

Forensic Image 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 an kind of analysis data.

The main features of Ghiro :

- **Metadata Extraction** : Metadata is divided into several categories depending on the standard where it comes from. Image metadata is 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 is detected to know the image type we are dealing with, in both contracted and extended form.
- **ELA** : ELA stands for Error Level Analysis. 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, 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.
- **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. I recommend the “OVA” version because it’s the fastest way to start using Ghiro.

After downloading the Ghiro, in a few minutes, we’ll have a fully functional Ghiro setup to start analyzing our images.

To download the Ghiro image analysis tool, click on this link :

<https://www.getghiro.org/>

After importing the OVA file in Virtual Box or VMWare, a screen similar to this pops up.

```
#####
# Welcome to Ghiro Appliance! #
#####

HOW TO START
-----

Appliance IP address is: 192.168.29.61
To start using Ghiro point your browser to http://192.168.29.61

Default credentials:
  username: ghiro
  password: ghiromanager

*** Remember to change the password at your first access. ***
ghiroappliance login: ghiro
Password:
Last login: Tue Apr  9 19:05:55 UTC 2024 on tty1
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.19.0-25-generic i686)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

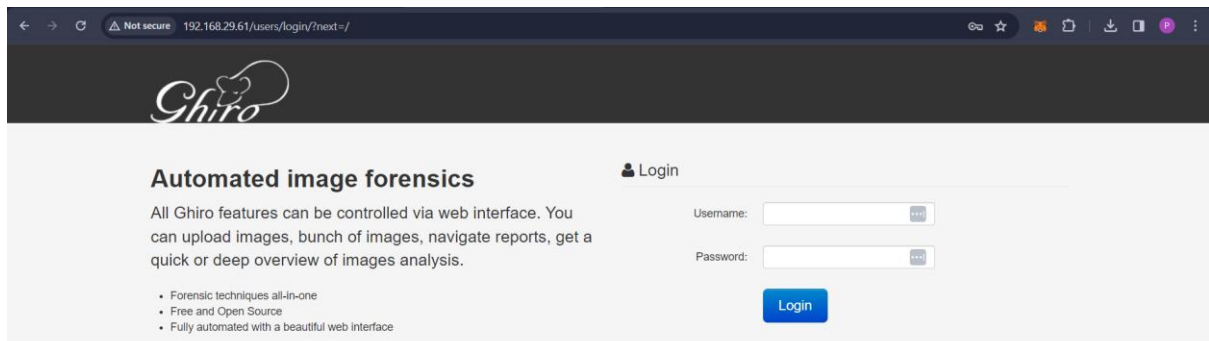
ghiro@ghiroappliance:~$ _
```

Notice the default credentials :

Username : ghiro

Password : ghiromanager

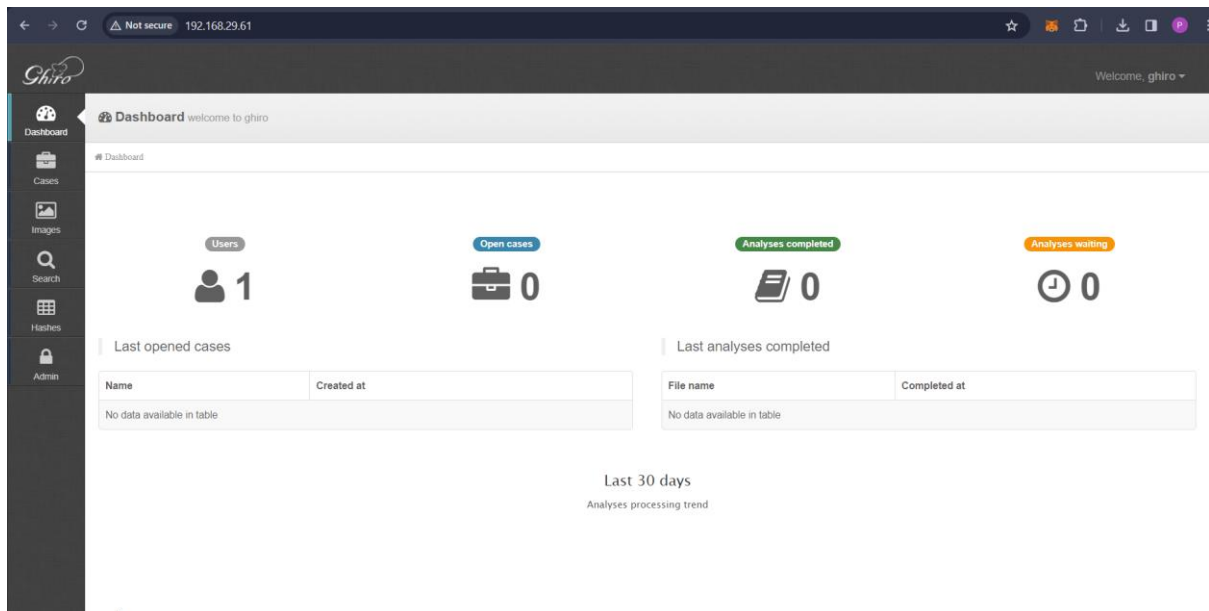
Now, open the Appliance IP Address in your browser.



