

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:

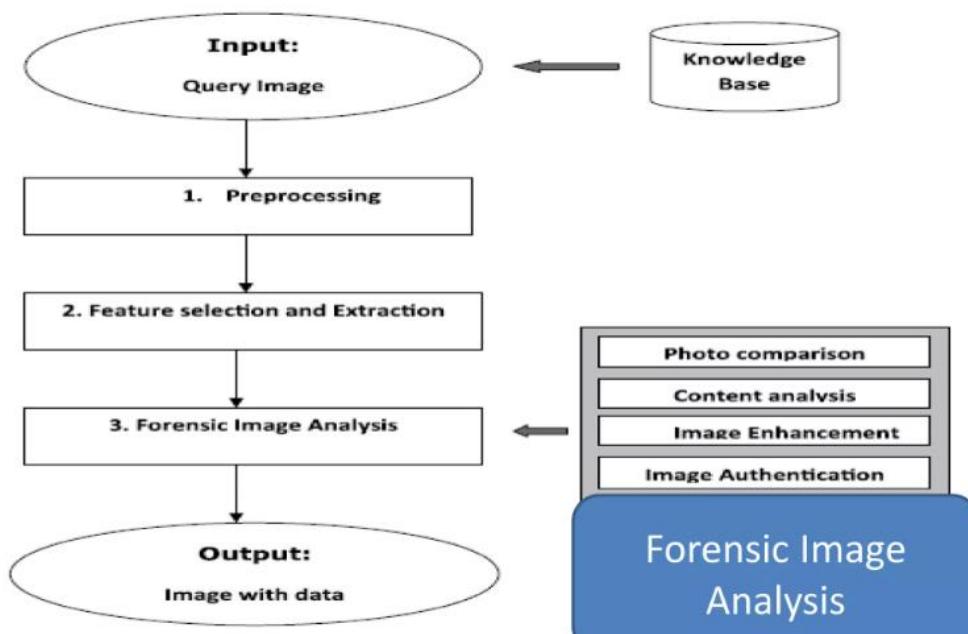


Image analysis –

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)-

The screenshot shows the FotoForensics analysis interface. On the left, a sidebar titled "Analysis:" lists several options: Digest (selected), ELA, Games, Hidden Pixels, ICC+, JPEG %, Metadata, Strings, and Source. Below the sidebar are sharing icons for Twitter, LinkedIn, Google+, Print, Email, and a magnifying glass. The main area features the FotoForensics logo and a thumbnail image of a tree at sunset. To the right is a detailed table of file properties:

Property	Value
Filename	download.jpeg
Filetime	2023-02-08 09:58:21 GMT
File Type	image/jpeg
Dimensions	285x177
Color Channels	3
Unique Colors	22388
File Size	5,495 bytes
MD5	a72050ce8d18c5e341ce539e923c77a0
SHA1	c8935478f939daf43e4e3abf0a1bb232115bd45a
SHA256	0ea7088749baf2e4899a08058c5a167765fca98475707e2b446bf1a27cf90d33
First Analyzed	2023-02-08 10:01:21 GMT

At the bottom of the page, there are links for "URL to this page: [Direct Link] [Annotated]", "View: [Uploaded Source Image]", "Share: " with icons for Twitter, LinkedIn, Google+, Print, Email, and Facebook, and a note: "What does this picture mean? See the [tutorials](#) for an explanation."

fotoforensics.com/analysis.php?id=c8935478f939daf43e4e3abf0a1bb232115bd45a.5495

FotoForensics

Analysis:

- Digest
- ELA
- Games
- Hidden Pixels
- ICC+
- JPEG %
- Metadata**
- Strings
- Source



File	
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Image Width	285
Image Height	177
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
Y Cb Cr Sub Sampling	YCbCr4:2:0 (2 2)

JFIF	
JFIF Version	1.01
Resolution Unit	None
X Resolution	1
Y Resolution	1

Composite	
Image Size	285x177
Megapixels	0.050

URL to this page: [\[Direct Link\]](#) [\[Annotated\]](#)

Ghiro

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

getghiro.org

Ghiro

HOME ABOUT DOWNLOAD FEATURES DOCUMENTATION COMMUNITY

Stable release package

Latest Ghiro stable release can be downloaded using the button on the right.

Stable package is available in both .zip and .tar.gz format. This is strongly suggested for all users.


zip

78DCDF36E67BF1E82B2775D4B45EB210

[GPG Signature](#)

ABE38E6B4B544F2E335FCF8B69635FAC

[GPG Signature](#)

Virtual Appliance

The faster way to start playing with Ghiro is to download the Ghiro Virtual Appliance. In few minutes you will have a fully functional Ghiro setup to start to analyze your images.

