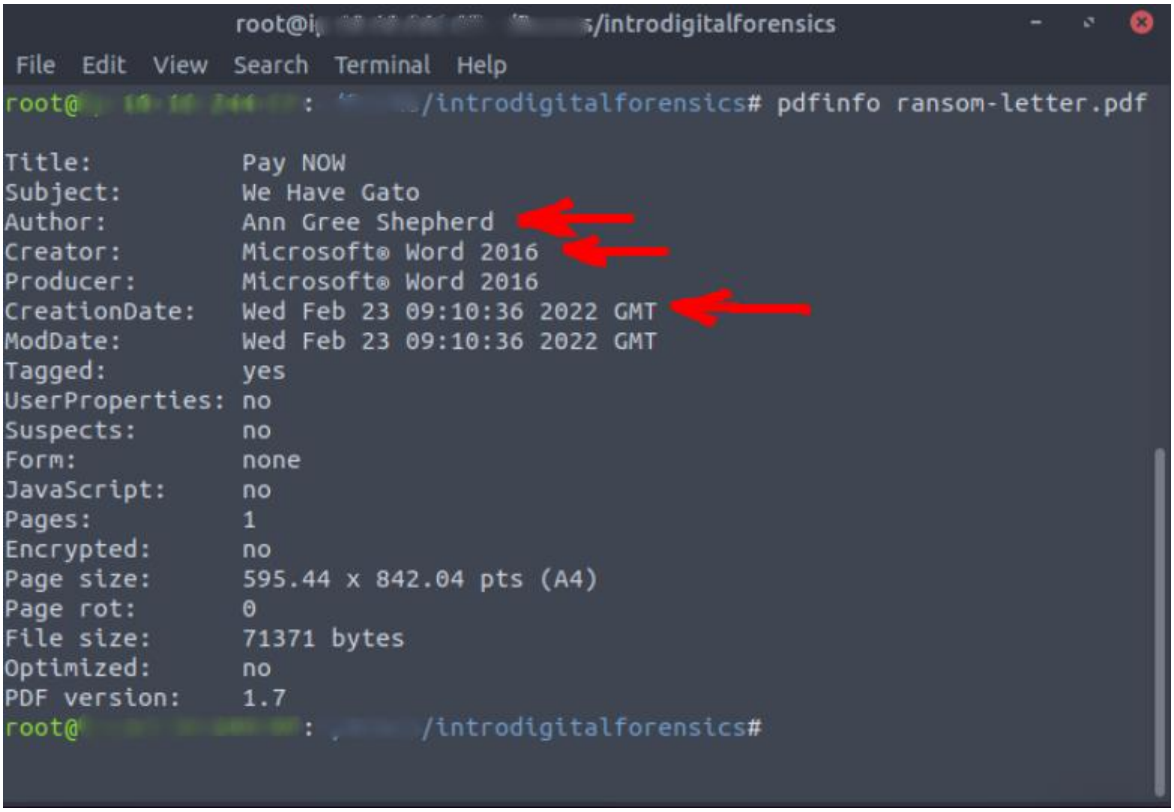
هر کاری که ما روی دستگاه های دیجیتال خود انجام می دهیم، از تلفن های هوشمند گرفته تا رایانه ها، ردپایی از خود بر جای می گذارد. بیایید ببینیم چگونه می توانیم از این در تحقیقات بعدی استفاده کنیم.

- **سناریو:** گربه ما، گادو، ربوده شده است. آدم ربا سندی را به همراه یک فایل JPG که عکس گربه ما هست، با درخواست های خود در قالب فایل PDF برای ما ارسال کرده است.

- **فراداده سند**(**Document Metadata**):

هنگامی که یک فایل متنی، TXT ایجاد می کنید، برخی از ابرداده ها توسط سیستم عامل ذخیره می شوند، مانند تاریخ ایجاد فایل و آخرین تاریخ اصلاح. با این حال، هنگامی که از ویرایشگر پیشرفته تری مانند MS Word استفاده می کنید، اطلاعات زیادی در فراداده فایل نگهداری می شود. روش های مختلفی برای خواندن فراداده فایل وجود دارد. ممکن است آنها را در ویرایشگر رسمی خود باز کنید یا از ابزار پزشکی قانونی مناسب استفاده کنید. توجه داشته باشید که صادر کردن فایل به فرمت‌های دیگر، مانند PDF ، بسته به نوع PDF نویسنده مورد استفاده، اکثر ابرداده‌های سند اصلی را حفظ می‌کند.

