Picture Analysis with Ghiro

what is Ghiro?

It is developed by Alessandro Tanasi Jekil and Marco Buoncristiano Burlone. It is a fully automated tool designed to run forensic analysis over a massive amount of images, just using a user-friendly and fancy web application.

Features of Ghiro

We can control all Ghiro features via the web interface. We can upload an image or a bunch of images to get a quick and deep overview of image analysis. We can group images in cases and search for any kind of analysis data.

The main features of Ghiro.

- **Metadata Extraction:** Metadata is divided into several categories depending on the standard where they are come from, Image metadata are extracted and categorized. EX- EXIF, IPTC, XMP.
- **GPS Localization:** It is Embedded in the image metadata sometimes there is a geotag, a bit of GPS data providing the longitude and latitude of where the photo was taken, it is read and the position is displayed on the map.
- **MIME Information:** The image MIME type detected to know the image type we are dealing with, in both contacted and extended form.
- **ELA:** ELA stands for Error Level Analysis. It identifies areas within an image that are at different compression levels. The entire picture should be at roughly the same level if a difference is detected, then it likely indicates a digital modification.
- **Thumbnail Extraction:** The thumbnails and data related to them are extracted from the image metadata and stored for review.
- **Thumbnail Consistency:** Sometimes when a photo is edited the original image is edited but the thumbnail not difference between the thumbnails and the images are detected.
- **Signature Engine:** They have over 120 signatures that provide evidence about the most critical data to highlight focal points and common exposures.
- **Hash Matching:** Suppose we are searching for an image and we have only the hash value. We can provide a list of hashes and all images matching are reported.

Setup Ghiro

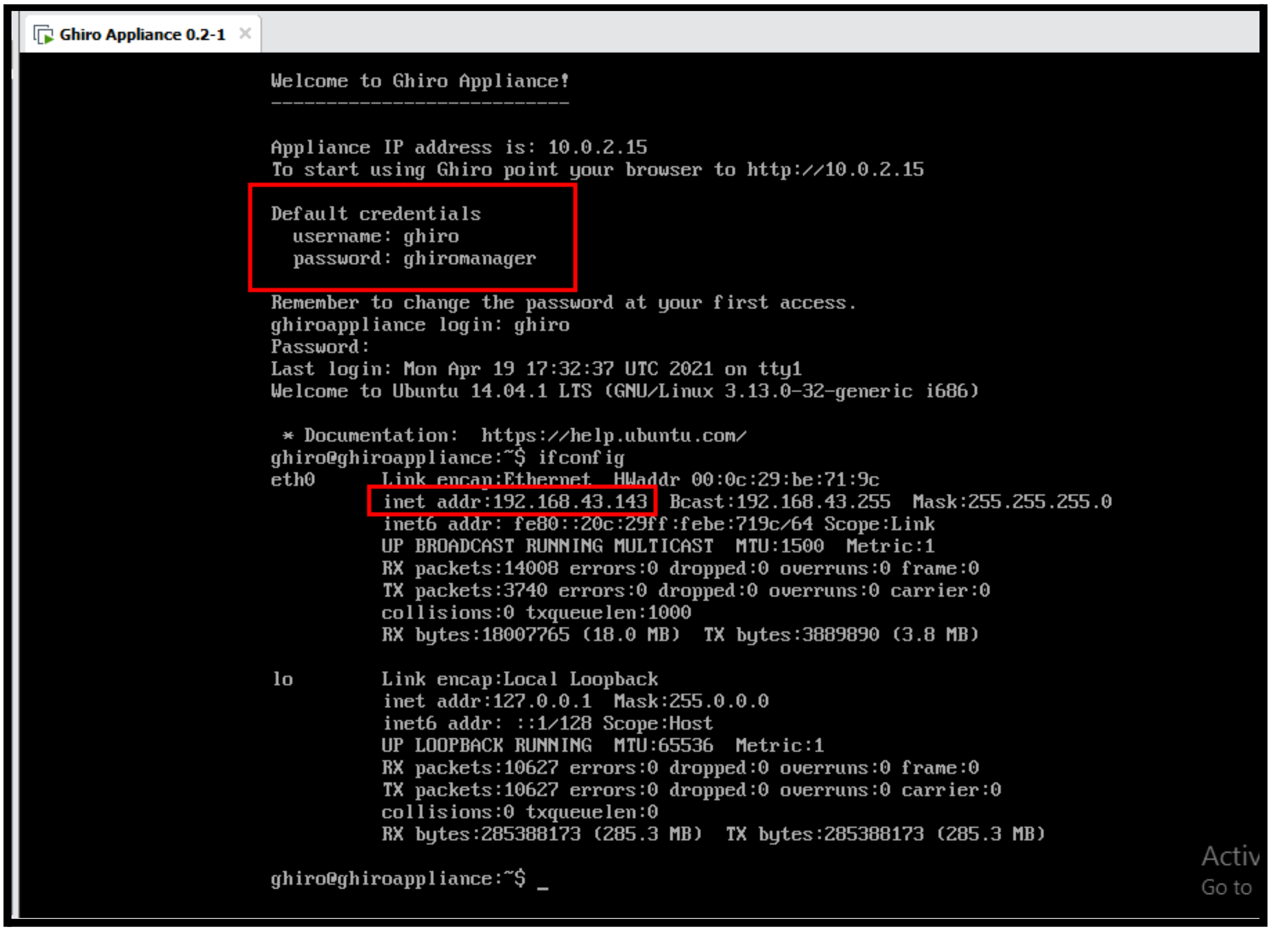
Now we need to set up our Ghiro, we recommend the “**OVA**” version because it is the faster way to start using the Ghiro. After downloading the Ghiro, in few minutes you will have a fully functional Ghiro set up to start to analyze our images.

To download the Ghiro image analysis tool, click on this link=>>https://www.getghiro.org/

After opening this OVA file in Virtual Box or VMWare, It will come up as a screen like this.

It is showing us the two details

After opening this OVA file in Virtual Box or VMWare, It will come up as a screen like this.

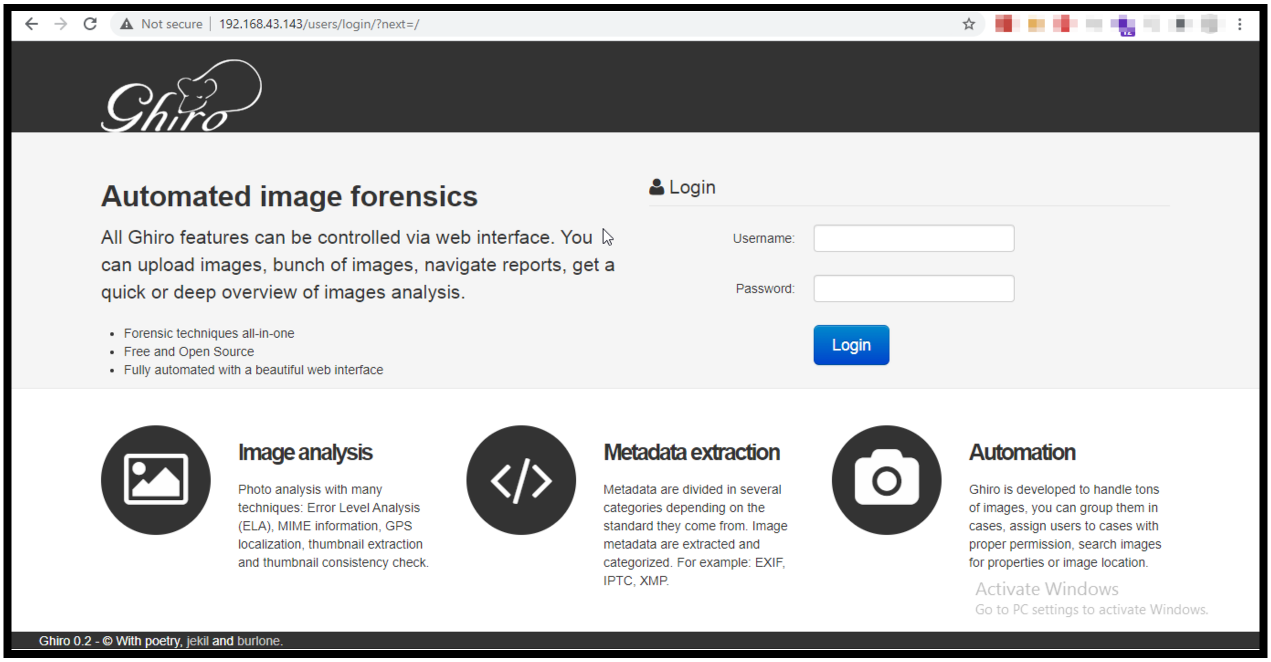


```
Welcome to Ghiro Appliance!
---------------------------

Appliance IP address is: 10.0.2.15
To start using Ghiro point your browser to http://10.0.2.15

Default credentials
  username: ghiro
  password: ghiromanager

Remember to change the password at your first access.
ghiroappliance login: ghiro
Password:
Last login: Mon Apr 19 17:32:37 UTC 2021 on tty1
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic i686)

 * Documentation:  https://help.ubuntu.com/
ghiro@ghiroappliance:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:be:71:9c
          inet addr:192.168.43.143  Bcast:192.168.43.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:febe:719c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:14008 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3740 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:18007765 (18.0 MB)  TX bytes:3889890 (3.8 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:10627 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10627 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:285388173 (285.3 MB)  TX bytes:285388173 (285.3 MB)

ghiro@ghiroappliance:~$ _
```

Now we open that IP address in our browser, to move further in the setup process.

