Image Forensics

Image analysis involves processing an image to extract meaningful information. Image analysis can include tasks such as finding shapes, detecting edges, removing noise, counting objects, and calculating statistics for texture analysis or image quality.

Forensic image analysis focuses on image authenticity and image content.

Digital image forensics is performed on local machines and can be used in both open and closed source investigations.

Categories of forensic image analysis –

- Photo image comparison
- Image content analysis (ICA)
- Image authentication
- Image enhancement and restoration

Investigators can mine everything from camera properties to individual pixels for information.

Image analysis can also be done to recover the original image or to enhance an original image to retrieve the information/evidence.

Image authentication refers to correct image blur, reducing noise adjusting brightness to bring out details.

A single image can be a source of digital evidence-

Image authenticity-

- Pixel data (e.g. colour information)
- Metadata (e.g. Creator's information and contact details. Copyright information. Descriptive information)
- Exif data (e.g. digital camera model, shutter speed, focal length)

Image content -

- Landmarks (e.g. apartment blocks, churches, schools)
- Visible languages (e.g. shops, road signs, road markings)

- Topography (e.g. hills, mountains, waterfalls)
- Street furniture (e.g. bollards, benches, bins)

Digital Image Forensics Techniques

Two common uses of digital image forensics techniques are:

A) When a suspect denies their presence in an image-
By enhancing the image, through Meta data, exif data that can prove the presence of suspect at crime scene

B) When a suspect claims that an incriminating image has been faked-

By performing error level analysis, through Meta data of the image.

METHODOLOGY:

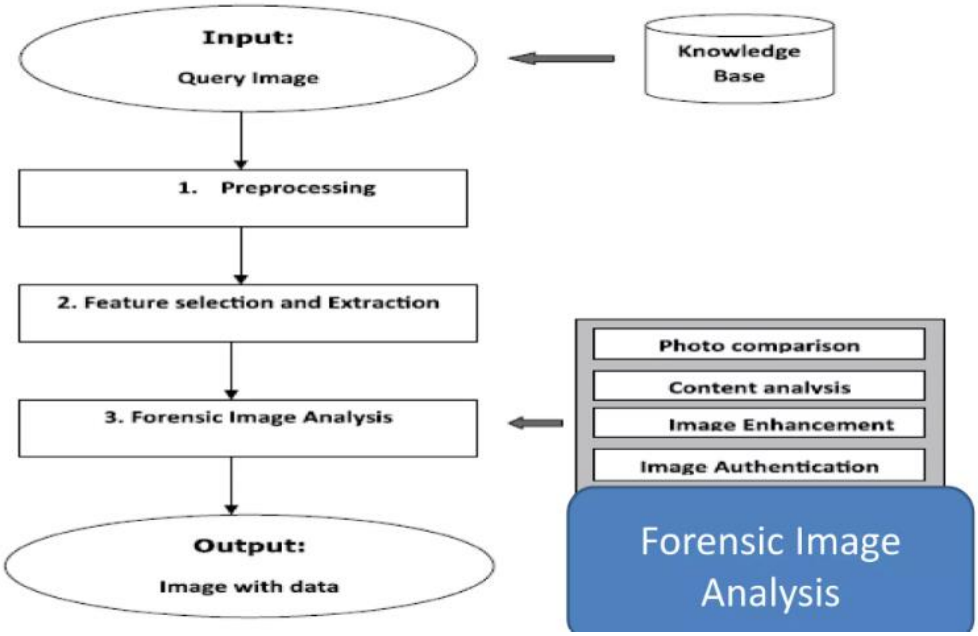


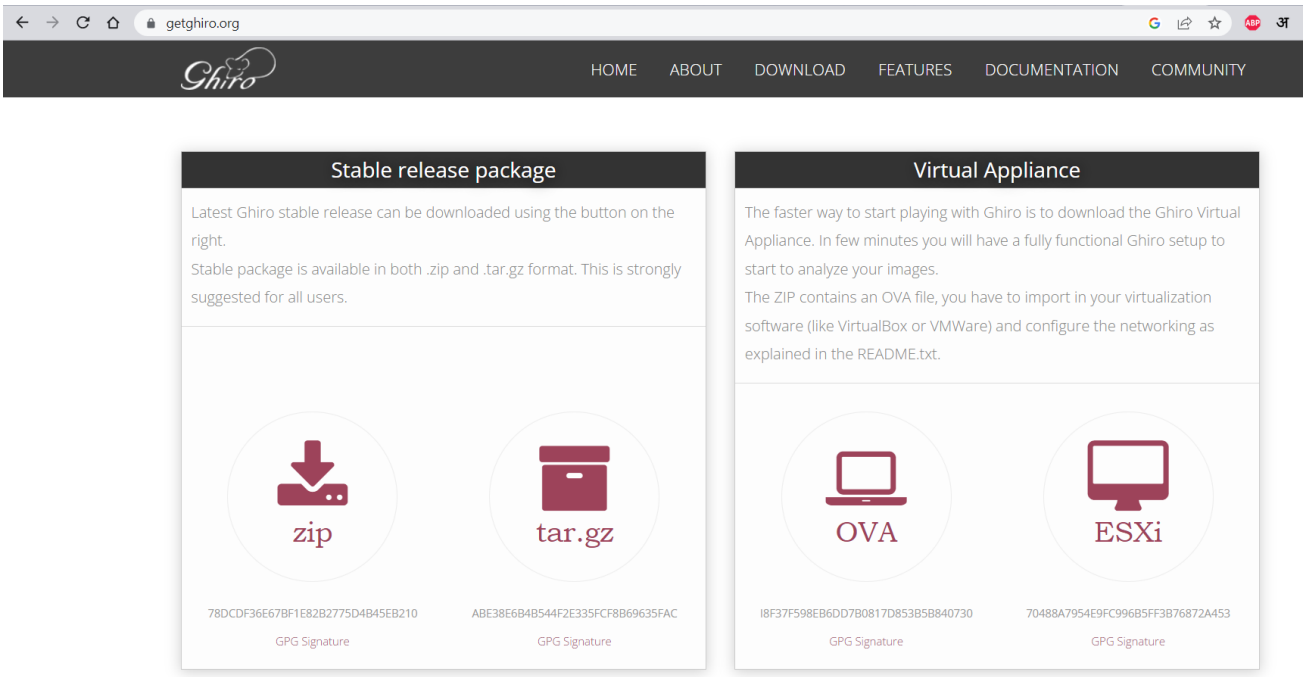
Image analysis –

When investigating image we need to consider two things that an image can be original or fake.

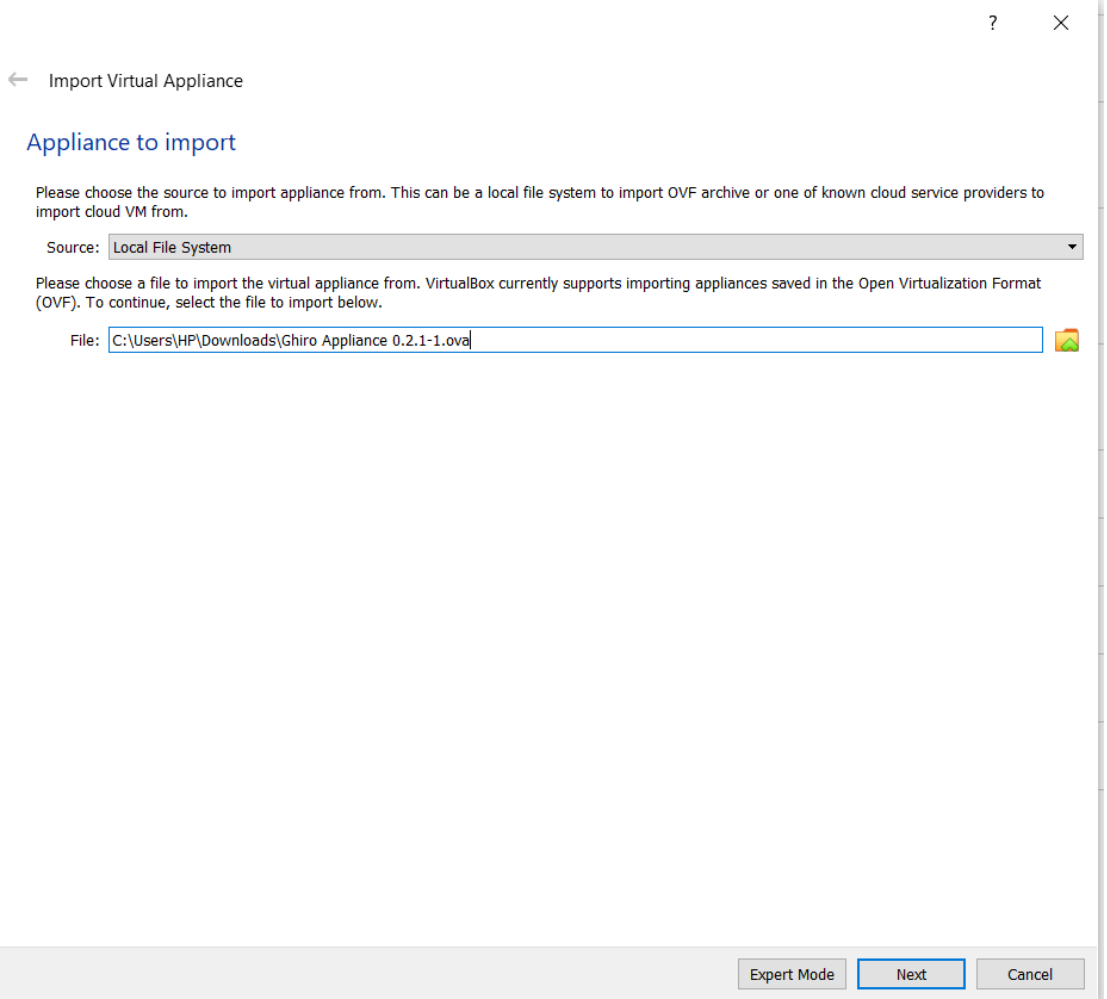
Through foto-forensic website (hash value, properties and Meta data)-

Ghiro

Go to ghiro official website and download the OVA file for easy installation,



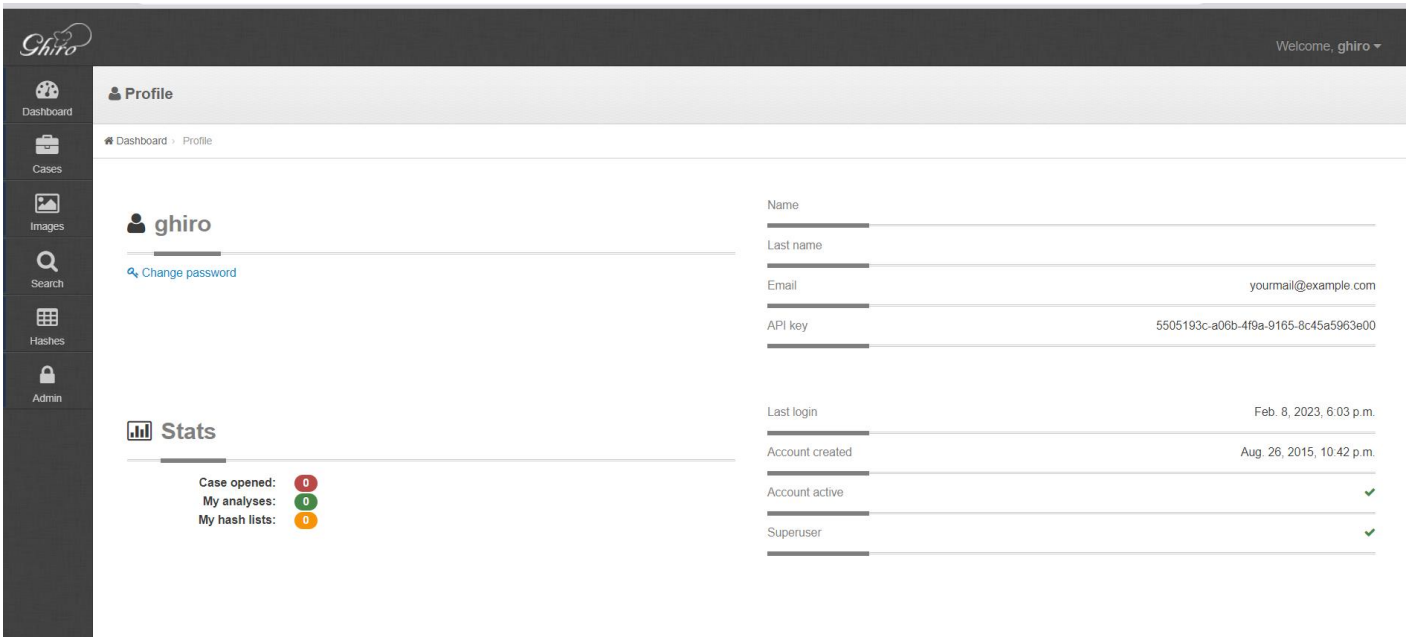
Go to your virtual box and click on import appliance and choose the extracted ghiro application,



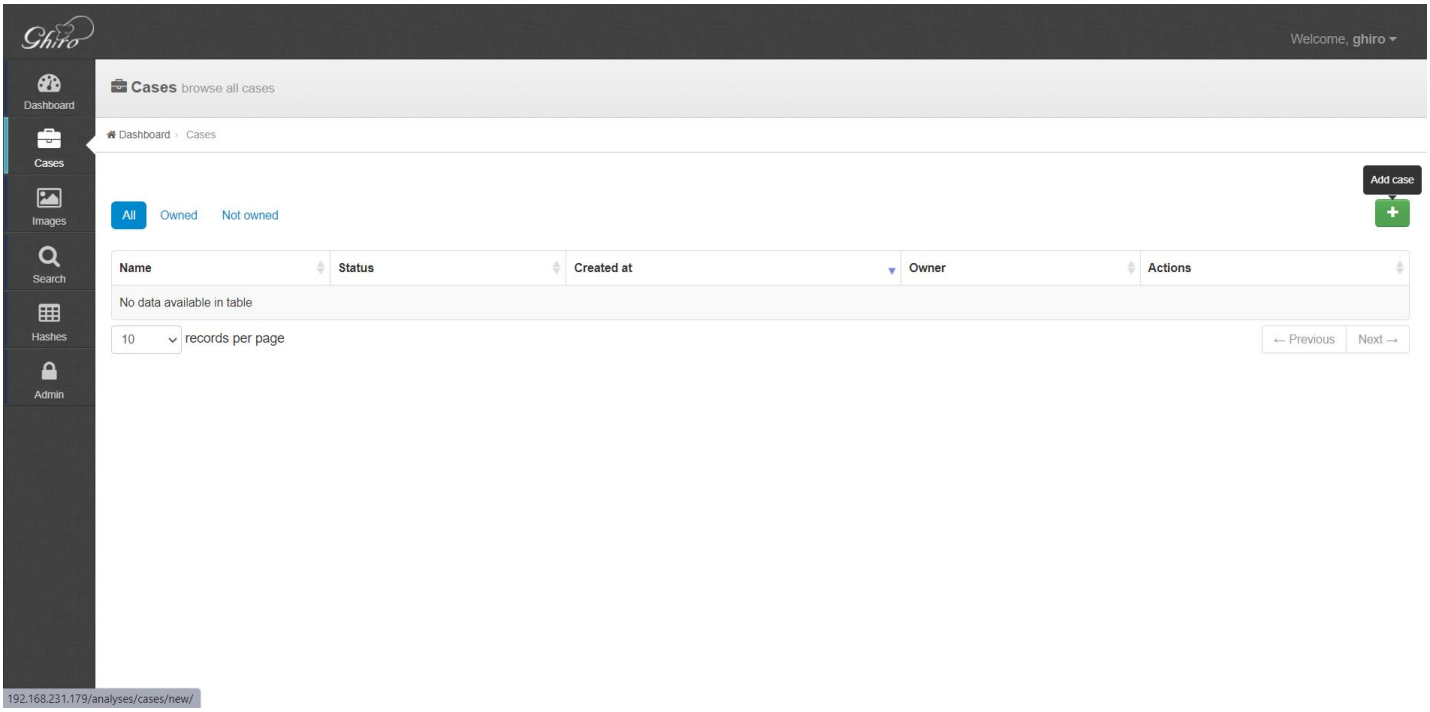
Now start the giro machine, the terminal will open login with the default id and password and then go to the respective ip address on your browser to login to ghiro and change the password,

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

HOW TO START
------------

Appliance IP address is: 192.168.1.7
To start using Ghiro point your browser to http://192.168.1.7

Default credentials:
  username: ghiro
  password: ghiromanager

*** Remember to change the password at your first access. ***
ghiroappliance login: ghiro
Password:
Last login: Thu Feb  9 06:13:12 UTC 2023 on tty1
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.19.0-25-generic i686)