❖ ما می توانیم سعی کنیم **MetaData**های سندهای PDF را با استفاده از برنامه **pdfinfo** بخوانیم.



با استفاده از نرم افزار pdfinfo سندی که آدم ربا ارسال کرده بود را مورد بررسی قرار دادیم.

فراداده PDF به وضوح نشان می دهد که نویسنده سند Ann Gree Shepherd، با استفاده از MS Word 2016 در ۲۳ فوریه ۲۰۲۲ ساعت ۹:۱۰ دقیقه ایجاد کرده است.

- **داده EXIF عکس (Photo EXIF Data):**

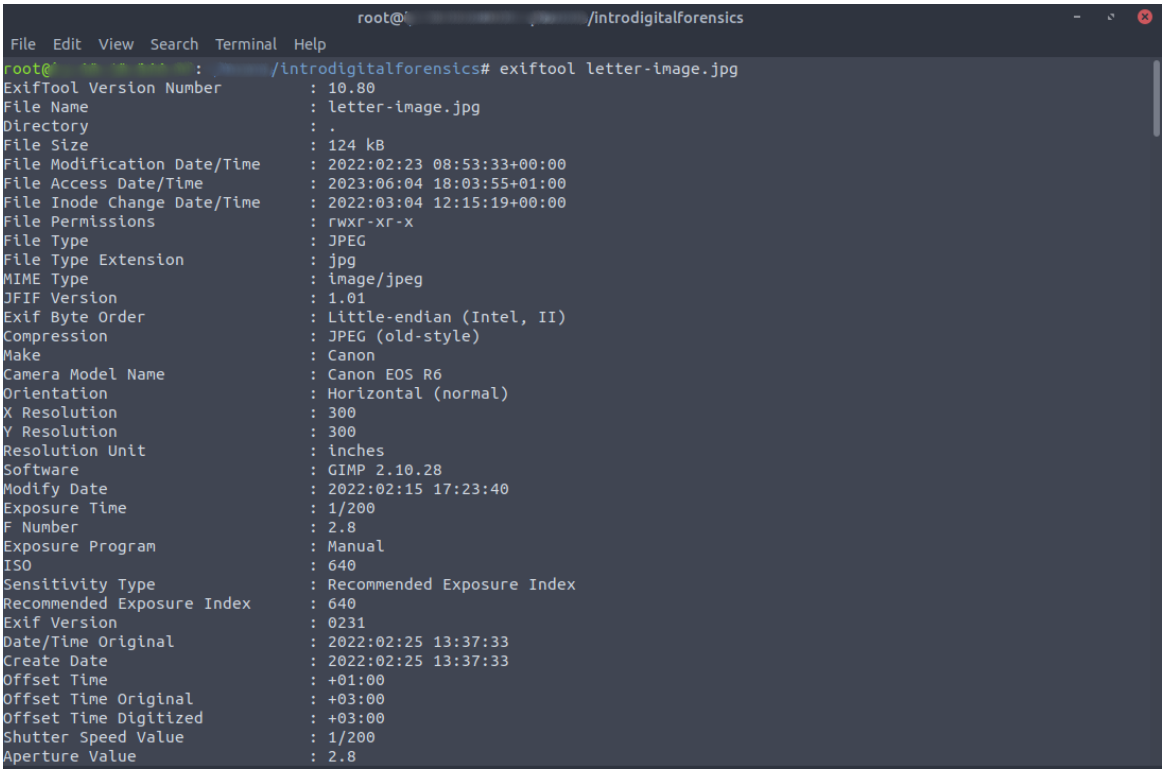
EXIF مخفف عبارت **Exchangeable Image File Format** است. استانداردی برای ذخیره ابرداده در فایل های تصویری است. هر زمان که با گوشی هوشمند یا دوربین دیجیتال خود عکس می گیرید، اطلاعات زیادی در تصویر جاسازی می شود. موارد زیر نمونه‌هایی از ابرداده‌هایی هستند که در تصاویر دیجیتال اصلی یافت می‌شوند:

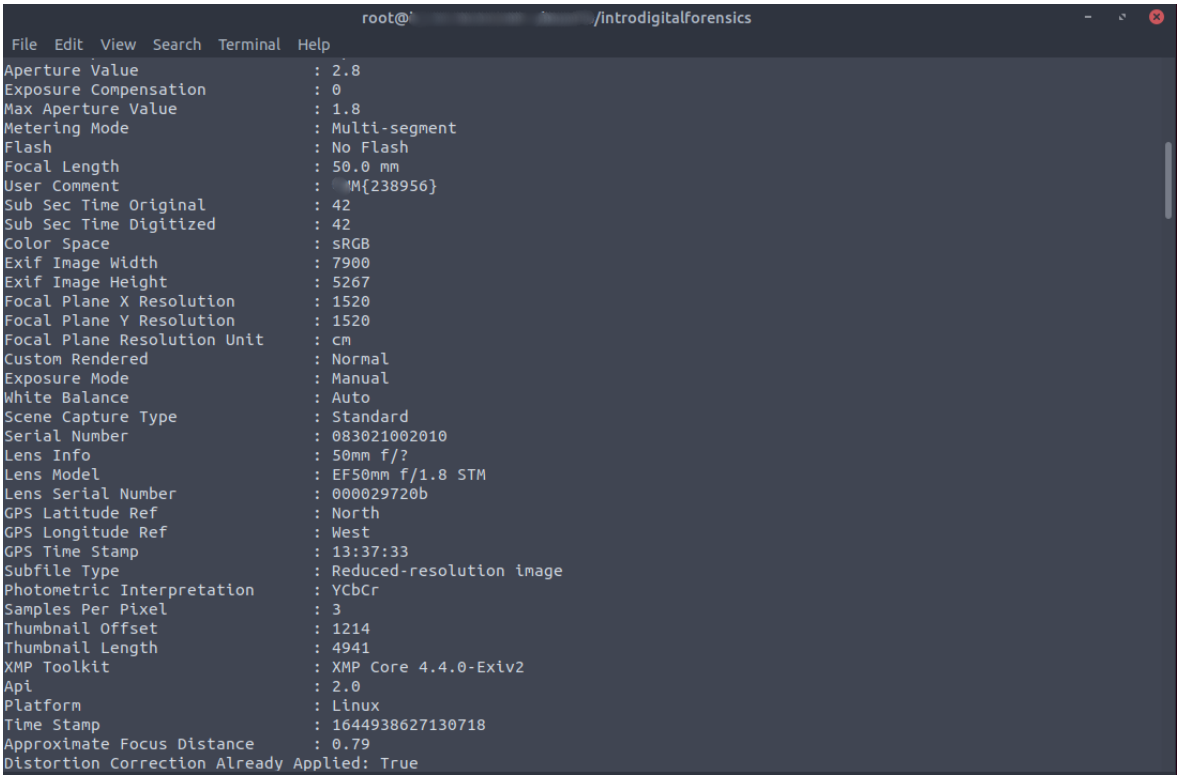
- مدل دوربین / مدل گوشی هوشمند
- تاریخ و زمان ثبت تصویر
- تنظیمات عکس مانند فاصله کانونی، دیافراگم، سرعت شاتر و تنظیمات ISO

