

# Forensic Investigation: Ghiro for Image Analysis

July 16, 2020 By Raj Chandel

In this article, we will learn how we can use the Ghiro image analysis tool in forensic investigation. Ghiro is a digital image forensic tool. Which is fully automated and opensource.

## Table of Content

- **What is Ghiro?**
- **Features of Ghiro**
- **Setup the Ghiro**
- **Working on case 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.

To know more about the Ghiro image analysis tool you click [here](#).

## 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 the 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 [here](#).

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

**IP address: 192.168.0.7**

We can use this detail to trigger our software.

Default credentials to log in Ghiro are

Username: ghiro

Password: ghiromanager

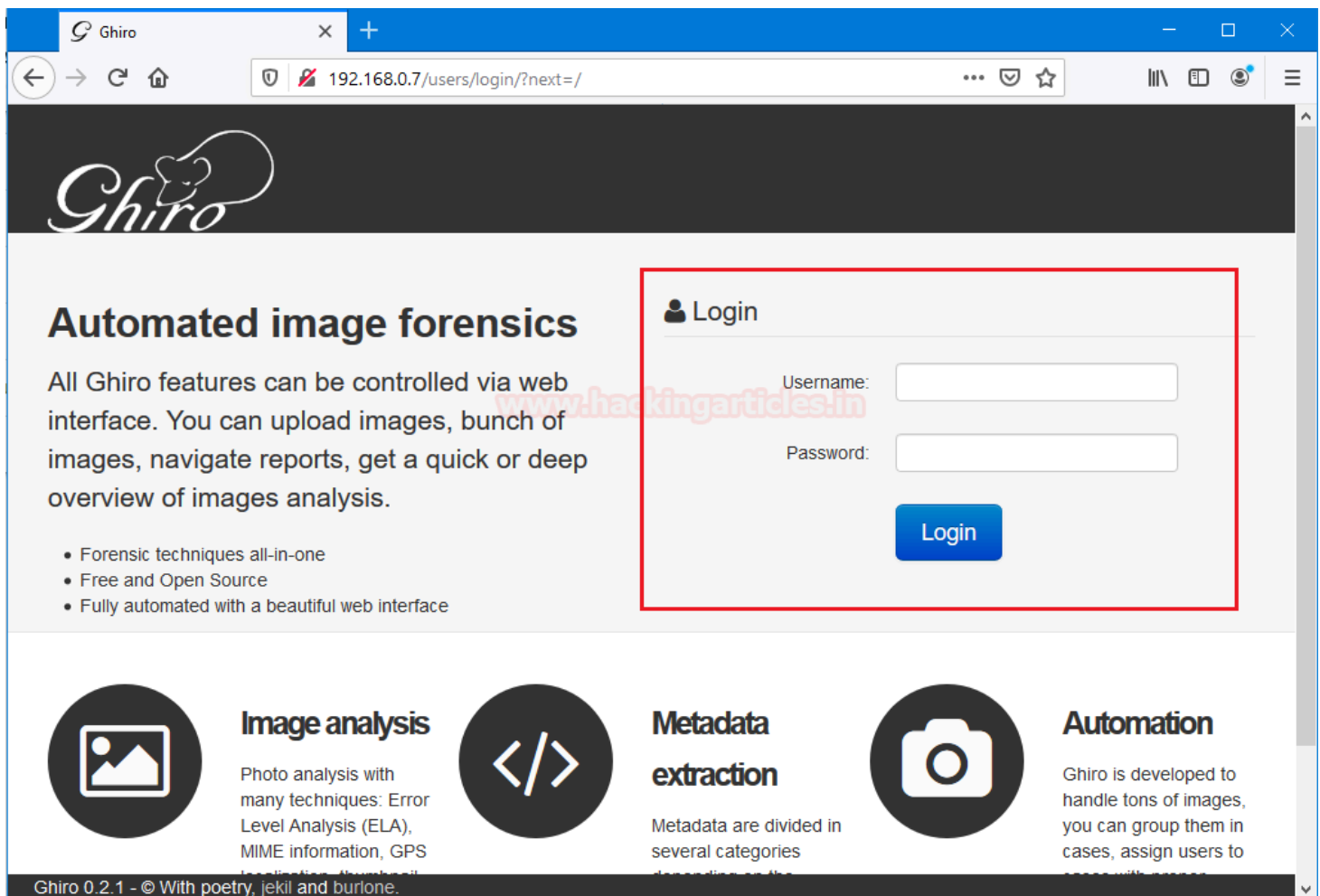
```
#####
# Welcome to Ghiro Appliance! #
#####

HOW TO START
-----

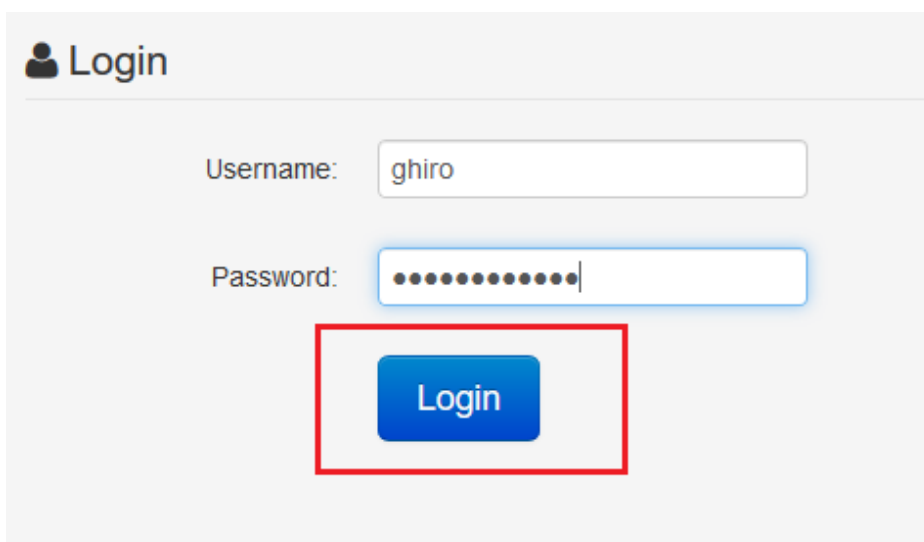
Appliance IP address is: 192.168.0.7
To start using Ghiro point your browser to http://192.168.0.7

Default credentials:
username: ghiro
password: ghiromanager
```

