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.

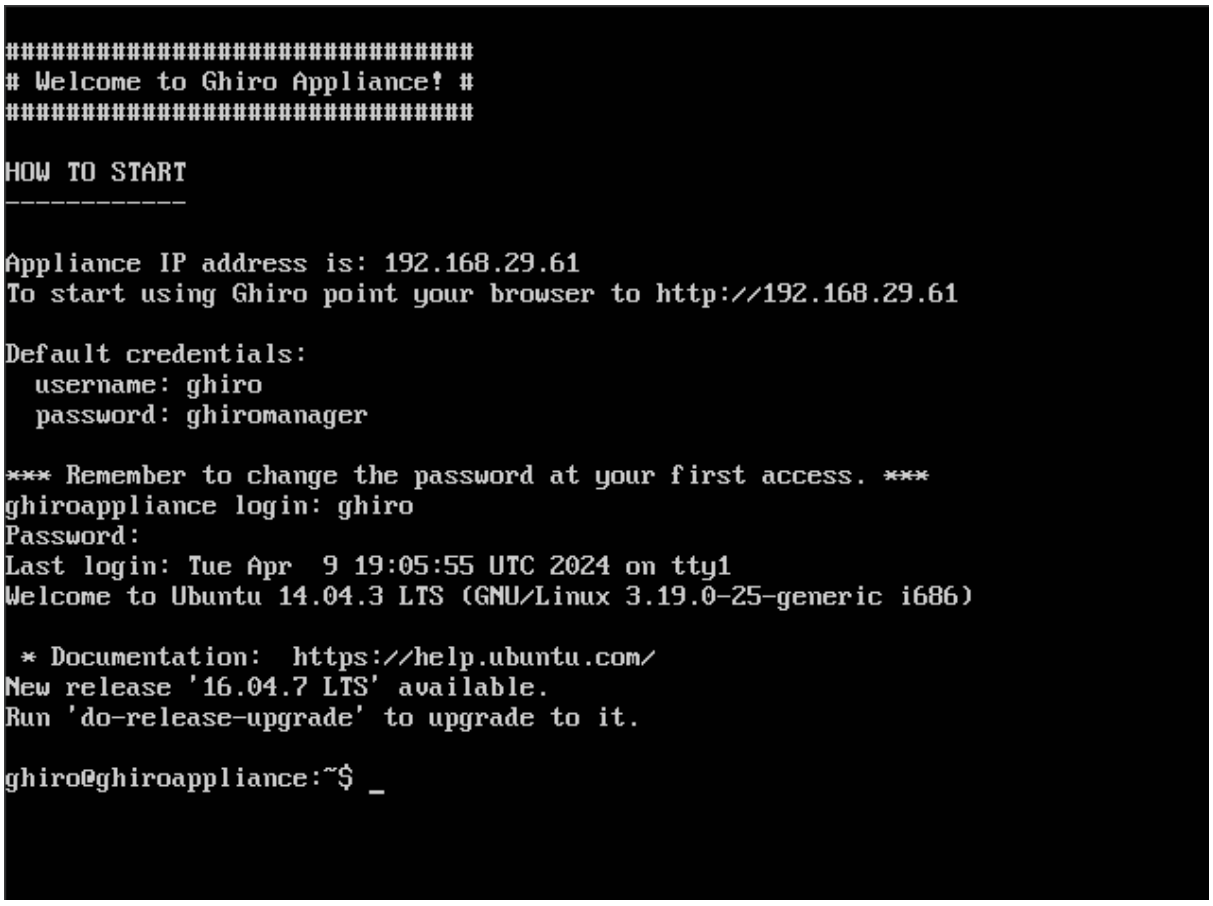
Setup Ghiro

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 out 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.

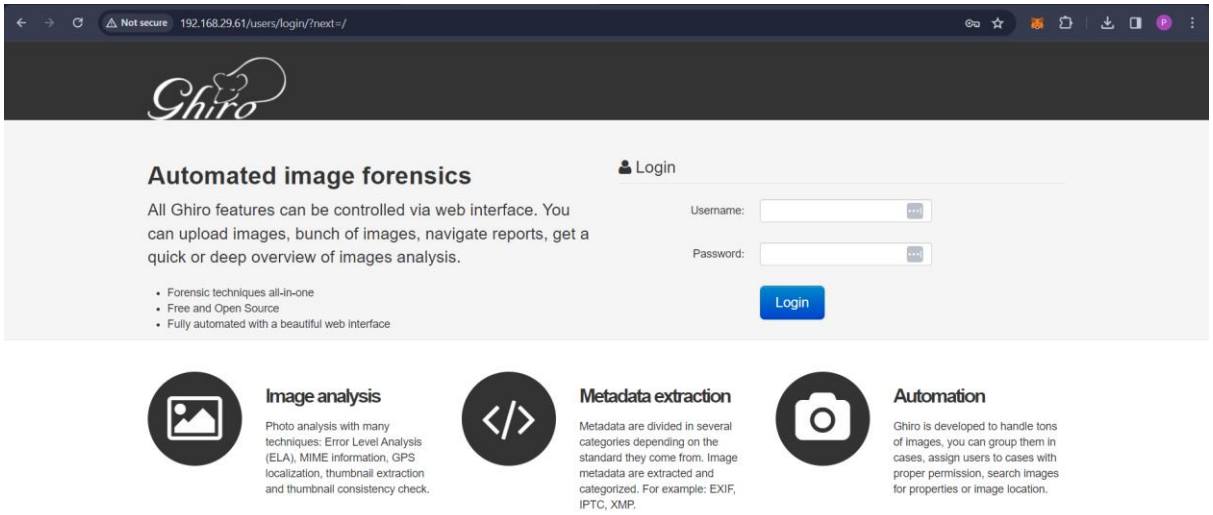


Notice the default credentials :

