Cookie Han Hoan

Challenge Code	digital-forensics-016
Tags	Printer Yellow Dot
Type	Digital Forensics
Season	Gitex-2023
Difficulty	Very Easy
Flag Prefix	CHH
Flag Content	Dell-20230727-1002

Description

We discovered that someone stole Cookie Han Hoan's character sketches and printed them. Several suspicious people were questioned. We need more evidence to conclude who is the bad guy. Please help me determine when the document was printed and which printer it was printed on.

The flag format is CHH{Manufacturer-YYYYMMDD-HHMM}

- YYYY: Year
- MM: Month
- DD: Day
- HH: Hour
- MM: Minute
- Manufacturer: Name of printer (eg, Epson, Dell, HP,..)

Writeup

```
└─○ exiftool CookieHanHoan.pdf
ExifTool Version Number         : 12.60
File Name                       : CookieHanHoan.pdf
Directory                       : .
File Size                       : 661 kB
```

```
File Modification Date/Time     : 2023:10:20 00:07:17+07:00
File Access Date/Time           : 2023:10:20 00:07:19+07:00
File Inode Change Date/Time     : 2023:10:20 00:07:17+07:00
File Permissions                : -rw-r--r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.3
Linearized                      : No
Page Count                      : 1
Profile CMM Type                : Linotronic
Profile Version                 : 2.1.0
Profile Class                   : Display Device Profile
Color Space Data                : RGB
Profile Connection Space        : XYZ
Profile Date Time               : 1998:02:09 06:49:00
Profile File Signature          : acsp
Primary Platform                : Microsoft Corporation
CMM Flags                       : Not Embedded, Independent
Device Manufacturer             : Hewlett-Packard
Device Model                    : sRGB
Device Attributes               : Reflective, Glossy, Positive, Color
Rendering Intent                : Perceptual
Connection Space Illuminant     : 0.9642 1 0.82491
Profile Creator                 : Hewlett-Packard
Profile ID                      : 0
Profile Copyright               : Copyright (c) 1998 Hewlett-Packard Company
Profile Description             : sRGB IEC61966-2.1
Media White Point               : 0.95045 1 1.08905
Media Black Point               : 0 0 0
Red Matrix Column               : 0.43607 0.22249 0.01392
Green Matrix Column             : 0.38515 0.71687 0.09708
Blue Matrix Column              : 0.14307 0.06061 0.7141
Device Mfg Desc                 : IEC http://www.iec.ch
Device Model Desc               : IEC 61966-2.1 Default RGB colour space - sRGB
Viewing Cond Desc               : Reference Viewing Condition in IEC61966-2.1
Viewing Cond Illuminant         : 19.6445 20.3718 16.8089
Viewing Cond Surround           : 3.92889 4.07439 3.36179
Viewing Cond Illuminant Type    : D50
Luminance                       : 76.03647 80 87.12462
Measurement Observer            : CIE 1931
Measurement Backing             : 0 0 0
Measurement Geometry            : Unknown
Measurement Flare               : 0.999%
Measurement Illuminant          : D65
Technology                      : Cathode Ray Tube Display
Red Tone Reproduction Curve     : (Binary data 2060 bytes, use -b option to extract)
Green Tone Reproduction Curve   : (Binary data 2060 bytes, use -b option to extract)
Blue Tone Reproduction Curve    : (Binary data 2060 bytes, use -b option to extract)
XMP Toolkit                     : Image::ExifTool 12.60
Producer                        : CHH{aHR0cHM6Ly9iaXQubHkvNDhVY2lTcA==}
```

A Machine Identification Code (MIC), also known as printer steganography, yellow dots, tracking dots, or secret dots, is a digital watermark that certain color laser printers and copiers leave on every printed page, allowing identification of the device which was used to print a document and giving clues to the originator.