 * Documentation:  https://help.ubuntu.com/
ghiro@ghiroappliance:~$ _
```

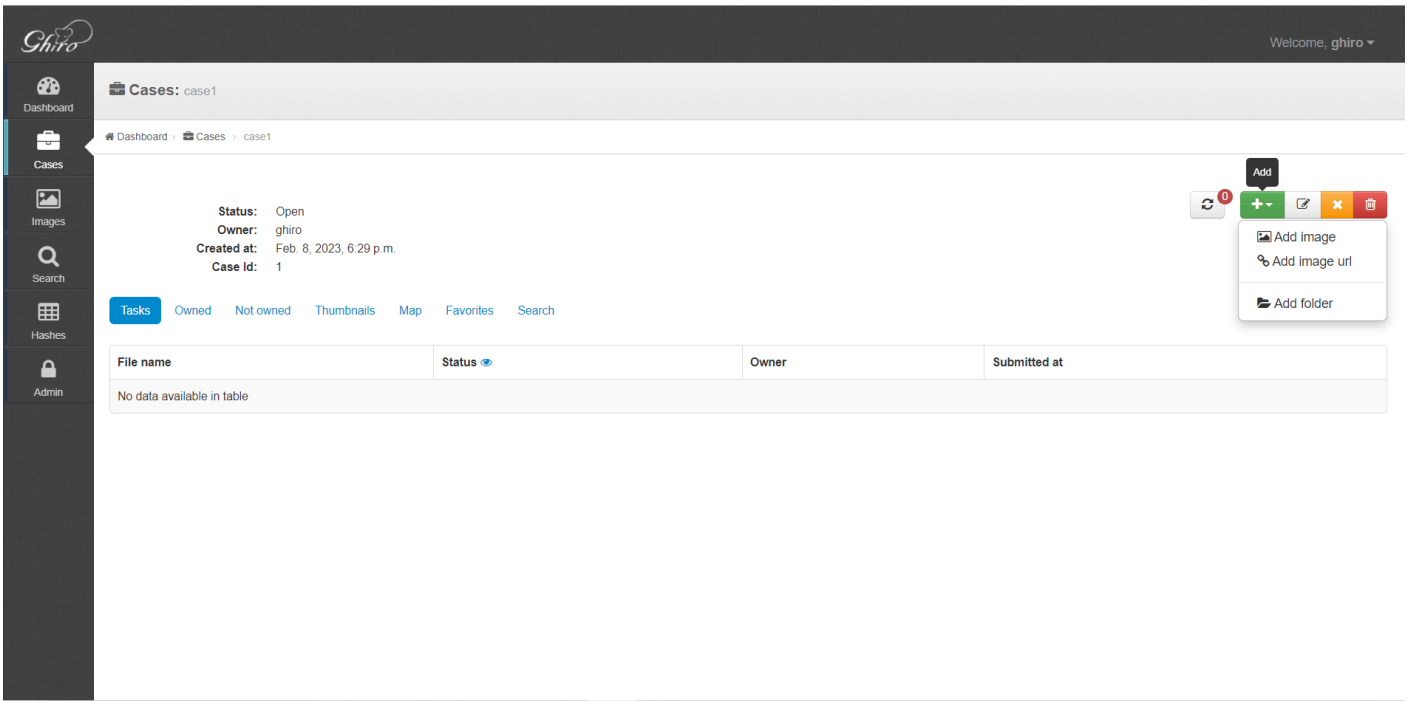
After login you can see the dashboard, For each user there is a unique API key,



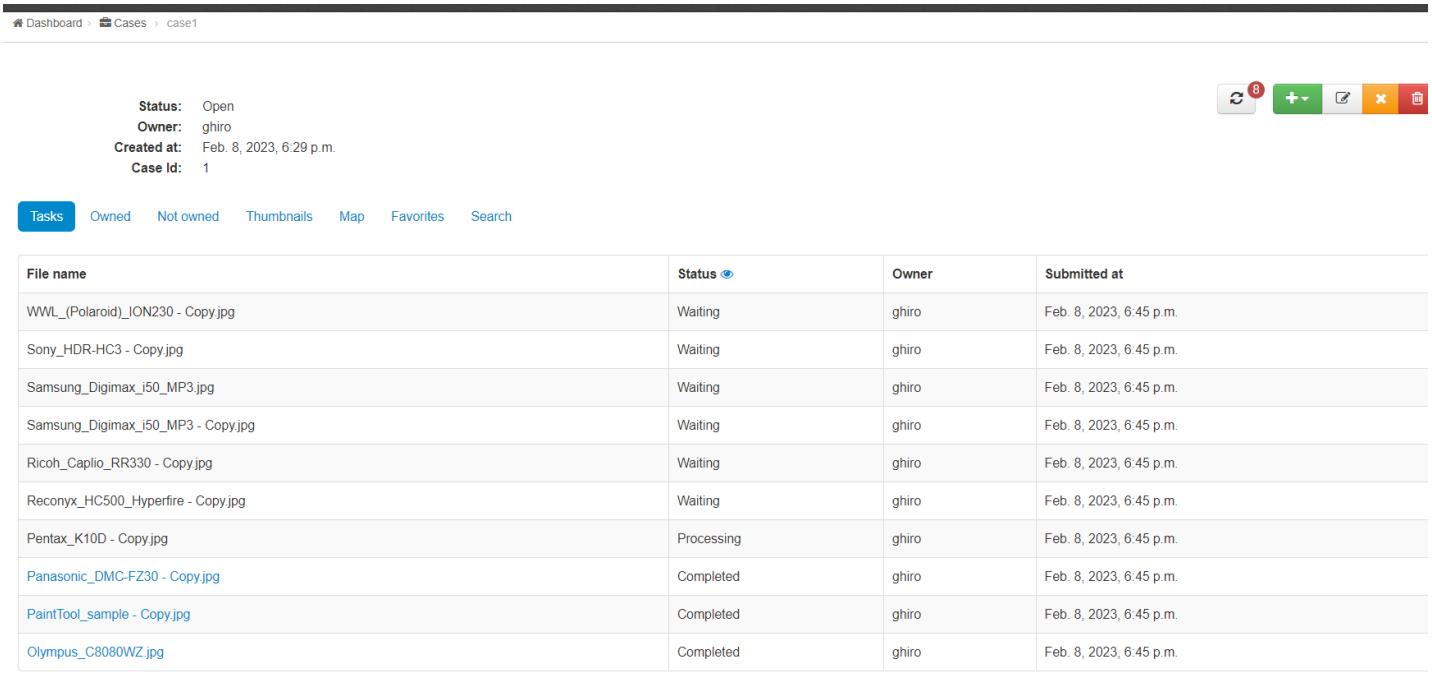
To start simply click on add case and provide the information like if the analysis is for any particular case then fill the details,



Simply add image, URL or a folder based on need,

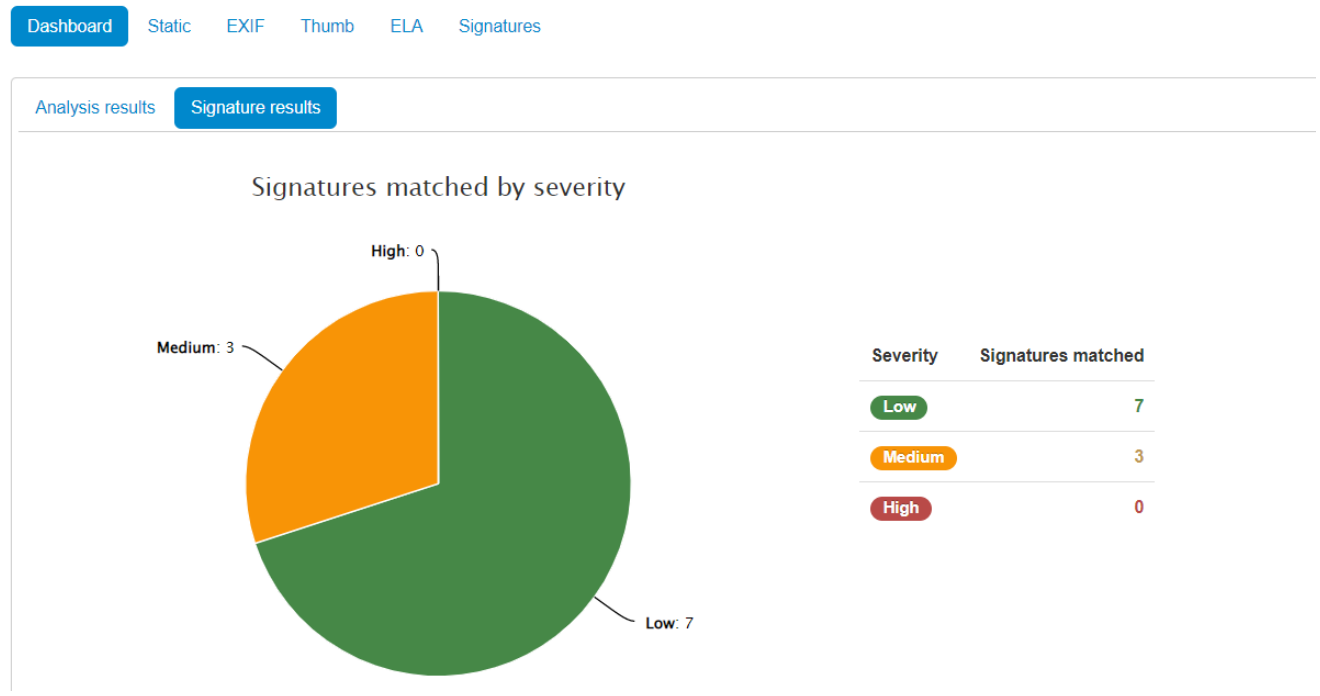


Added some images while its processing,

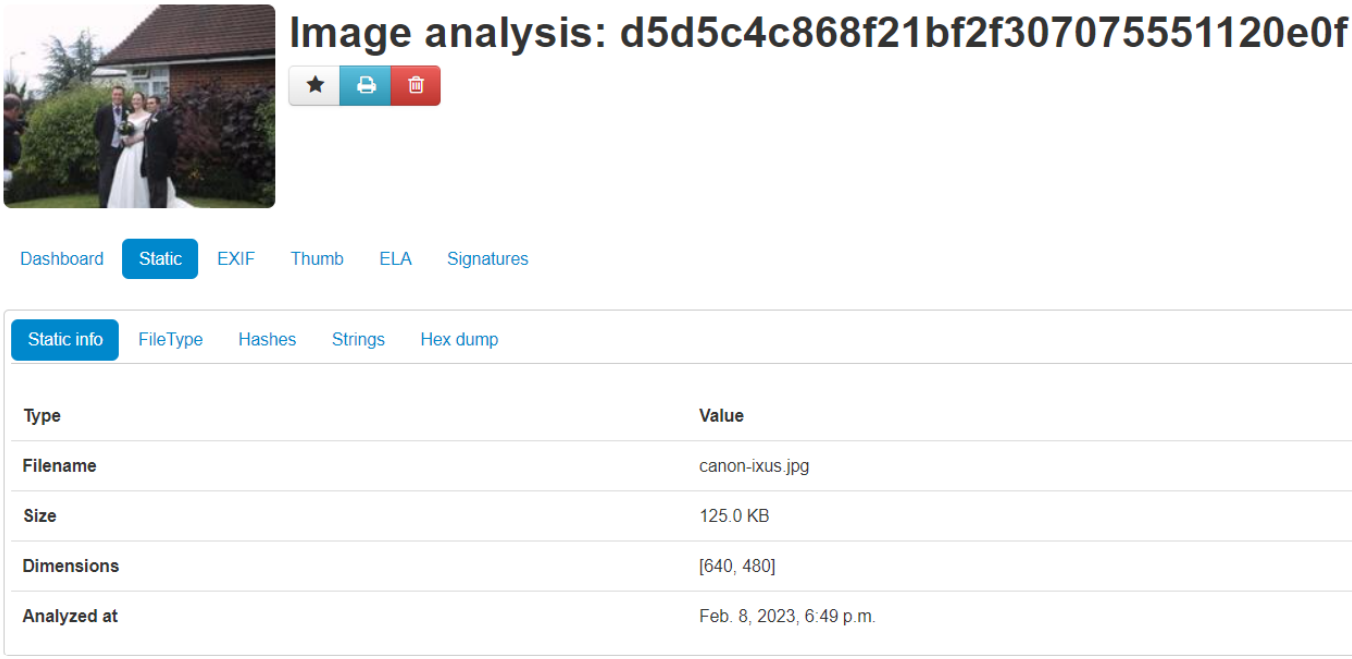


Analyzing each image here we found EXIF meta data, static data and other details from the below image,

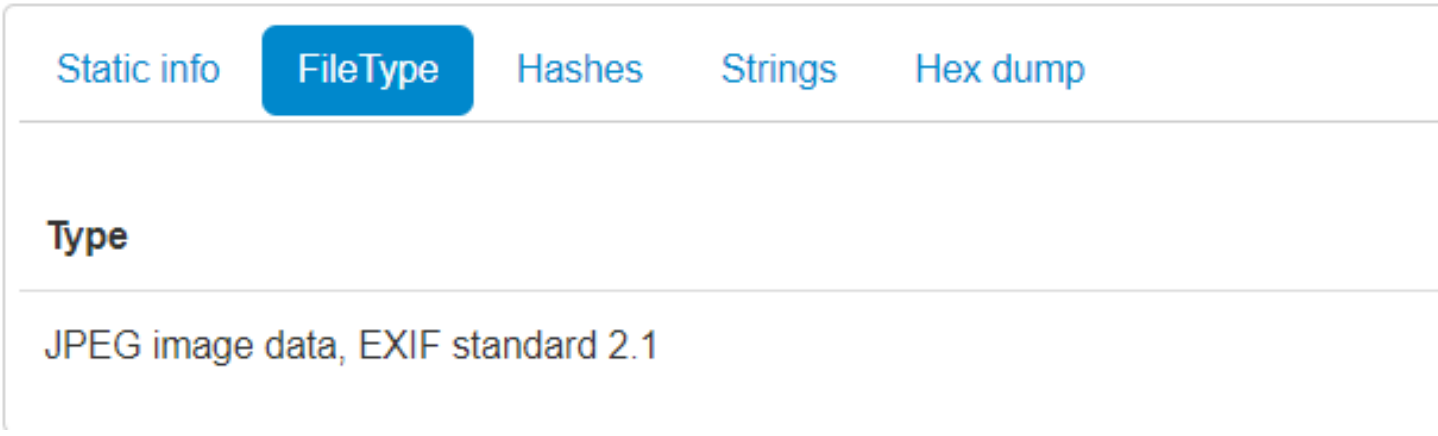
Here in the signature section it shows the severity of signature matched it means if an image file have a hash value and it is used somewhere else then the hash value still remains same, so this graph indicates how many times the image files has been used in other platforms.



Under the static section there is details of the images like- name, size, dimensions, time and date of analyzing



In file type there is information of format,



Hashes of the image file under hashes section,

Image analysis: d5d5c4c868f21bf2f307075551120e0f

Dashboard | Static | EXIF | Thumb | ELA | Signatures

Static info | FileType | Hashes | Strings | Hex dump

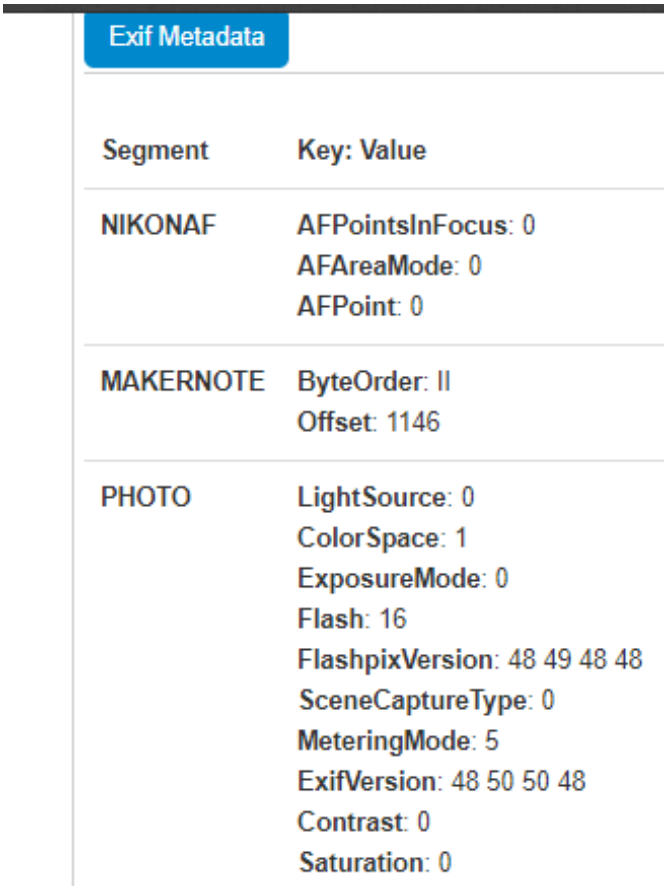
Type	Value
SHA1	82c61c54275982e72e1cfb13e4e3bba3e26b3da0
SHA224	b0a4ca9487beda8a0448b0993e01d3599500181d9f2297d9ca0c8535
SHA384	2597d28addeb5f76a00348ae5d718664287692ca3c4a7c35f66e2f58589fbb6bac8c06ed9f3aba2201037825aa0d9ce5
CRC32	786eae27
SHA256	b2d085bdb261cb2c56d8ba10d79175e38c0acd0d429afe19a4610eddee3b06fe
SHA512	d91edd0d0f3c78442032d571a2c0f0f53c124e811063852fc3c4e06a01b607c5cb7e7dd40954310f5b027d8ac7486d108b15f371965f3f9339ef6685637300ef
MD5	d5d5c4c868f21bf2f307075551120e0f

Here we can get Hexa value also that interprets the header of image file -

Static info | FileType | Hashes | Strings | **Hex dump**