Username : ghiro

Password : ghiromanager

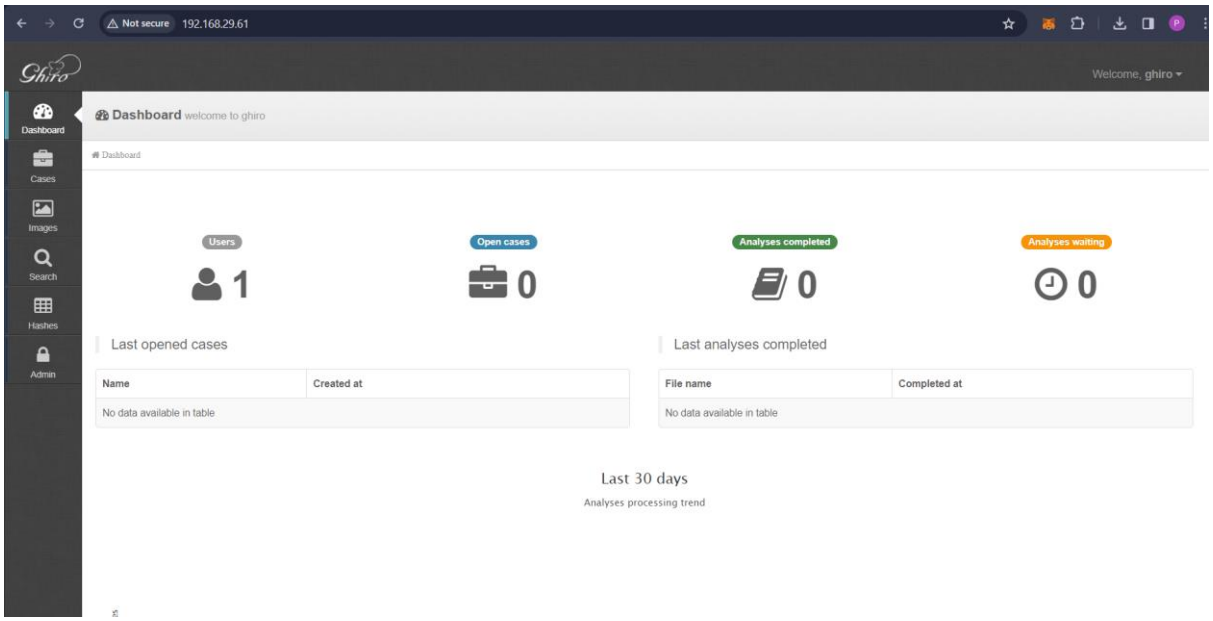
Now, open the Appliance IP Address in your browser.



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.

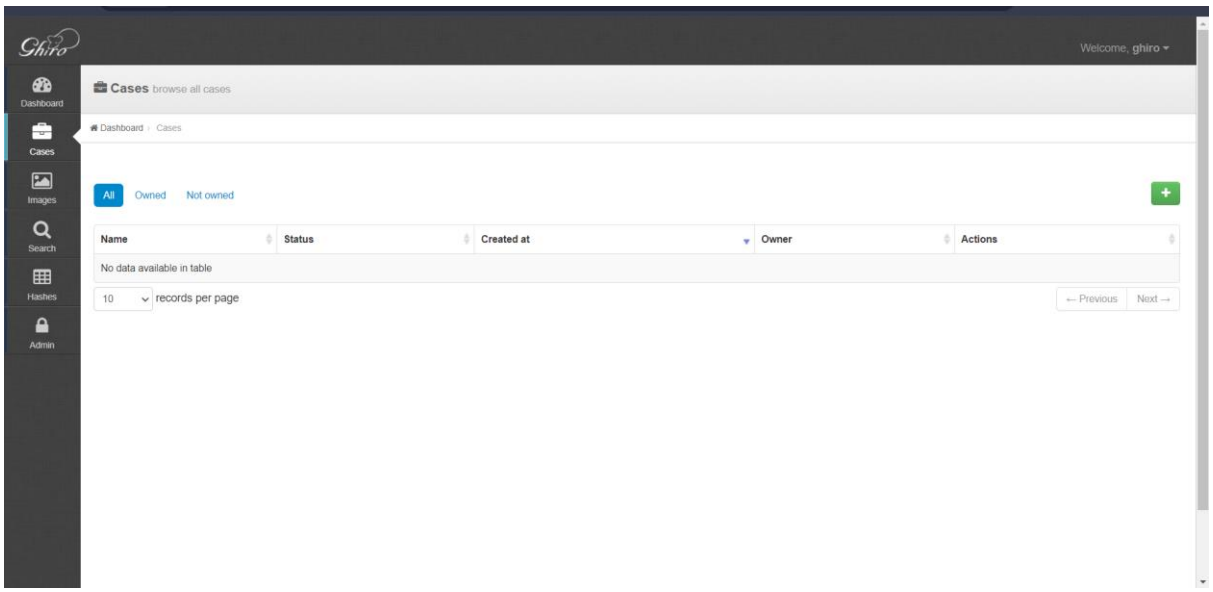
Go to the profile section and change the default password to a password of your choice.

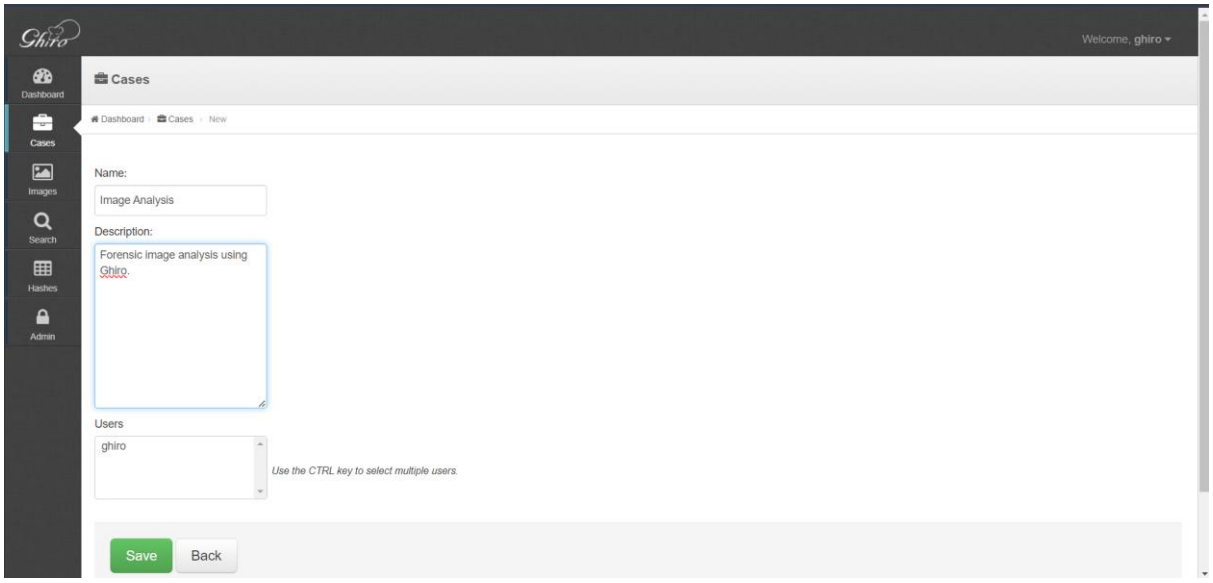
As we can see that it has the user : ghiro, through which we log in to the software. At the initial point, it shows zero cases and zero analyses left because we just set up this software.