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

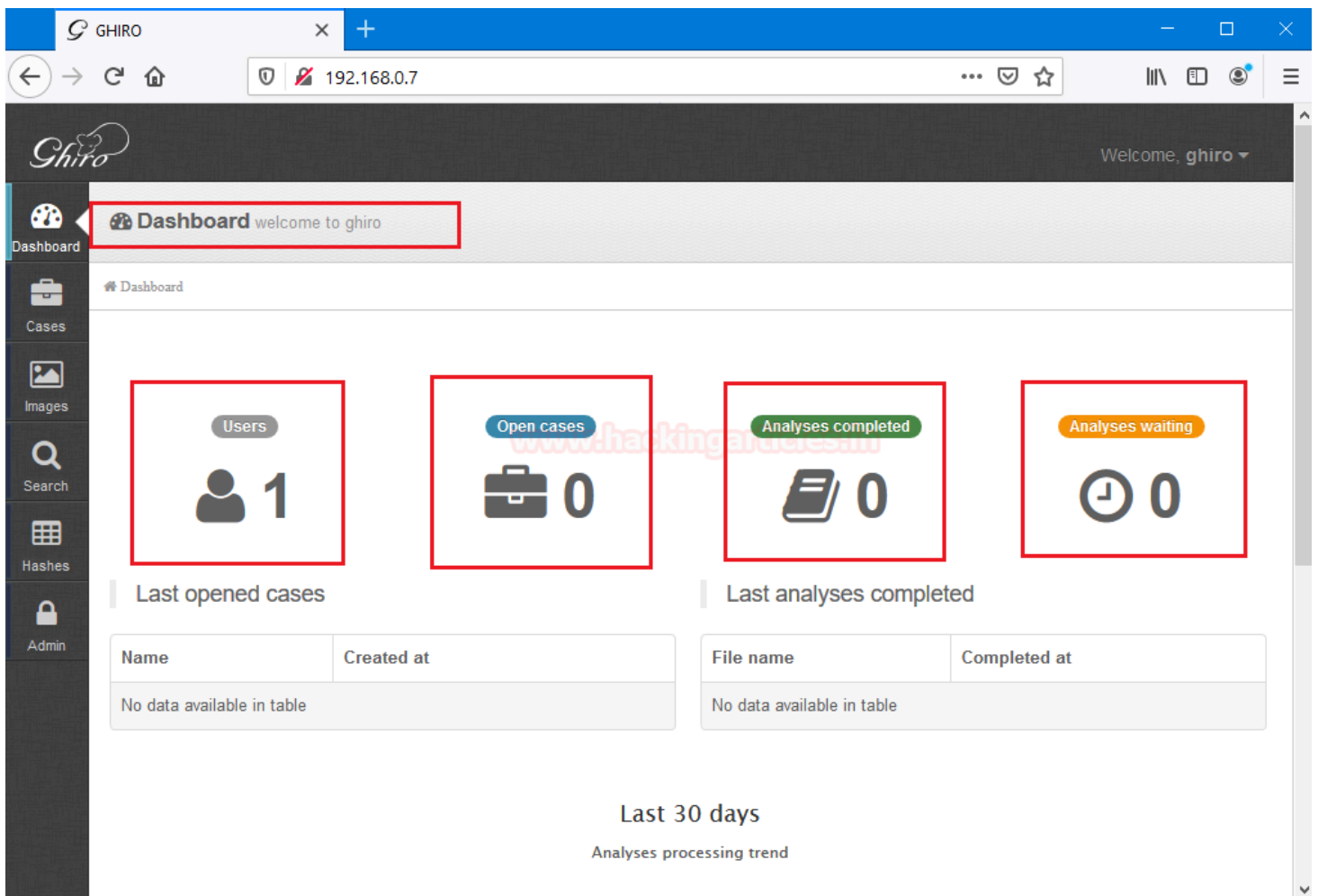


Straight away we focus on the login screen and fill up its credentials. After filling up the details click on the login button.