```
0000  FF D8 FF E1 1B FE 45 78 69 66 00 00 49 49 2A 00 08 00 00 00 09 00 0F 01 02 00 06 00 00 00 7A 00  ......Exif..II*.............z.
0020  00 00 10 01 02 00 14 00 00 00 80 00 00 00 12 01 03 00 01 00 00 00 01 00 00 00 1A 01 05 00 01 00  ................................
0040  00 00 94 00 00 00 1B 01 05 00 01 00 00 00 9C 00 00 00 28 01 03 00 01 00 00 00 02 00 00 00 32 01  ................(...........2.
0060  02 00 14 00 00 00 A4 00 00 00 13 02 03 00 01 00 00 00 01 00 00 00 69 87 04 00 01 00 00 00 B8 00  ..................i.........
0080  00 00 76 04 00 00 43 61 6E 6F 6E 00 43 61 6E 6F 6E 20 44 49 47 49 54 41 4C 20 49 58 55 53 00 00  ..v...Canon.Canon DIGITAL IXUS..
00A0  B4 00 00 00 01 00 00 00 B4 00 00 00 01 00 00 00 32 30 30 31 3A 30 36 3A 30 39 20 31 35 3A 31 37  ................2001:06:09 15:17
00C0  3A 33 32 00 1B 00 9A 82 05 00 01 00 00 00 CA 02 00 00 9D 82 05 00 01 00 00 00 D2 02 00 00 00 90  :32............................
00E0  07 00 04 00 00 00 30 32 31 30 03 90 02 00 14 00 00 00 02 02 00 00 04 90 02 00 14 00 00 00 16 02  ......0210......................
0100  00 00 01 91 07 00 04 00 00 00 01 02 03 00 02 91 05 00 01 00 00 00 B2 02 00 00 01 92 0A 00 01 00  ................................
0120  00 00 BA 02 00 00 02 92 05 00 01 00 00 00 C2 02 00 00 04 92 0A 00 01 00 00 00 DA 02 00 00 05 92  ................................
0140  05 00 01 00 00 00 E2 02 00 00 06 92 05 00 01 00 00 00 EA 02 00 00 07 92 03 00 01 00 00 00 02 00  ................................
0160  00 00 09 92 03 00 01 00 00 00 00 00 00 00 0A 92 05 00 01 00 00 00 F2 02 00 00 7C 92 07 00 36 01  ..........................|...6.