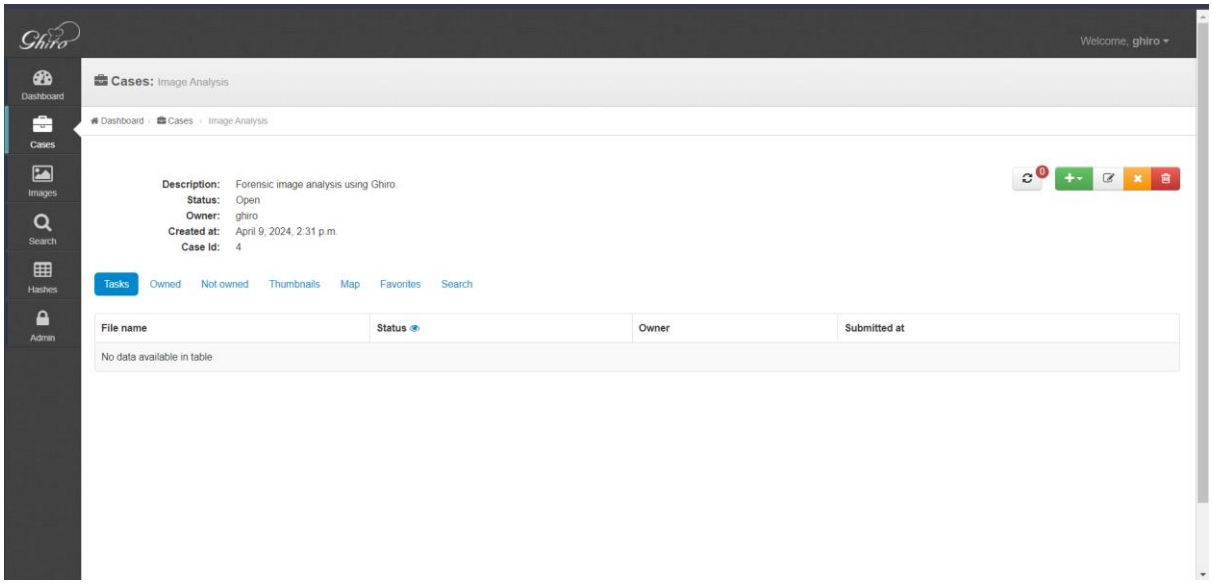


To start working with Ghiro for image analysis, we need to click on *cases*, where we can see that it is completely blank. There's a **[+]** to add any case to this directory.

