Haystack,有ELK

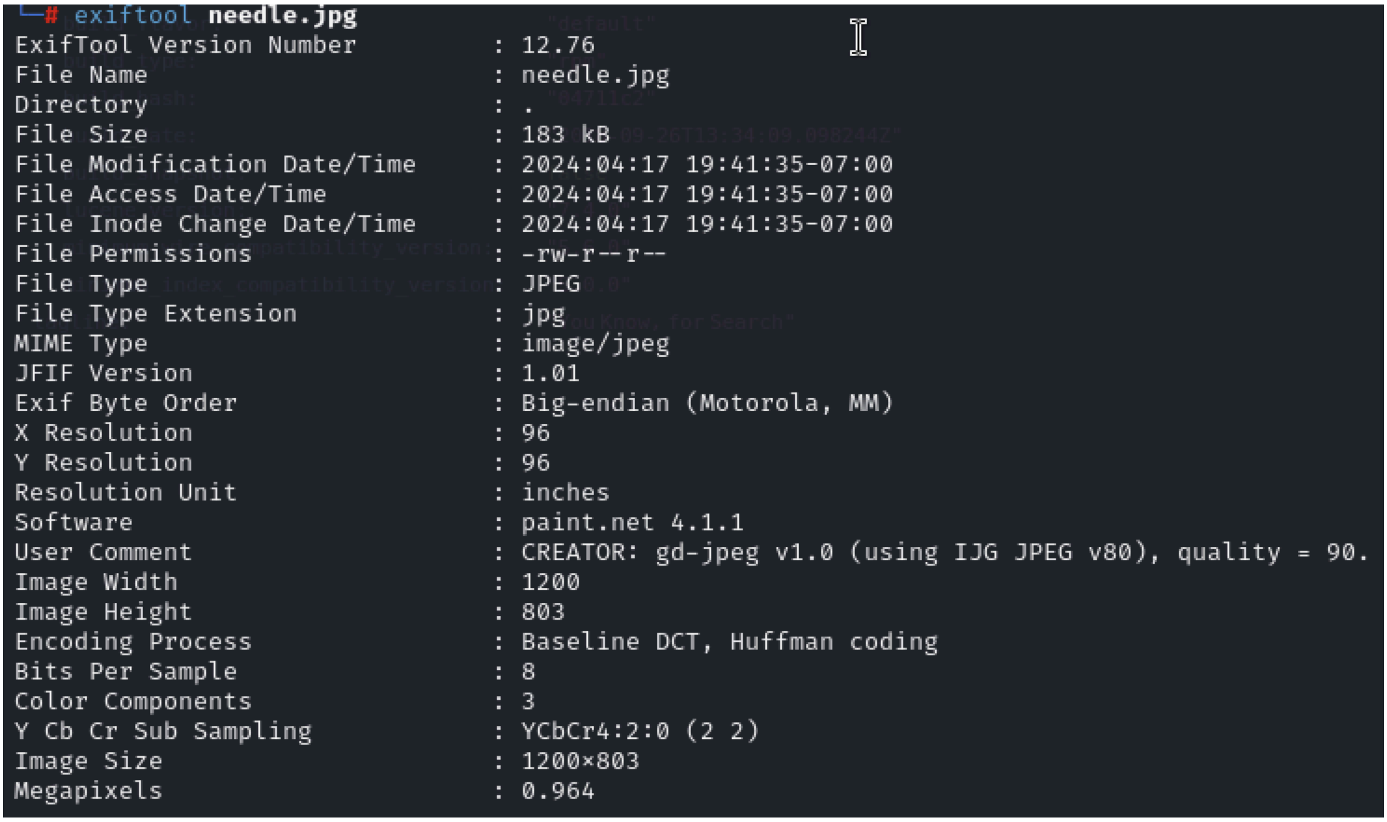
```
└─# nmap -sCV -p 22,80,9200 -A 10.10.10.115
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-17 19:29 PDT
Nmap scan report for 10.10.10.115
Host is up (0.21s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 2a:8d:e2:92:8b:14:b6:3f:e4:2f:3a:47:43:23:8b:2b (RSA)
|   256 e7:5a:3a:97:8e:8e:72:87:69:a3:0d:d1:00:bc:1f:09 (ECDSA)
|_  256 01:d2:59:b2:66:0a:97:49:20:5f:1c:84:eb:81:ed:95 (ED25519)
80/tcp   open  http    nginx 1.12.2
|_http-server-header: nginx/1.12.2
|_http-title: Site doesn't have a title (text/html).
9200/tcp open  http    nginx 1.12.2
|_http-title: 502 Bad Gateway
|_http-server-header: nginx/1.12.2
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|storage-misc
Running (JUST GUESSING): Linux 5.X|3.X|4.X (90%), Crestron 2-Series (86%), HP embedded (85%), Oracle VM Server 3.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:5.0 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:crestron:2_series cpe:/h:hp:p2000_g3 cpe:/o:oracle:vm_server:3.4.2 cpe:/o:linux:linux_kernel:4.1
Aggressive OS guesses: Linux 5.0 (90%), Linux 3.10 - 4.11 (90%), Linux 3.18 (90%), Linux 3.2 - 4.9 (90%), Linux 5.1 (90%), Crestron XPanel control system (86%), Linux 3.16 (86%), HP P2000 G3 NAS device (85%), Oracle VM Server 3.4.2 (Linux 4.1) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   208.21 ms 10.10.14.1
2   208.62 ms 10.10.10.115

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.10 seconds
```