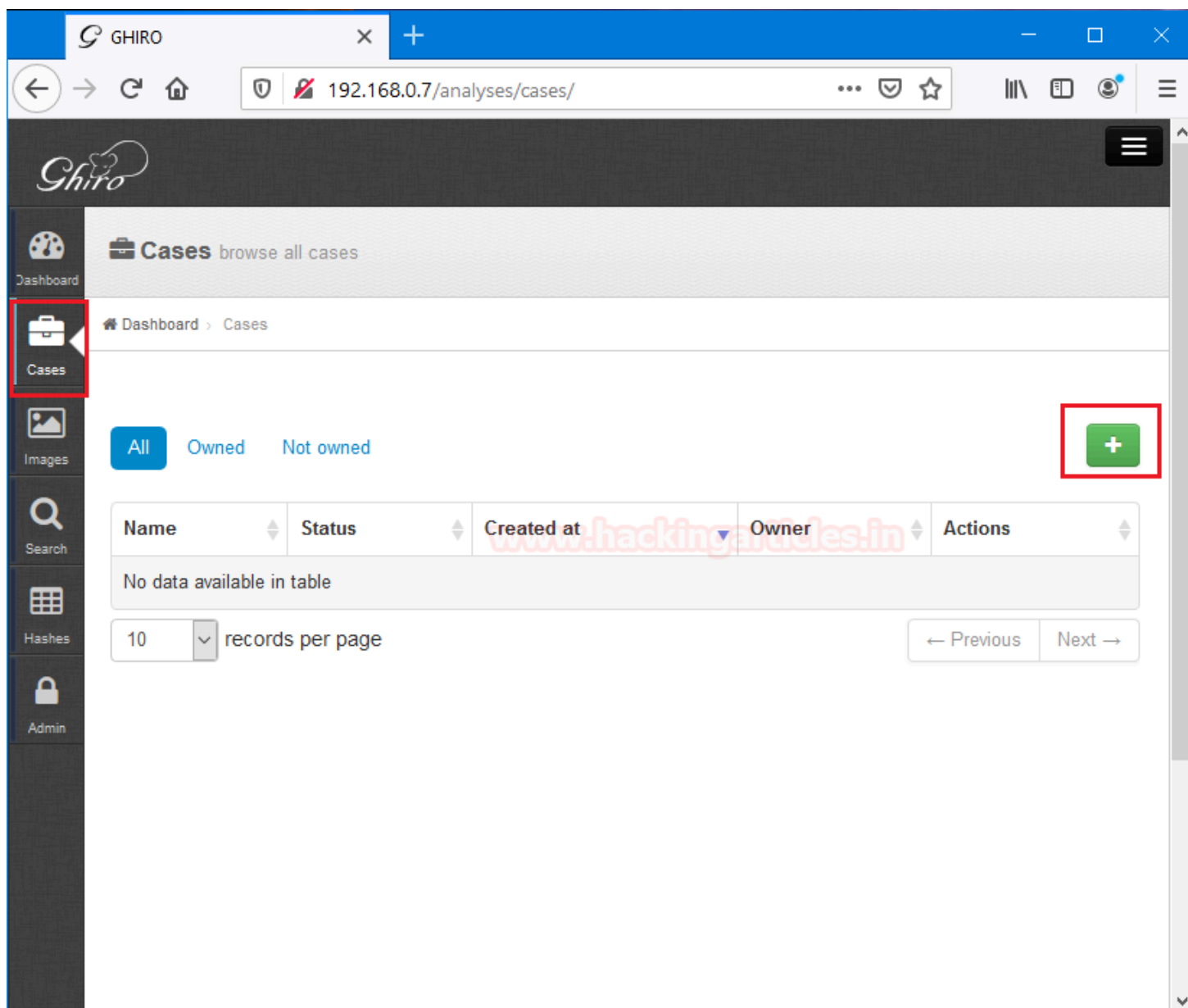
Now, we can see that we successfully set up the Ghiro, the dashboard in the home screen says that welcome to Ghiro, Which confirms that our setup is successful.

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.



## Working with Ghiro

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.

The screenshot shows the GHIRO web application interface. The browser address bar displays the URL `192.168.0.7/analyses/cases/new/`. The application has a dark sidebar with navigation links: Dashboard, Cases, Images, Search, Hashes, and Admin. The main content area is titled 'Cases' and shows a breadcrumb trail: Dashboard > Cases > New. The form contains the following fields:

- Name:** A text input field containing 'Case 1'.
- Description:** A text area containing 'Image Analysis'.
- Users:** A dropdown menu with 'ghiro' selected. A note below the dropdown states: 'Use the CTRL key to select multiple users.'