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

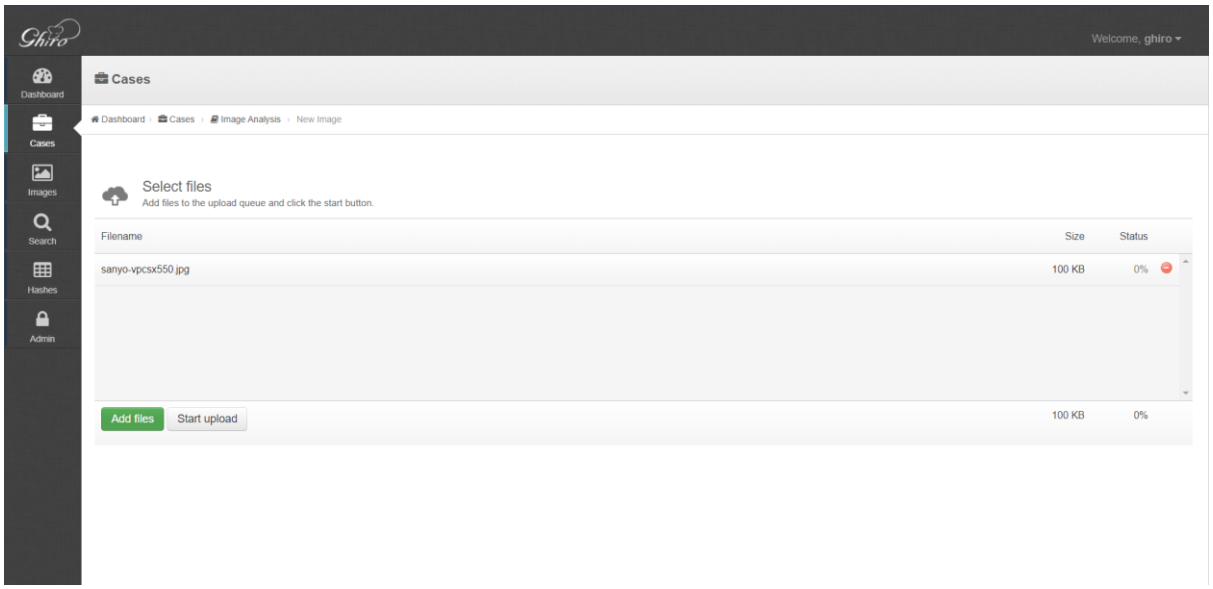




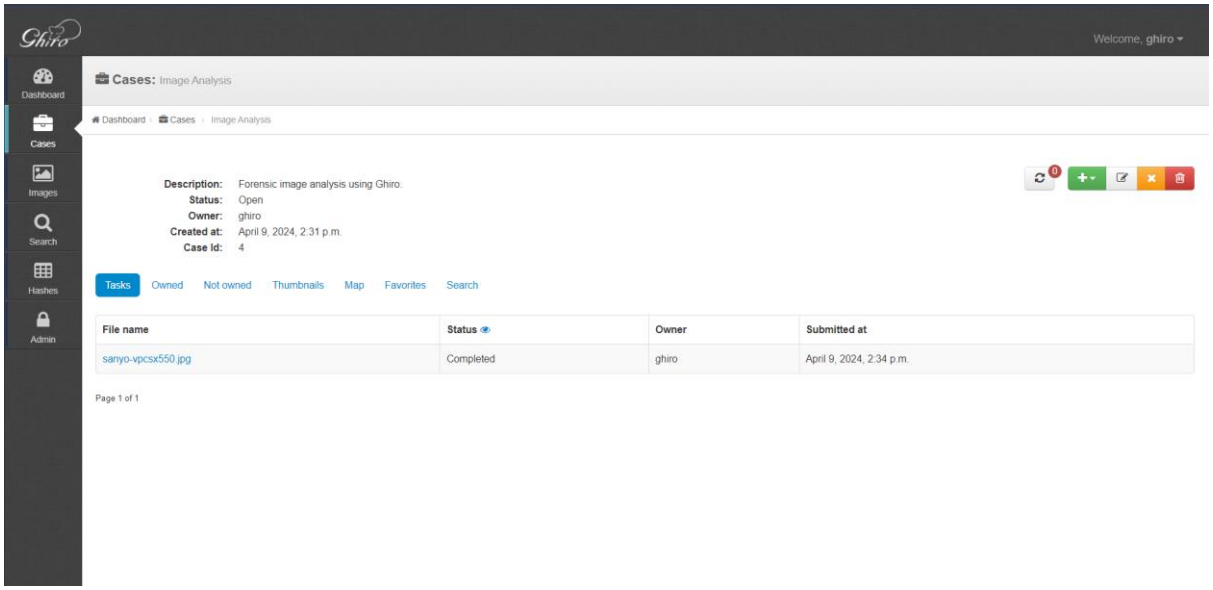


After saving the details regarding the forensic case, it will confirm these details and ask us to add images to analysis. To add images, click **[+]** button.

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.

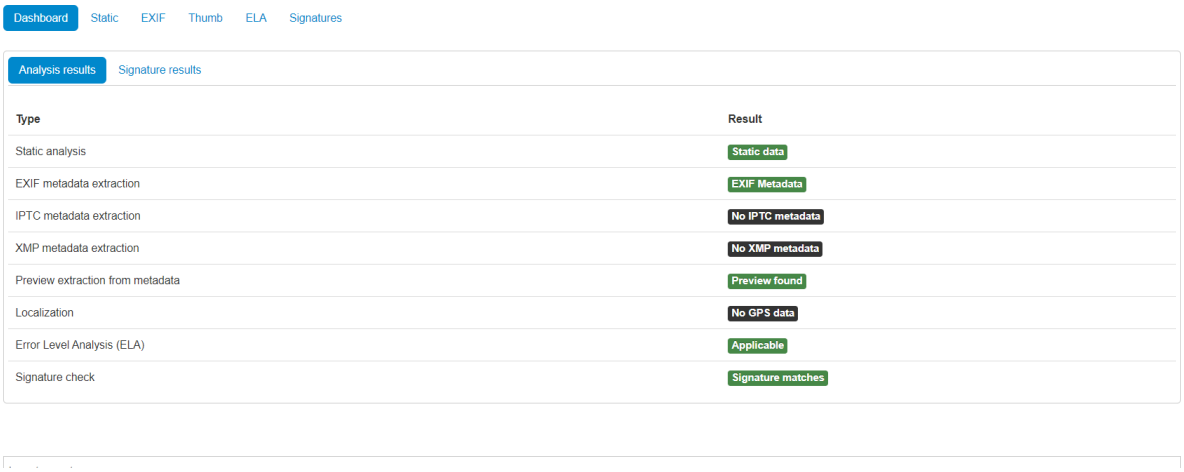


After uploading the files, it will show us the files and their status of uploading these images. In this uploading process, click on the refresh button to finish the upload.

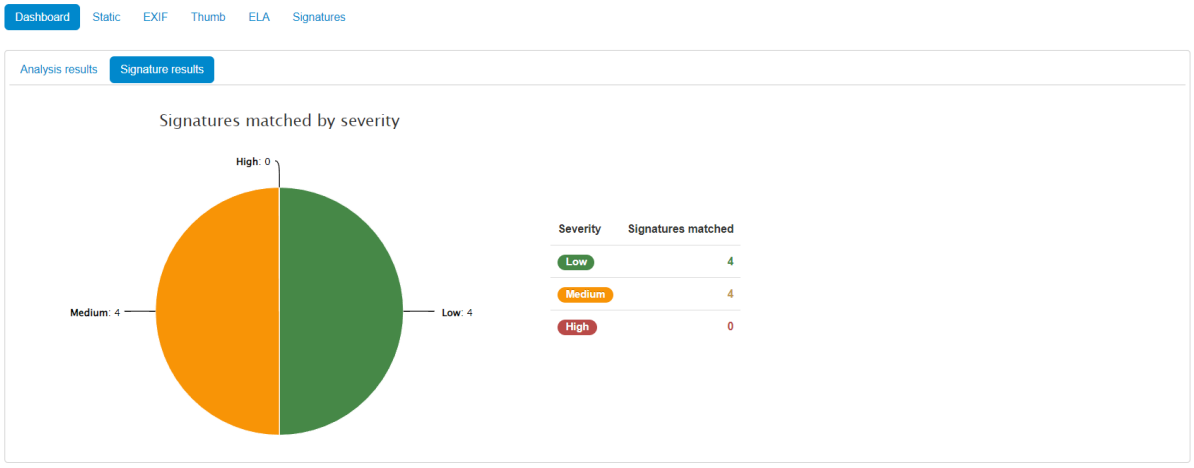


We can see that the file upload process is just finished. Now we have two options to analyze the image. The first option is to directly click on the image name to view their details. The second option is to click on the images tab and then click on the image we want to the details of.