Now, we can see that we successfully set up the Ghiro, the dashboard in the home screen says that *Welcome, ghiro* which confirms that our setup is successful.

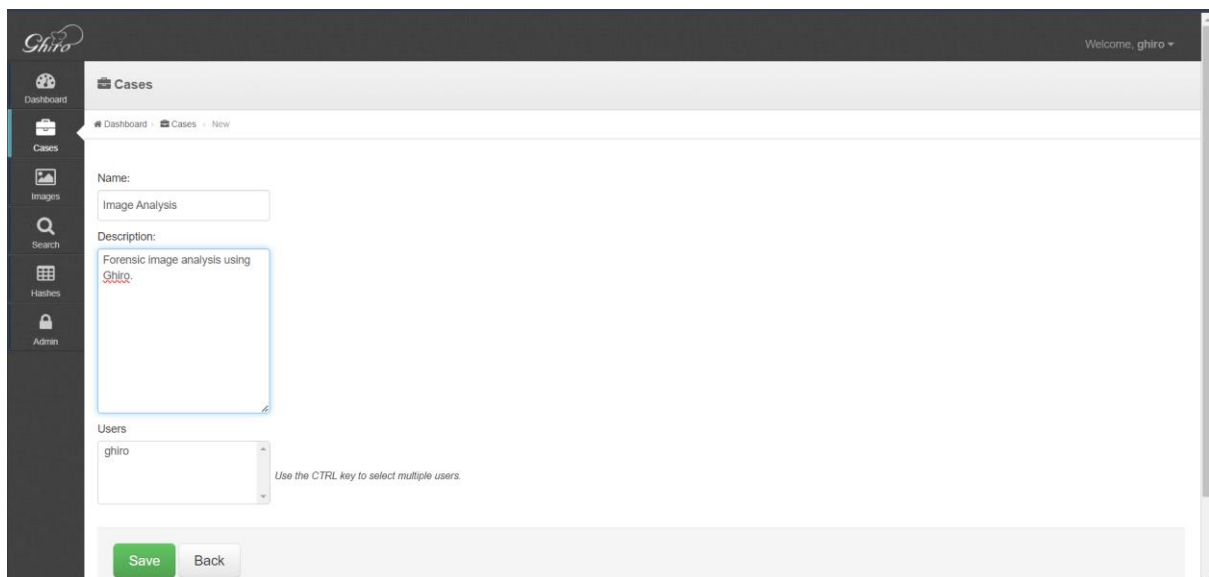
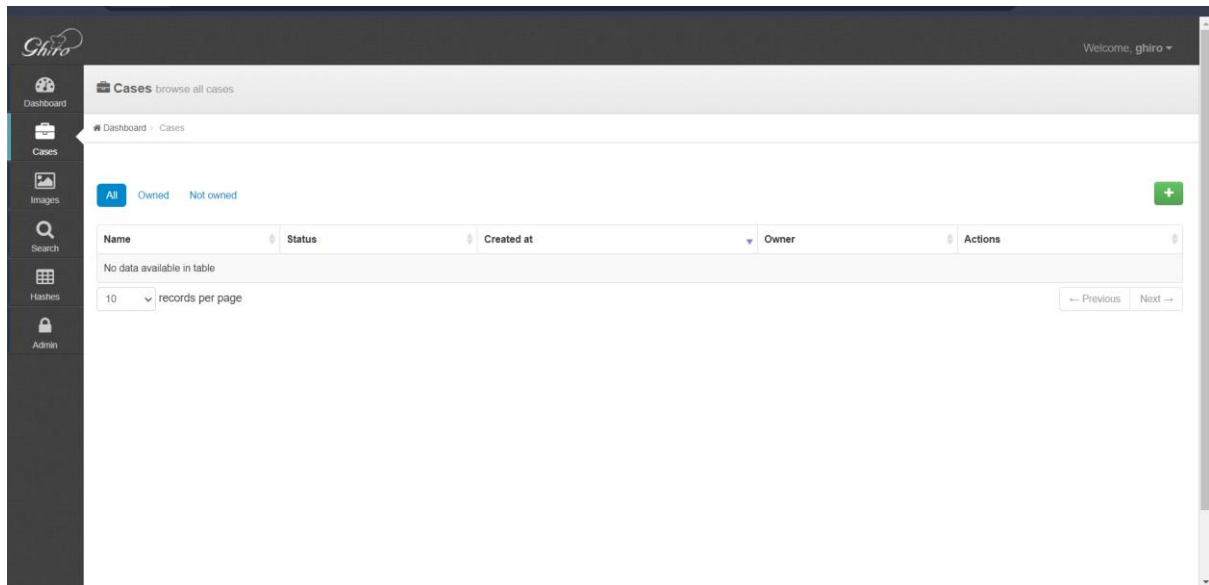
Go to the profile section and change the default password to a password of your choice.