At the bottom of the form, there are two buttons: a green 'Save' button and a grey 'Back' button. The 'Save' button is highlighted with a red rectangular box.

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.

GHIRO

192.168.0.7/analyses/cases/show/1/list/

**Cases: Case 1**

Dashboard > Cases > Case 1

Description: Image Analysis

Status: Open

Owner: ghiro

Created at: July 12, 2020, 11:02 a.m.

Case Id: 1

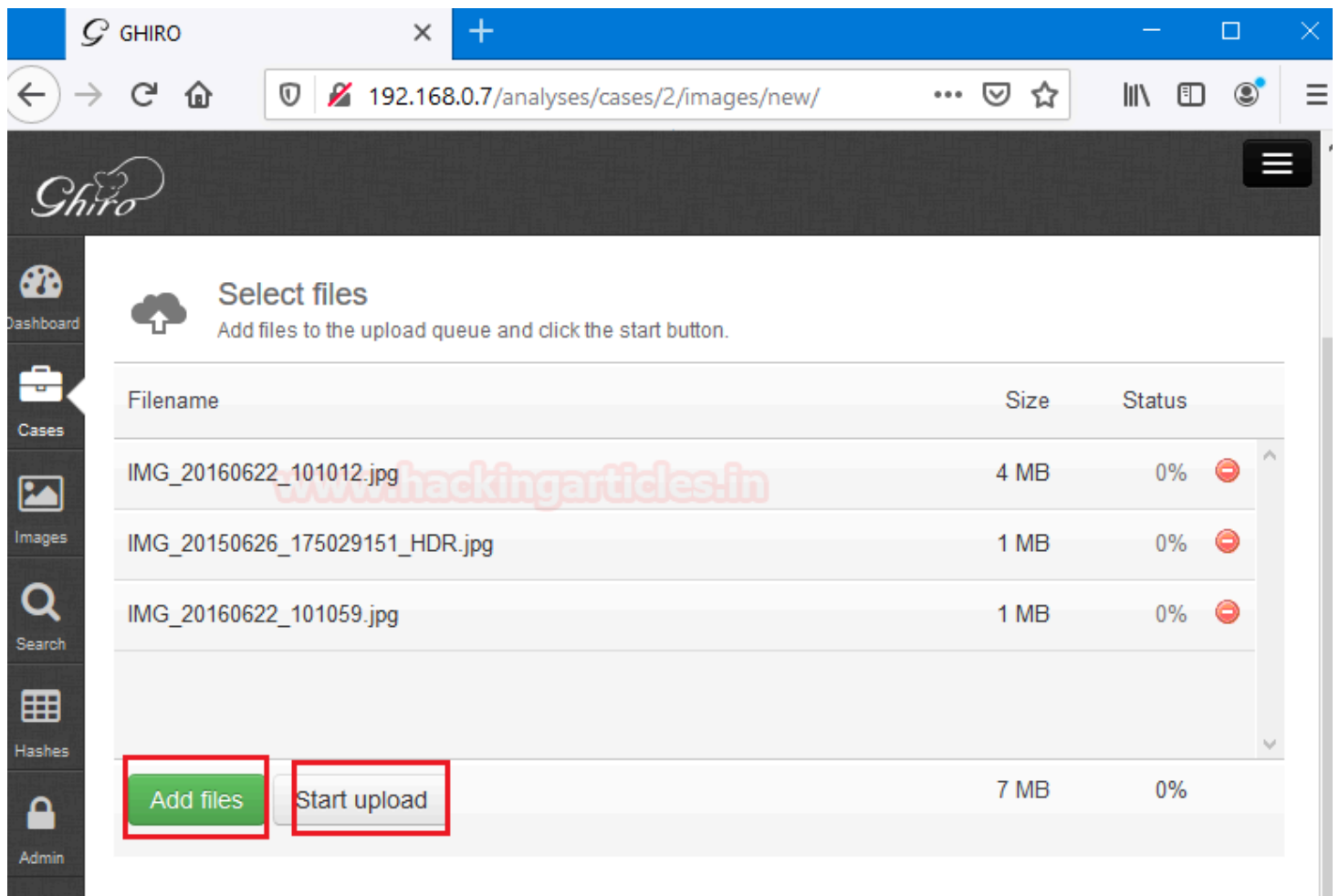
0

+

Tasks Owned Not owned Thumbnails Map Favorites Search

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.



After uploading these files it will show us the files and their status of uploading these images. In this uploading process, Ghiro demands us to **refresh** this screen by clicking on the highlighted refresh button. Click on the refresh button to finishing up the upload.