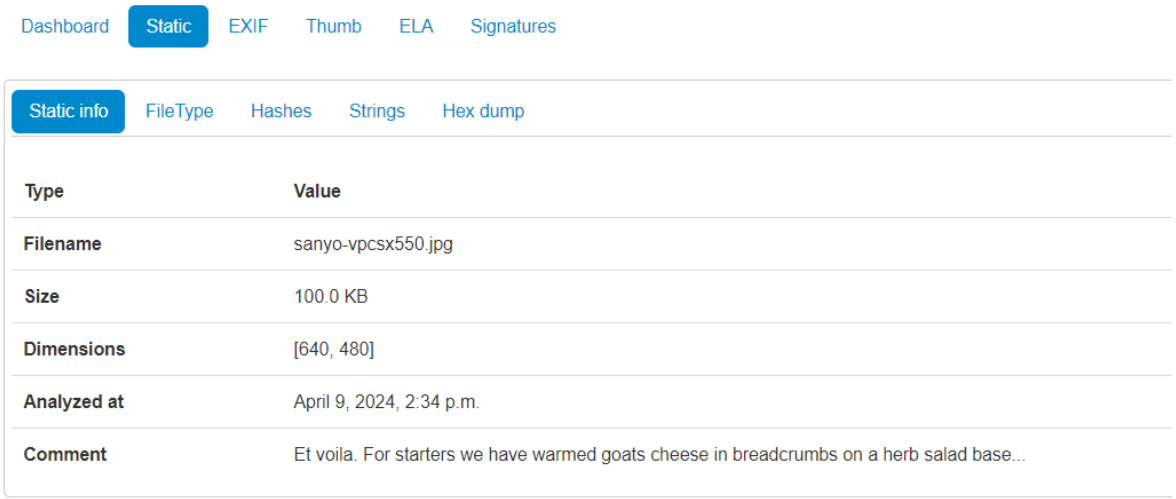
Click on the image we want to analyze. It will show us the basic details regarding the image in the dashboard which shows us all the analysis results like **static analysis, EXIF, IPTC, XMP, Signature check** etc.



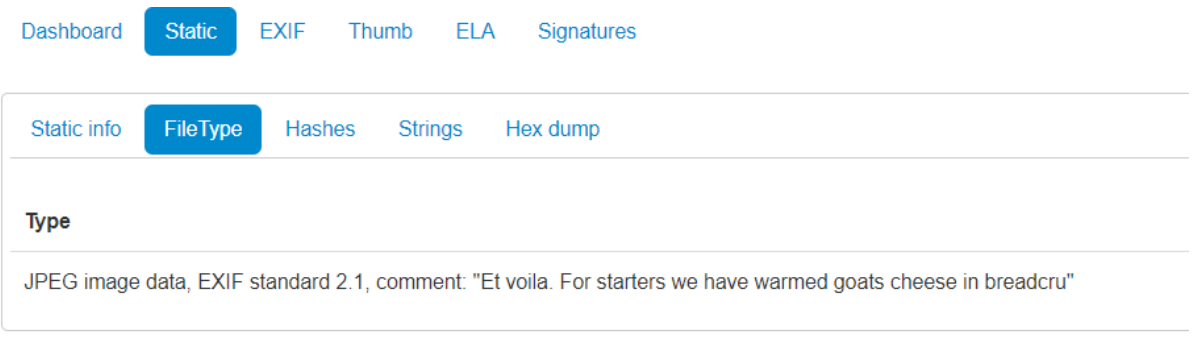
Now keep clicking on all the options and see the analysis results. Let’s click on the second option offered by the dashboard menu which is Signature results. It shows us all the signatures matched by severity. In this case, there are 4 low and 4 medium.



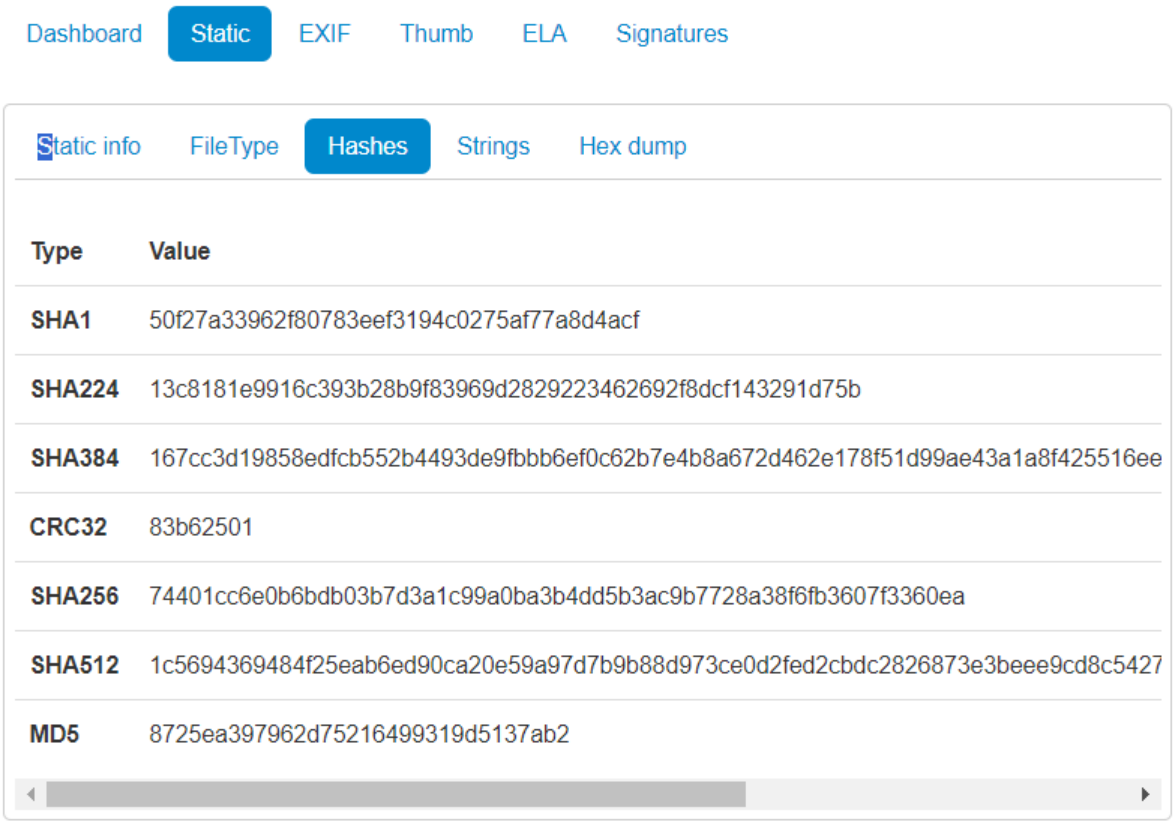
In the second tab, we have static and it's first option is static info. Here, we see all the basic information about the image.