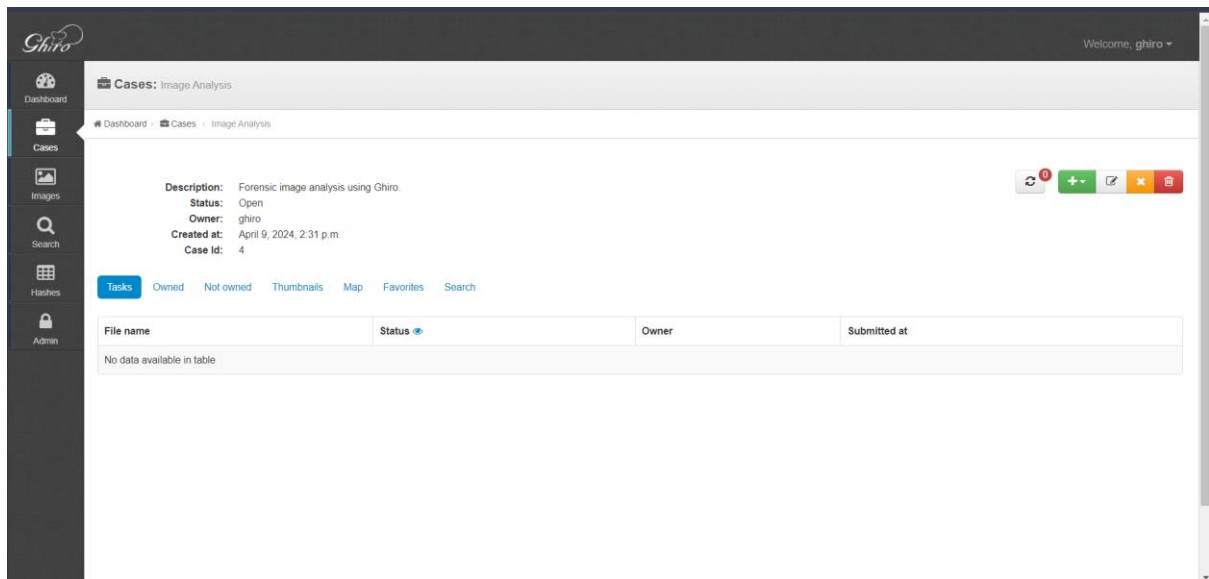
As we can see that it has the user : ghiro, through which we log in to the software. At the initial point, it shows zero cases and zero analyses left because we just set up this software.