因80port目錄掃不出來，針對圖片進行處理



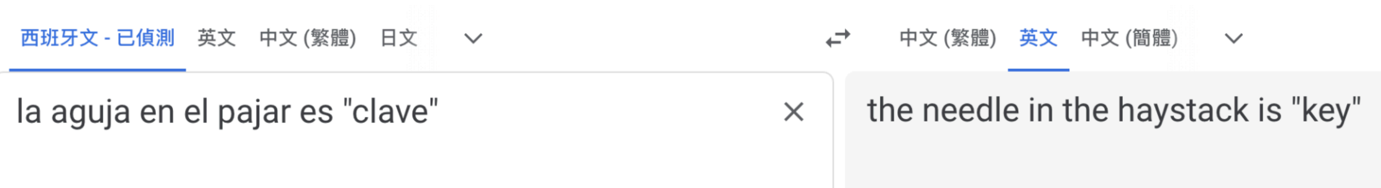
```
└─# exiftool needle.jpg
ExifTool Version Number         : 12.76
File Name                       : needle.jpg
Directory                       : .
File Size                       : 183 kB
File Modification Date/Time     : 2024:04:17 19:41:35-07:00
File Access Date/Time           : 2024:04:17 19:41:35-07:00
File Inode Change Date/Time     : 2024:04:17 19:41:35-07:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Exif Byte Order                 : Big-endian (Motorola, MM)
X Resolution                    : 96
Y Resolution                    : 96
Resolution Unit                 : inches
Software                        : paint.net 4.1.1
User Comment                    : CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90.
Image Width                     : 1200
Image Height                    : 803
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 1200x803
Megapixels                      : 0.964
```

```
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
bGEgYWdlamEgZW4gZWwgcGFqYXIgZXMgImNsYXZlIg==
```

發現是base64進行解

```
└─# echo "bGEgYWdlamEgZW4gZWwgcGFqYXIgZXMgImNsYXZlIg==" |base64 -d
la aguja en el pajar es "clave"
```

進行翻譯



la aguja en el pajar es "clave"

the needle in the haystack is "key"

http://10.10.10.115:9200/ 取得以下資訊：

```
{
  "name" : "iQEYHgS",
  "cluster_name" : "## elasticsearch",
  "cluster_uuid" : "pjrX7V_gSFmJY-DxP4tCQg",
  "version" : {
    "number" : "## 6.4.2",
    "build_flavor" : "default",
    "build_type" : "rpm",
    "build_hash" : "04711c2",
    "build_date" : "2018-09-26T13:34:09.098244Z",
    "build_snapshot" : false,
    "lucene_version" : "7.4.0",
    "minimum_wire_compatibility_version" : "5.6.0",
    "minimum_index_compatibility_version" : "5.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

找文件：https://www.elastic.co/guide/en/elasticsearch/reference/6.4/cat.html