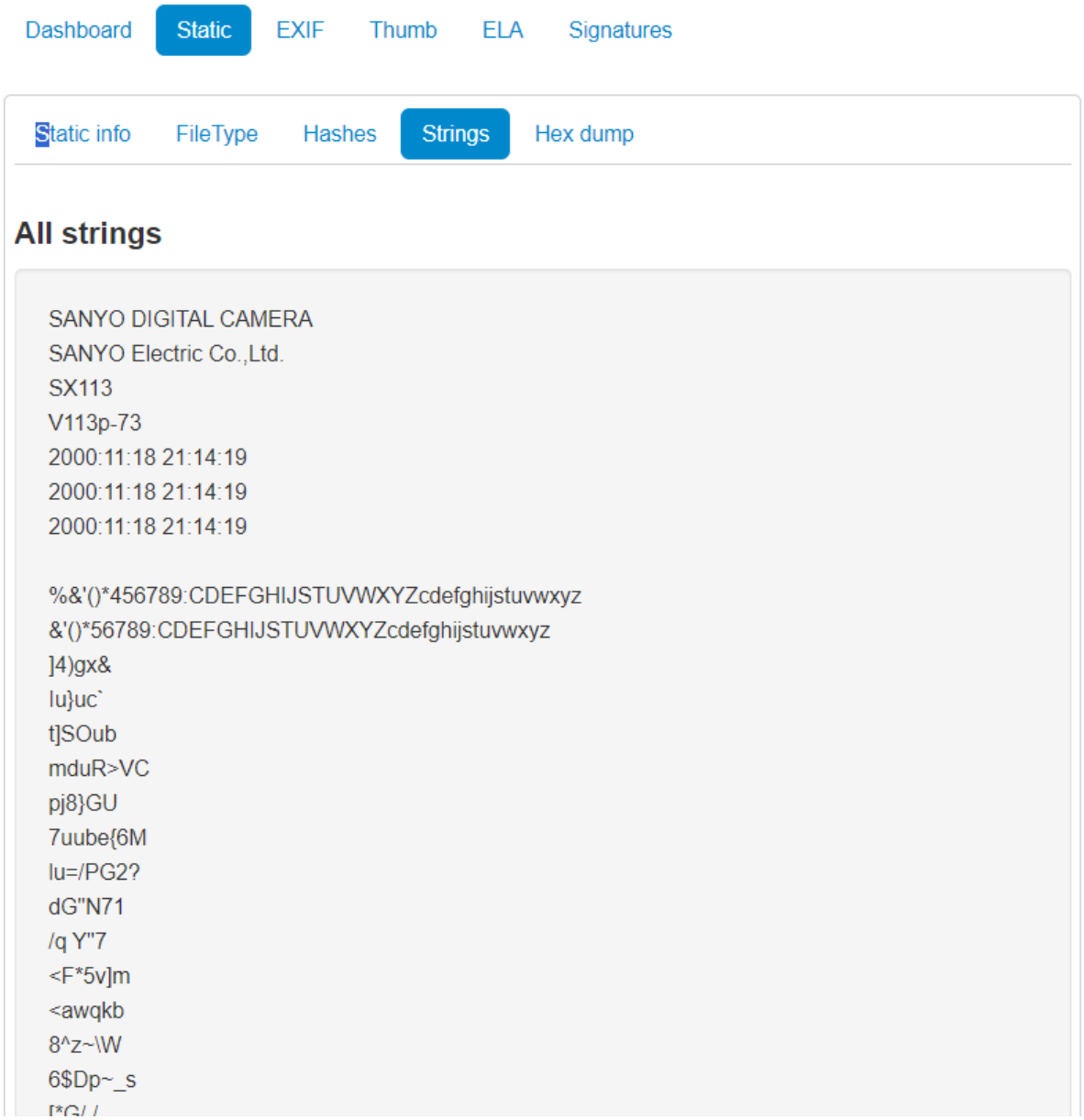
The second option is filetype. It says here that the image is of type JPEG in the EXIF standard.



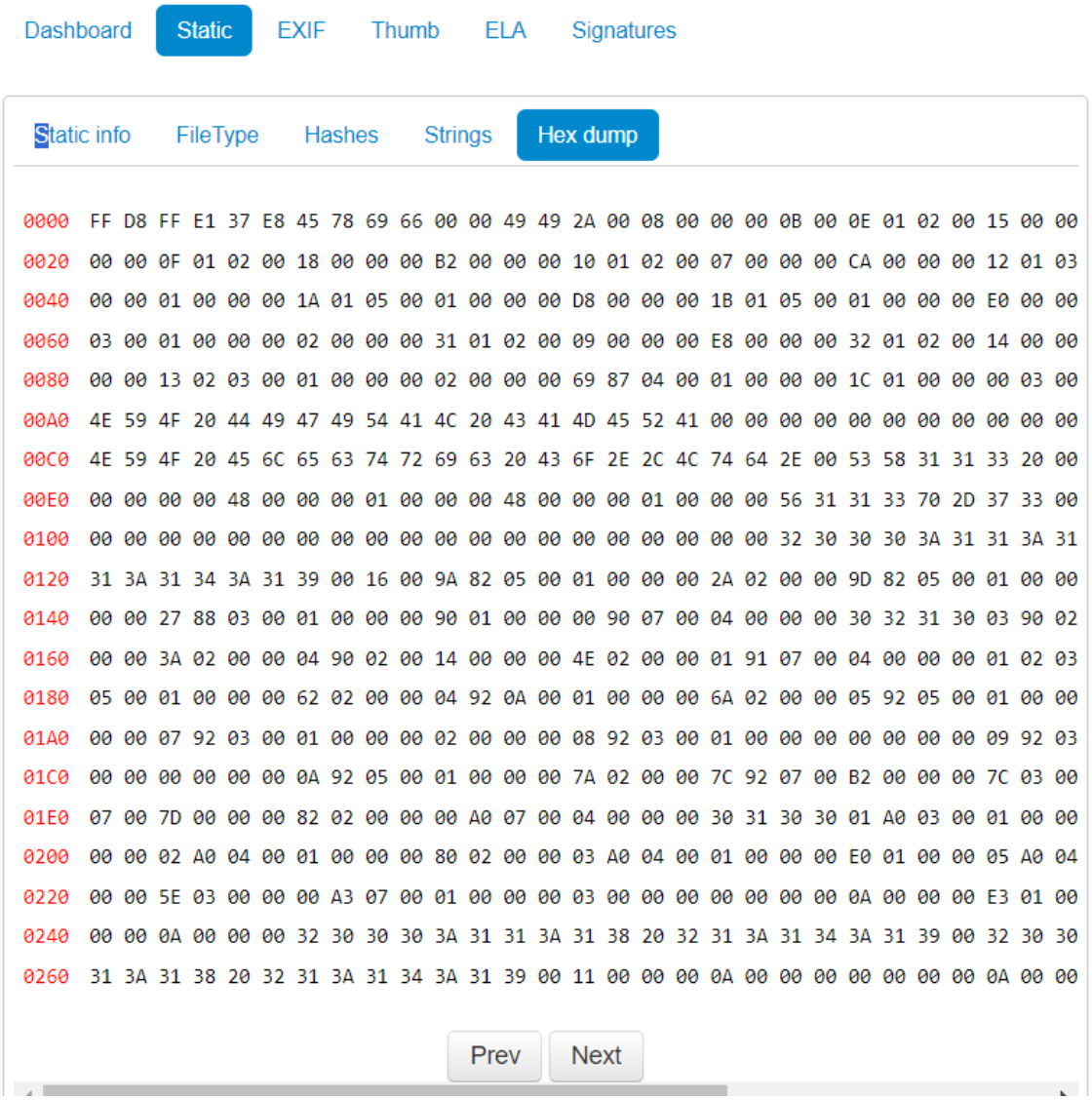
The third option shows us all the hash values of this file within different algorithms. If we focus hard, we can see that MD5 hash values are the file name when we clicked on the image for analysis.