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

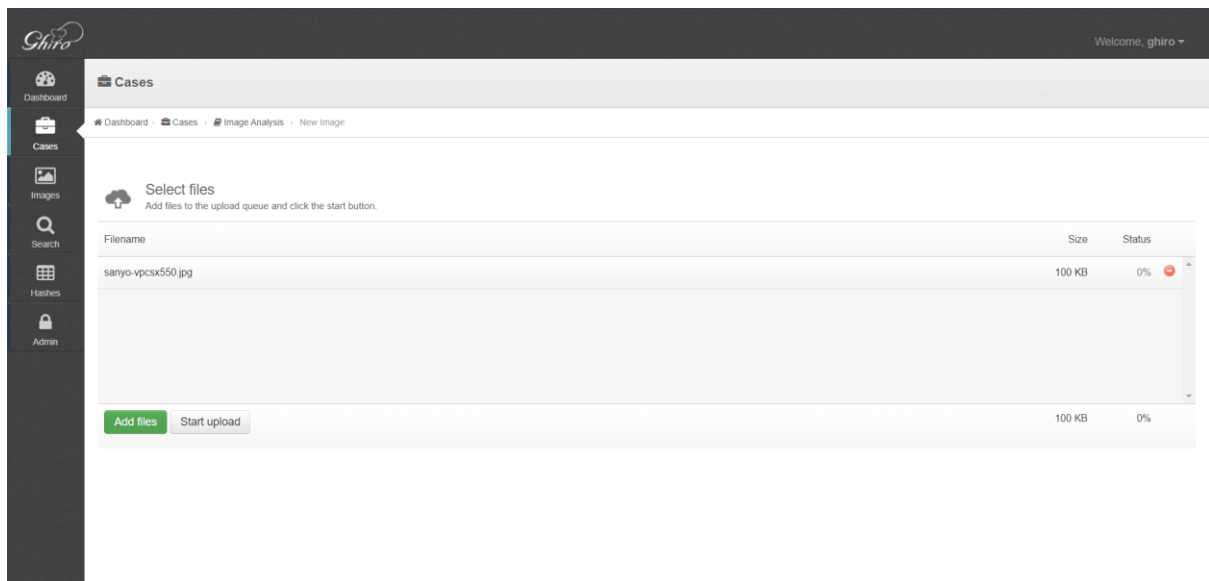
Now, we need to fill up the details regarding the forensic case like **case name**, **case description** and it's **Investigation user**.



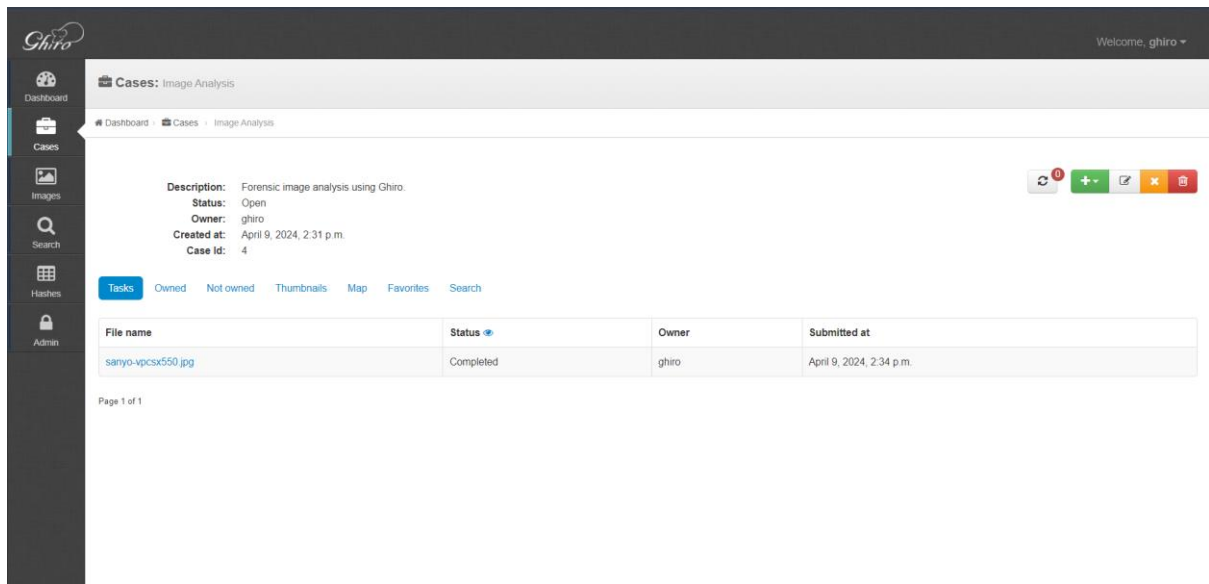


After saving the details regarding the forensic case, it will confirm these details and ask us to add images to analysis. To add images, click **[+]** button.

