

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)

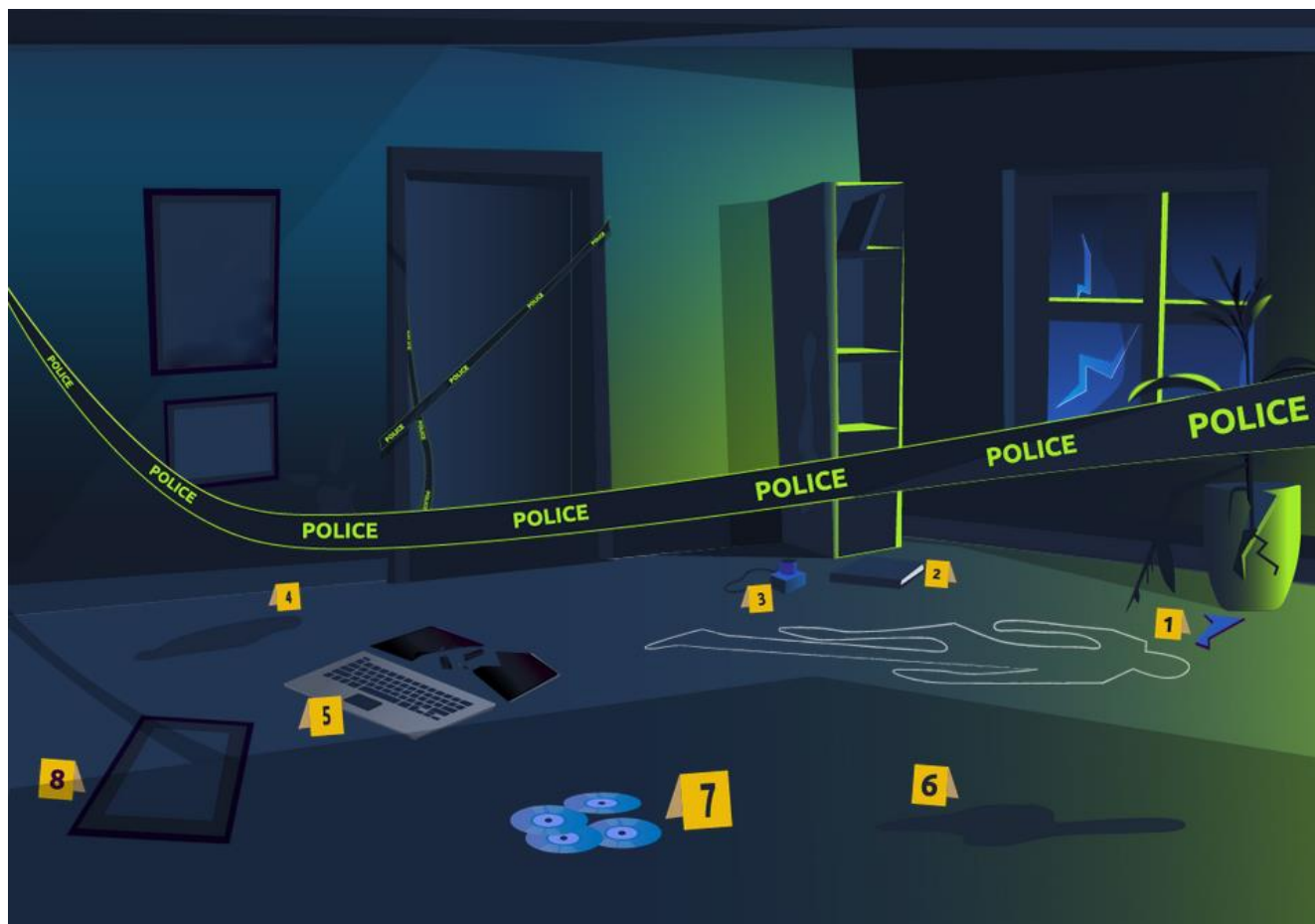
فهرست

مقدمه ای بر پزشکی قانونی دیجیتال صفحه ۳ - ۵

فرآیند پزشکی قانونی دیجیتال صفحه ۵ - ۷

مثال عملی پزشکی قانونی دیجیتال صفحه ۷ - ۱۰

• مقدمه ای بر پزشکی قانونی دیجیتال (Digital Forensics) :