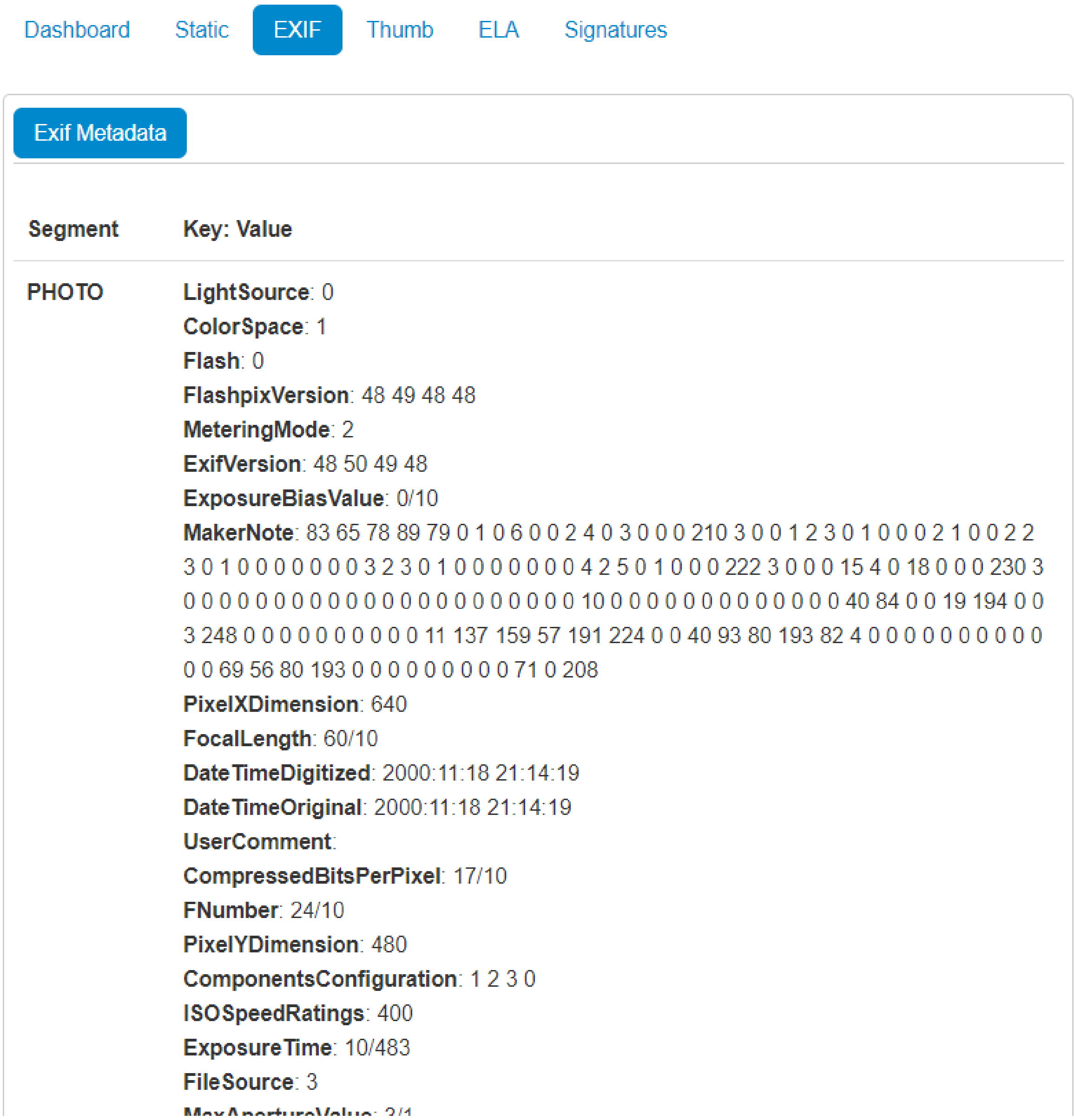
The fourth option we see is Strings. It shows us all the strings behind the image file with the slight details of the metadata of this image file.



The next option is Hex dump.



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.