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



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



We can see that the file upload process is just finished. Now we have two options to analyze the image. The first option is to directly 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 the details of.

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.

Dashboard Static EXIF Thumb ELA Signatures	
Analysis results Signature results	
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 keep clicking on all the options and see the analysis results. Let's click on the second option offered by the dashboard menu which is Signature results. It shows us all the signatures matched by severity. In this case, there are 4 low and 4 medium.



In the second tab, we have static and it's first option is static info. Here, we see all the basic information about the image.

Dashboard Static EXIF Thumb ELA Signatures

Static info FileType Hashes Strings Hex dump

Type	Value
Filename	sanyo-vpcsx550.jpg
Size	100.0 KB
Dimensions	[640, 480]
Analyzed at	April 9, 2024, 2:34 p.m.
Comment	Et voila. For starters we have warmed goats cheese in breadcrumbs on a herb salad base...

The second option is filetype. It says here that the image is of type JPEG in the EXIF standard.

Dashboard Static EXIF Thumb ELA Signatures

Static info FileType Hashes Strings Hex dump

Type
JPEG image data, EXIF standard 2.1, comment: "Et voila. For starters we have warmed goats cheese in breadcru"

The third option shows us 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.

[Dashboard](#)[Static](#)[EXIF](#)[Thumb](#)[ELA](#)[Signatures](#)[Static info](#)[FileType](#)[Hashes](#)[Strings](#)[Hex dump](#)

Type	Value
SHA1	50f27a33962f80783eef3194c0275af77a8d4acf
SHA224	13c8181e9916c393b28b9f83969d2829223462692f8dcf143291d75b
SHA384	167cc3d19858edfcb552b4493de9fbbb6ef0c62b7e4b8a672d462e178f51d99ae43a1a8f425516ee
CRC32	83b62501
SHA256	74401cc6e0b6bdb03b7d3a1c99a0ba3b4dd5b3ac9b7728a38f6fb3607f3360ea
SHA512	1c5694369484f25eab6ed90ca20e59a97d7b9b88d973ce0d2fed2cbdc2826873e3beee9cd8c5427
MD5	8725ea397962d75216499319d5137ab2

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

[Dashboard](#)[Static](#)[EXIF](#)[Thumb](#)[ELA](#)[Signatures](#)[Static info](#)[FileType](#)[Hashes](#)[Strings](#)[Hex dump](#)

All strings

SANYO DIGITAL CAMERA
SANYO Electric Co.,Ltd.
SX113
V113p-73
2000:11:18 21:14:19
2000:11:18 21:14:19
2000:11:18 21:14:19

%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
]4)gx&
lu}uc`
t]SOub
mduR>VC
pj8}GU
7uube{6M
lu=/PG2?
dG"N71
/q Y"7
<F*5v]m
<awqkb
8^z~\W
6\$Dp~_s
[*G/ /

The next option is Hex dump.