GHIRO

192.168.0.7/analyses/cases/show/2/list/

**Cases: Case 1**

Dashboard > Cases > Case 1

**Description:** Image Analysis  
**Status:** Open  
**Owner:** ghiro  
**Created at:** July 12, 2020, 11:06 a.m.  
**Case Id:** 2

Tasks Owned Not owned Thumbnails Map Favorites Search

File name	Status	Owner	Submitted at
IMG_20160622_101059.jpg	Waiting	ghiro	July 12, 2020, 11:08 a.m.
IMG_20160622_101012.jpg	Processing	ghiro	July 12, 2020, 11:08 a.m.
IMG_20150626_175029151_HDR.jpg	Processing	ghiro	July 12, 2020, 11:08 a.m.

Page 1 of 1

We can see that the file upload process is 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.

GHIRO

192.168.0.7/analyses/cases/show/2/list/

**Cases:** Case 1

Dashboard > Cases > Case 1

**Description:** Image Analysis  
**Status:** Open  
**Owner:** ghiro  
**Created at:** July 12, 2020, 11:06 a.m.  
**Case Id:** 2

Tasks Owned Not owned Thumbnails Map Favorites Search

File name	Status	Owner	Submitted at
<a href="#">IMG_20160622_101059.jpg</a>	Completed	ghiro	July 12, 2020, 11:08 a.m.
<a href="#">IMG_20160622_101012.jpg</a>	Completed	ghiro	July 12, 2020, 11:08 a.m.
<a href="#">IMG_20150626_175029151_HDR.jpg</a>	Completed	ghiro	July 12, 2020, 11:08 a.m.

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.

GHIRO

192.168.0.7/analyses/images/list/

**Ghiro**

Images browse all images

Dashboard > Images

Dashboard

Cases










Images

Search

Hashes

Admin

List Thumbnails Map Favorites

File name	Owner	Submitted at	Actions
<a href="#">IMG_20160622_101059.jpg</a>	ghiro	July 12, 2020, 11:08 a.m.	  
<a href="#">IMG_20160622_101012.jpg</a>	ghiro	July 12, 2020, 11:08 a.m.	  
<a href="#">IMG_20150626_175029151_HDR.jpg</a>	ghiro	July 12, 2020, 11:08 a.m.	  

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.