Default credentials to log in Ghiro are

Username: ghiro
Password: ghiromanager



Automated image forensics

All Ghiro features can be controlled via web interface. You can upload images, bunch of images, navigate reports, get a quick or deep overview of images analysis.

- Forensic techniques all-in-one
- Free and Open Source
- Fully automated with a beautiful web interface

Login

Username:

Password:

Image analysis

Photo analysis with many techniques: Error Level Analysis (ELA), MIME information, GPS localization, thumbnail extraction and thumbnail consistency check.

Metadata extraction

Metadata are divided in several categories depending on the standard they come from. Image metadata are extracted and categorized. For example: EXIF, IPTC, XMP.

Automation

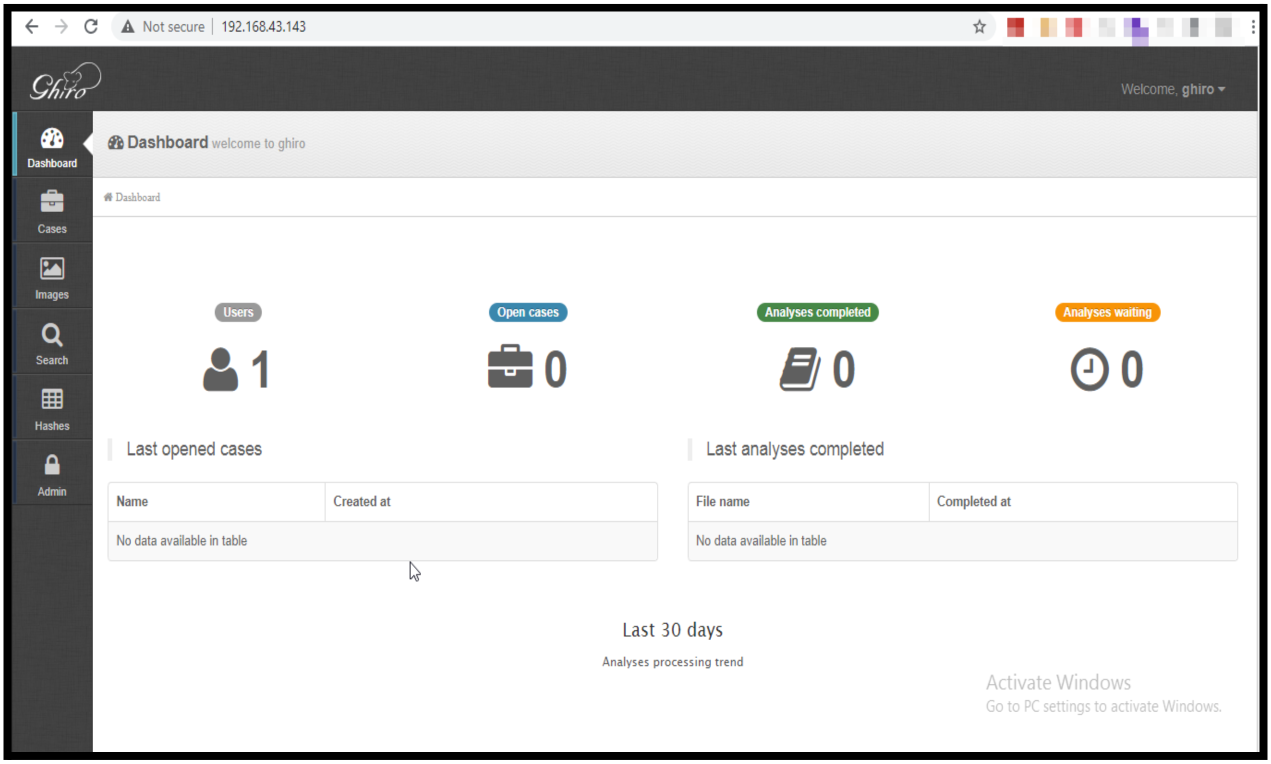
Ghiro is developed to handle tons of images, you can group them in cases, assign users to cases with proper permission, search images for properties or image location.

Activate Windows
Go to PC settings to activate Windows.

Ghiro 0.2 - © With poetry, jekil and burlone.

Now, we can see that we successfully set up the Ghiro, the dashboard in the home screen says that welcome to Ghiro, Which confirms that our setup is successful.

As we can see that it has we user which **user: ghiro** through which we log in the software. At the initial point, it shows zero cases and zeroes analysis left because we just set up this software.



Dashboard welcome to ghiro

Dashboard

Users 1

Open cases 0

Analyses completed 0

Analyses waiting 0

Last opened cases

Name	Created at
No data available in table	

Last analyses completed

File name	Completed at
No data available in table	

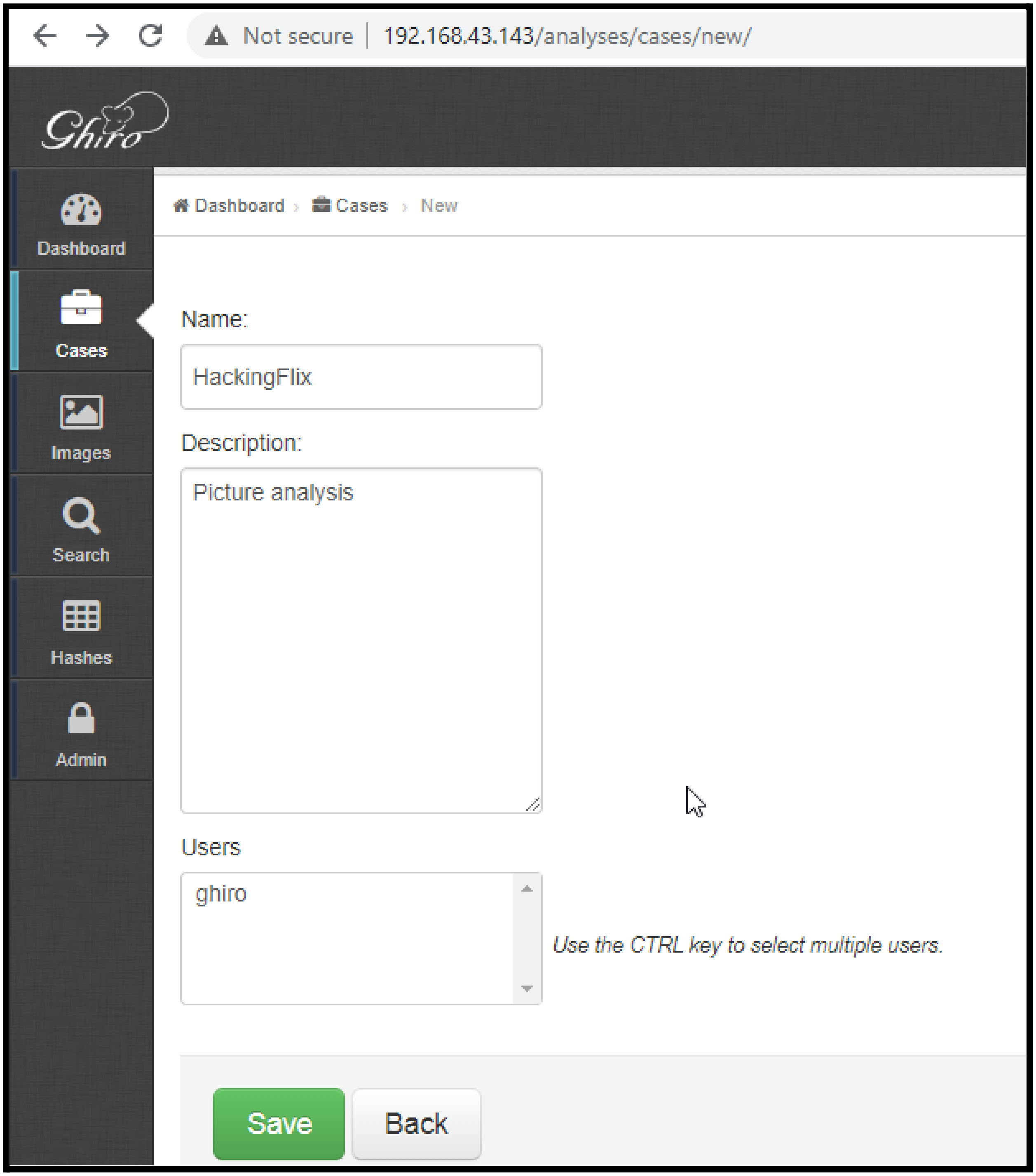
Last 30 days

Analyses processing trend

Activate Windows
Go to PC settings to activate Windows.