0180  00 00 FA 02 00 00 86 92 07 00 88 00 00 00 2A 02 00 00 00 A0 07 00 04 00 00 00 30 31 30 30 01 A0  ..............*...........0100..
01A0  03 00 01 00 00 00 01 00 00 00 02 A0 03 00 01 00 00 00 80 02 00 00 03 A0 03 00 01 00 00 00 E0 01  ................................
01C0  00 00 05 A0 04 00 01 00 00 00 40 04 00 00 0E A2 05 00 01 00 00 00 30 04 00 00 0F A2 05 00 01 00  ..........@...........0.........
01E0  00 00 38 04 00 00 10 A2 03 00 01 00 00 00 02 00 00 00 17 A2 03 00 01 00 00 00 02 00 00 00 00 A3  ..8.............................
0200  07 00 01 00 00 00 03 00 00 00 00 00 00 00 32 30 30 31 3A 30 36 3A 30 39 20 31 35 3A 31 37 3A 33  ..............2001:06:09 15:17:3
0220  32 00 32 30 30 31 3A 30 36 3A 30 39 20 31 35 3A 31 37 3A 33 32 00 00 00 00 00 00 00 00 00 00 00  2.2001:06:09 15:17:32...........
0240  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 00 00  ................................
0260  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 00 00  ................................
```

Under EXIF section – we can find Exif Meta data of image file like (file name , size, capturing details, time of capture, resolution , focal length , file date, location details, image orientation , IOP etc.) -

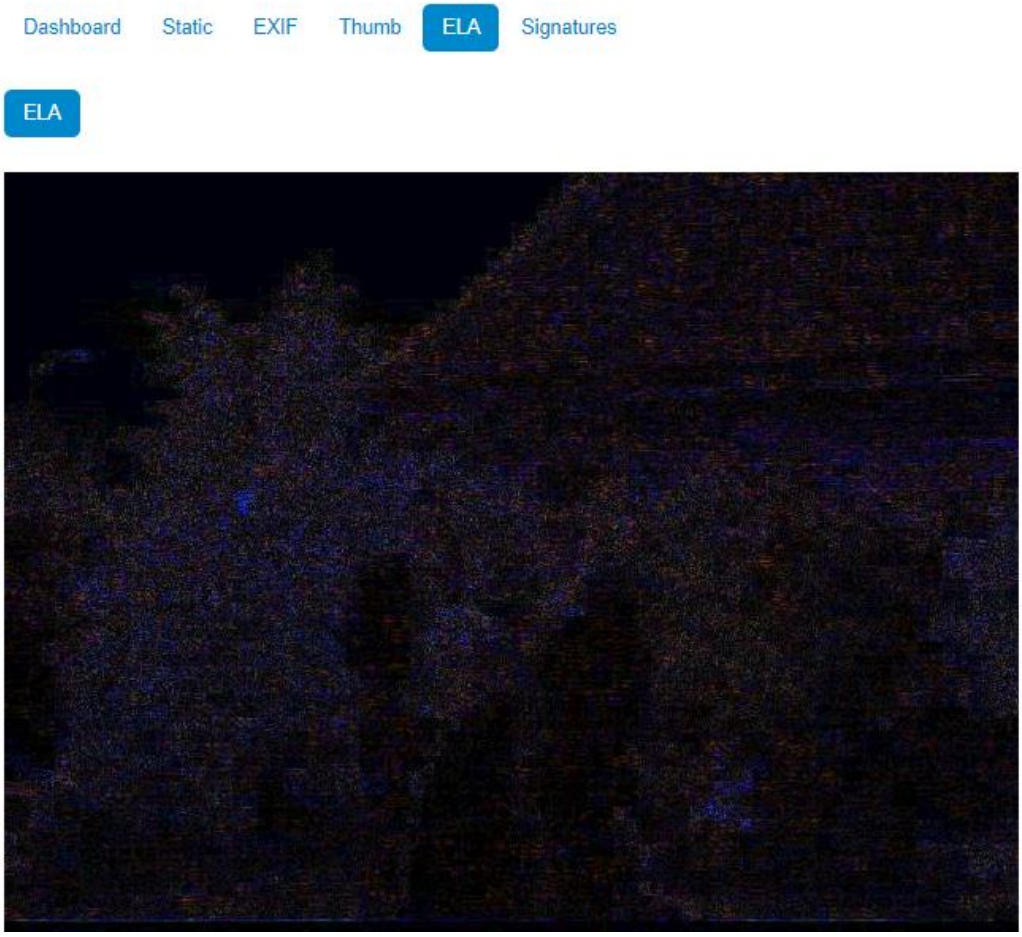


	82 77 65 76 32 32 0 0 48 49 48 48 83 84 65 78 68 65 82 68 32 32 32 0 0 0 0 0 0 0 0 0 83 84 65 78 68 65 82 68 32 32 32 0 0 0 0 0 0 0 0 0 1 0 0 0 2 130 0 0 255 128 255 25 **ExposureProgram**: 2 **FocalLengthIn35mmFilm**: 38 **PixelXDimension**: 640 **FocalLength**: 81/10 **ExposureBiasValue**: 0/10 **DateTimeOriginal**: 2008:10:22 16:43:21 **UserComment**: charset="Ascii" **SceneType**: 1 **SubjectDistanceRange**: 0 **WhiteBalance**: 0 **DateTimeDigitized**: 2008:10:22 16:43:21 **FNumber**: 37/10 **CustomRendered**: 0 **PixelYDimension**: 480 **ComponentsConfiguration**: 1 2 3 0 **ISOSpeedRatings**: 64 **ExposureTime**: 813669/100000000 **FileSource**: 3 **MaxApertureValue**: 29/10 **Sharpness**: 0 **InteroperabilityTag**: 896 **GainControl**: 0 **DigitalZoomRatio**: 0/100
NIKON3	**ColorMode**: COLOR **NoiseReduction**: OFF **Version**: 48 50 49 48 **Saturation**: 0 **0x00bd**: 48 49 48 48 83 84 65 78 68 65 82 68 32 32 32 0 0 0 0 0 0 0 0 0 83 84 65 78 68 65 82 68 32 32 32 0 0 0 0 0 0 0 0 0 1 0 0 0 2 130 0 0 255 128 255 255 255 255 **ScanIFD**: 3292 **ImageAdjustment**: NORMAL **FlashSetting**: **0x000a**: 9321/1000

	ISOSelection: AUTO SceneAssist: Sharpening: NORMAL AuxiliaryLens: OFF ImageStabilization: VR-ON ISOSpeed: 0 0 0x009d: 0 0x009b: 0 0 0x0021: 1 0 64 1 240 0 0 0 RetouchHistory: 0 0 0 0 0 0 ShotInfo: 0 0 0 0 3 0 0 0 0 0 0 0 0 0 0 68 67 0 0 Focus: AF-S WhiteBalance: AUTO SceneMode: DigitalZoom: 1/1 CaptureVersion: COOLPIX P6000V1.0 0x002f: 0 ActiveDLighting: 0 0x00b2: NORMAL 0x0e22: 0 0 0 0 Quality: FINE
GPSINFO	GPSTimeStamp: 14/1 41/1 4903/100 GPSLongitude: 11/1 52/1 538859999/10000000 GPSLatitudeRef: N GPSDateStamp: 2008:10:23 GPSSatellites: 05 GPSLatitude: 43/1 28/1 611400000/100000000 GPSMapDatum: WGS-84 GPSLongitudeRef: E GPSAltitudeRef: 0
IMAGE	YResolution: 300/1 GPSTag: 926 ExifTag: 268 Make: NIKON ImageDescription: ResolutionUnit: 2 DateTime: 2008:11:01 21:15:09 YCbCrPositioning: 1 XResolution: 300/1 Orientation: 1 Model: COOLPIX P6000 Software: Nikon Transfer 1.1 W