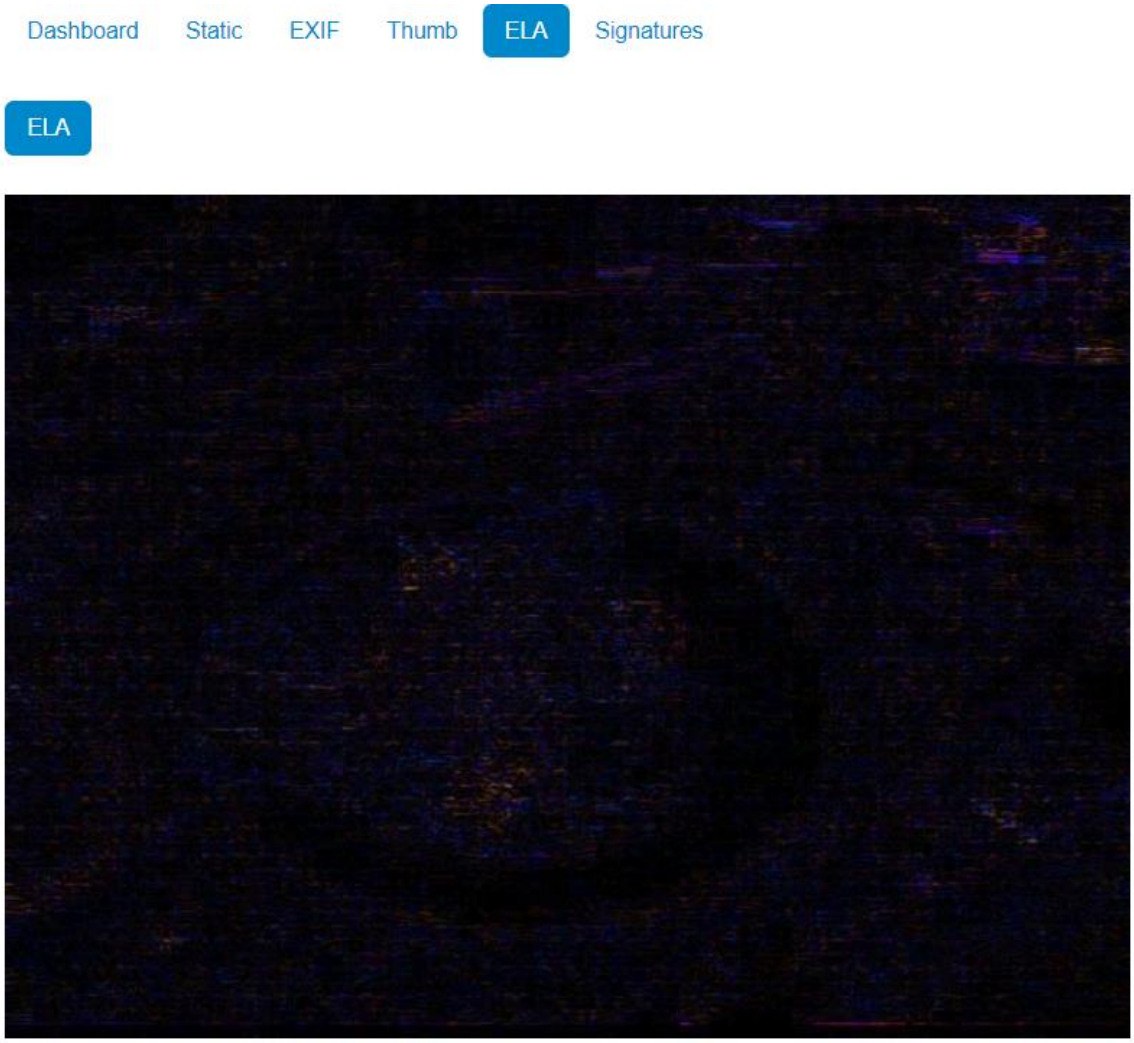


Scroll down to get full segments of the metadata of image files that can become handy in forensic investigation regarding GPS, thumbnails and IOP.

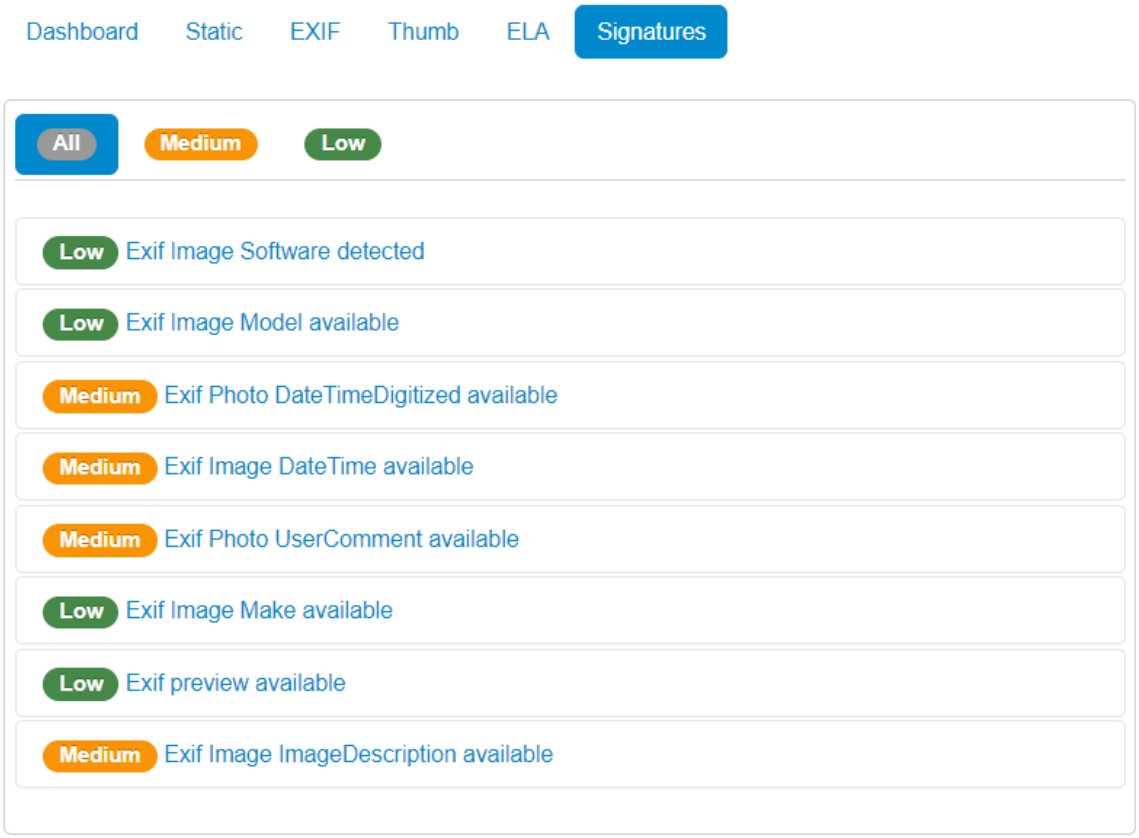
	FileSource: 3 **MaxApertureValue**: 3/1 **InteroperabilityTag**: 862
IMAGE	**YResolution**: 72/1 **ResolutionUnit**: 2 **Orientation**: 1 **Make**: SANYO Electric Co.,Ltd. **ImageDescription**: SANYO DIGITAL CAMERA **DateTime**: 2000:11:18 21:14:19 **ExifTag**: 284 **YCbCrPositioning**: 2 **XResolution**: 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

Previews

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



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



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