To start working with Ghiro for image analysis we need to click on cases. Where we can see that it is completely blank, then notice a **[+]** to add any case to this directory.

Now, we need to fill up the details regarding the forensic case like **case name, case description**, and its Investigating user.



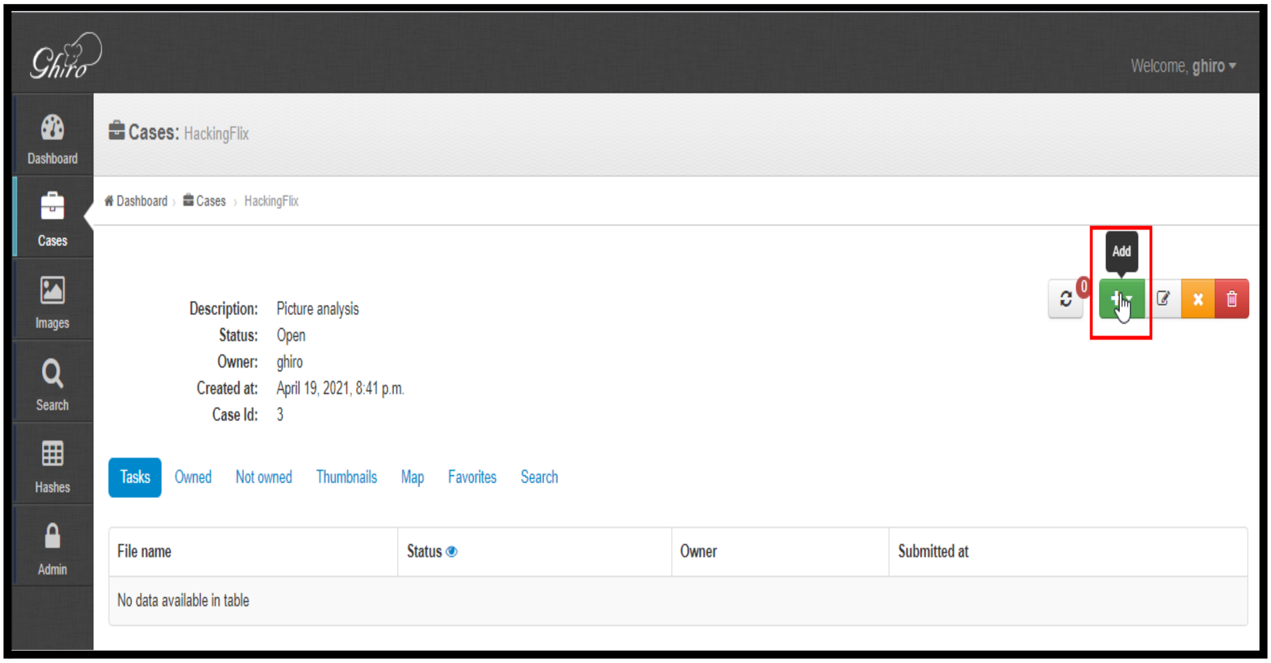
Name: HackingFlix

Description: Picture analysis

Users: ghiro

Use the CTRL key to select multiple users.

After saving the details regarding this forensic case, It will confirm these details and ask us to add images to analysis. To add images click **[+]** button.



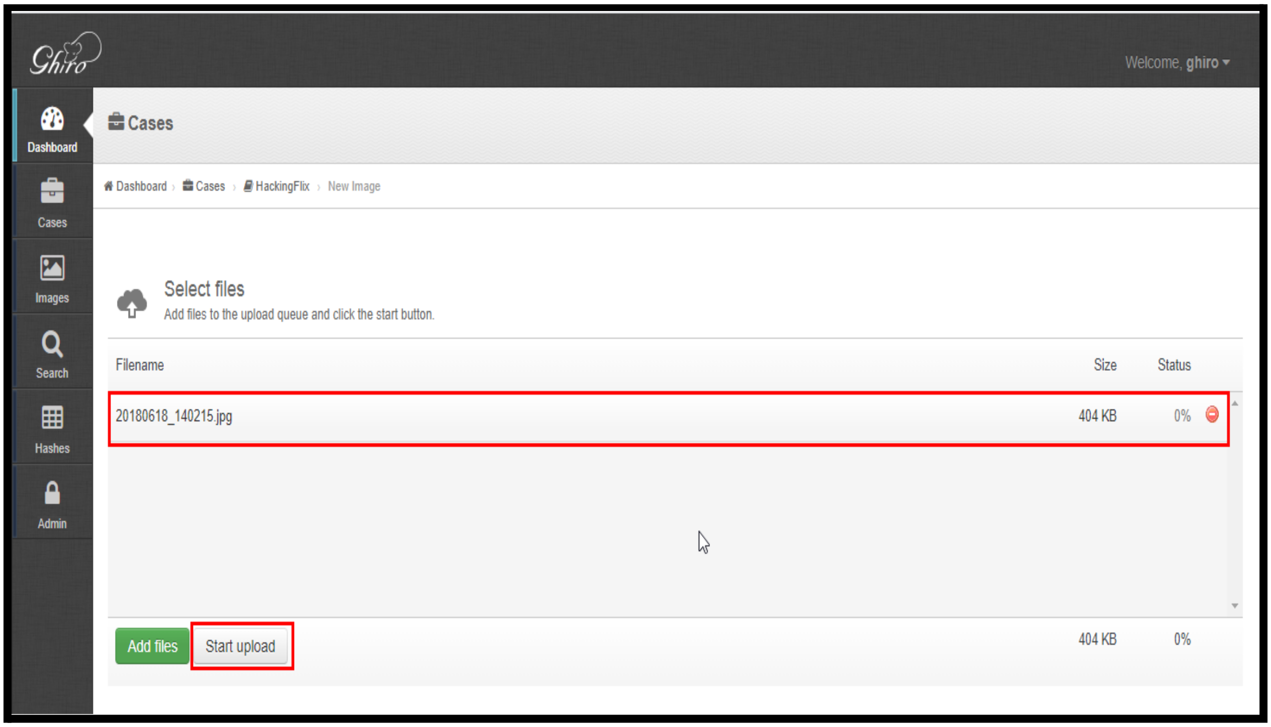
Cases: HackingFlix

Dashboard › Cases › HackingFlix

Description: Picture analysis
Status: Open
Owner: ghiro
Created at: April 19, 2021, 8:41 p.m.
Case Id: 3

File name	Status	Owner	Submitted at
No data available in table			

To will lead us to a window through which we can add images by clicking in the **add file** option. Browse the file you want to analyze. After adding those files click on the **start upload** button.



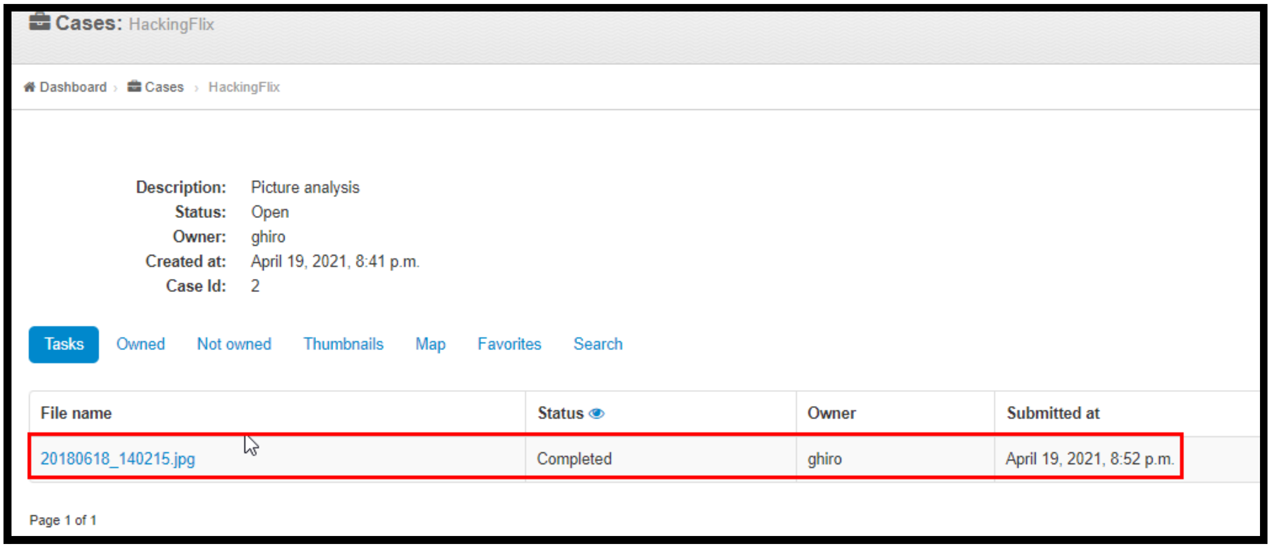
Cases

Dashboard › Cases › HackingFlix › New Image

Select files
Add files to the upload queue and click the start button.