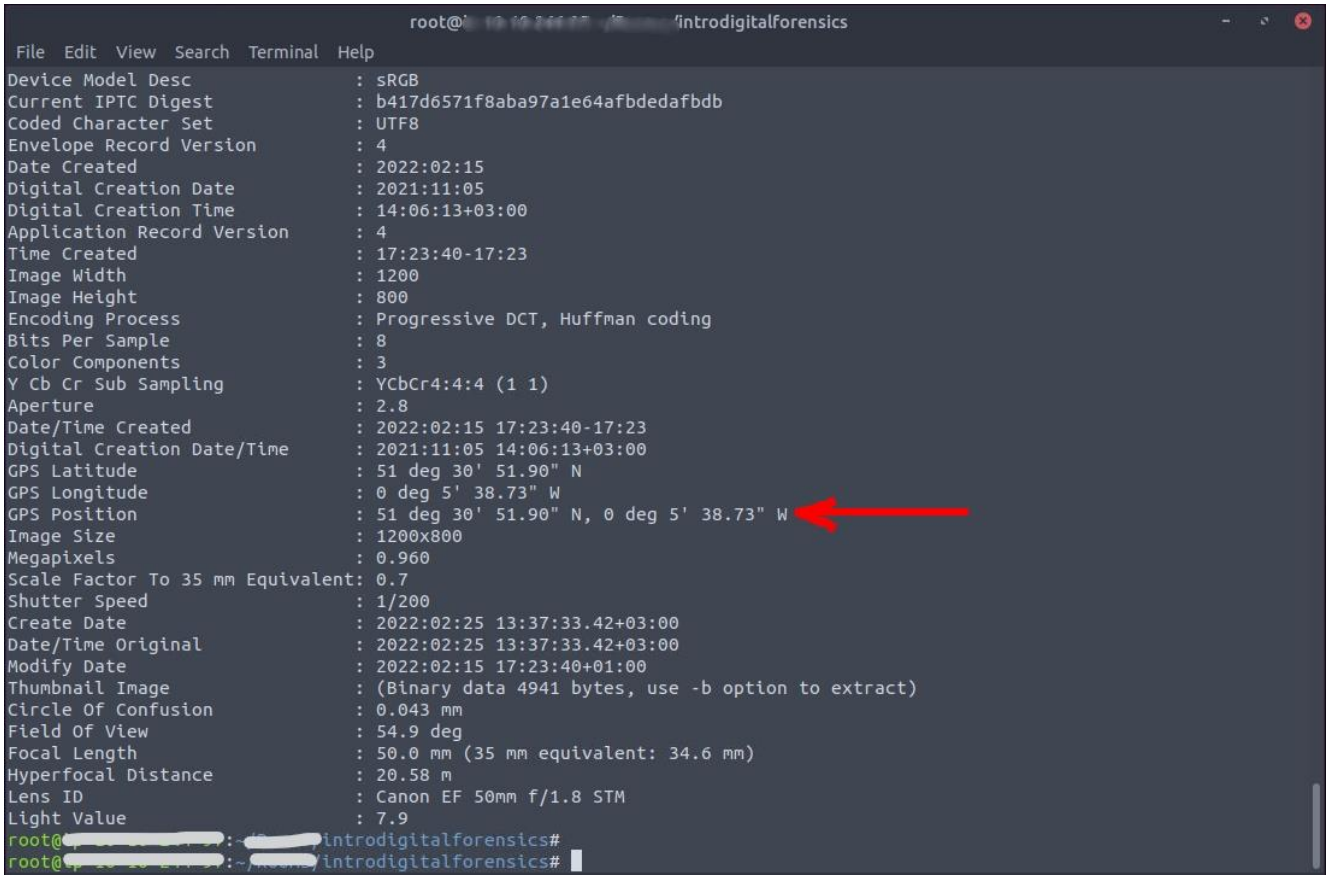
از آنجایی که گوشی های هوشمند مجهز به سنسور GPS هستند، یافتن مختصات GPS تعبیه شده در تصویر بسیار محتمل است. مختصات GPS، یعنی طول و عرض جغرافیایی، به طور کلی مکانی را که عکس گرفته شده نشان می دهد.

ابزارهای آنلاین و آفلاین زیادی برای خواندن داده های EXIF از تصاویر وجود دارد. یکی از ابزارهای خط فرمان exiftool است.

مقداری از خروجی MetaData در عکسی که آدم ربا برای ما ارسال کرده است، با استفاده از نرم افزار exiftool:







اگر به این خروجی ها دقت کنیم میبینیم که اطلاعات بسیار مفیدی از آدم ربا بدست آوردیمه.. مانند موقعیت مکانی که عکس گرفته شده.

اگر مختصات بالا را بگیرید و یکی از نقشه های آنلاین را جستجو کنید، در مورد این مکان بیشتر خواهید آموخت. **جستجوی نقشه های بینگ مایکروسافت یا نقشه های گوگل** برای **51° 31' 4.00" N, 0° 5' 48.30" W** نشان می دهد که این مختصات نشان می دهد که تصویر بسیار نزدیک به موزه لندن گرفته شده است. (ما فقط درجه را با ° جایگزین کردیم تا جستجوی ما کار کند.) متوجه شدیم که مختصات به نمایش دهدهی در صفحه جستجو تبدیل شده است: **51.517776, -0.09675**

بله پیداش کردیم، آدم ربا این عکس رو از خیابان **Milk Street** در شهر لندن گرفته است.

امیدوارم این مقاله برای علاقمندان به امنیت اطلاعات حوزه Digital Forensics مفید و جالب بوده باشه.

این مقاله برگرفته از سایت tryhackme.com بوده است.