IOP	InteroperabilityIndex: R98 InteroperabilityVersion: 48 49 48 48
THUMBNAIL	YResolution: 72/1 ResolutionUnit: 2 Compression: 6 XResolution: 72/1 JPEGInterchangeFormatLength: 5628 JPEGInterchangeFormat: 4548

Under thumbnail section, we can see preview of the image file,

Under ELA (error level analysis) section, we can see image file in this format and if any object in the image is of different color shade it can be interpreted as a manipulated one.



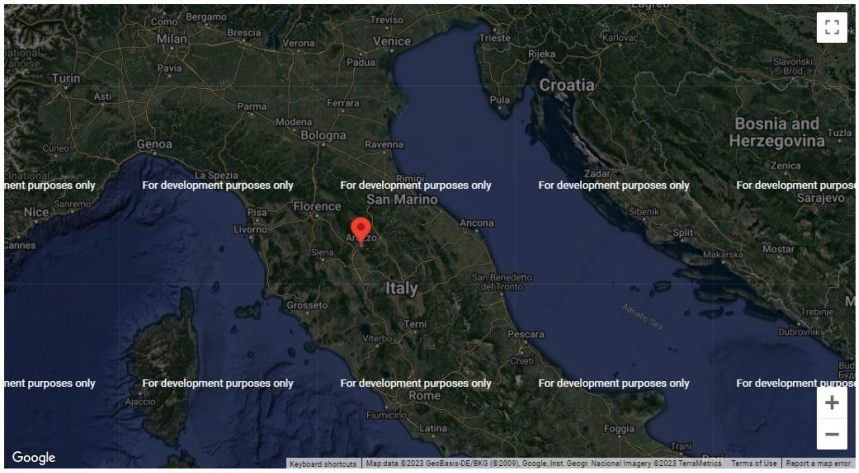
Xmp Metadata shows other information like the software used for photoshop if any, and other details,

XMP Metadata

Segment	Key: Value
XMPMM	InstanceID: uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b
TIFF	Orientation: 1 software: Microsoft Windows Photo Gallery 6.0.6001.18000
XMP	creatortool: Microsoft Windows Photo Gallery 6.0.6001.18000

Under GPS we have latitude and longitude,

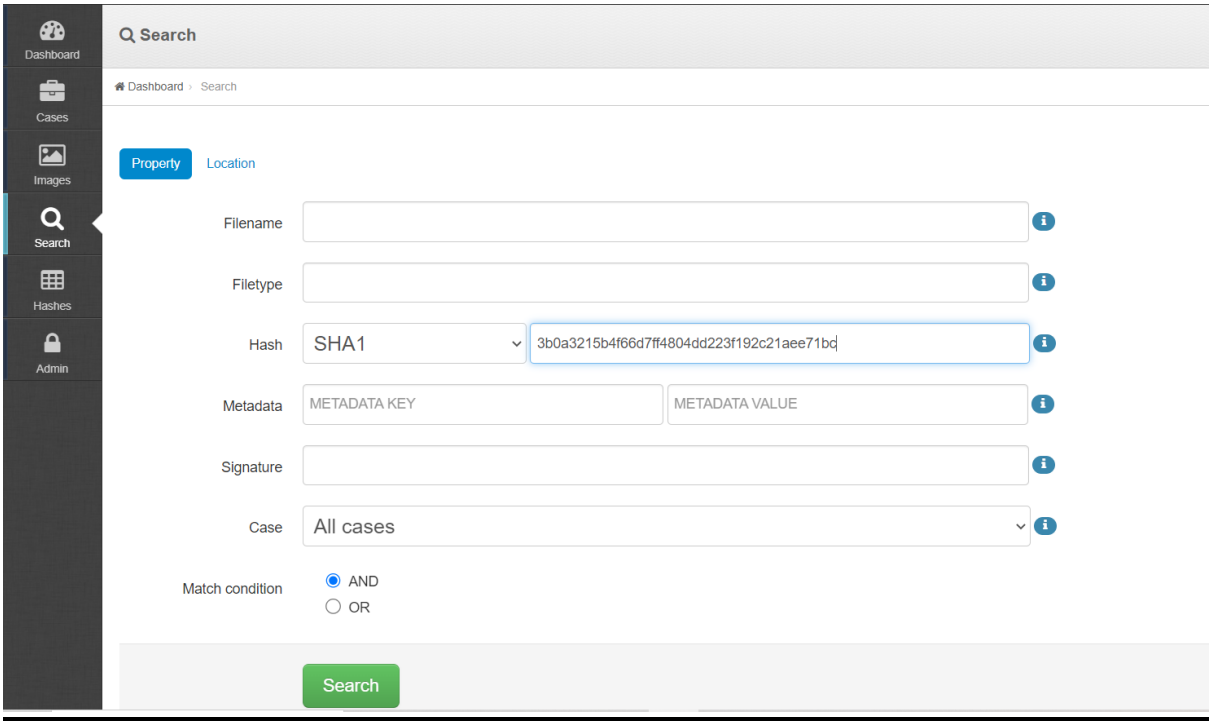
GPS Localization

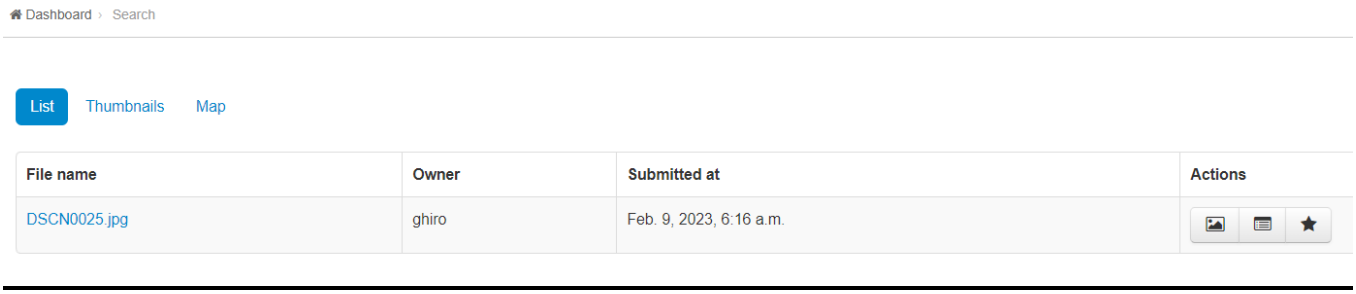


GPSTIMESTAMP	14/1 41/1 4903/100
GPSLONGITUDE	11/1 52/1 538859999/10000000
GPSLATITUDEREF	N
GPSDATESTAMP	2008:10:23
GPSSATELLITES	05
GPSLATITUDE	43/1 28/1 611400000/100000000
GPSMAPDATUM	WGS-84
GPSLONGITUDEREF	E
GPSALTITUDEREF	0

Latitude	43.468365
Longitude	11.881635
Altitude	0.0

In the search section we can search for an image file if we have any of the information from the fields here we are searching through hash value -





sherloq

It is a python-based digital image forensics tool using qt as GUI.

User may need to install python and related packages to run this app.