Filename	Size	Status
20180618_140215.jpg	404 KB	0%
	404 KB	0%

After uploading these files it will show us the files and their status of uploading these images. In this uploading process, Click on the refresh button to finishing up the upload.



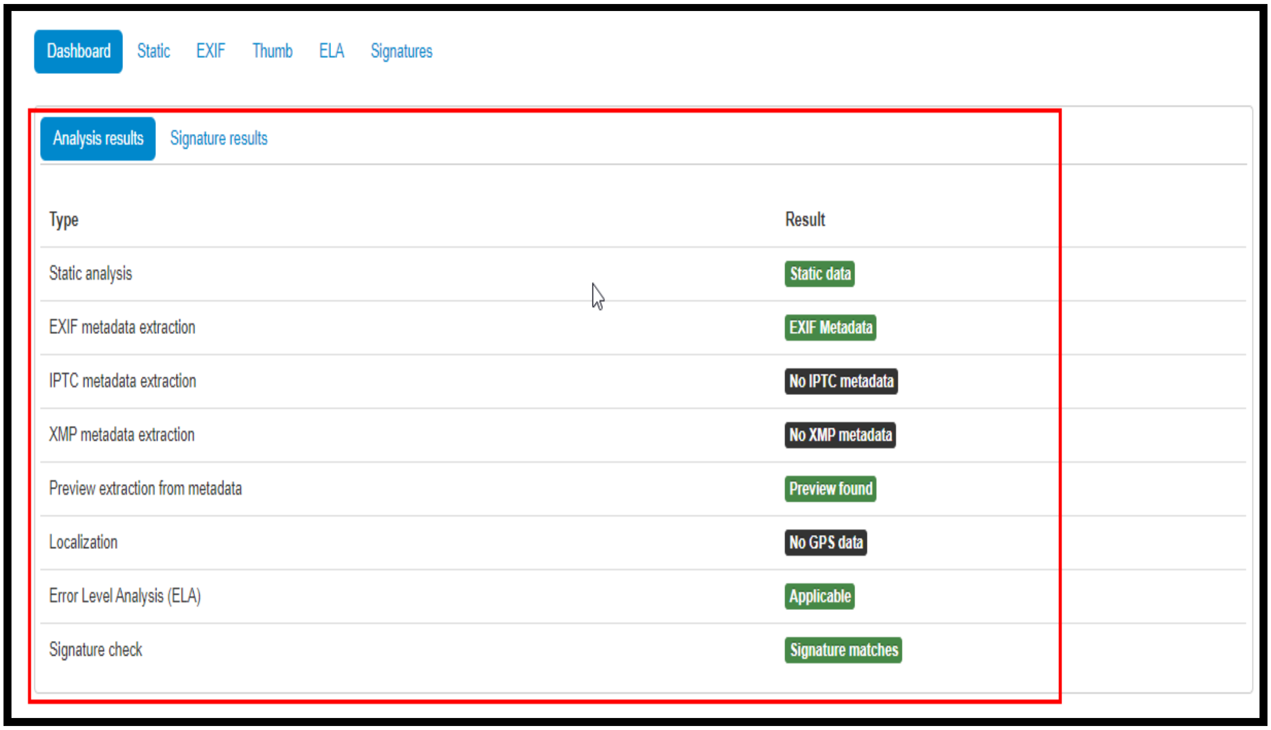
Description: Picture analysis
Status: Open
Owner: ghiro
Created at: April 19, 2021, 8:41 p.m.
Case Id: 2

File name	Status	Owner	Submitted at
20180618_140215.jpg	Completed	ghiro	April 19, 2021, 8:52 p.m.

Page 1 of 1

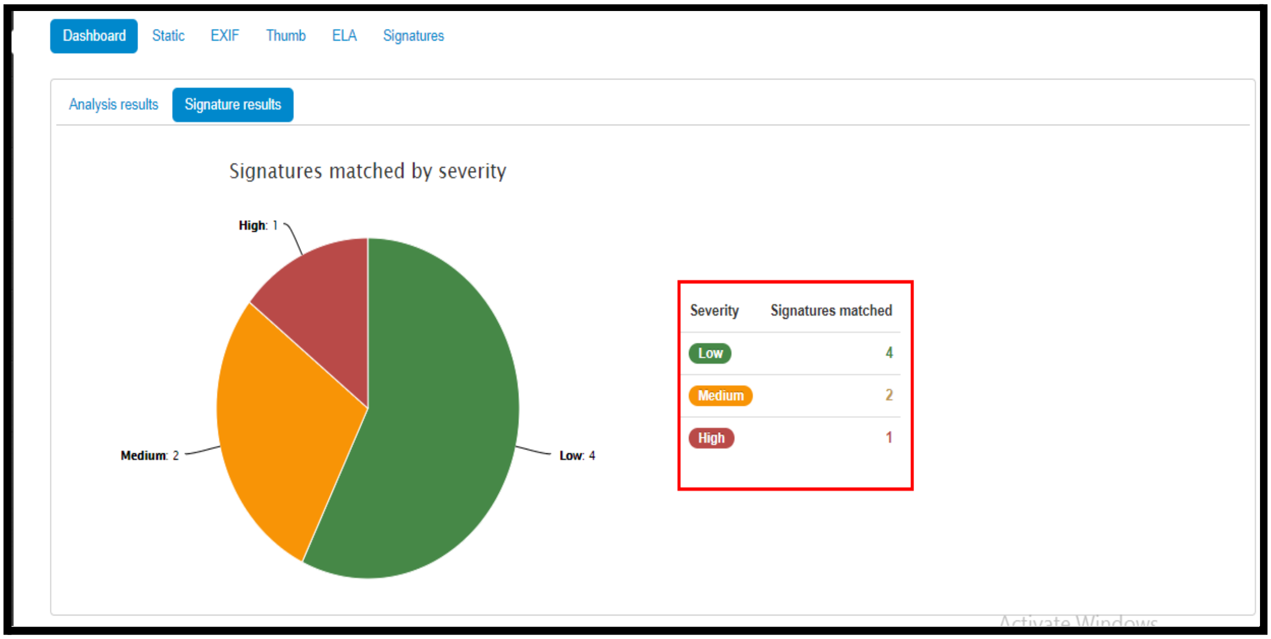
We can see that the file upload process in just finished now we have two options to analyze the image. The first option is directly to click on the image name to view their details. The second option is to click on the images tab and then click on the image we want to see their details. Both of them are kind of the same it doesn’t affect the forensic investigation process.

Click on the image we want to analyze, it will show us the basic details regarding the image in the dashboard which shows us all the analysis results like **static analysis, EXIF, IPTC, XMP, Signature check,** etc.