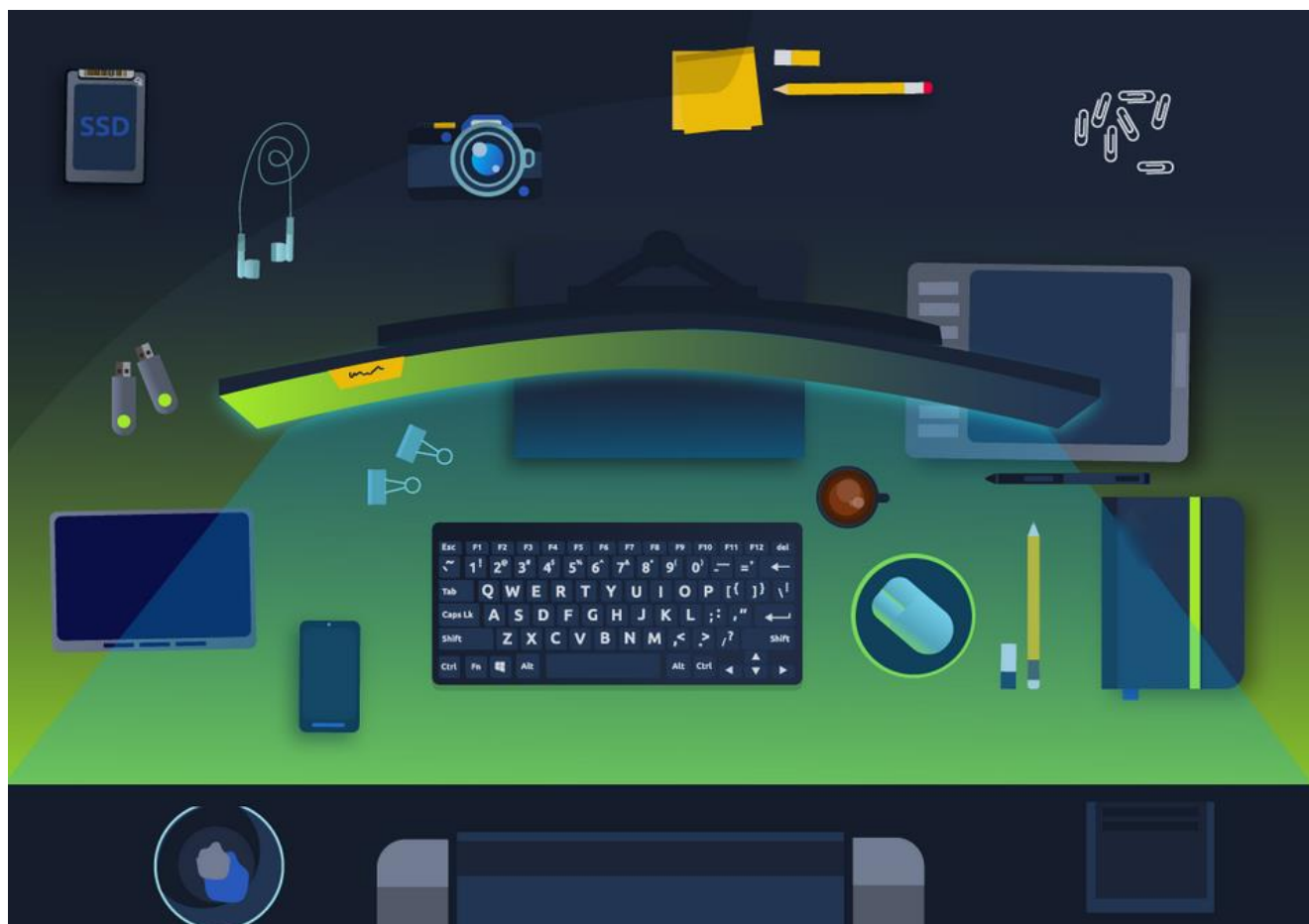


پزشکی قانونی کاربرد علم برای بررسی جرایم و اثبات حقایق است. با استفاده و گسترش سیستم‌های دیجیتال مانند رایانه‌ها و تلفن‌های هوشمند، شاخه جدیدی از پزشکی قانونی برای بررسی جرایم مرتبط متولد شد: پزشکی قانونی کامپیوتری (Digital Forensics) که بعداً به پزشکی قانونی دیجیتال تبدیل شد.