It has more advanced image forensics tools such as Copy-Move Forgery, Composite Splicing, and others etc.

Interface-

Support for many formats (JPEG, PNG, TIFF, BMP, WebP, PGM, PFM, GIF)

Highly responsive image viewer with real-time pan and zoom

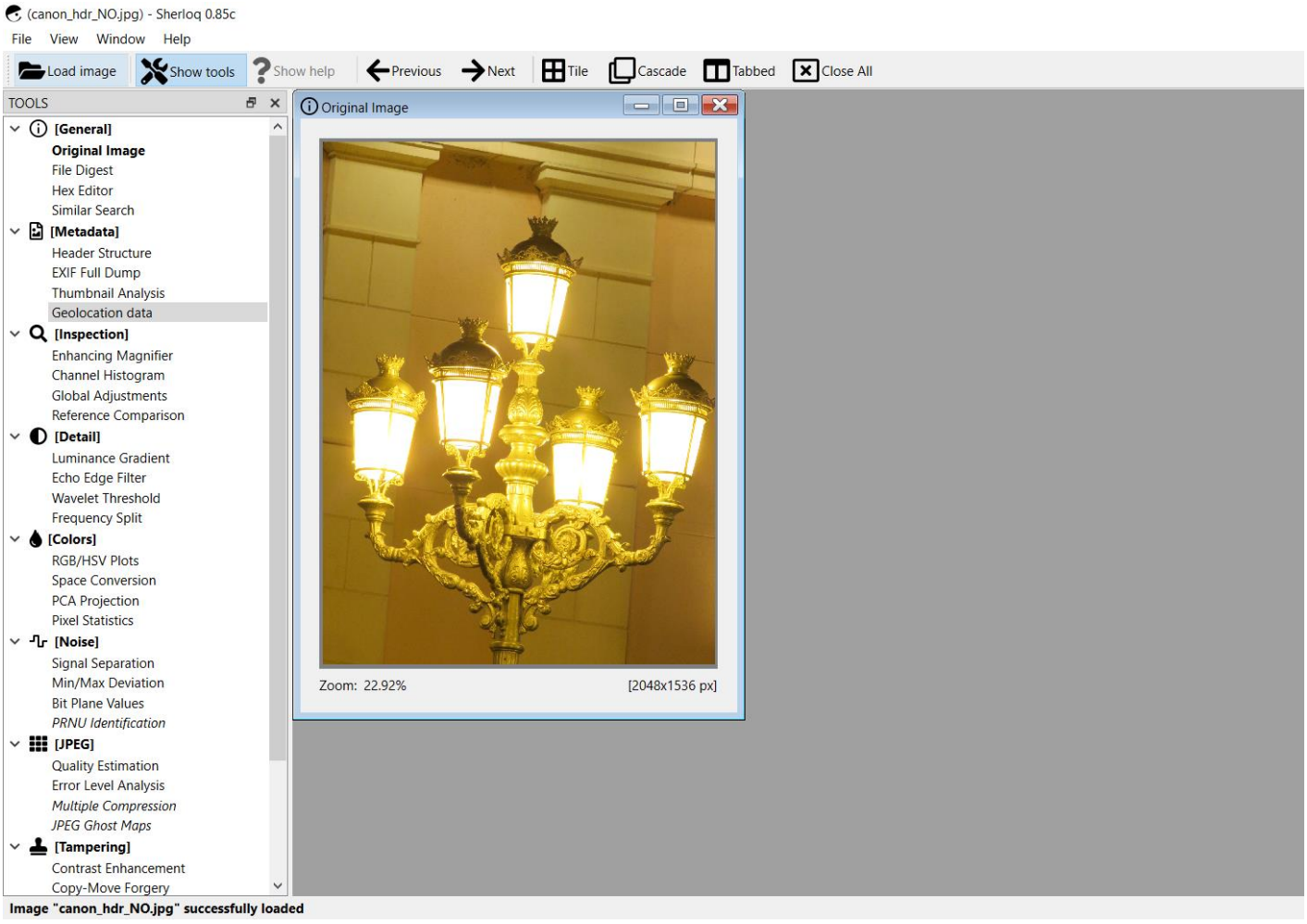
Export both visual and textual results of the analysis

Install the tool from the github based on the OS (windows/Linux/MacOS)-

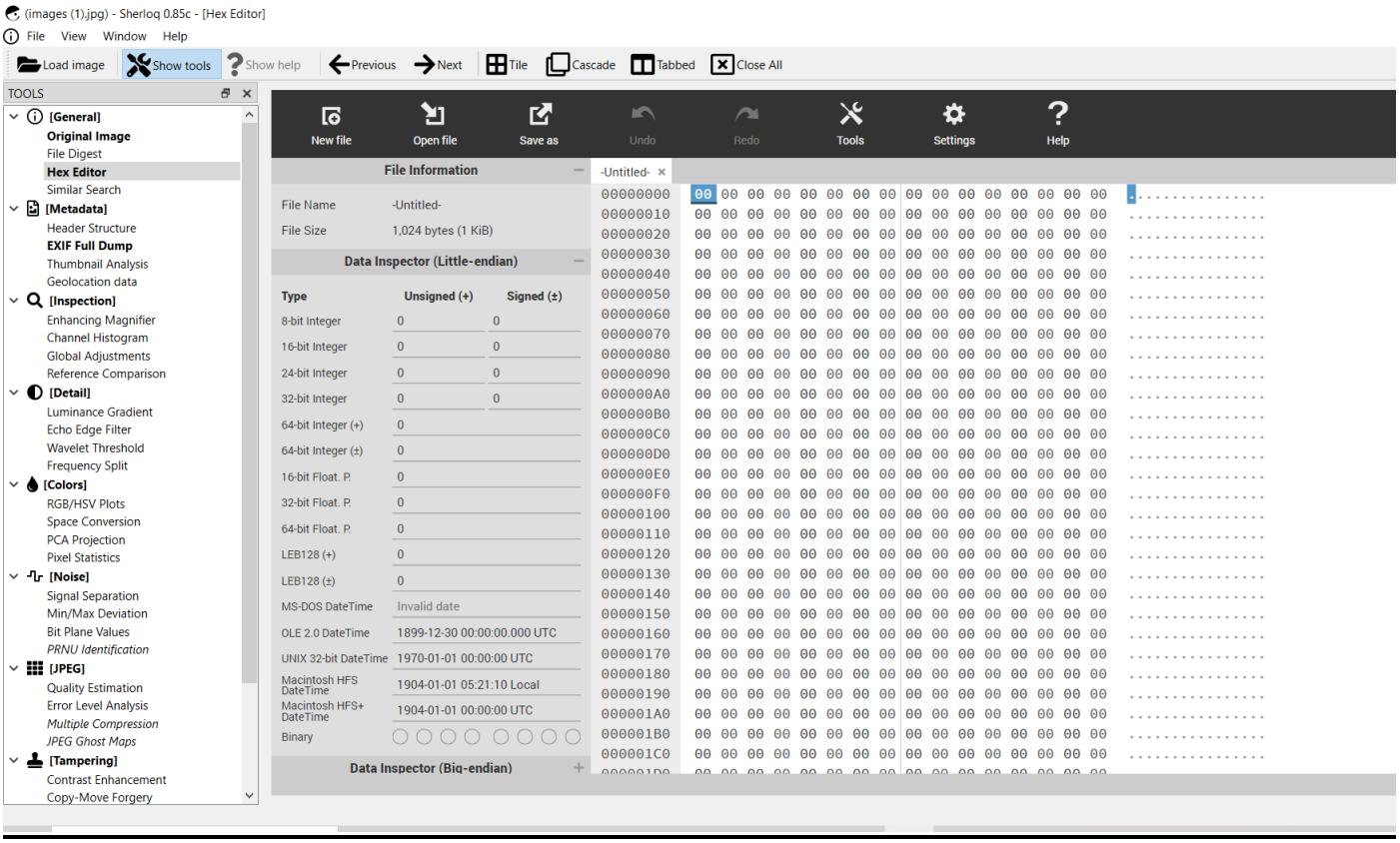
https://github.com/GuidoBartoli/sherloq

Follow the instruction to install the tool and run the command “python sherlo.py” to start the GUI interface of the tool,

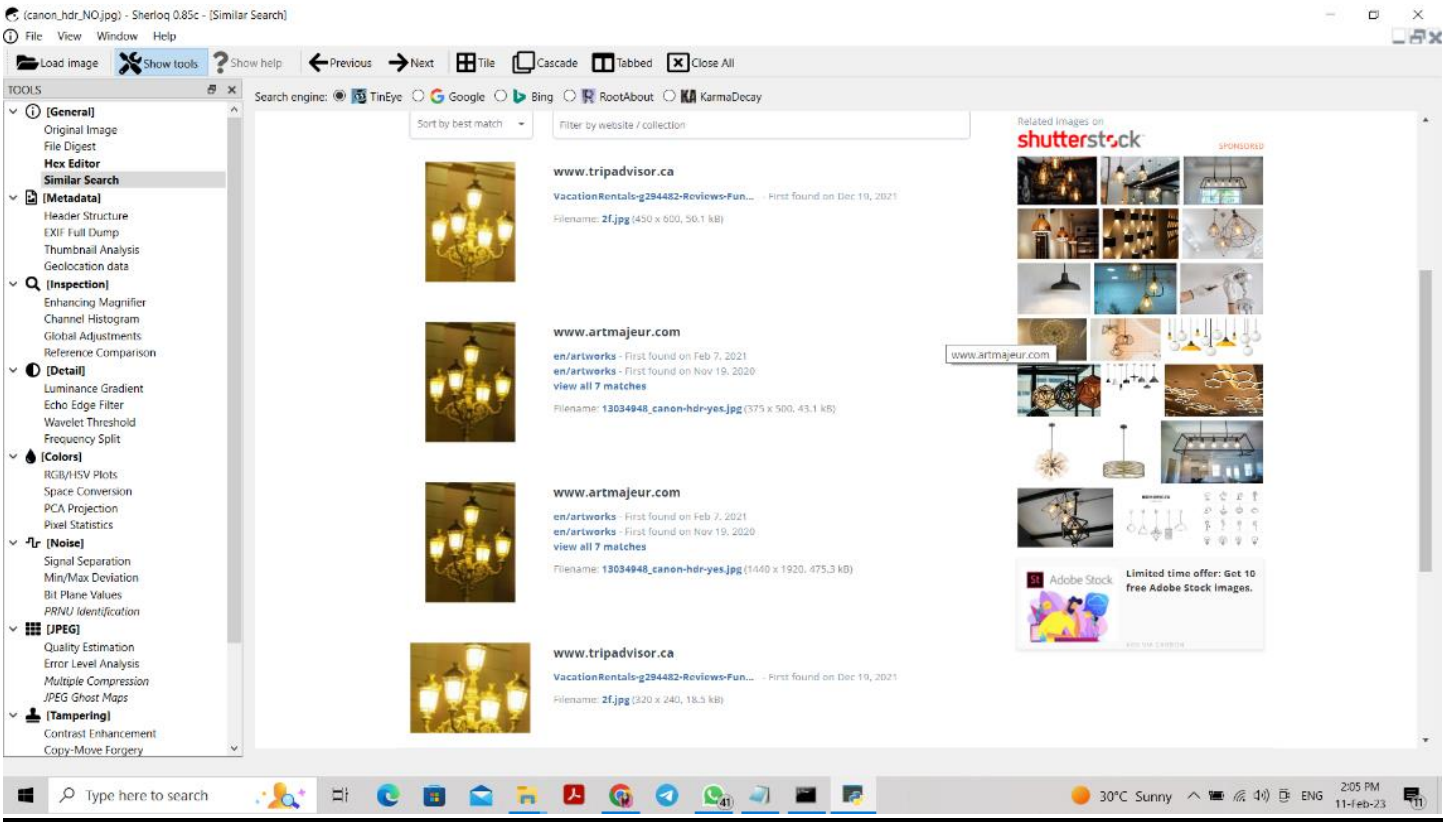
Load the image in the working interface –



Under General information of the image we can find the hex editor,

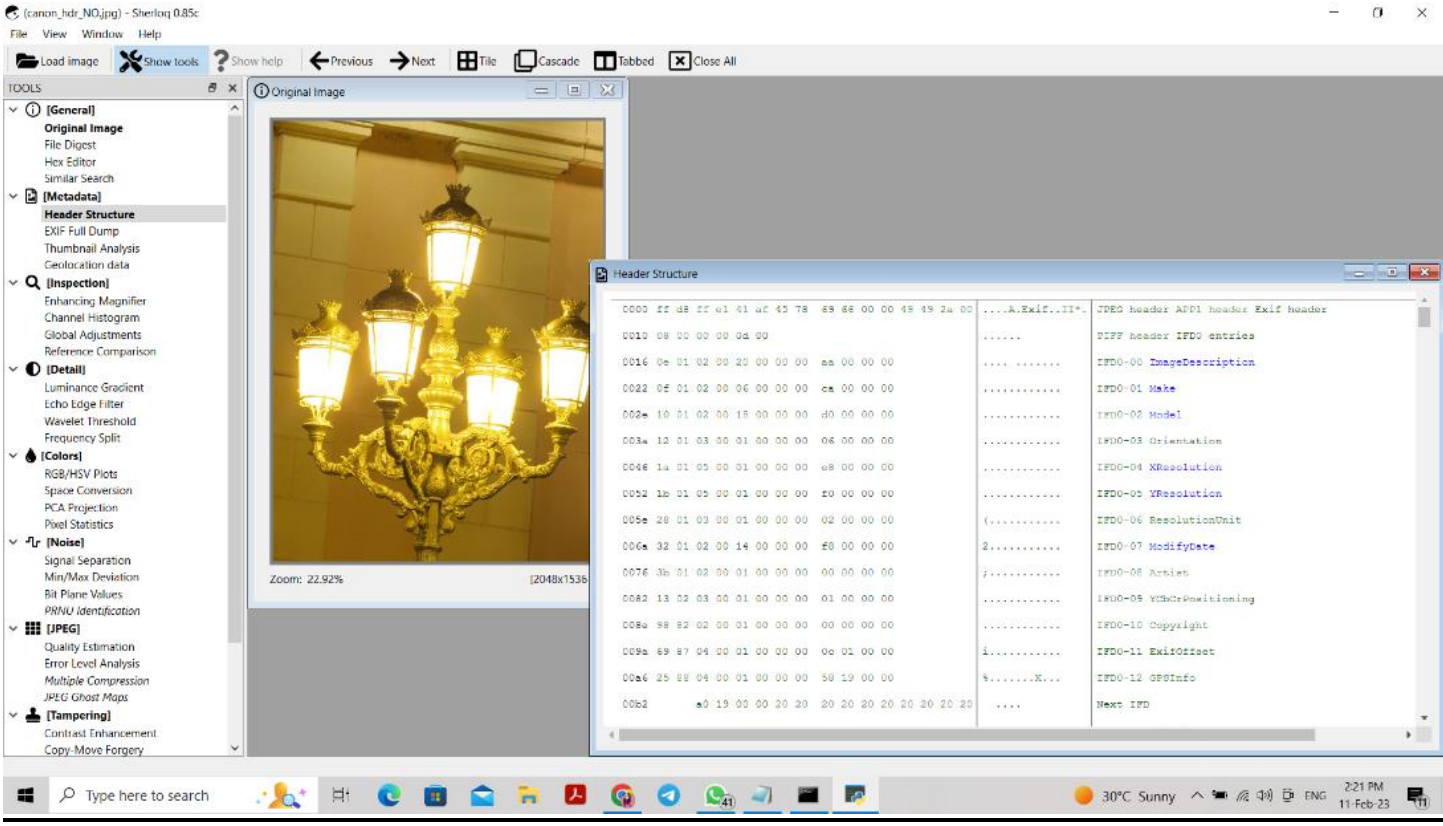


Similar search tool where can find similar images from web –

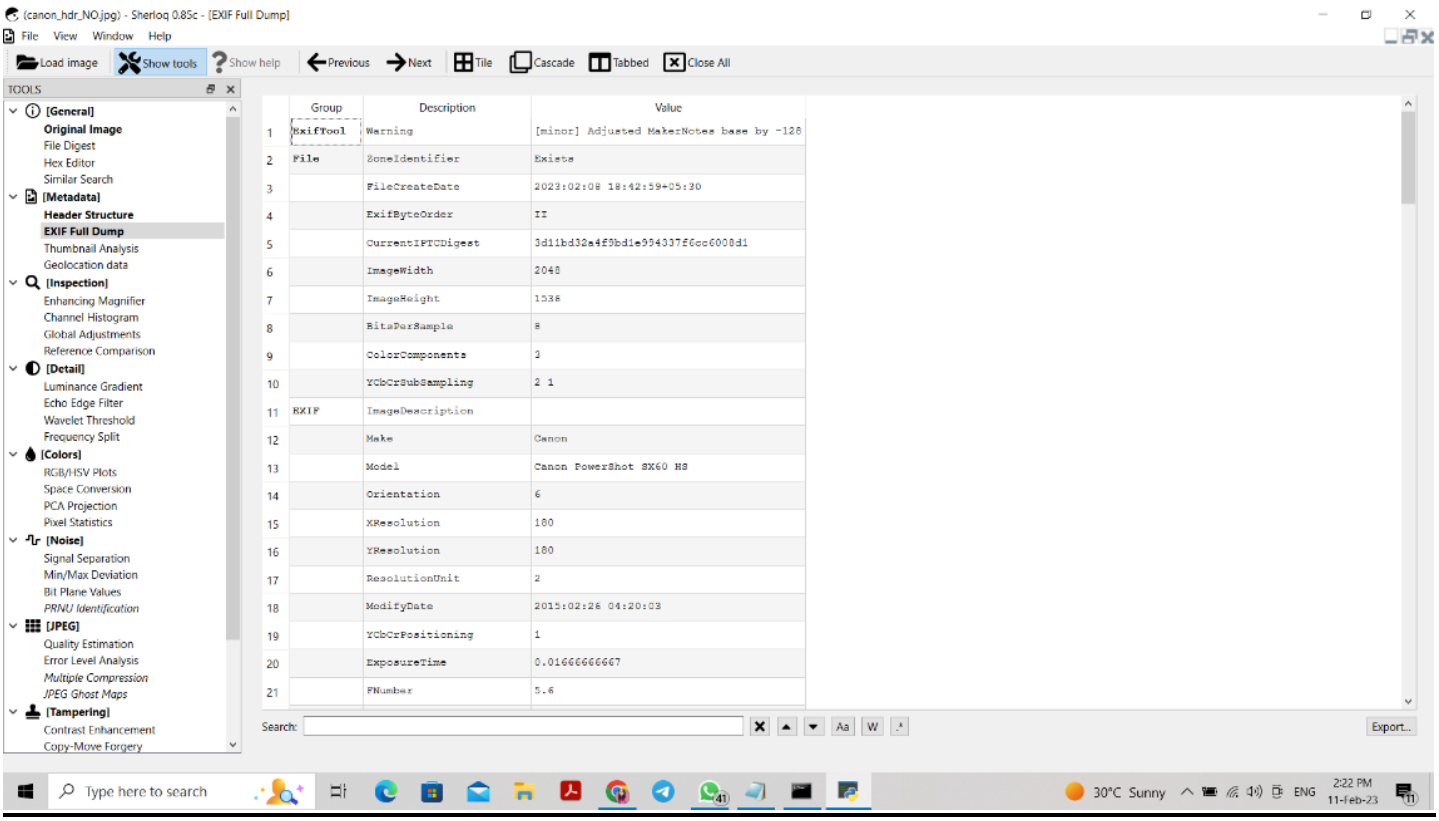


Under Meta data,

Header structure-

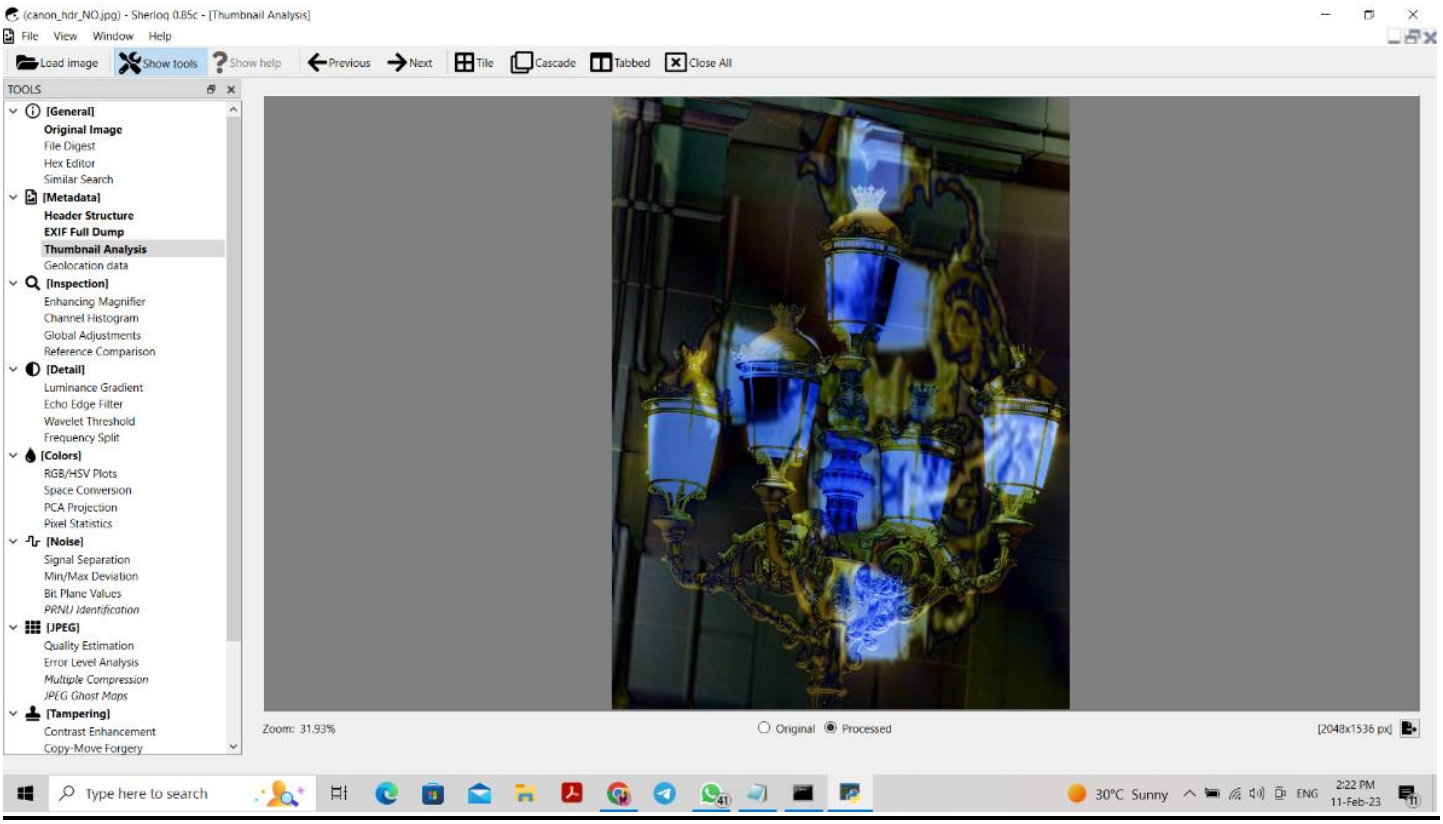


Exif full Dump-



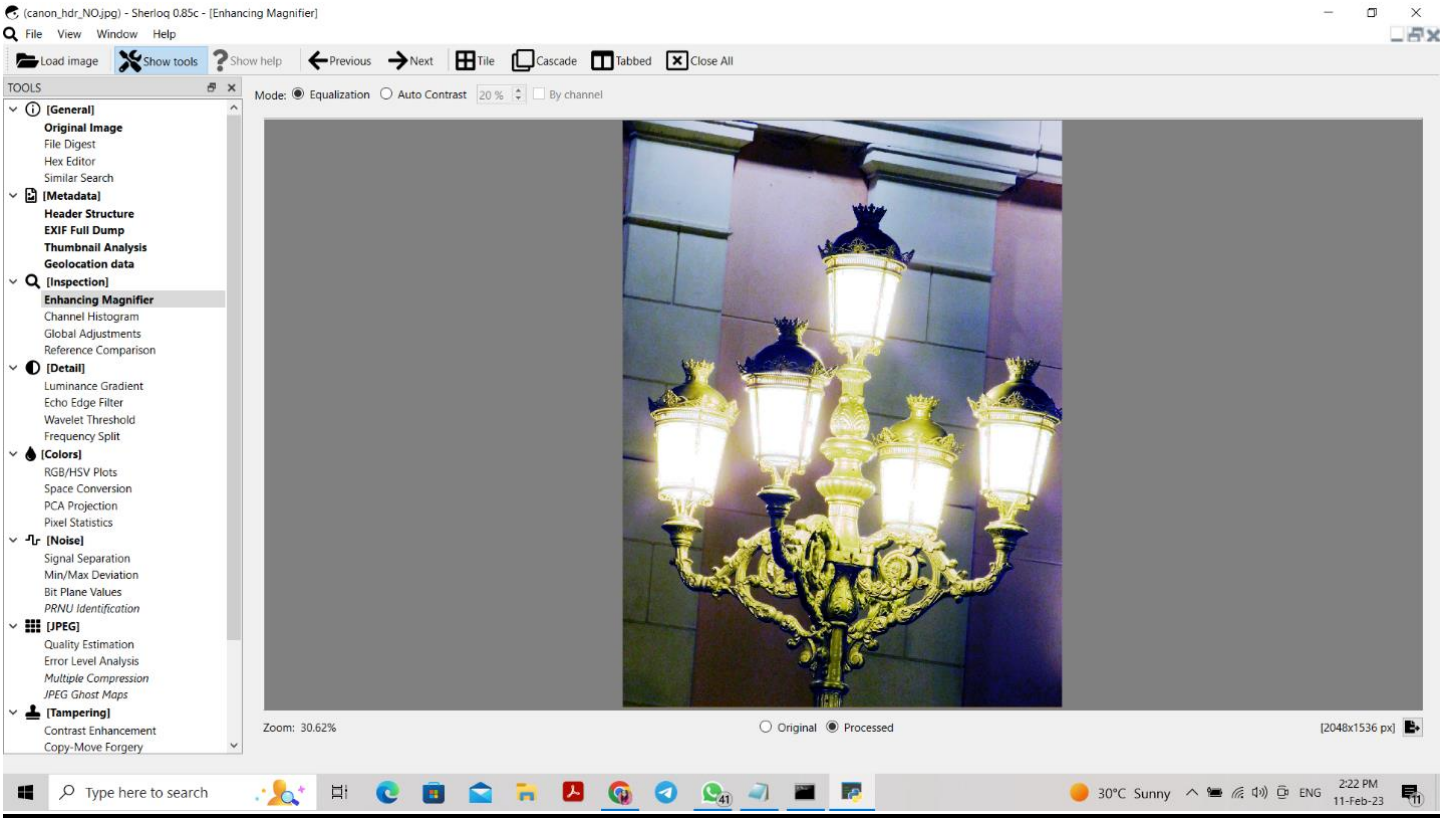
	Group	Description	Value
1	ExifTool	Warning	[minor] Adjusted MakerNotes base by -128
2	File	ZoneIdentifier	Exists
3		FileCreateDate	2023:02:08 18:42:59+05:30
4		ExifByteOrder	II
5		CurrentIPTCDigest	3d11bd32a4f9bd1e994337f6cc6008d1
6		ImageWidth	2048
7		ImageHeight	1536
8		BitsPerSample	8
9		ColorComponents	3
10		YCbCrSubSampling	2 1
11	EXIF	ImageDescription	
12		Make	Canon
13		Model	Canon PowerShot SX60 HS
14		Orientation	6
15		XResolution	180
16		YResolution	180
17		ResolutionUnit	2
18		ModifyDate	2015:02:26 04:20:03
19		YCbCrPositioning	1