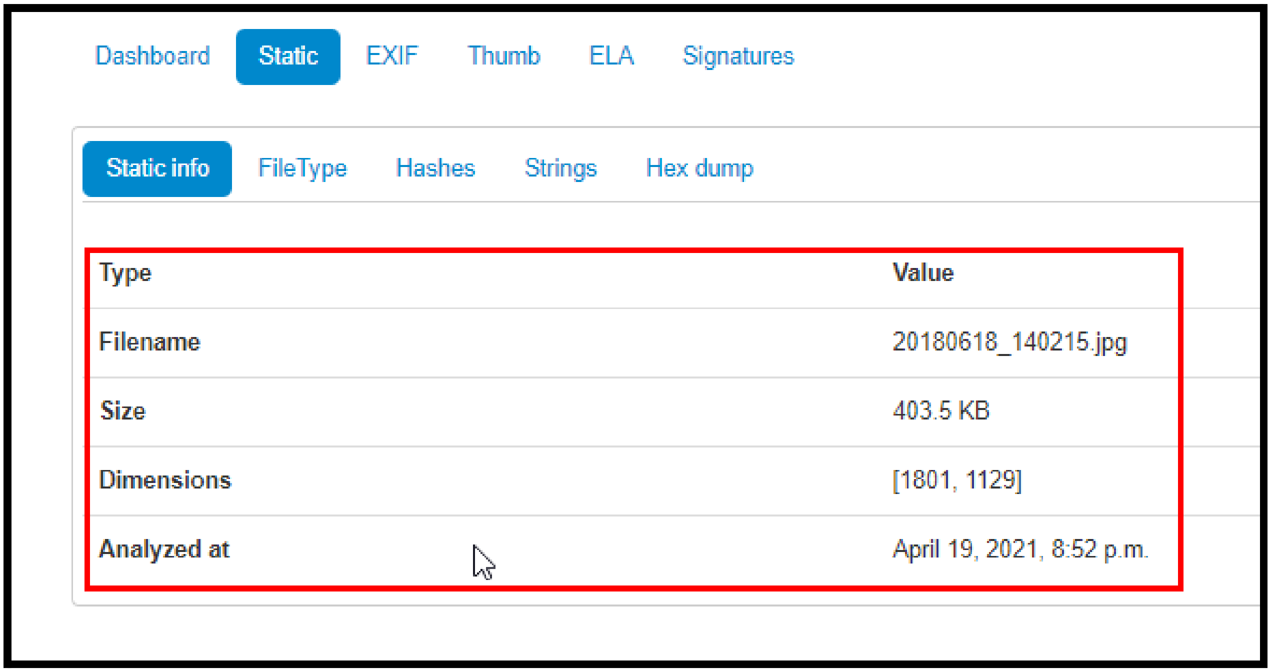
Type	Result
Static analysis	Static data
EXIF metadata extraction	EXIF Metadata
IPTC metadata extraction	No IPTC metadata
XMP metadata extraction	No XMP metadata
Preview extraction from metadata	Preview found
Localization	No GPS data
Error Level Analysis (ELA)	Applicable
Signature check	Signature matches

Now we clicked on the second options offer by the dashboard menu which is Signature results. Which shows us all the signature matched by severity. In case 4 are low, 2 are medium and 1 is high.



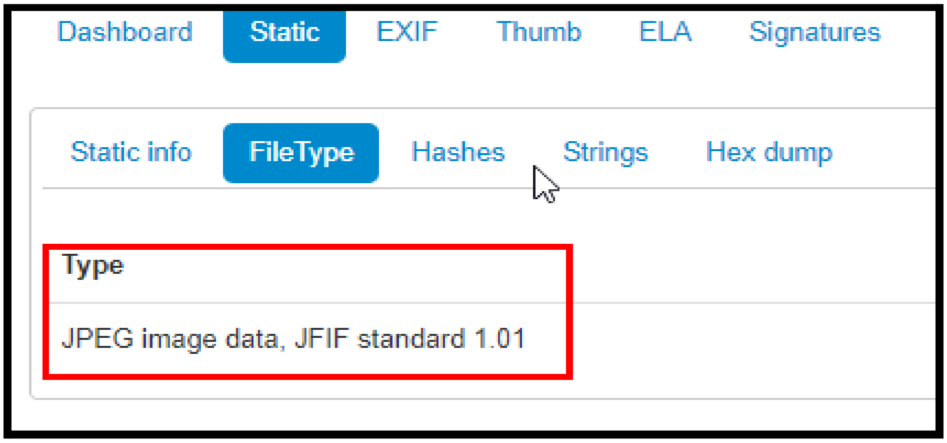
Severity	Signatures matched
Low	4
Medium	2
High	1

In the second tab, we see static and its first option is static info. In the static info option, we see all the basic information about the image.



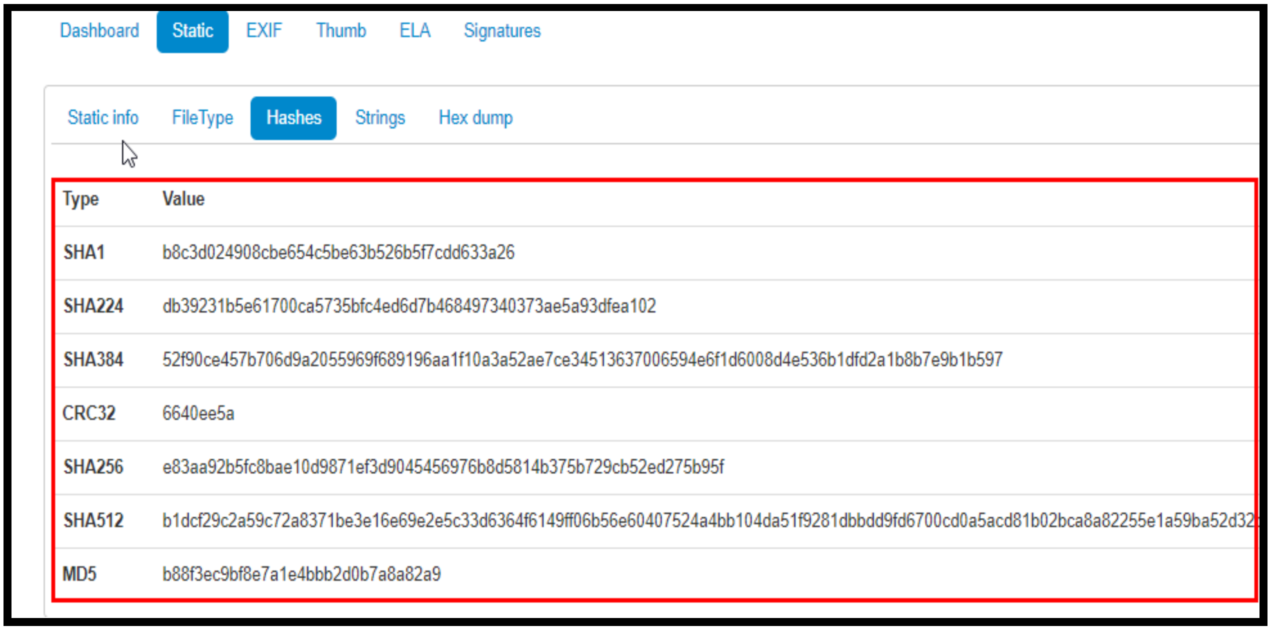
Type	Value
Filename	20180618_140215.jpg
Size	403.5 KB
Dimensions	[1801, 1129]
Analyzed at	April 19, 2021, 8:52 p.m.

the second option which is FileType. Which says it is a jpeg file.JFIF standard



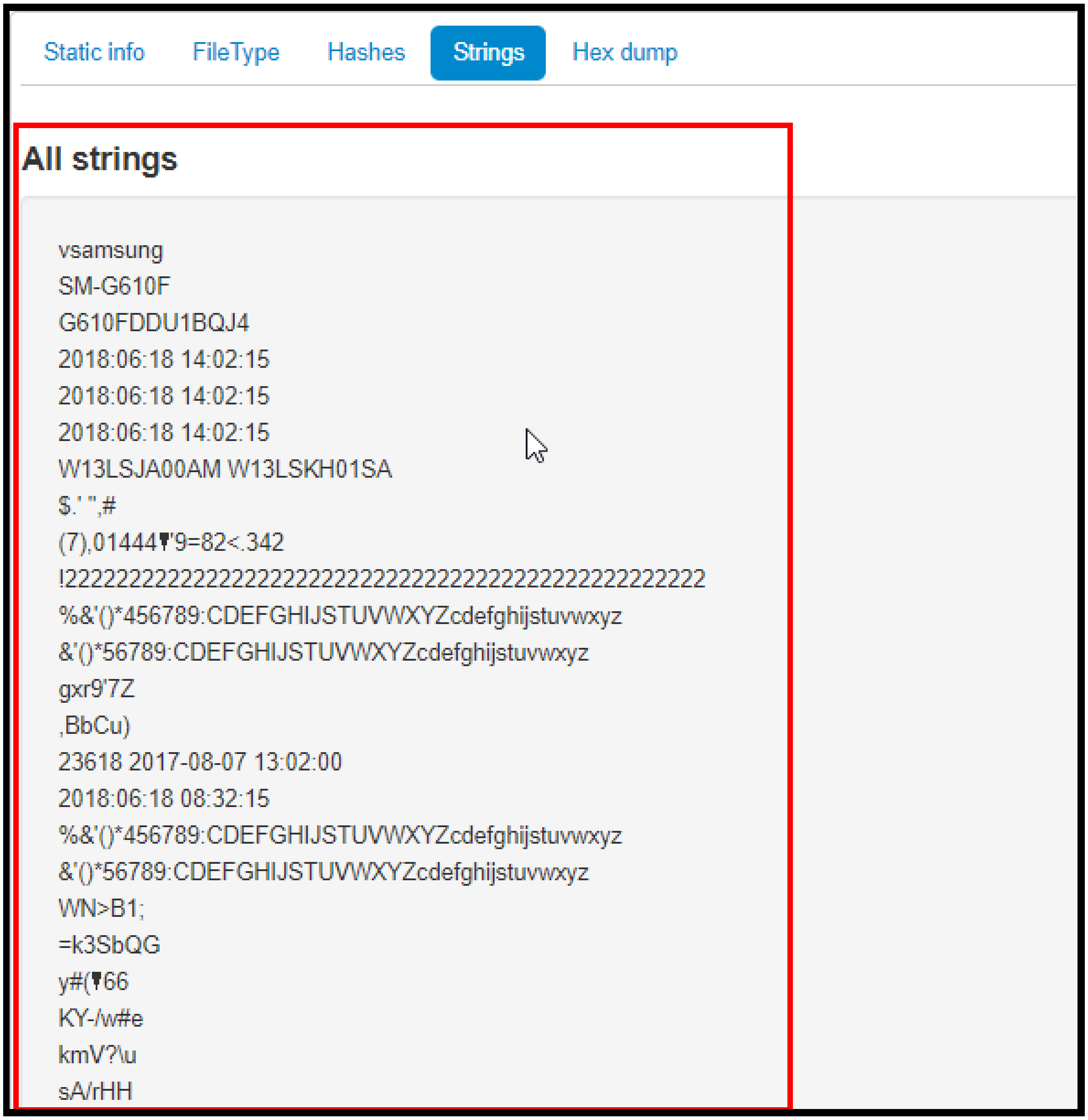
Type
JPEG image data, JFIF standard 1.01