به سناریوی زیر فکر کنید. ماموران مجری قانون به صحنه جرم می‌رسند. با این حال، بخشی از این صحنه جرم شامل وسایل دیجیتال و رسانه‌ها می‌شود. دستگاه‌های دیجیتال شامل رایانه‌های رومیزی، لپ‌تاپ، دوربین‌های دیجیتال، پخش‌کننده‌های موسیقی و گوشی‌های هوشمند می‌شوند. رسانه‌های دیجیتال شامل سی‌دی، دی‌وی‌دی، درایو فلش مموری USB و حافظه خارجی است. چند سوال پیش می‌آید:

- پلیس چگونه باید مدارک دیجیتالی مانند گوشی‌های هوشمند و لپ‌تاپ‌ها را جمع‌آوری کند؟ اگر رایانه و تلفن هوشمند در حال اجرا هستند، چه مرحله‌ای 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 می‌شویم. هر یک از این دستگاه‌ها ممکن است حاوی مجموعه‌ای از اطلاعات باشد که می‌تواند به بررسی کمک کند. پردازش اینها به عنوان شواهد به پزشکی قانونی دیجیتال نیاز دارد.

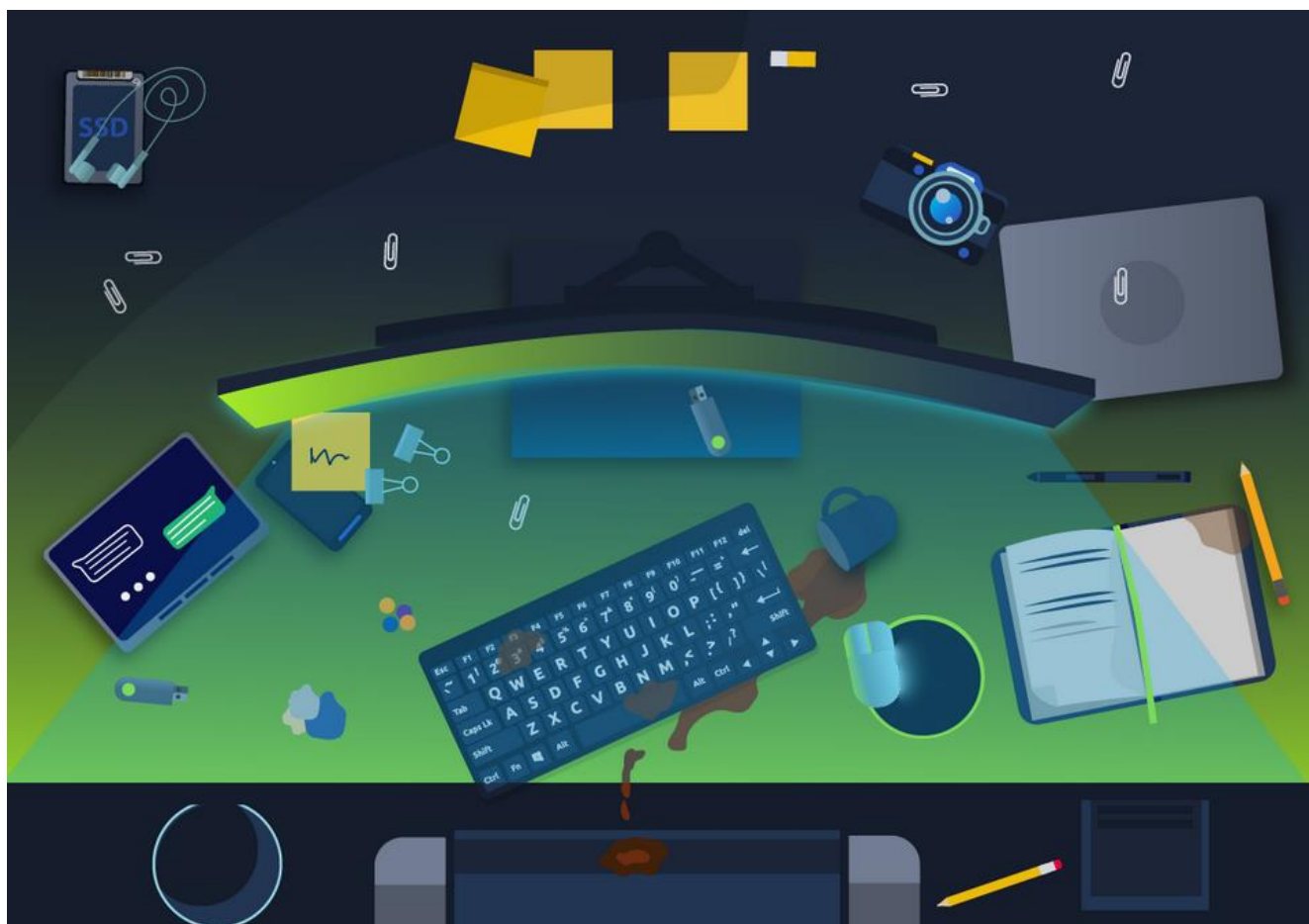
به طور رسمی تر، پزشکی قانونی دیجیتال کاربرد علم کامپیوتر برای بررسی شواهد دیجیتال برای اهداف قانونی است. پزشکی قانونی دیجیتال در دو نوع تحقیقات استفاده می‌شود:

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 لپ تاپ ها و رایانه ها 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: می خواهید مطمئن شوید که شواهد آسیب نمی بینند. 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.

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 هاش، می توانیم 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):** یافته های پزشکی قانونی دیجیتال تا زمانی که مهارت ها 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.

▪ **فرا داده سند (Document Metadata):**

هنگامی که یک فایل متنی، TXT ایجاد می کنید، برخی از ابر داده 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 فرمت های دیگر، مانند PDF، بسته به نوع PDF نویسنده مورد استفاده، اکثر ابر داده های سند اصلی را حفظ می کند.

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

```
root@ig:~# cd /introdigitalforensics
File Edit View Search Terminal Help
root@ig:~# cd /introdigitalforensics# pdftinfo ransom-letter.pdf
Title:      Pay NOW
Subject:    We Have Gato
Author:     Ann Gree Shepherd
Creator:    Microsoft® Word 2016
Producer:   Microsoft® Word 2016
CreationDate: Wed Feb 23 09:10:36 2022 GMT
ModDate:    Wed Feb 23 09:10:36 2022 GMT
Tagged:     yes
UserProperties: no
Suspects:   no
Form:       none
JavaScript: no
Pages:      1
Encrypted:   no
Page size:  595.44 x 842.04 pts (A4)
Page rot:   0
File size:  71371 bytes
Optimized:  no
PDF version: 1.7
root@ig:~# cd /introdigitalforensics#
```

با استفاده از نرم افزار pdftinfo 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. استاندارد برای ذخیره ابر داده 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 نمونه هایی از ابر داده هایی هستند که در تصاویر دیجیتال اصلی یافت می شوند:

- 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:

```
root@~: /introdigitalforensics
File Edit View Search Terminal Help
root@~: /introdigitalforensics# exiftool letter-image.jpg
ExifTool Version Number      : 10.80
File Name                    : letter-image.jpg
Directory                    : .
File Size                    : 124 kB
File Modification Date/Time   : 2022:02:23 08:53:33+00:00
File Access Date/Time        : 2023:06:04 18:03:55+01:00
File Inode Change Date/Time   : 2022:03:04 12:15:19+00:00
File Permissions              : rwxr-xr-x
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Exif Byte Order               : Little-endian (Intel, II)
Compression                  : JPEG (old-style)
Make                         : Canon
Camera Model Name             : Canon EOS R6
Orientation                  : Horizontal (normal)
X Resolution                  : 300
Y Resolution                  : 300
Resolution Unit               : inches
Software                     : GIMP 2.10.28
Modify Date                   : 2022:02:15 17:23:40
Exposure Time                 : 1/200
F Number                      : 2.8
Exposure Program              : Manual
ISO                           : 640
Sensitivity Type              : Recommended Exposure Index
Recommended Exposure Index    : 640
Exif Version                  : 0231
Date/Time Original            : 2022:02:25 13:37:33
Create Date                   : 2022:02:25 13:37:33
Offset Time                   : +01:00
Offset Time Original          : +03:00
Offset Time Digitized         : +03:00
Shutter Speed Value           : 1/200
Aperture Value                : 2.8
```

```
root@~: /introdigitalforensics
File Edit View Search Terminal Help
Aperture Value                : 2.8
Exposure Compensation         : 0
Max Aperture Value            : 1.8
Metering Mode                 : Multi-segment
Flash                         : No Flash
Focal Length                  : 50.0 mm
User Comment                   : M{238956}
Sub Sec Time Original         : 42
Sub Sec Time Digitized        : 42
Color Space                   : sRGB
Exif Image Width              : 7900
Exif Image Height             : 5267
Focal Plane X Resolution      : 1520
Focal Plane Y Resolution      : 1520
Focal Plane Resolution Unit    : cm
Custom Rendered               : Normal
Exposure Mode                 : Manual
White Balance                 : Auto
Scene Capture Type            : Standard
Serial Number                  : 083021002010
Lens Info                     : 50mm f/?
Lens Model                    : EF50mm f/1.8 STM
Lens Serial Number            : 000029720b
GPS Latitude Ref              : North
GPS Longitude Ref             : West
GPS Time Stamp                : 13:37:33
Subfile Type                  : Reduced-resolution image
Photometric Interpretation     : YCbCr
Samples Per Pixel             : 3
Thumbnail Offset              : 1214
Thumbnail Length              : 4941
XMP Toolkit                   : XMP Core 4.4.0-Exiv2
Api                           : 2.0
Platform                      : Linux
Time Stamp                    : 1644938627130718
Approximate Focus Distance     : 0.79
Distortion Correction Already Applied: True
```

```
root@10.10.2.10: /introdigitalforensics
File Edit View Search Terminal Help
Device Model Desc : sRGB
Current IPTC Digest : b417d6571f8aba97a1e64afbdefafbdb
Coded Character Set : UTF8
Envelope Record Version : 4
Date Created : 2022:02:15
Digital Creation Date : 2021:11:05
Digital Creation Time : 14:06:13+03:00
Application Record Version : 4
Time Created : 17:23:40-17:23
Image Width : 1200
Image Height : 800
Encoding Process : Progressive DCT, Huffman coding
Bits Per Sample : 8
Color Components : 3
Y Cb Cr Sub Sampling : YCbCr4:4:4 (1 1)
Aperture : 2.8
Date/Time Created : 2022:02:15 17:23:40-17:23
Digital Creation Date/Time : 2021:11:05 14:06:13+03:00
GPS Latitude : 51 deg 30' 51.90" N
GPS Longitude : 0 deg 5' 38.73" W
GPS Position : 51 deg 30' 51.90" N, 0 deg 5' 38.73" W
Image Size : 1200x800
Megapixels : 0.960
Scale Factor To 35 mm Equivalent: 0.7
Shutter Speed : 1/200
Create Date : 2022:02:25 13:37:33.42+03:00
Date/Time Original : 2022:02:25 13:37:33.42+03:00
Modify Date : 2022:02:15 17:23:40+01:00
Thumbnail Image : (Binary data 4941 bytes, use -b option to extract)
Circle Of Confusion : 0.043 mm
Field Of View : 54.9 deg
Focal Length : 50.0 mm (35 mm equivalent: 34.6 mm)
Hyperfocal Distance : 20.58 m
Lens ID : Canon EF 50mm f/1.8 STM
Light Value : 7.9
root@10.10.2.10: /introdigitalforensics#
root@10.10.2.10: /introdigitalforensics#
```

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 دهنده 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.