GHIO

192.168.0.7/analyses/show/6/

**Cases**

Dashboard > Cases > Case 1 > Report

**Image analysis:**

**20683c11203e64ca36f7f7980597e17c**

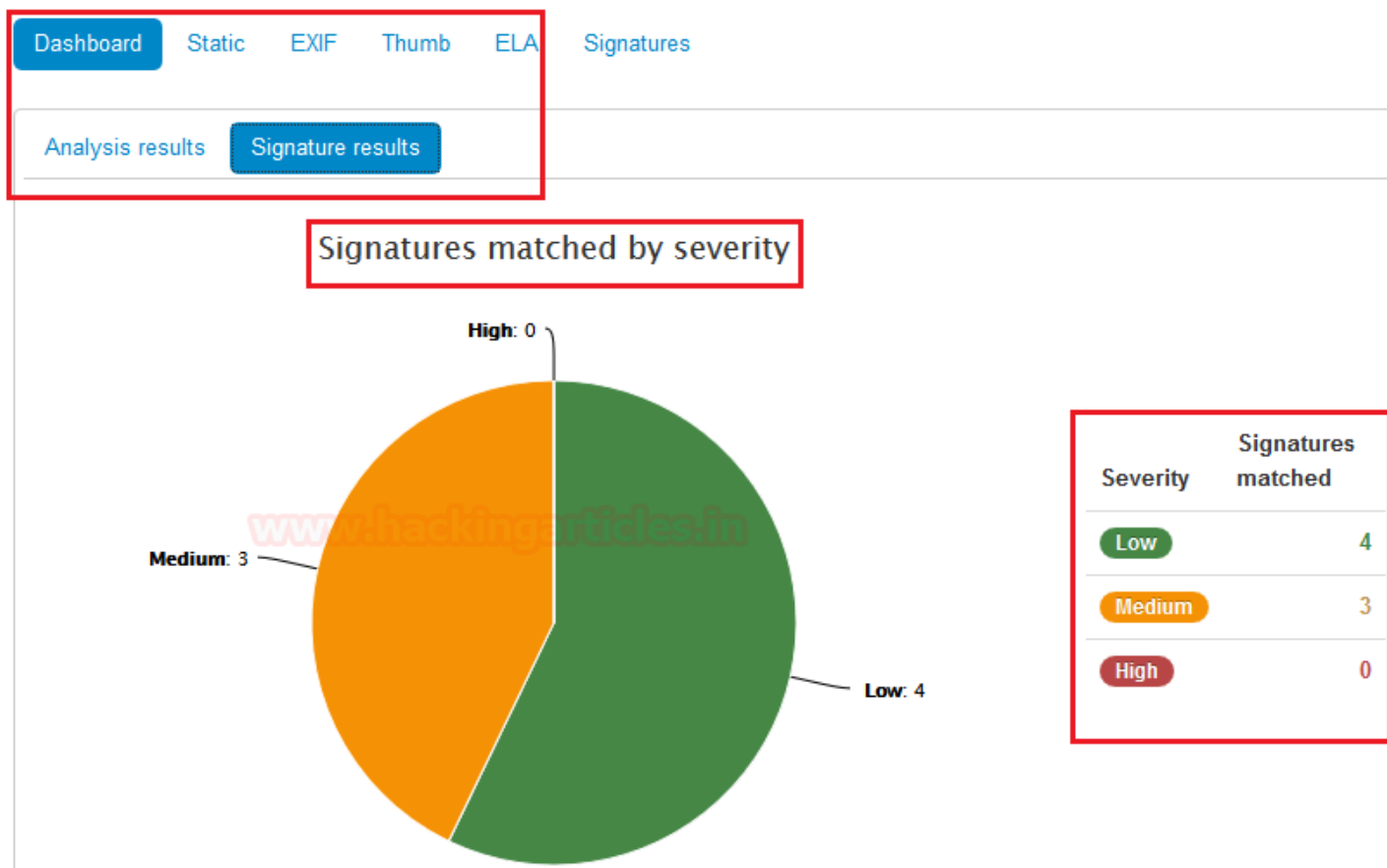
★ 🖨️ 🗑️ Download Export

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 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, 3 are medium and nothing is high.



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.

Dashboard Static EXIF Thumb ELA Signatures

Static info FileType Hashes Strings Hex dump

Type	Value
Filename	IMG_20160622_101059.jpg
Size	1.4 MB
Dimensions	[4096, 2304]
Analyzed at	July 12, 2020, 11:08 a.m.

We switched to the second option which is FileType. Which says it is a jpeg file standard for EXIF.

Dashboard **Static** EXIF Thumb ELA Signatures

Static info **FileType** Hashes Strings Hex dump

Type

JPEG image data, EXIF standard

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.

Dashboard **Static** EXIF Thumb ELA Signatures

Static info FileType **Hashes** Strings Hex dump

Type	Value
SHA1	638ca6f083707cf66ee870174083cb37a3ed169e
SHA224	13ebb881bcd8ffaee8a6882afbdf1a2b57e4cc22cf0ea202435133cf
SHA384	77f744438b662112ffc0b0ddddd27c63c2f6f1cb6f7abc1f135a65f3f593b466c3791a47c4ef1199905fbd3a3801a15a5
CRC32	9d1eb32a
SHA256	496305fcea21d2a91ca164328f0b14eb1917fd5f54e3bf15fdc8aabf1c24688f
SHA512	eccec798a625bb5bc52d16f1bd349507419545b6b0b8234b01d5a25f28b6152a734580df3e3e354a6c3c48dd28c
MD5	20683c11203e64ca36f7f7980597e17c

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

```
Lenovo K50a40
2016:06:22 10:11:00
Lenovo Camera
Lenovo
2016:06:22 10:11:00
2016:06:22 10:11:00
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
pjVbizA
F;bR77
wo41Gk
Mb--ux<%3
|Eeeo-
+6#|k
U<>)N+D
'8b0A8
]xsY";ME,
'{$}\+
2C*I&B
9VBzW
zXyNSuo
|E8iv~$k
VJ'PMB
N#Ww?{
8_PE~}
vWQH/#
```

The final option offered by the static is the Hex dump. It will show us the hexadecimal value of that image file through which can get some small details about that image file.

```
0000 FF D8 FF E1 34 91 45 78 69 66 00 00 49 49 2A 00 08 00 00 00 12 00 25 88 04 00 01 00 00 00 4A 03 ....4.Exif..II*..
0020 00 00 10 01 02 00 20 00 00 00 E6 00 00 00 22 02 04 00 01 00 00 00 00 00 00 00 20 02 04 00 01 00 ..... " ..
0040 00 00 00 00 00 00 23 02 04 00 01 00 00 00 00 00 00 00 0E 01 02 00 20 00 00 00 06 01 00 00 12 01 .....#.....
0060 03 00 01 00 00 00 01 00 00 00 21 02 04 00 01 00 00 00 00 00 00 00 24 02 04 00 01 00 00 00 01 00 .....!.....
0080 00 00 32 01 02 00 14 00 00 00 26 01 00 00 13 02 03 00 01 00 00 00 02 00 00 00 28 01 03 00 01 00 ..2.....&.....
00A0 00 00 02 00 00 00 25 02 02 00 20 00 00 00 3A 01 00 00 1B 01 05 00 01 00 00 00 5A 01 00 00 31 01 .....%... :...
00C0 02 00 20 00 00 00 62 01 00 00 69 87 04 00 01 00 00 00 AA 01 00 00 1A 01 05 00 01 00 00 00 82 01 .. ...b...i.....
00E0 00 00 0F 01 02 00 20 00 00 00 8A 01 00 00 70 03 00 00 4C 65 6E 6F 76 6F 20 4B 35 30 61 34 30 00 .....p..
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 32 30 31 36 3A 30 36 3A 32 32 20 31 30 3A .....
0140 31 31 3A 30 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11:00.....
0160 00 00 00 00 00 00 48 00 00 00 01 00 00 00 4C 65 6E 6F 76 6F 20 43 61 6D 65 72 61 00 00 00 00 00 .....H.....Ler
0180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 01 00 00 00 4C 65 6E 6F 76 6F 00 00 00 00 .....H..
01A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 00 01 A0 03 00 01 00 00 00 .....
01C0 01 00 00 00 04 90 02 00 14 00 00 00 DC 02 00 00 9D 82 05 00 01 00 00 00 F0 02 00 00 22 88 03 00 .....
01E0 01 00 00 00 00 00 00 00 0A 92 05 00 01 00 00 00 F8 02 00 00 03 A4 03 00 01 00 00 00 00 00 00 .....
0200 02 A0 04 00 01 00 00 00 10 00 00 90 92 02 00 03 00 00 00 32 31 00 00 08 92 03 00 01 00 00 00 .....
0220 FF 00 00 00 07 92 03 00 01 00 00 00 02 00 00 00 02 A4 03 00 01 00 00 00 00 00 00 00 03 90 02 00 .....
0240 14 00 00 00 00 03 00 00 92 92 02 00 03 00 00 00 32 31 00 00 01 91 07 00 04 00 00 00 01 02 03 00 .....2
0260 03 A0 04 00 01 00 00 00 09 00 00 09 92 03 00 01 00 00 00 00 00 00 00 90 07 00 04 00 00 00 .....