Static info	FileType	Hashes	Strings	Hex dump
0000	FF D8 FF E1 37 E8 45 78 69 66 00 00 49 49 2A 00 08 00 00 00 0B 00 0E 01 02 00 15 00 00			
0020	00 00 0F 01 02 00 18 00 00 00 B2 00 00 00 10 01 02 00 07 00 00 00 CA 00 00 00 12 01 03			
0040	00 00 01 00 00 00 1A 01 05 00 01 00 00 00 D8 00 00 00 1B 01 05 00 01 00 00 00 E0 00 00			
0060	03 00 01 00 00 00 02 00 00 00 31 01 02 00 09 00 00 00 E8 00 00 00 32 01 02 00 14 00 00			
0080	00 00 13 02 03 00 01 00 00 00 02 00 00 00 69 87 04 00 01 00 00 00 1C 01 00 00 00 03 00			
00A0	4E 59 4F 20 44 49 47 49 54 41 4C 20 43 41 4D 45 52 41 00 00 00 00 00 00 00 00 00 00 00			
00C0	4E 59 4F 20 45 6C 65 63 74 72 69 63 20 43 6F 2E 2C 4C 74 64 2E 00 53 58 31 31 33 20 00			
00E0	00 00 00 00 48 00 00 00 01 00 00 00 48 00 00 00 01 00 00 00 56 31 31 33 70 2D 37 33 00			
0100	00 32 30 30 30 3A 31 31 3A 31			
0120	31 3A 31 34 3A 31 39 00 16 00 9A 82 05 00 01 00 00 00 2A 02 00 00 9D 82 05 00 01 00 00			
0140	00 00 27 88 03 00 01 00 00 00 90 01 00 00 00 90 07 00 04 00 00 00 30 32 31 30 03 90 02			
0160	00 00 3A 02 00 00 04 90 02 00 14 00 00 00 4E 02 00 00 01 91 07 00 04 00 00 00 01 02 03			
0180	05 00 01 00 00 00 62 02 00 00 04 92 0A 00 01 00 00 00 6A 02 00 00 05 92 05 00 01 00 00			
01A0	00 00 07 92 03 00 01 00 00 00 02 00 00 00 08 92 03 00 01 00 00 00 00 00 00 00 09 92 03			
01C0	00 00 00 00 00 00 0A 92 05 00 01 00 00 00 7A 02 00 00 7C 92 07 00 B2 00 00 00 7C 03 00			
01E0	07 00 7D 00 00 00 82 02 00 00 00 A0 07 00 04 00 00 00 30 31 30 30 01 A0 03 00 01 00 00			
0200	00 00 02 A0 04 00 01 00 00 00 80 02 00 00 03 A0 04 00 01 00 00 00 E0 01 00 00 05 A0 04			
0220	00 00 5E 03 00 00 00 A3 07 00 01 00 00 00 03 00 00 00 00 00 00 00 0A 00 00 00 E3 01 00			
0240	00 00 0A 00 00 00 32 30 30 30 3A 31 31 3A 31 38 20 32 31 3A 31 34 3A 31 39 00 32 30 30			
0260	31 3A 31 38 20 32 31 3A 31 34 3A 31 39 00 11 00 00 00 0A 00 00 00 00 00 00 00 0A 00 00			

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

LightSource: 0
ColorSpace: 1
Flash: 0
FlashpixVersion: 48 49 48 48
MeteringMode: 2
ExifVersion: 48 50 49 48
ExposureBiasValue: 0/10
MakerNote: 83 65 78 89 79 0 1 0 6 0 0 2 4 0 3 0 0 0 2 10 3 0 0 1 2 3 0 1 0 0 0 2 1 0 0 2 2
 3 0 1 0 0 0 0 0 0 0 3 2 3 0 1 0 0 0 0 0 0 0 4 2 5 0 1 0 0 0 2 2 2 3 0 0 0 1 5 4 0 1 8 0 0 0 2 3 0 3
 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 4 0 8 4 0 0 1 9 1 9 4 0 0
 3 2 4 8 0 0 0 0 0 0 0 0 0 0 0 1 1 1 3 7 1 5 9 5 7 1 9 1 2 2 4 0 0 4 0 9 3 8 0 1 9 3 8 2 4 0 0 0 0 0 0 0 0 0 0
 0 0 6 9 5 6 8 0 1 9 3 0 0 0 0 0 0 0 0 0 0 0 7 1 0 2 0 8
PixelXDimension: 640
FocalLength: 60/10
DateTimeDigitized: 2000:11:18 21:14:19
DateTimeOriginal: 2000:11:18 21:14:19
UserComment:
CompressedBitsPerPixel: 17/10
FNumber: 24/10
PixelYDimension: 480
ComponentsConfiguration: 1 2 3 0
ISO Speed Ratings: 400
ExposureTime: 10/483
FileSource: 3
MaxApertureValue: 2/1

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

FileSource: 3
MaxApertureValue: 3/1
InteroperabilityTag: 862

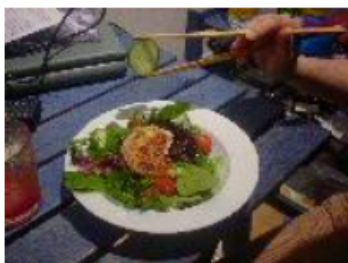
IMAGE YResolution: 72/1
ResolutionUnit: 2
Orientation: 1
Make: SANYO Electric Co.,Ltd.
ImageDescription: SANYO DIGITAL CAMERA
DateTime: 2000:11:18 21:14:19
ExifTag: 284
YCbCrPositioning: 2
XResolution: 72/1
Model: SX113
Software: V113p-73

THUMBNAIL YResolution: 72/1
ResolutionUnit: 2
Compression: 6
XResolution: 72/1
JPEGInterchangeFormatLength: 13234
JPEGInterchangeFormat: 1070