The Third option shows all the Hash values of this file within different algorithms. If we Focus hard we can see that MD5 hash values are the file name, when we clicked on the image for analysis.



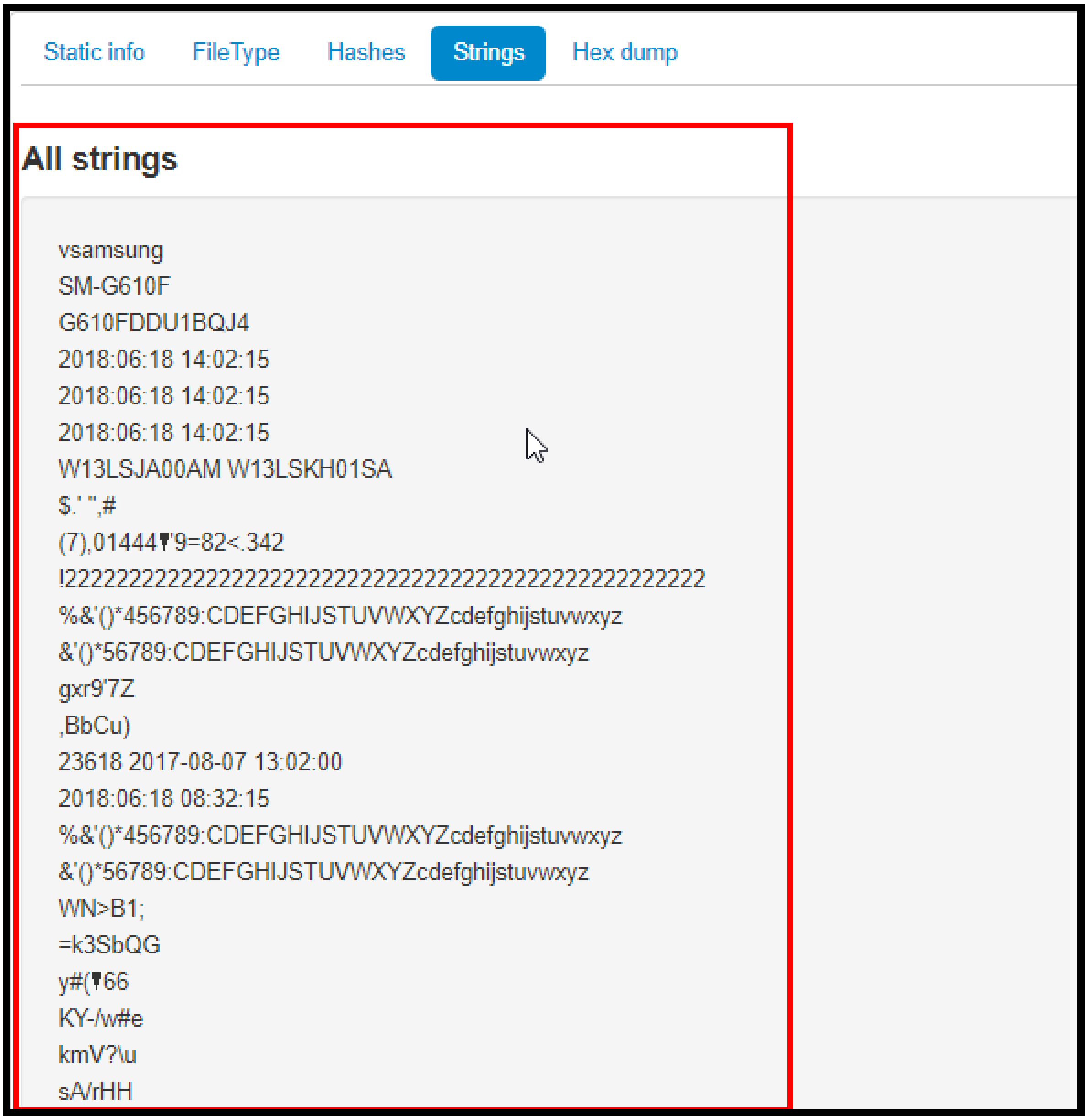
Type	Value
SHA1	b8c3d024908cbe654c5be63b526b5f7cdd633a26
SHA224	db39231b5e61700ca5735bfc4ed6d7b468497340373ae5a93dfea102
SHA384	52f90ce457b706d9a2055969f689196aa1f10a3a52ae7ce34513637006594e6f1d6008d4e536b1dfd2a1b8b7e9b1b597
CRC32	6640ee5a
SHA256	e83aa92b5fc8bae10d9871ef3d9045456976b8d5814b375b729cb52ed275b95f
SHA512	b1dcf29c2a59c72a8371be3e16e69e2e5c33d6364f6149ff06b56e60407524a4bb104da51f9281dbbdd9fd6700cd0a5acd81b02bca8a82255e1a59ba52d32
MD5	b88f3ec9bf8e7a1e4bbb2d0b7a8a82a9

The fourth option which we see is Strings. It will show us all strings behind this image file with the slight details of the metadata of this image file.



All strings

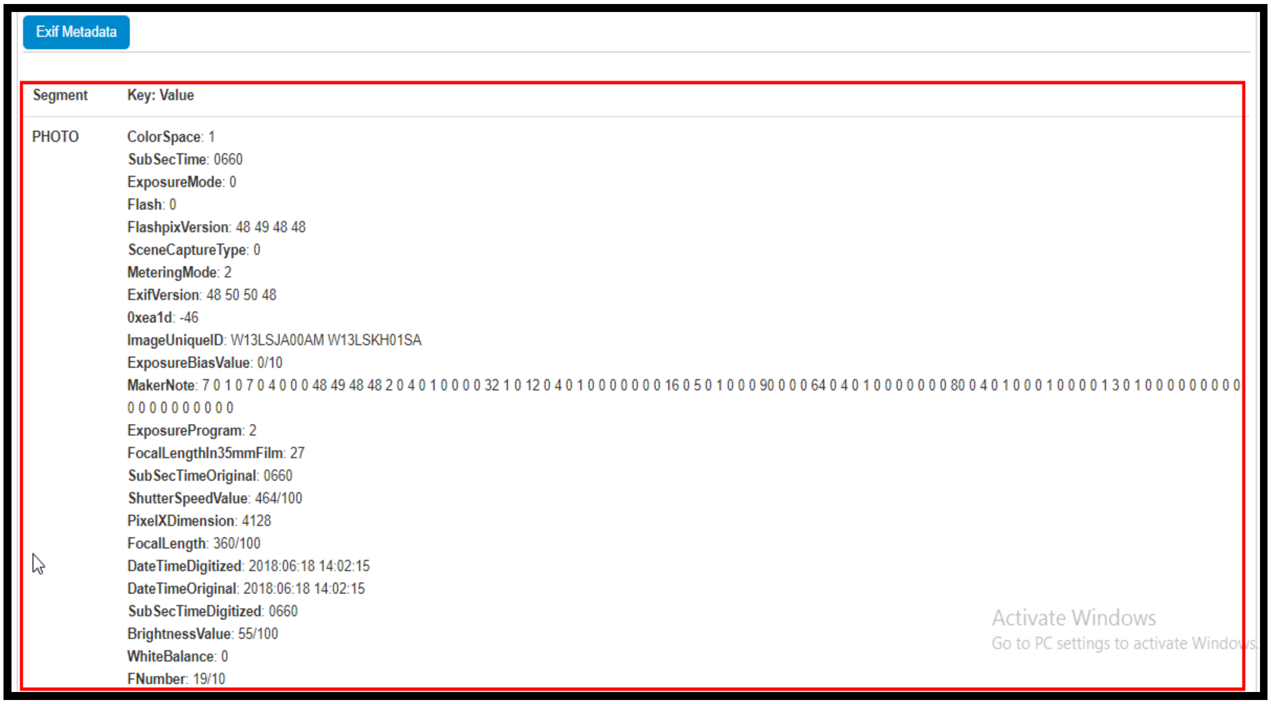
```
vsamsung
SM-G610F
G610FDDU1BQJ4
2018:06:18 14:02:15
2018:06:18 14:02:15
2018:06:18 14:02:15
W13LSJA00AM W13LSKH01SA
$.' ",#
(7),01444▼'9=82<.342
!22222222222222222222222222222222222222222222222222
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
gxr9'7Z
,BbCu)
23618 2017-08-07 13:02:00
2018:06:18 08:32:15
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
WN>B1;
=k3SbQG
y#(▼66
KY-/w#e
kmV?\u
sA/rHH
```