The ZIP contains an OVA file, you have to import in your virtualization software (like VirtualBox or VMWare) and configure the networking as explained in the README.txt.


OVA

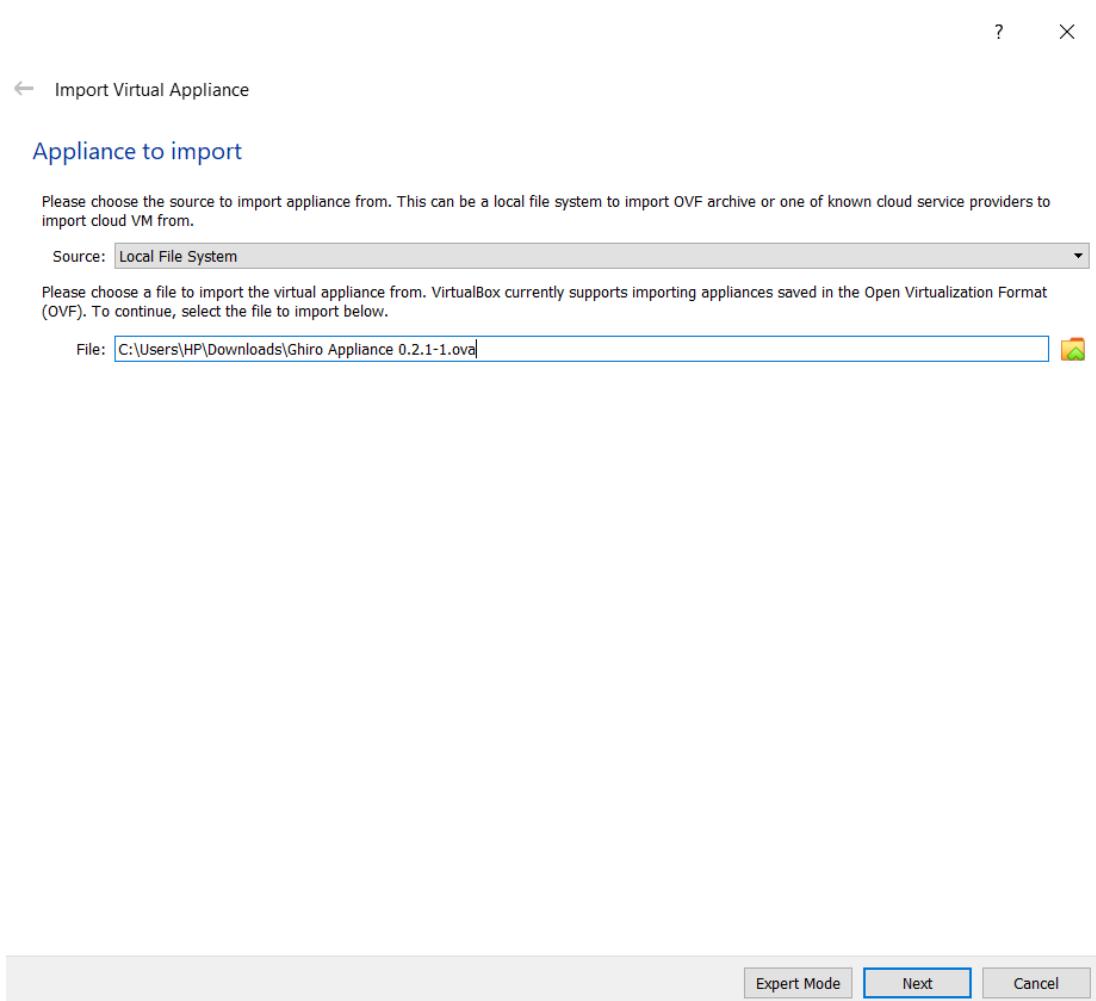
I8F37F598EB6DD7B0817D853B5B840730

[GPG Signature](#)

70488A7954E9FC996B5FF3B76872A453

[GPG Signature](#)

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,

The screenshot shows the Ghiro appliance dashboard. On the left is a sidebar with icons for Dashboard, Cases, Images, Search, Hashes, and Admin. The main area has a header "Ghiro" and "Welcome, ghiro".

Profile Section:

- Profile sub-section: Shows the user "ghiro".
- Change password link.
- Form fields for Name, Last name, Email (set to "youmail@example.com"), and API key (set to "5505193c-a06b-4f9a-9165-8c45a5963e00").
- Account details: Last login (Feb. 8, 2023, 6:03 p.m.), Account created (Aug. 26, 2015, 10:42 p.m.), Account active (checked), and Superuser (checked).