20		ExposureTime	0.01666666667
21		FNumber	5.6

Thumbnail analysis-

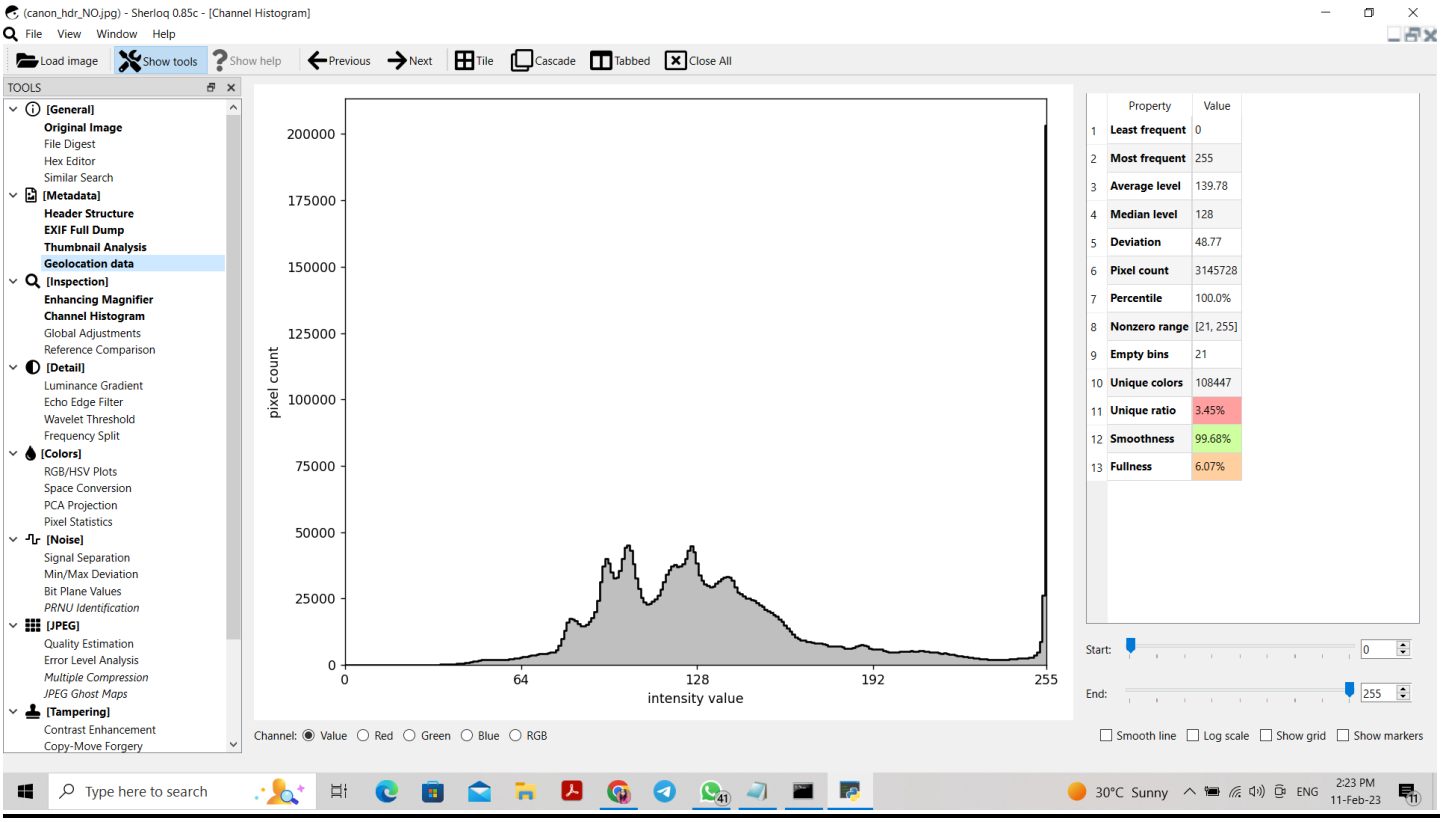


Under Inspection,

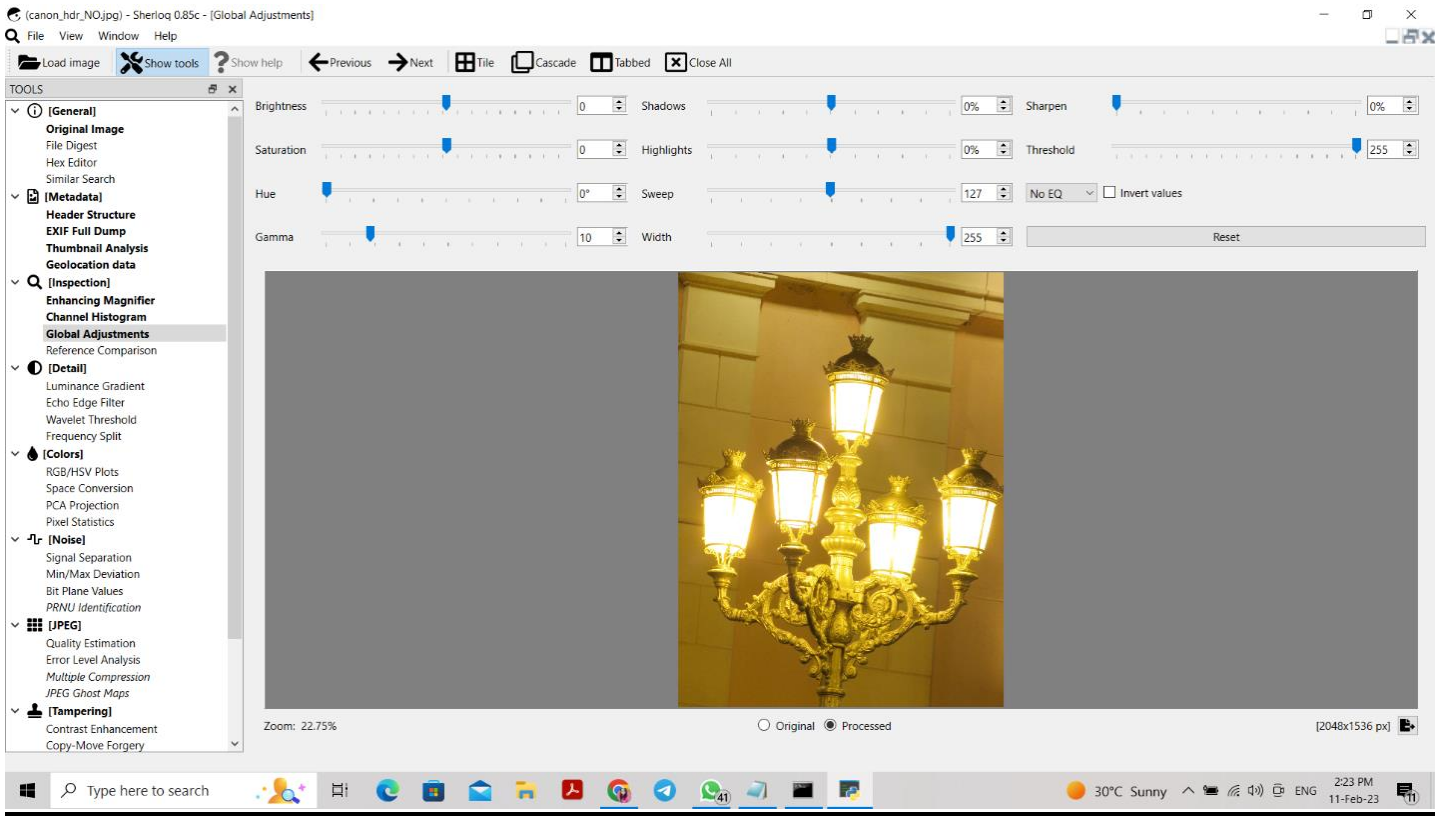
Enhancing magnifier-



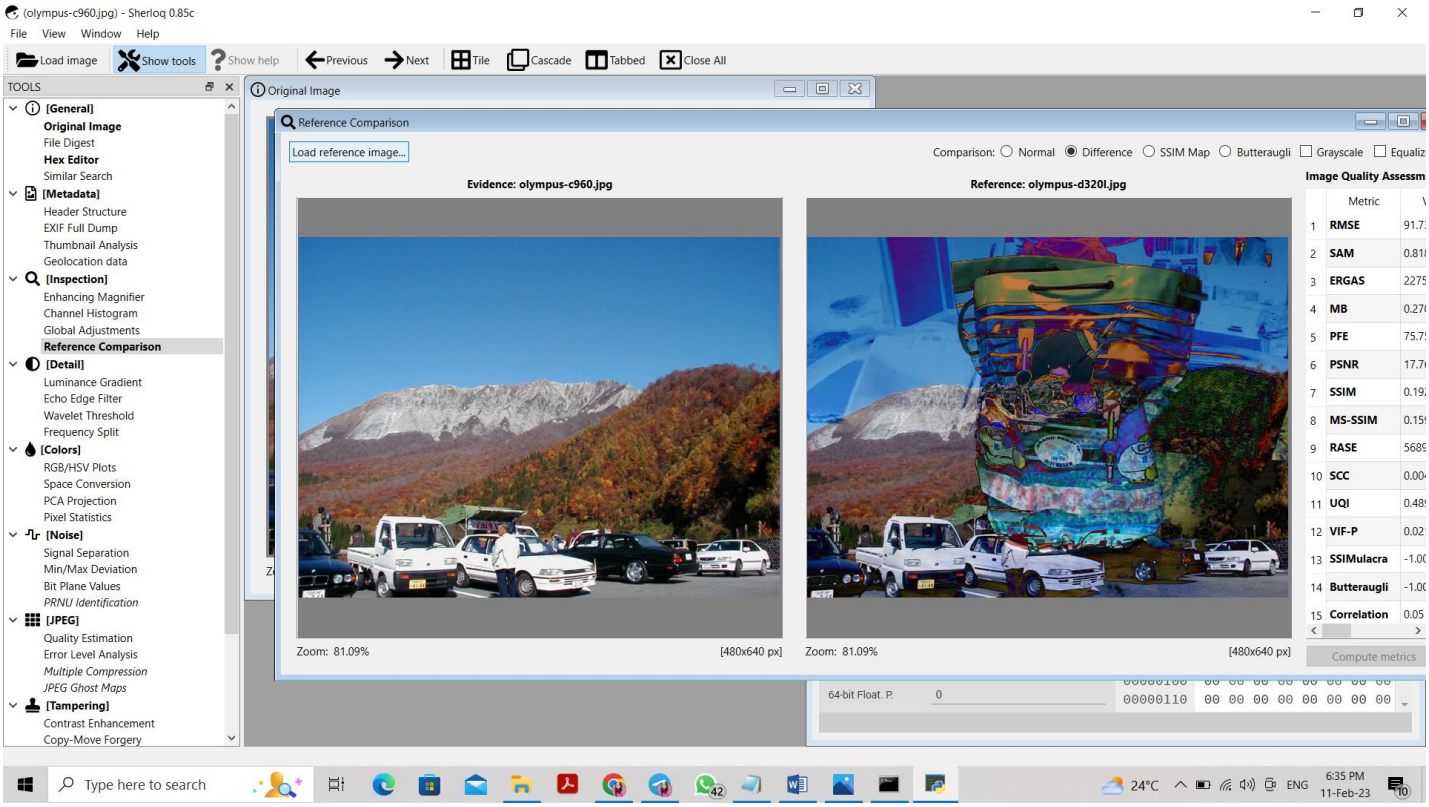
Channel histogram-



Global adjustments-

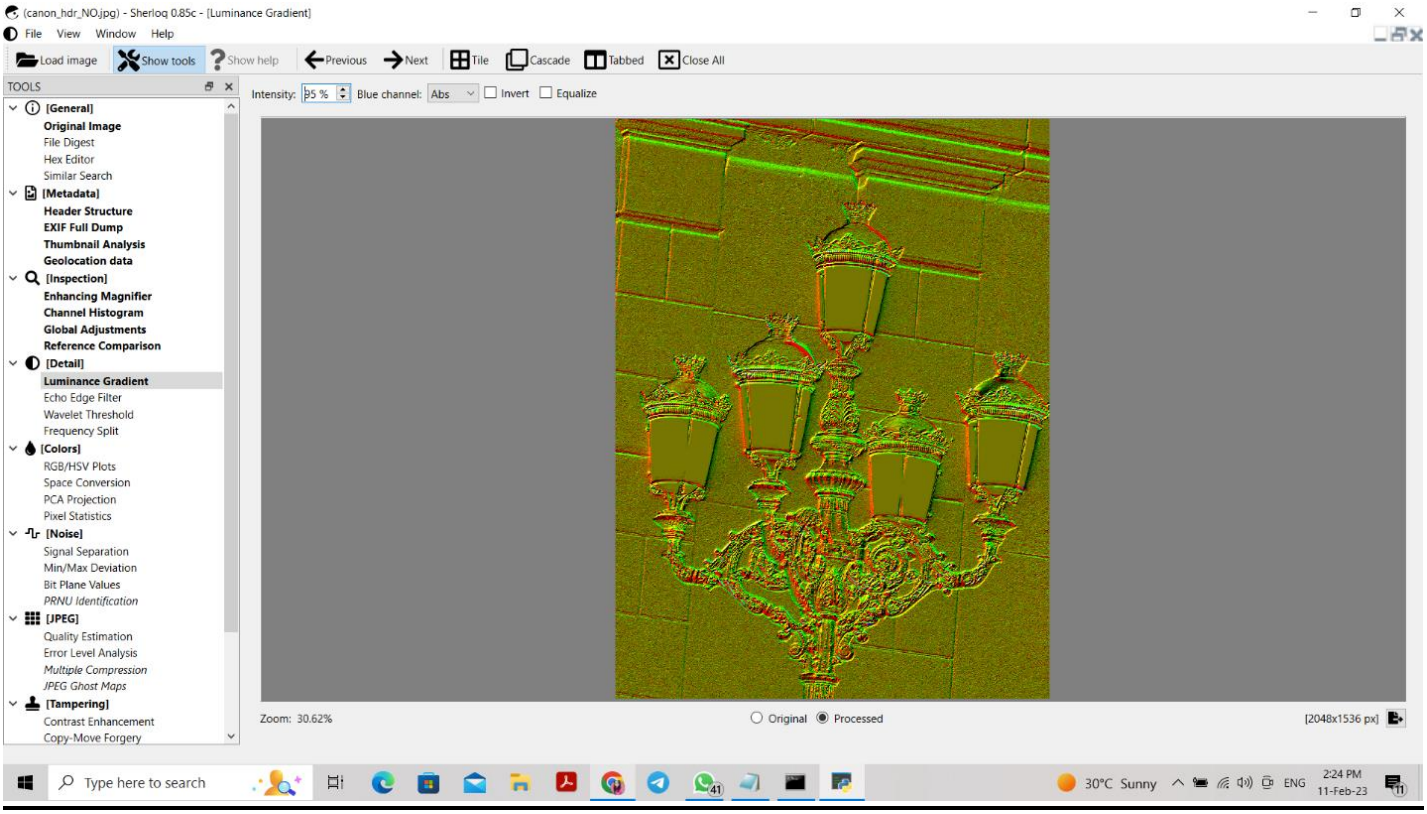


Reference Comparison-

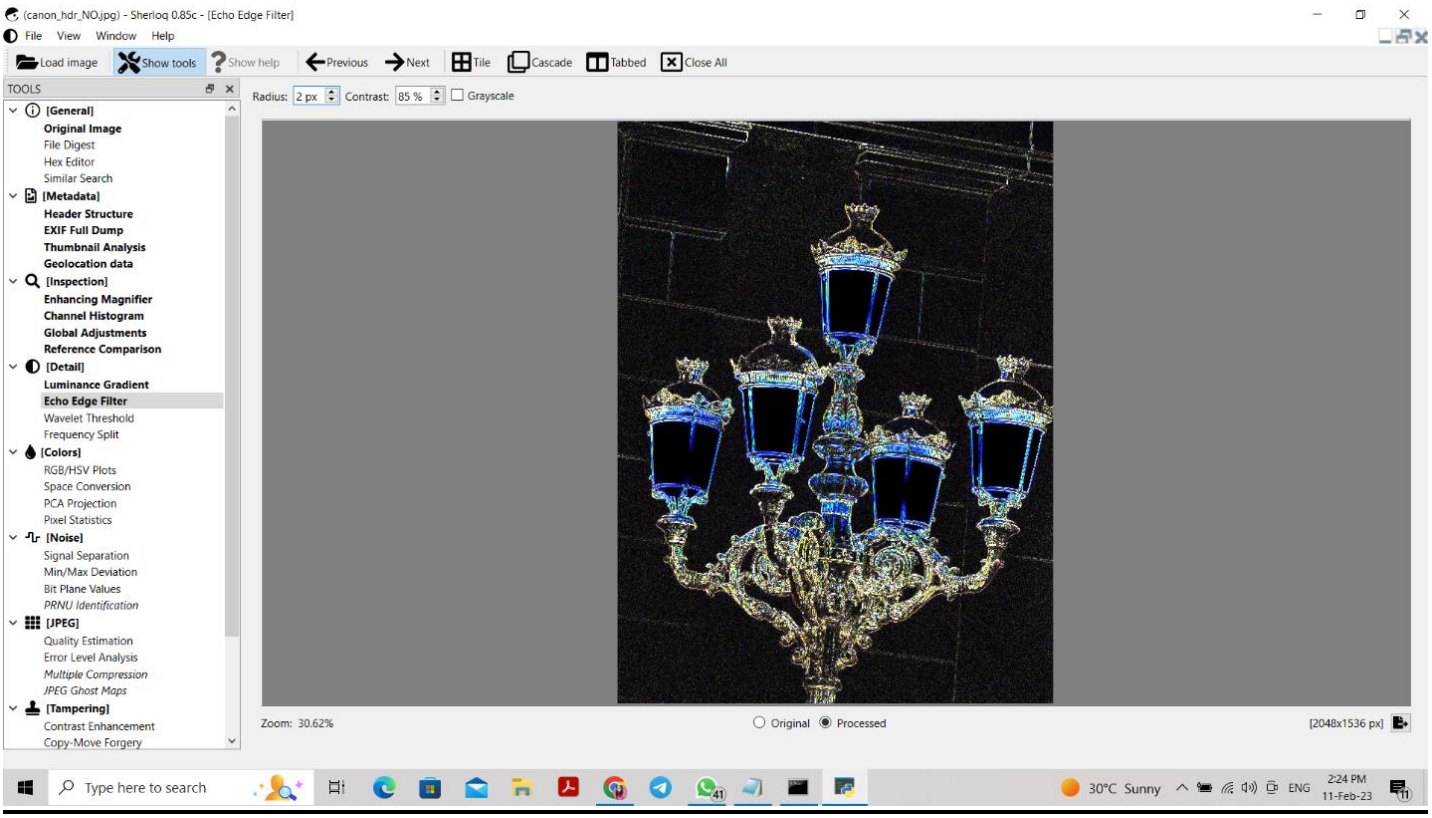


Under detail,

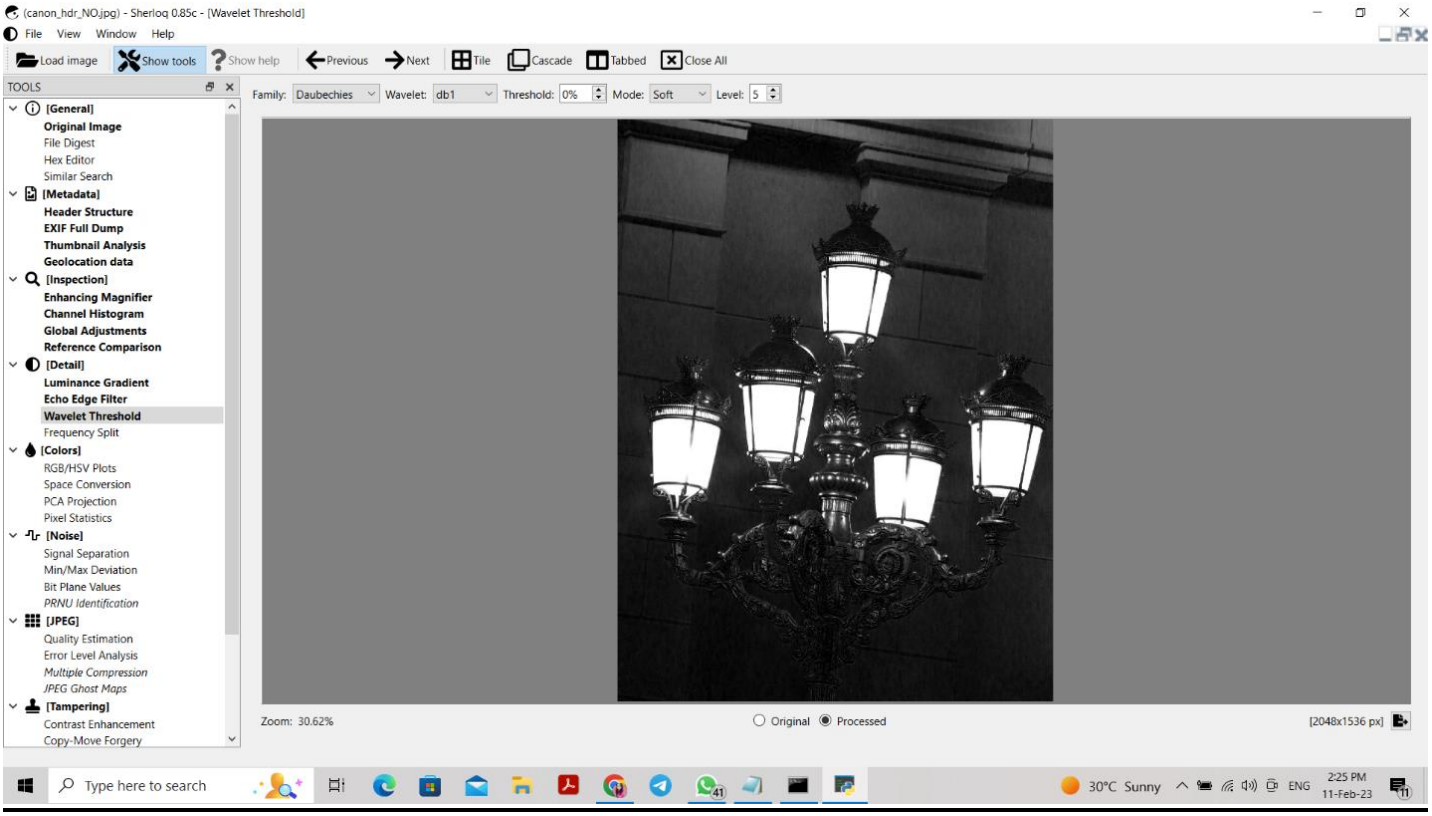
Luminance gradient -



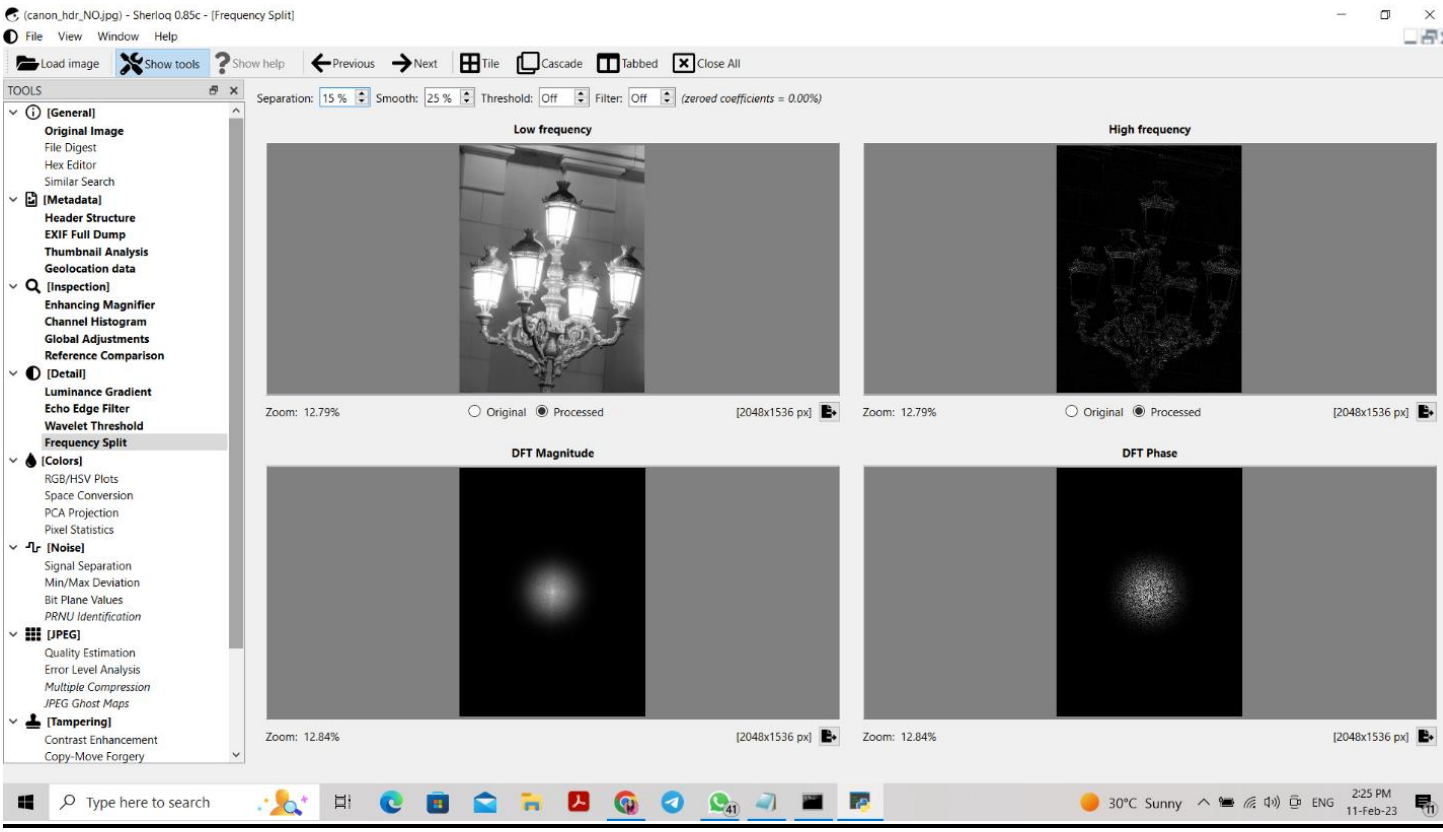
Echo edge filter-



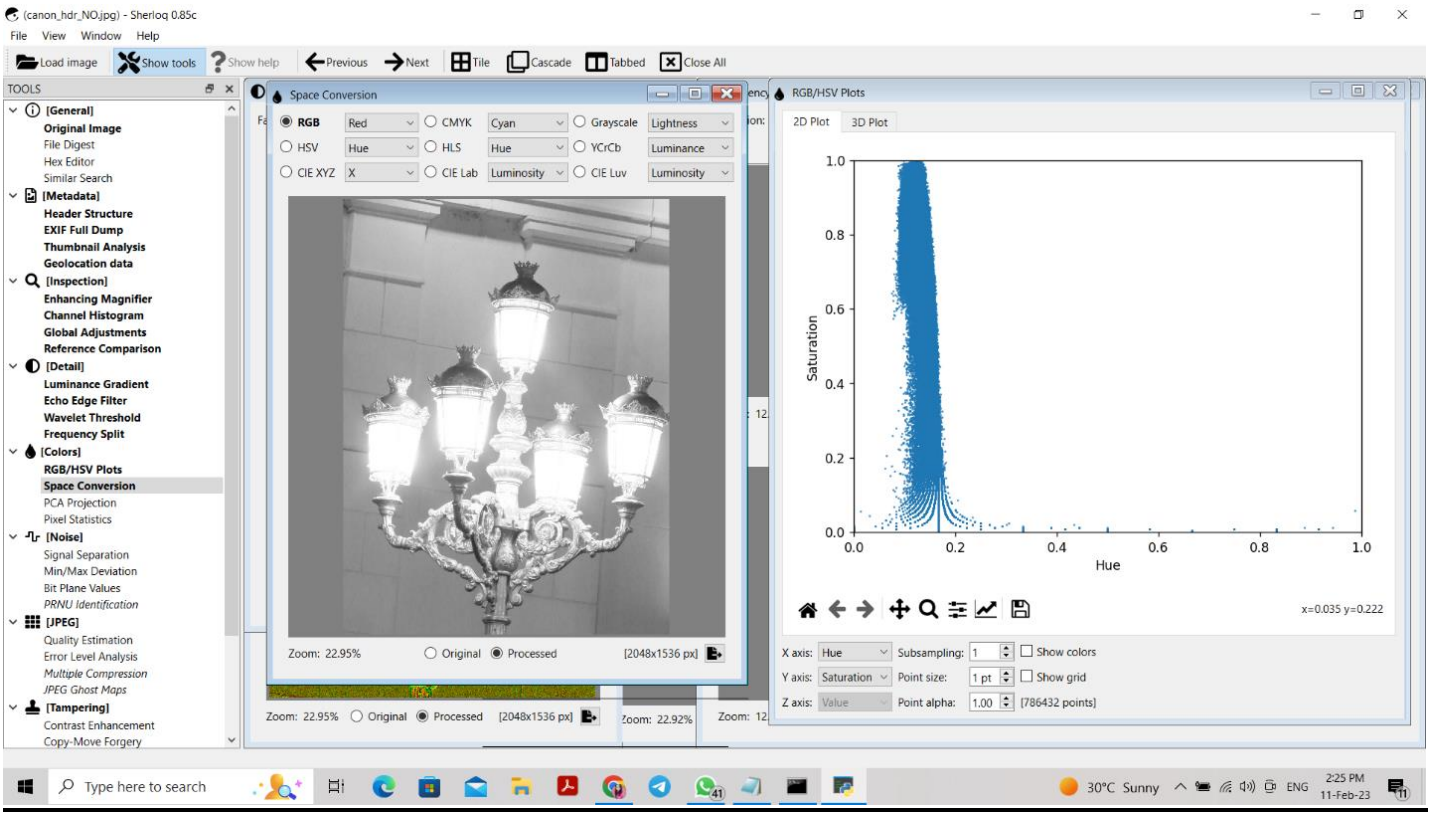
Wavelet Threshold-



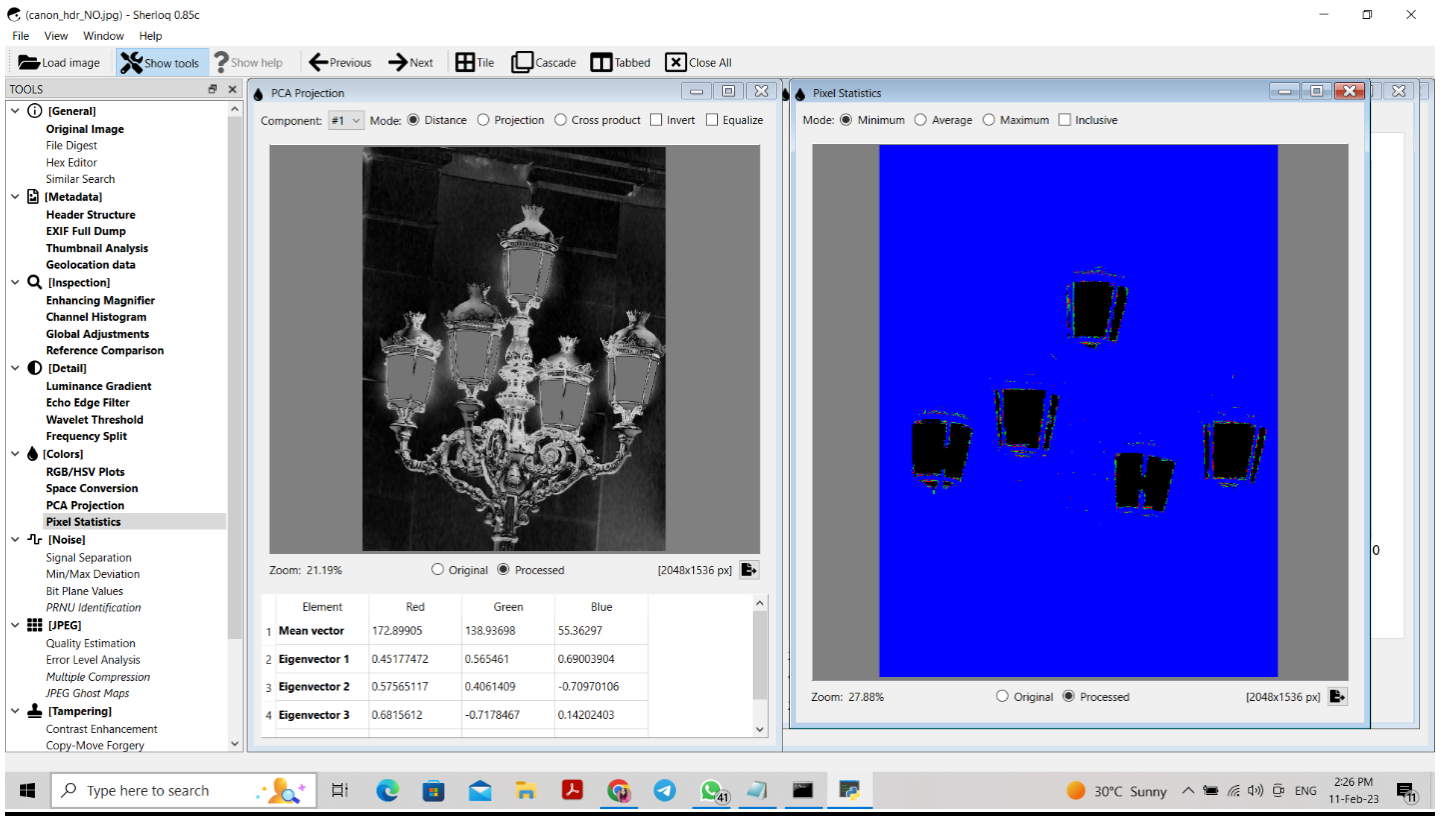
Frequency Split-



RGB/HSV Plots and space conversion-

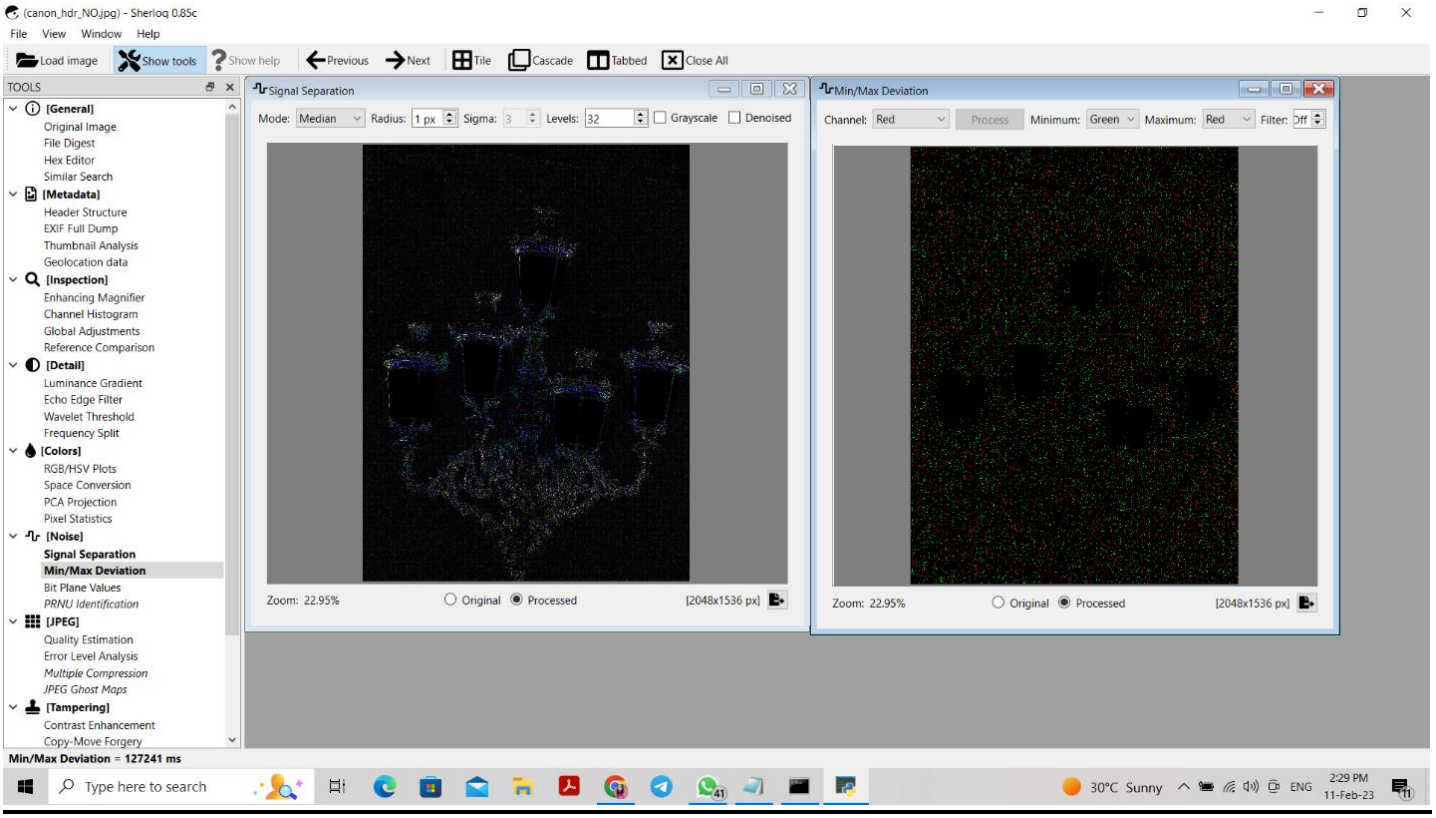


PCA Projection and Pixel statistics-

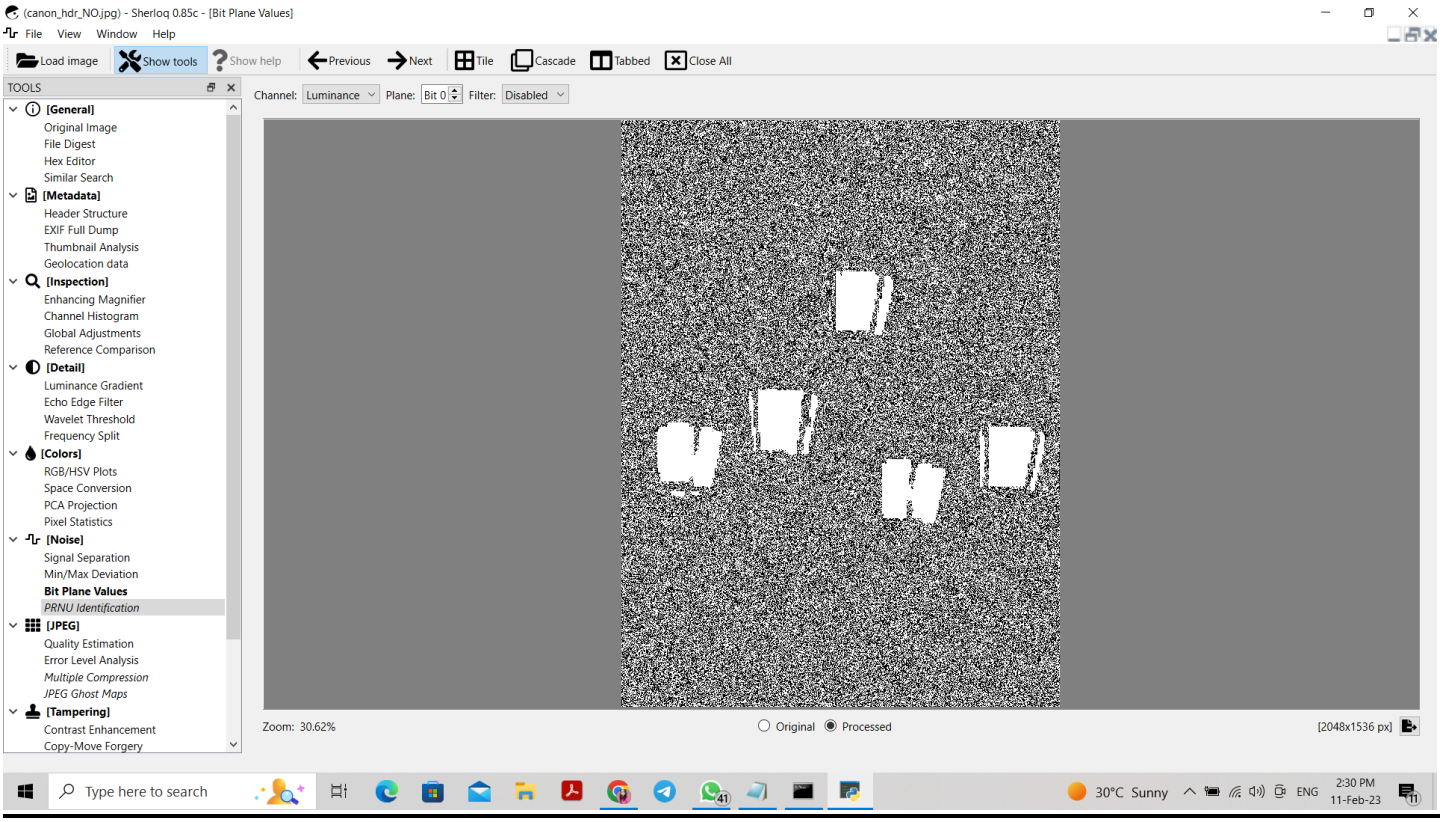


Under Noise,

Signal separation and Min/Max deviation -

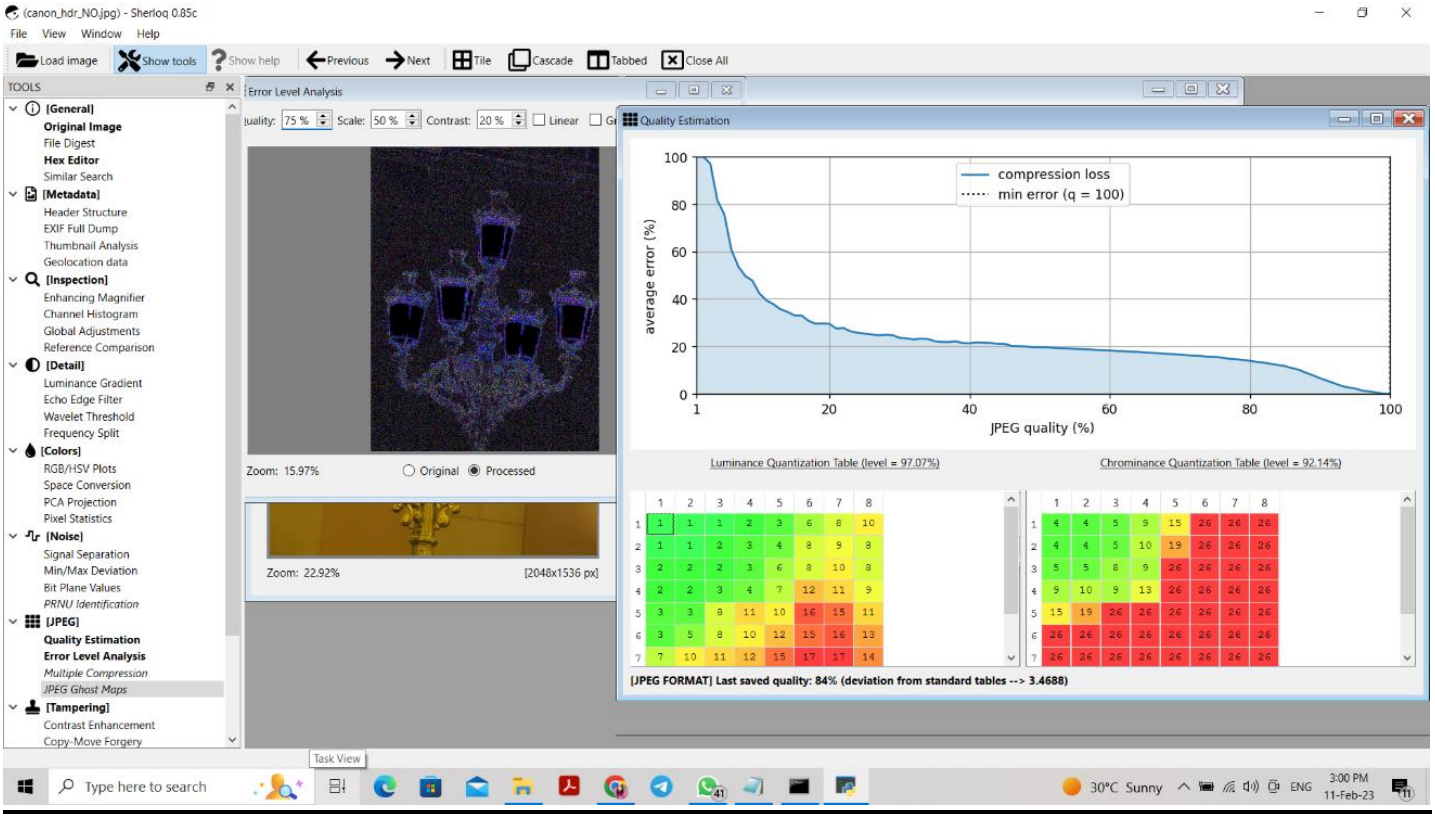


Bit Plane Values-



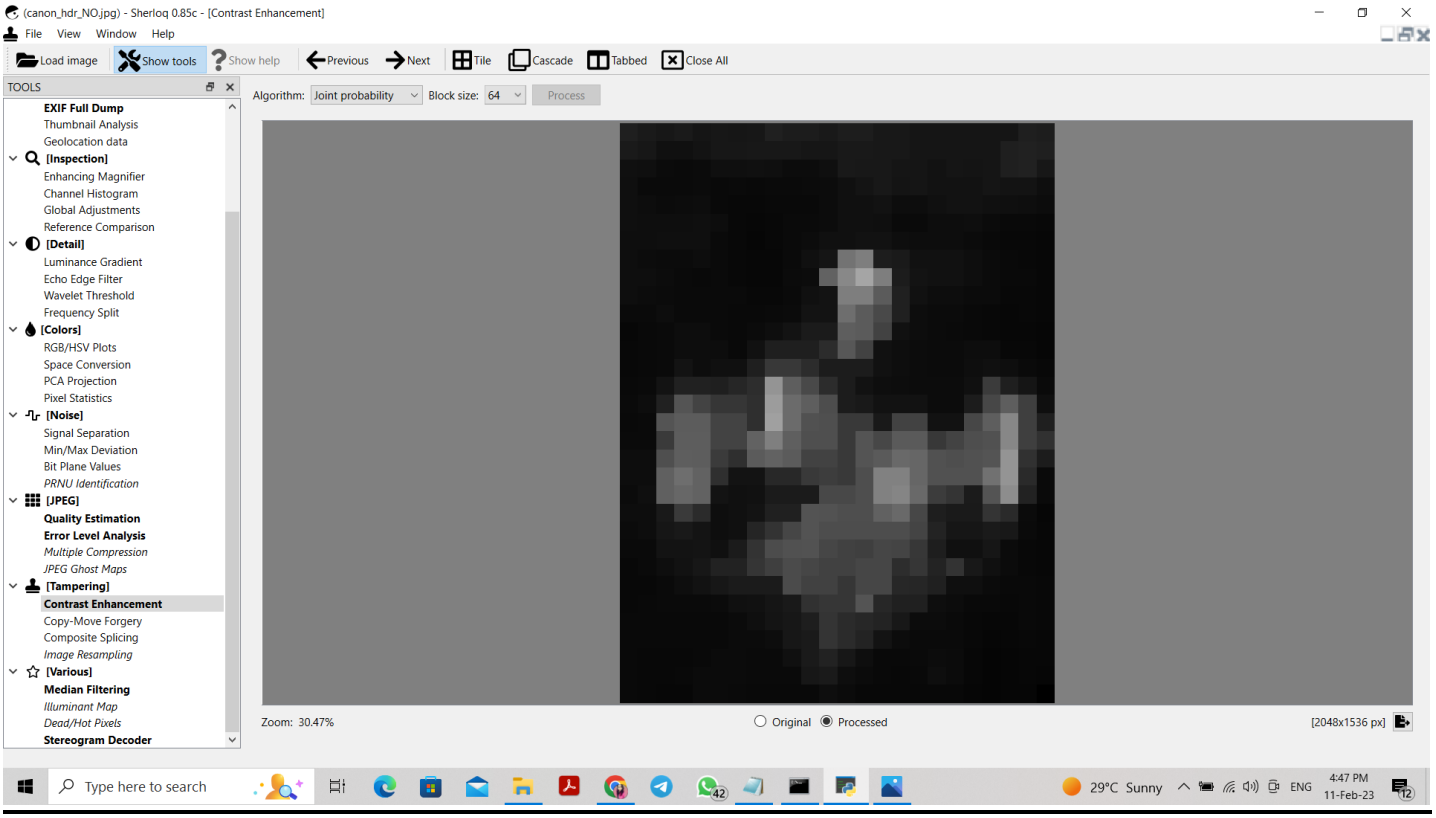
Under JPEG,

Quality Estimation and Error level analysis-

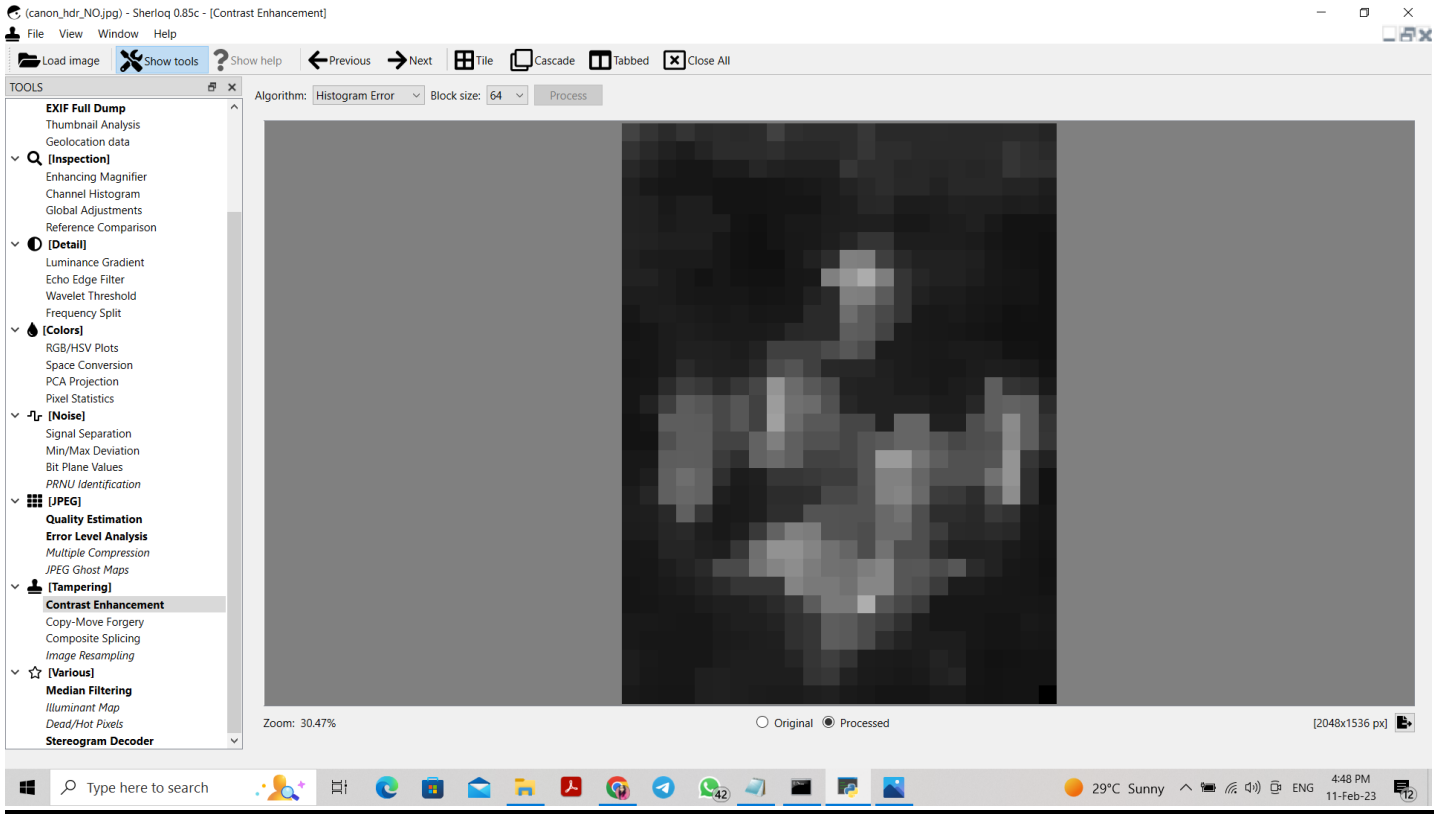


Under Tampering,

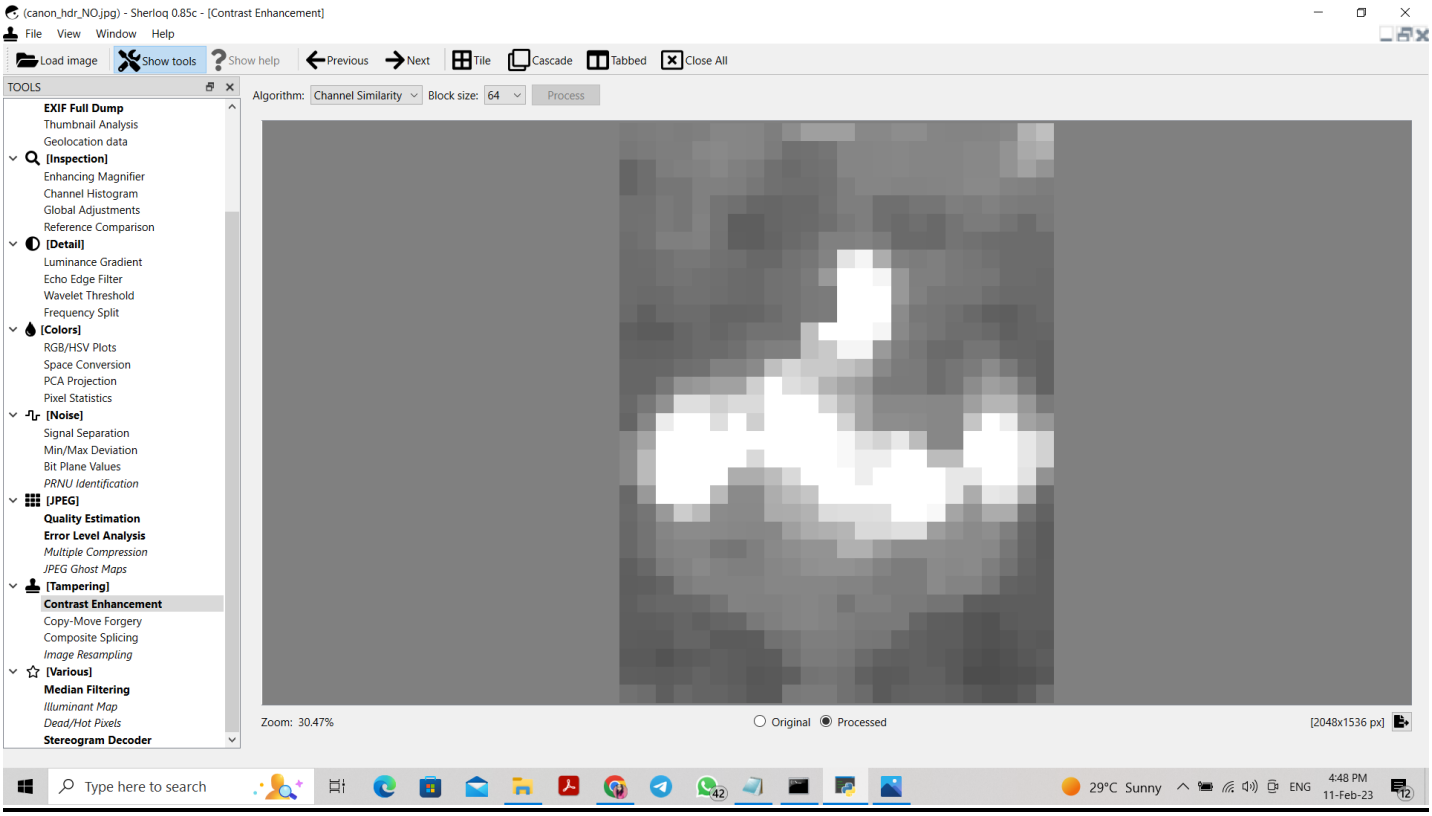
Contrast Enhancement (Joint probability algo)-



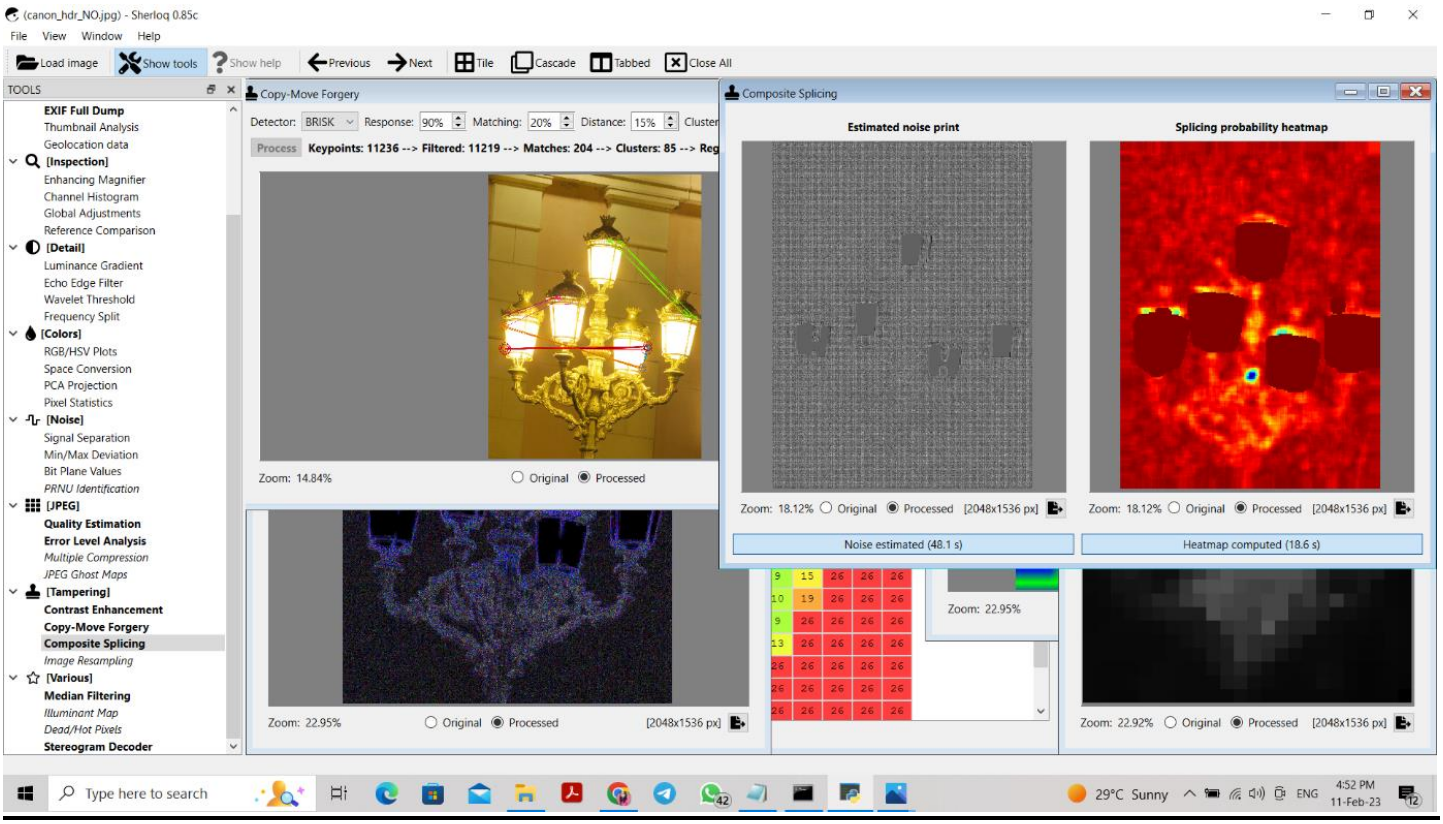
Contrast Enhancement (Histogram Error)-



Contrast Enhancement (Channel Similarity algo)-

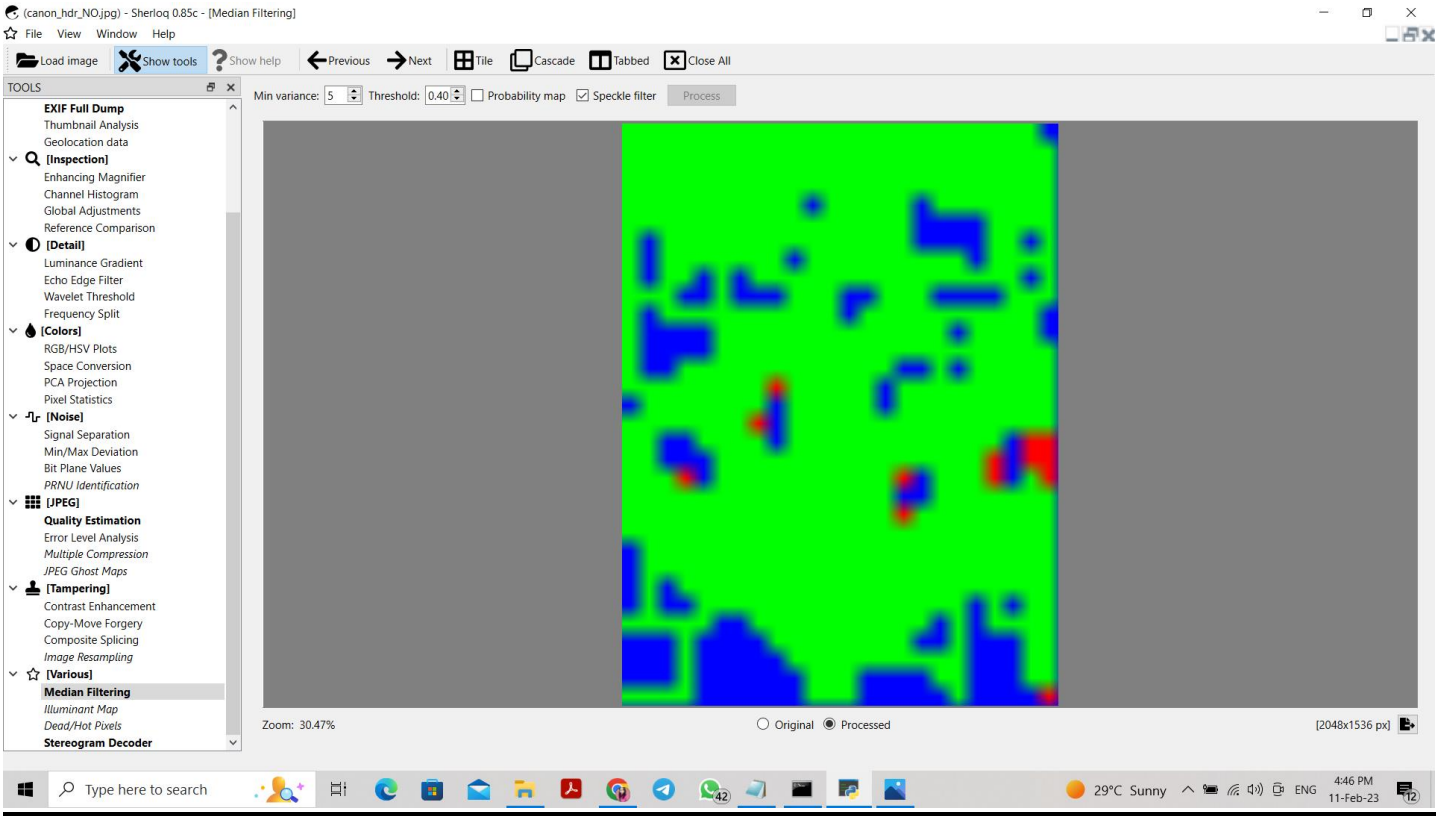


Copy move forgery and Composite Splicing -



Under Various,

Media filtering -



References-

https://forensicfield.blog/forensic-image-analysis/

https://www.slideshare.net/venatimunishareddy/image-processing-in-forensic-science

https://github.com/GuidoBartoli/sherloq