```

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.



Exif Metadata

Segment	Key: Value
PHOTO	LightSource: 255
	PixelXDimension: 4096
	SubSecTime: 21
	ExposureMode: 0
	Flash: 0
	FlashpixVersion: 48 49 48 48
	SceneCaptureType: 0
	MeteringMode: 2
	ExifVersion: 48 50 50 48
	ExposureBiasValue: 0/10
	ExposureProgram: 0
	SubSecTimeOriginal: 21
	ColorSpace: 1
	FocalLength: 356/100
	DateTimeDigitized: 2016:06:22 10:11:00
	DateTimeOriginal: 2016:06:22 10:11:00
	SubSecTimeDigitized: 21
	WhiteBalance: 0
	FNumber: 20/10
	PixelYDimension: 2304
	ComponentsConfiguration: 1 2 3 0
	ISOSpeedRatings: 83
	ExposureTime: 591/1000000
	InteroperabilityTag: 812
	DigitalZoomRatio: 348/100

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 GPSTag: 842 ExifTag: 426 Make: Lenovo ResolutionUnit: 2 DateTime: 2016:06:22 10:11:00 0x0222: 0 0x0223: 0 0x0220: 0 0x0221: 0 YCbCrPositioning: 2 XResolution: 72/1 0x0224: 1 Orientation: 1 Model: Lenovo K50a40 Software: Lenovo Camera
-------	--

GPSINFO	GPSImgDirectionRef: M GPSImgDirection: 158/1
---------	---

THUMBNAIL	YResolution: 72/1 ResolutionUnit: 2 Compression: 6 YCbCrPositioning: 2 XResolution: 72/1 JPEGInterchangeFormatLength: 12451 JPEGInterchangeFormat: 998 Orientation: 1
-----------	--

IOP	InteroperabilityIndex: R98 InteroperabilityVersion: 48 49 48 48
-----	--

After switching the one more we found out the thumb tab. This shows us all details regarding the thumbnail of the image. Regarding Mime type, Extension, and Dimension.