All strings

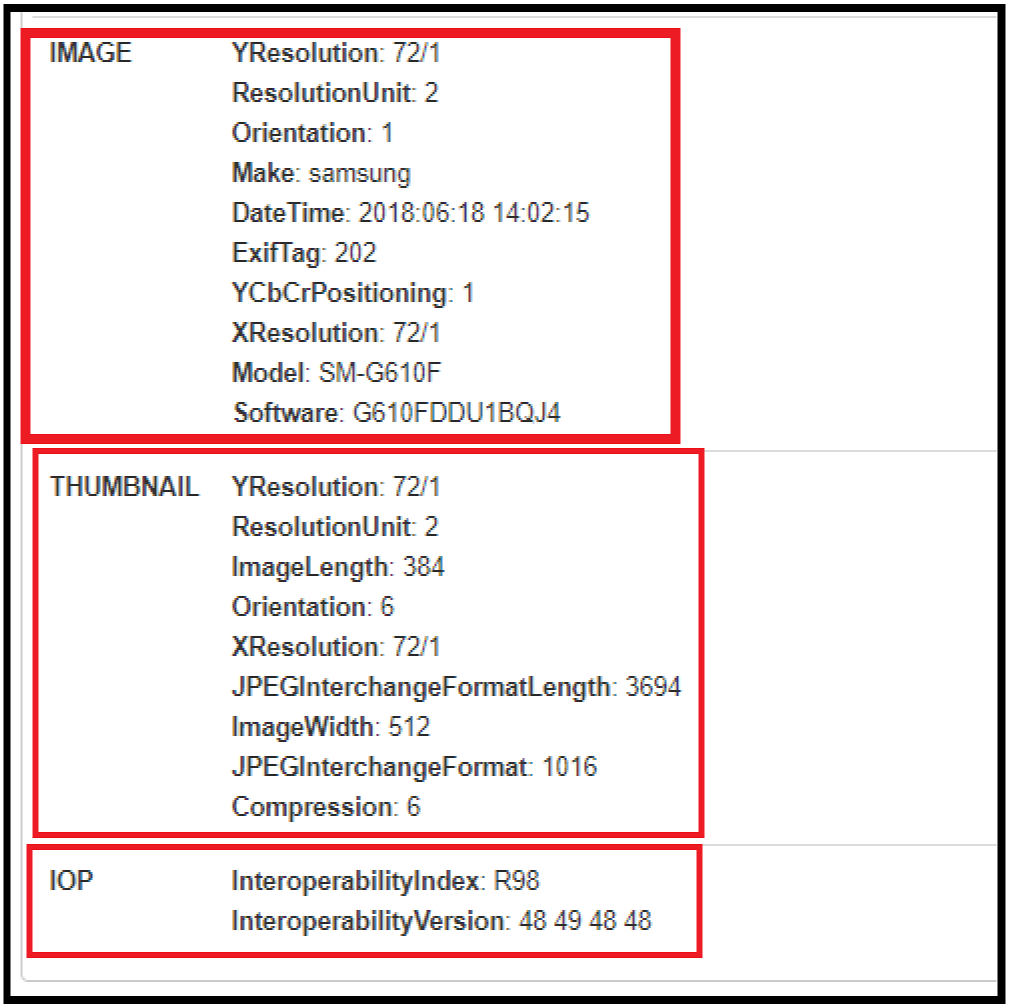
```
vsamsung
SM-G610F
G610FDDU1BQJ4
2018:06:18 14:02:15
2018:06:18 14:02:15
2018:06:18 14:02:15
W13LSJA00AM W13LSKH01SA
$.' ",#
(7),01444▼'9=82<.342
!22222222222222222222222222222222222222222222222222
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
gxr9'7Z
,BbCu)
23618 2017-08-07 13:02:00
2018:06:18 08:32:15
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
WN>B1;
=k3SbQG
y#(▼66
KY-/w#e
kmV?\u
sA/rHH
```

Now switch on the third tab EXIF, which has only one option which says about EXIF the metadata. We get some of the major details for our forensic investigation.



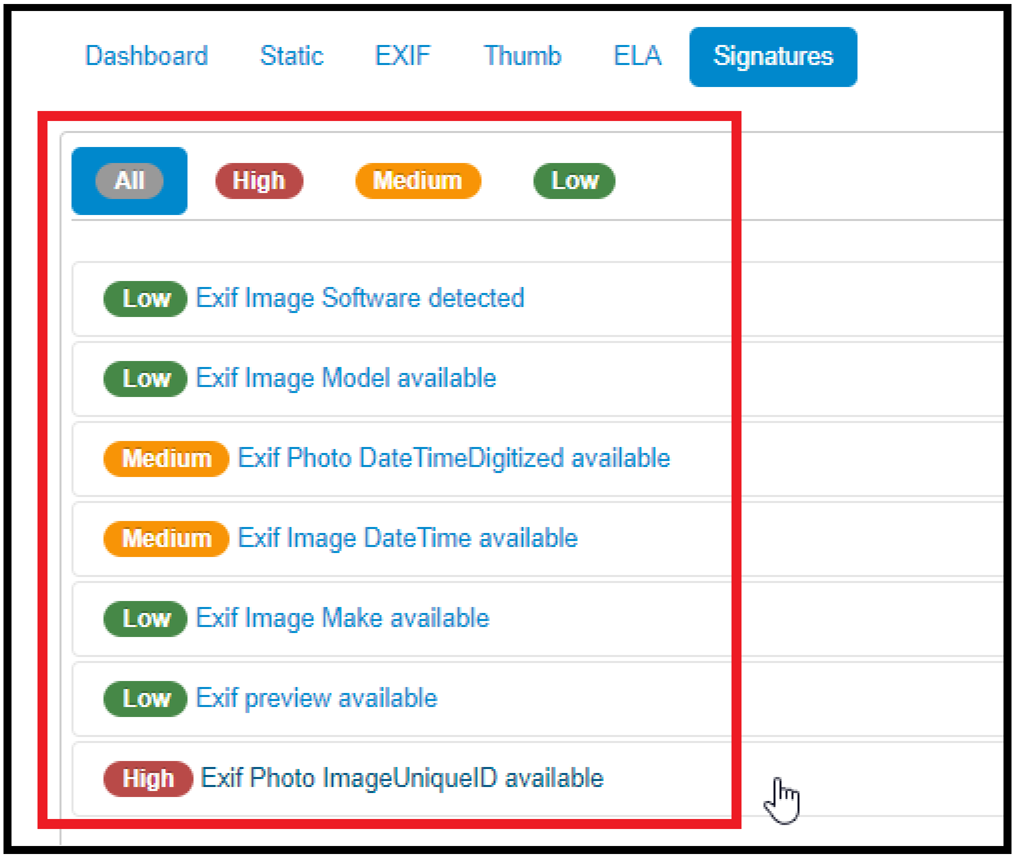
```
Segment   Key: Value

PHOTO     ColorSpace: 1
          SubSecTime: 0660
          ExposureMode: 0
          Flash: 0
          FlashpixVersion: 48 49 48 48
          SceneCaptureType: 0
          MeteringMode: 2
          ExifVersion: 48 50 50 48
          0xea1d: -46
          ImageUniqueID: W13LSJA00AM W13LSKH01SA
          ExposureBiasValue: 0/10
          MakerNote: 7 0 1 0 7 0 4 0 0 0 48 49 48 48 2 0 4 0 1 0 0 0 0 32 1 0 12 0 4 0 1 0 0 0 0 0 0 0 16 0 5 0 1 0 0 0 90 0 0 0 64 0 4 0 1 0 0 0 0 0 0 0 80 0 4 0 1 0 0 0 1 0 0 0 0 1 3 0 1 0 0 0 0 0 0 0 0 0 0
          0 0 0 0 0 0 0 0 0 0
          ExposureProgram: 2
          FocalLengthIn35mmFilm: 27
          SubSecTimeOriginal: 0660
          ShutterSpeedValue: 464/100
          PixelXDimension: 4128
          FocalLength: 360/100
          DateTimeDigitized: 2018:06:18 14:02:15
          DateTimeOriginal: 2018:06:18 14:02:15
          SubSecTimeDigitized: 0660
          BrightnessValue: 55/100
          WhiteBalance: 0
          FNumber: 19/10
```