Stats Section:

- Shows Case opened: 0, My analyses: 0, and My hash lists: 0.

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

The screenshot shows the Ghiro web application interface. On the left is a dark sidebar with icons for Dashboard, Cases (selected), Images, Search, Hashes, and Admin. The main area has a header 'Cases browse all cases' and a breadcrumb 'Dashboard > Cases'. A top right corner shows 'Welcome, ghiro'. Below the header is a table with columns: Name, Status, Created at, Owner, and Actions. The table is currently empty with the message 'No data available in table'. At the bottom of the table are dropdowns for 'records per page' (set to 10) and navigation buttons for 'Previous' and 'Next'. In the top right corner of the main area, there is a green button labeled 'Add case' with a '+' icon. The URL bar at the bottom of the browser window shows '192.168.231.179/analyses/cases/new/'.

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

The screenshot shows the Ghiro web application interface on a specific case details page. The sidebar and header are identical to the previous screenshot. The main area shows a case named 'case1' with the following details: Status: Open, Owner: ghiro, Created at: Feb. 8, 2023, 6:29 p.m., and Case Id: 1. Below this, a table lists file names, their status, owner, and submission date. The table is currently empty with the message 'No data available in table'. To the right of the table is a floating action bar with several buttons: a red 'Add' button with a '0' badge, a green '+' button, a blue edit/pencil icon, an orange 'X' icon, a grey trash bin icon, and a yellow 'Add image' icon. Below these buttons are three menu items: 'Add image', 'Add image url', and 'Add folder'. The URL bar at the bottom shows '192.168.231.179/analyses/cases/case1'.

Added some images while its processing,

The screenshot shows a digital forensic tool's interface. At the top, there is a navigation bar with links for 'Dashboard', 'Cases', and 'case1'. To the right of the navigation are several icons: a square with '8', a green plus sign, a magnifying glass, a red X, and a trash can. Below the navigation, a summary box displays the following details:

Status:	Open
Owner:	ghiro
Created at:	Feb. 8, 2023, 6:29 p.m.
Case Id:	1

Below this summary is a table with the following columns: 'File name', 'Status', 'Owner', and 'Submitted at'. The table lists ten files, each with its status (Waiting or Processing), owner (ghiro), and submission time (Feb. 8, 2023, 6:45 p.m.).

File name	Status	Owner	Submitted at
WWL_(Polaroid)_ION230 - Copy.jpg	Waiting	ghiro	Feb. 8, 2023, 6:45 p.m.
Sony_HDR-HC3 - Copy.jpg	Waiting	ghiro	Feb. 8, 2023, 6:45 p.m.
Samsung_Digimax_i50_MP3.jpg	Waiting	ghiro	Feb. 8, 2023, 6:45 p.m.
Samsung_Digimax_i50_MP3 - Copy.jpg	Waiting	ghiro	Feb. 8, 2023, 6:45 p.m.
Ricoh_Caplio_RR330 - Copy.jpg	Waiting	ghiro	Feb. 8, 2023, 6:45 p.m.
Reconyx_HC500_Hyperfire - Copy.jpg	Waiting	ghiro	Feb. 8, 2023, 6:45 p.m.
Pentax_K10D - Copy.jpg	Processing	ghiro	Feb. 8, 2023, 6:45 p.m.
Panasonic_DMC-FZ30 - Copy.jpg	Completed	ghiro	Feb. 8, 2023, 6:45 p.m.
PaintTool_sample - Copy.jpg	Completed	ghiro	Feb. 8, 2023, 6:45 p.m.
Olympus_C8080WZ.jpg	Completed	ghiro	Feb. 8, 2023, 6:45 p.m.