IOP InteroperabilityIndex: R98
InteroperabilityVersion: 48 49 48 48

Dashboard Static EXIF **Thumb** ELA Signatures

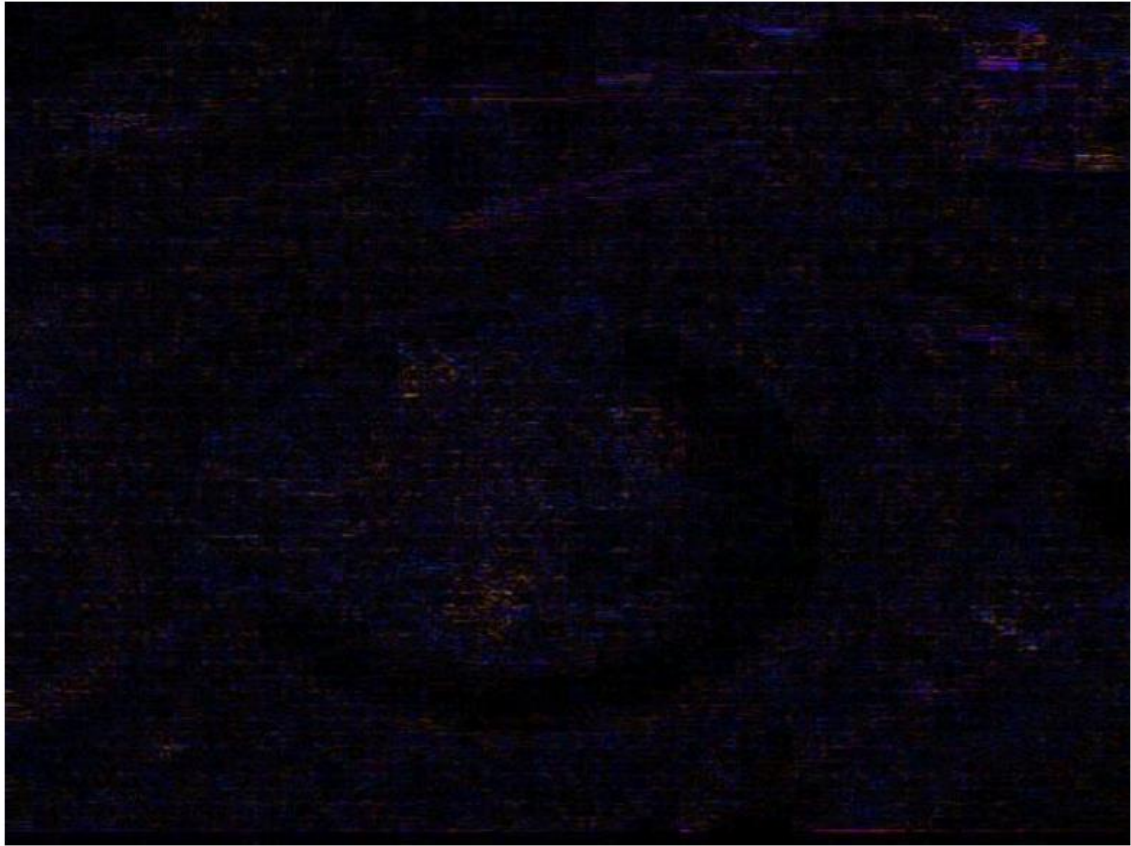
Previews



Size: 13234 bytes
Mime type: image/jpeg
Extension: .jpg
Dimension: [160L, 120L]

Dashboard Static EXIF Thumb **ELA** Signatures

ELA



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

[Dashboard](#) [Static](#) [EXIF](#) [Thumb](#) [ELA](#) [Signatures](#)

[All](#) [Medium](#) [Low](#)

Low

Exif Image Software detected

Low

Exif Image Model available

Medium

Exif Photo DateTimeDigitized available

Medium

Exif Image DateTime available

Medium

Exif Photo UserComment available

Low

Exif Image Make available

Low

Exif preview available

Medium

Exif Image ImageDescription available

At last, we can export the report of our investigation in html or pdf format.



Image analysis:

8725ea397962d75216499319d5137ab2

★

🖨️

🗑️

Download

Export

PDF report

HTML report

[Dashboard](#) [Static](#) [EXIF](#) [Thumb](#) [ELA](#) [Signatures](#)

[All](#) [Medium](#) [Low](#)