Scroll down to get full segments of the metadata of image files that can become handy in forensic investigation. Regarding GPS, Thumbnails, and IOP.



```
IMAGE        YResolution: 72/1
             ResolutionUnit: 2
             Orientation: 1
             Make: samsung
             DateTime: 2018:06:18 14:02:15
             ExifTag: 202
             YCbCrPositioning: 1
             XResolution: 72/1
             Model: SM-G610F
             Software: G610FDDU1BQJ4
THUMBNAIL    YResolution: 72/1
             ResolutionUnit: 2
             ImageLength: 384
             Orientation: 6
             XResolution: 72/1
             JPEGInterchangeFormatLength: 3694
             ImageWidth: 512
             JPEGInterchangeFormat: 1016
             Compression: 6
IOP          InteroperabilityIndex: R98
             InteroperabilityVersion: 48 49 48 48
```

The final tab shows us the signature values in the image analysis. Which we already discussed above.



Low Exif Image Software detected

Low Exif Image Model available

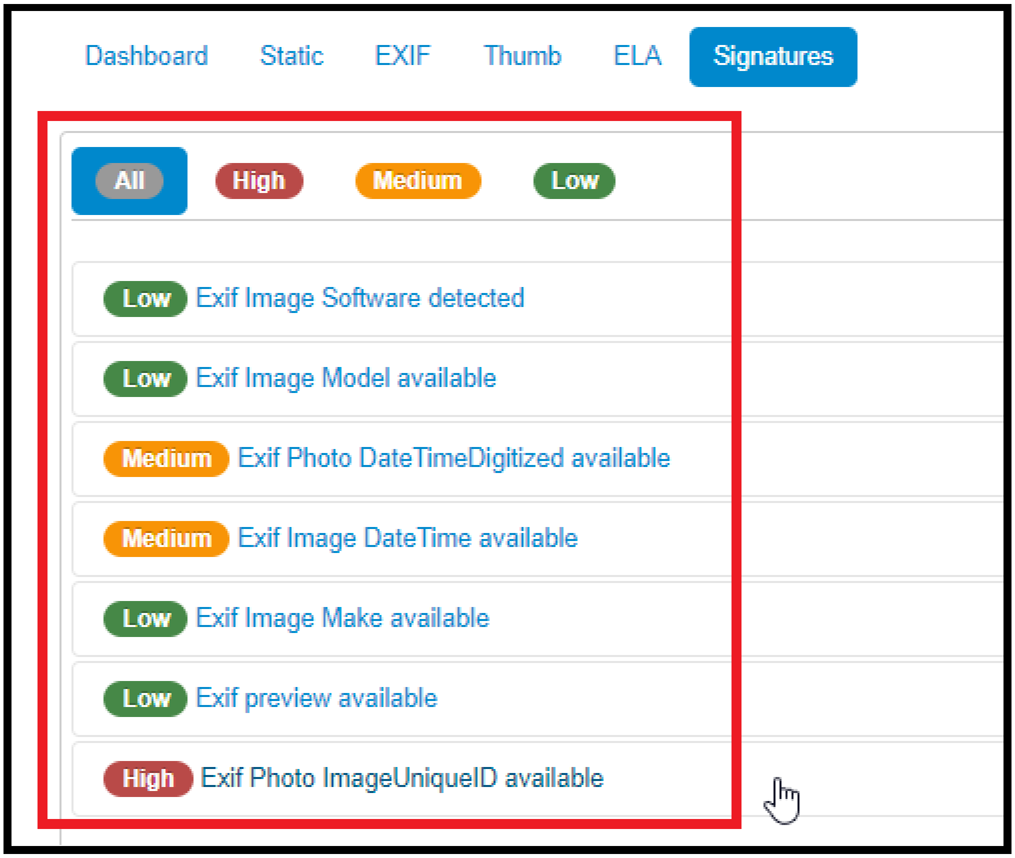
Medium Exif Photo DateTimeDigitized available

Medium Exif Image DateTime available

Low Exif Image Make available

Low Exif preview available

High Exif Photo ImageUniqueID available



Low Exif Image Software detected

Low Exif Image Model available

Medium Exif Photo DateTimeDigitized available

Medium Exif Image DateTime available

Low Exif Image Make available

Low Exif preview available

High Exif Photo ImageUniqueID available

We can export report in html and pdf

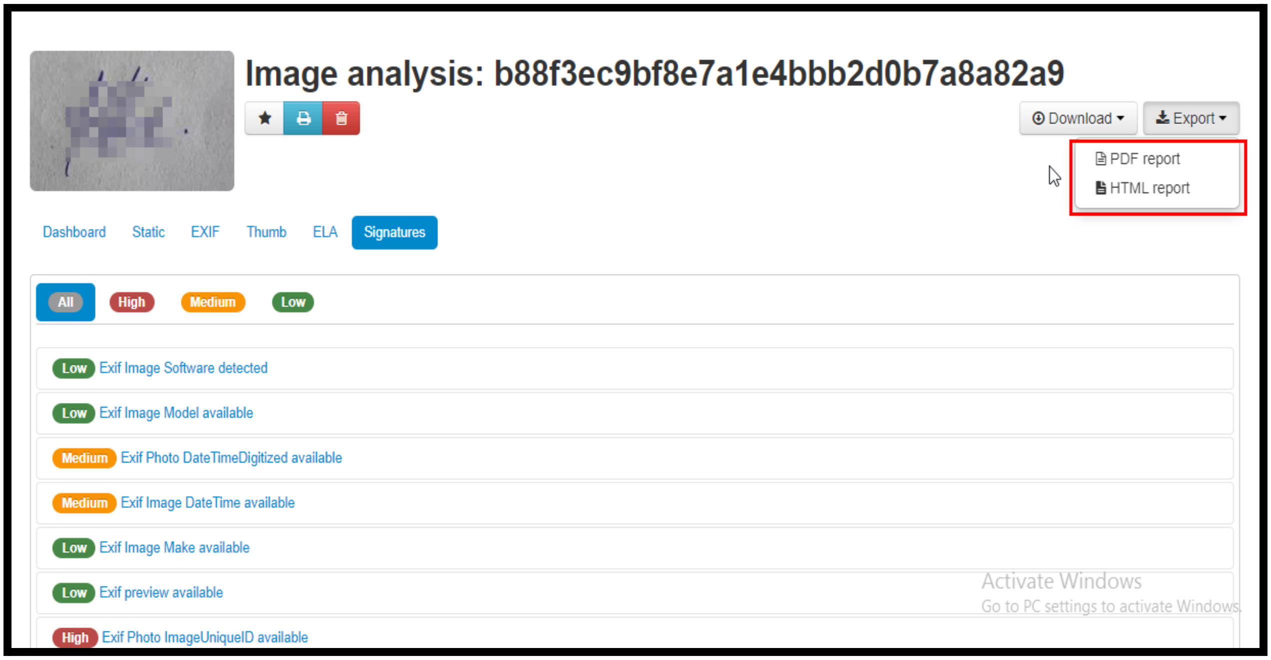


Image analysis: b88f3ec9bf8e7a1e4bbb2d0b7a8a82a9

Low Exif Image Software detected

Low Exif Image Model available

Medium Exif Photo DateTimeDigitized available

Medium Exif Image DateTime available

Low Exif Image Make available

Low Exif preview available

High Exif Photo ImageUniqueID available