Previews



Size: 12451 bytes

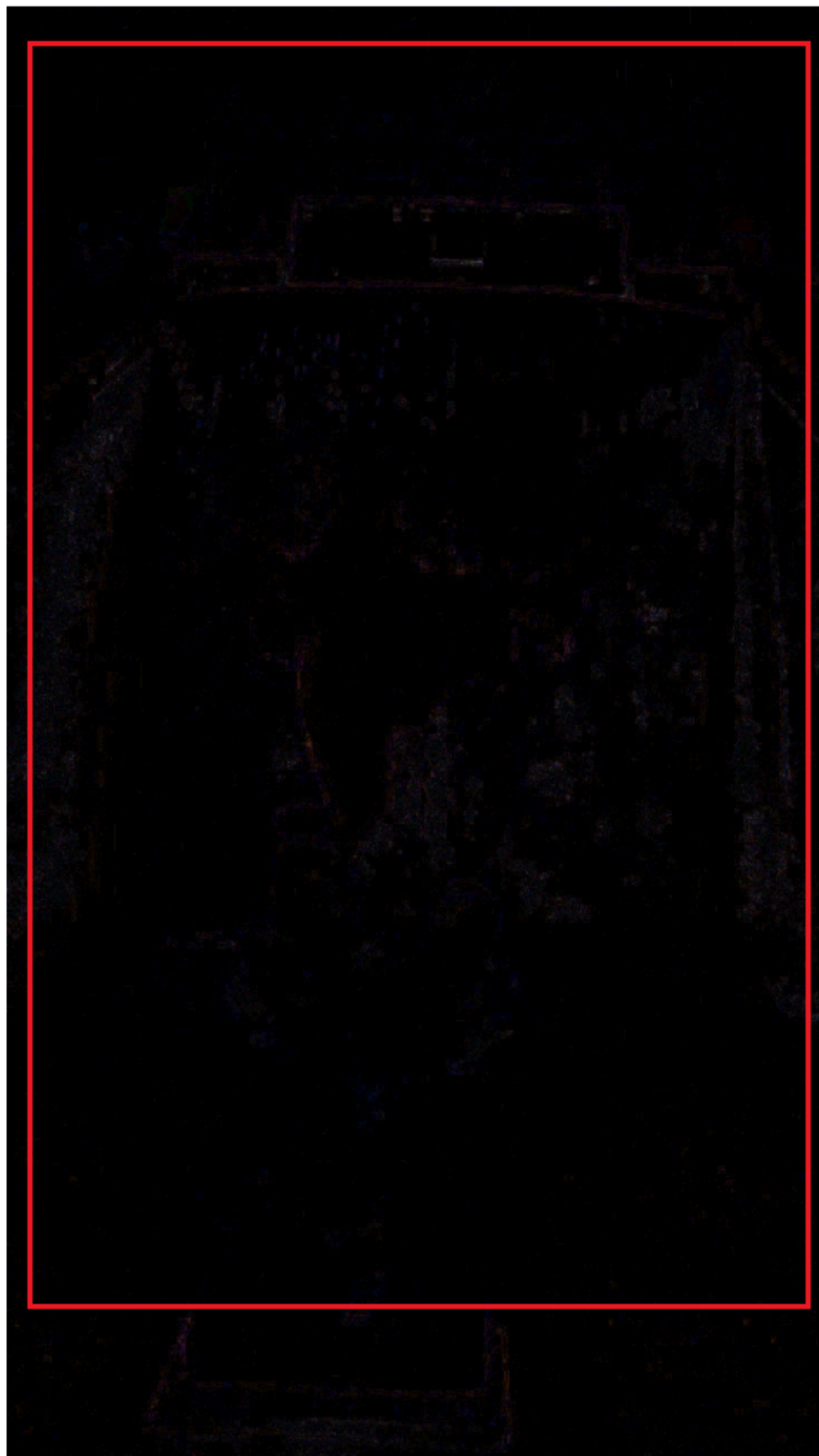
Mime type: image/jpeg

Extension: .jpg

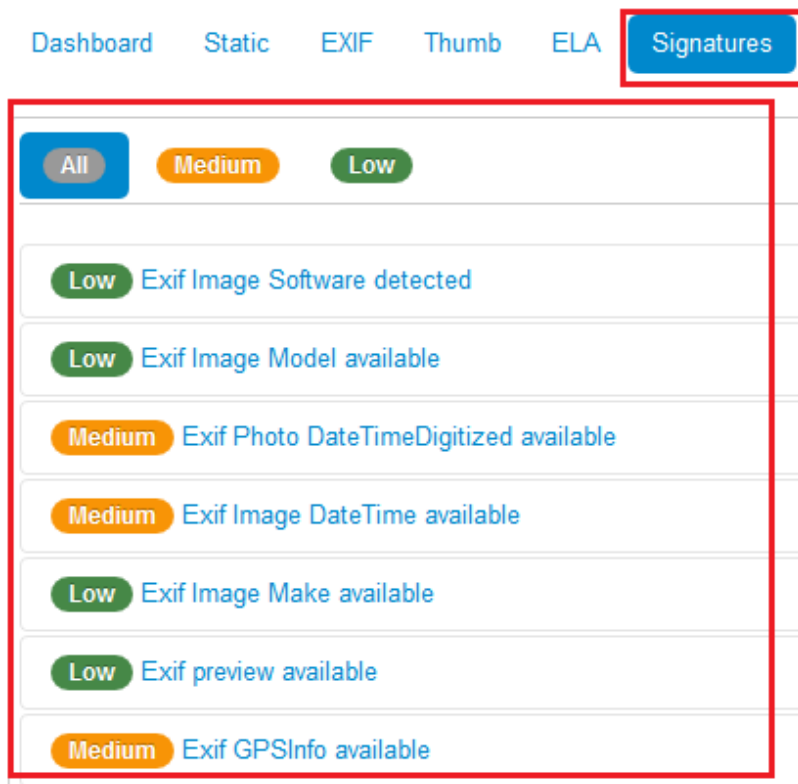
Dimension: [160L, 128L]

The fifth tab of Ghire image analysis we get ELA. Error Level Analysis (ELA) permits identifying areas within an image that are at different compression levels. With JPEG images, the entire picture should be at roughly the same level. If a section of the image is at a significantly different error level, then it likely indicates a digital modification.

If we focus hard and keep the brightness high we can see the Error image analysis of our image as well.



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



Overall Ghireo is the complete image analysis tool that can be quite beneficial in any Forensic Investigation.