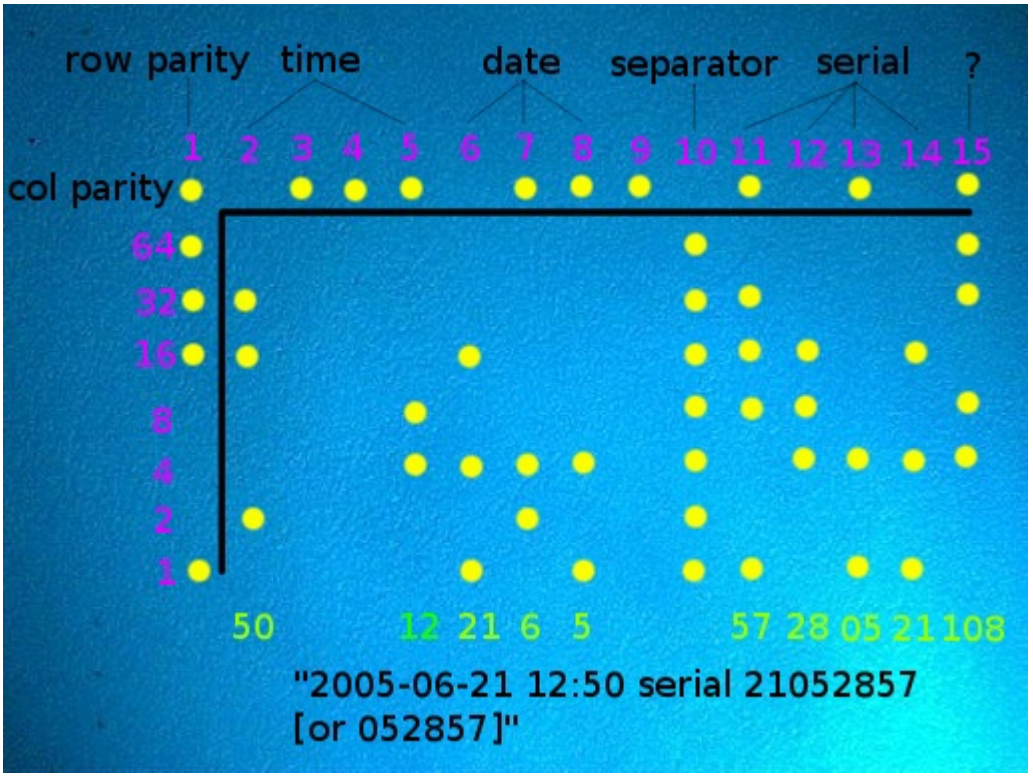
Developed by Xerox and Canon in the mid-1980s, its existence became public only in 2004. In 2018, scientists developed privacy software to anonymize prints to support whistleblowers publishing their work.

The photo below shows the yellow Dot represents information on a piece of paper

Một số máy in và photocopy màu sẽ để lại một mã bí mật màu vàng (**Yellow Dot**) trên mỗi trang khi in ra, nó sẽ được biểu diễn theo một thuật toán. Chúng ta chỉ có thể thấy khi dùng tia cực tím và dễ dàng giải được mã để biết tài liệu này được in trên máy nào, ngày nào và giờ nào

Được phát triển bởi Xerox và Canon vào giữa những năm 1980, sự tồn tại của nó chỉ được công khai vào năm 2004. Năm 2018, các nhà khoa học đã phát triển phần mềm bảo mật nhằm ẩn danh các bản in nhằm hỗ trợ người tố giác xuất bản tác phẩm của họ.

Bức ảnh dưới đây cho ta biết Yellow Dot được biểu diễn thông tin trên tờ giấy



We use the `pdftoppm` tool to convert pdf files into images for easier viewing.

Để quan sát dễ dàng hơn, chúng ta sử dụng công cụ `pdftoppm` để chuyển đổi file pdf thành dạng hình ảnh.

```
$ pdftoppm CookieHanHoan.pdf cookie -png
```

To decode these dots, we use `deda_parse_print` from deda to parse the image files for the identification information contained within. So if we do that and test out `deda_parse_print` on the first PDF page, we get the following output

Để giải mã những dấu chấm này, chúng tôi sử dụng `deda_parse_print` từ deda để phân tích các tệp hình ảnh để tìm thông tin nhận dạng có trong đó.

```
$ pip3 install deda
$ pip3 install 'PyPDF2<3.0'
```

```
└─○ deda_parse_print cookie-1.png
Detected pattern 4


_|0|1|2|3|4|5|6|7
0|
1|.
2|.
3|.       . .
4|.   .       .
5|    . . .
6|.
7|.
8|.     .   . . .
9|           . . .
0|.     . .   . .
1|.       .   .
2|.     .   .
3|.
4|             .
5|. . . . . . .
  41 dots.



<TDM of Pattern 4 at 0.00 x 0.00 inches>
Decoded:
```

```
manufacturer: Dell
serial: None
timestamp: 2023-07-27 10:02:00
raw: 00001234560000230727102000002
minutes: 02
hour: 10
day: 27
month: 07
year: 23
unknown1: 00
unknown3: 00
unknown4: 00
unknown5: 00
printer: 00123456
```

The flag format is CHH{Manufacturer-YYYYMMDD-HHMM}.

So the Flag is CHH{Dell-2023-07-27-1002}

Fact

The photocopier will store the content you photocopy/scan onto a hard drive. And "information miners" rely on that hard drive to find your important documents. In banks, credit funds, and large hospitals, people will often be responsible for handling these hard drives if the photocopier is broken and must be replaced.

However, a high-end copier is manufactured with higher security features; it will not save ultimately to the hard drive but instead:

- Scan images to hard drive in raw format.
- Process images for your use, then do what you request (print, email, share online, etc.).
- Then, the file is removed from the hard drive.

Máy photo nó sẽ lưu trữ các nội dung mà bạn photo/scan vào một ổ cứng. Và những người "đào thông tin" sẽ dựa vào ổ cứng đó mà tìm ra các tài liệu quan trọng của bạn. Ở các ngân hàng, quỹ tín dụng, bệnh viện lớn thường sẽ có những người đảm nhận việc xử lý các ổ cứng này nếu như máy photo bị hỏng và phải thay mới.

Tuy nhiên, một máy photocopy cao cấp được sản xuất với các tính năng bảo mật cao hơn, nó sẽ không lưu hoàn toàn vào ổ cứng mà thay vào đó :

- Quét hình ảnh vào ổ cứng ở định dạng thô.
- Xử lý hình ảnh để bạn sử dụng, sau đó thực hiện những gì bạn yêu cầu (in, gửi email, share qua mạng, v.v.).
- Sau đó file khỏi ổ cứng.

Sometimes, it retains information until it goes to sleep or the user logs out. Some copiers can save a copy of the image locally, such as RICOH's "Document Server." In this case, files are committed to the hard drive by default and then deleted after three days.

However, this feature can be set to keep files indefinitely.
Files on any hard drive (copier, computer, laptop, etc.) can be accessed with data recovery software even after the deleted files. The deleted data can be recovered if the information has not been rewritten with new data. So, if hackers can physically access your copier's drive, they have access to unencrypted data (most copiers do not encrypt data) on that hard drive.

Đôi khi, nó lưu giữ thông tin cho đến khi chuyển sang chế độ sleep hoặc người dùng đăng xuất. Một số máy photocopy có tùy chọn lưu cục bộ bản sao của hình ảnh như "Document Server" của RICOH. Trong trường hợp này, theo mặc định, các file được lưu vào ổ cứng rồi bị xóa sau 3 ngày.

Tuy nhiên, tính năng này có thể được đặt để giữ các tệp vô thời hạn. Các tệp trên bất kỳ ổ cứng nào (máy photocopy, máy tính, máy tính xách tay, v.v.) đều có thể được truy cập bằng phần mềm khôi phục dữ liệu ngay cả sau khi các file đã bị xóa. Nếu thông tin chưa được ghi lại bằng dữ liệu mới thì có thể khôi phục dữ liệu đã xóa. Nên nếu hacker có thể truy cập vật lý vào ổ đĩa máy photocopy của bạn thì chúng có quyền truy cập vào dữ liệu không được mã hóa (đa số máy photocpy đều k đc mã hoá dữ liệu) trên ổ cứng đó.