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

Image analysis: d5d5c4c868f21bf2f307075551120e0f



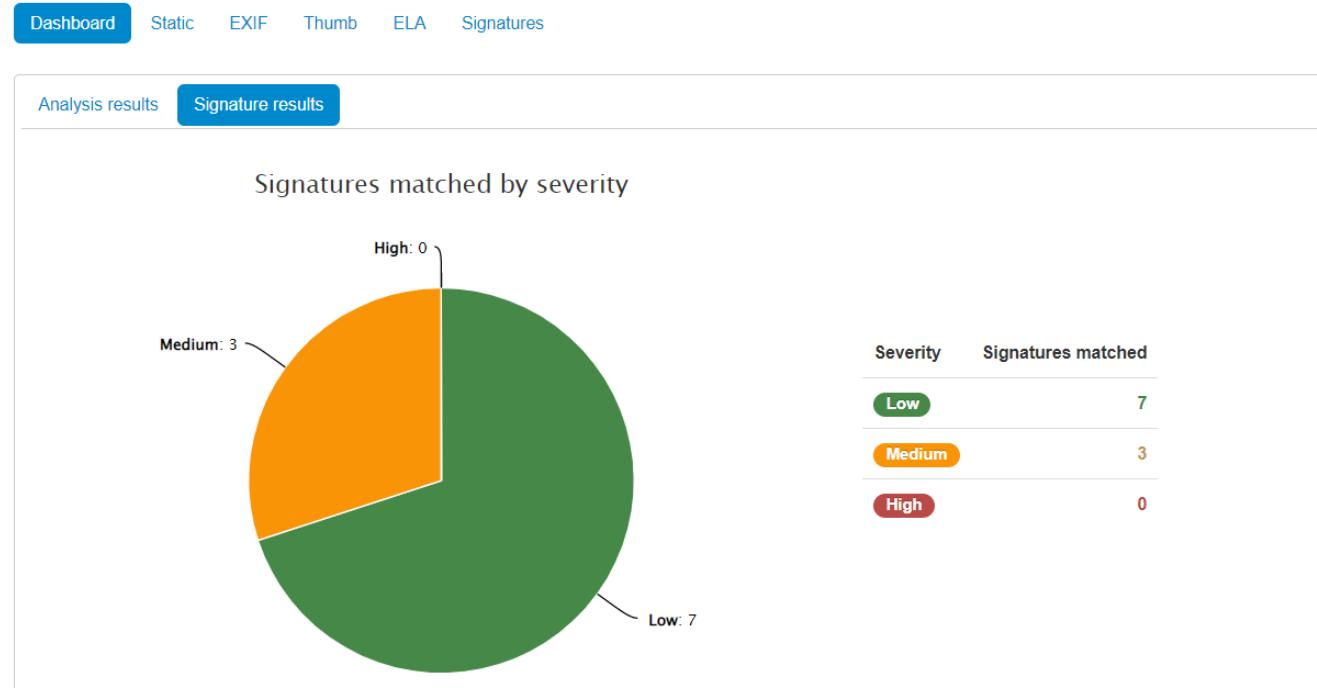
Download

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

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

The screenshot shows a web-based image analysis tool. At the top, there is a thumbnail image of a couple standing outdoors. To the right of the thumbnail, the text "Image analysis: d5d5c4c868f21bf2f307075551120e0f" is displayed. Below the thumbnail are three small buttons: a star icon, a print icon, and a trash icon.

Below the image and buttons, there is a navigation bar with several tabs: "Dashboard", "Static" (which is highlighted in blue), "EXIF", "Thumb", "ELA", and "Signatures".

Under the "Static" tab, there is a sub-navigation bar with five options: "Static info" (which is highlighted in blue), "FileType", "Hashes", "Strings", and "Hex dump".

The main content area displays a table of static file information:

Type	Value
Filename	canon-ixus.jpg
Size	125.0 KB
Dimensions	[640, 480]
Analyzed at	Feb. 8, 2023, 6:49 p.m.

In file type there is information of format,

The screenshot shows a FileType analysis interface. At the top, there is a navigation bar with five tabs: "Static info", "FileType" (which is highlighted in blue), "Hashes", "Strings", and "Hex dump".

Below the navigation bar, the word "Type" is displayed in bold black text.

Under the "Type" heading, the text "JPEG image data, EXIF standard 2.1" is displayed in blue.

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	2597d28addeb5f76a00348ae5d718664287692ca3c4a7c35f66e2f58589fb6bac8c06ed9f3aba2201037825aa0d9ce5
CRC32	786eae27
SHA256	b2d085bdb261cb2c56d8ba10d79175e38c0acd0d429afe19a4610eddee3b06fe
SHA512	d91edd0d0f3c78442032d571a2c0f0f53c124e811063852fc3c4e06a01b607c5cb7e7dd40954310f5b027d8ac7486d108b15f371965f3f9339ef06685637300ef
MD5	d5d5c4c868f21bf2f307075551120e0f

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

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.) -

Exif Metadata	
Segment	Key: Value
NIKONAF	AFPointsInFocus: 0 AFAreaMode: 0 AFPoint: 0
MAKERNOTE	ByteOrder: II Offset: 1146
PHOTO	LightSource: 0 ColorSpace: 1 ExposureMode: 0 Flash: 16 FlashpixVersion: 48 49 48 48 SceneCaptureType: 0 MeteringMode: 5 ExifVersion: 48 50 50 48 Contrast: 0 Saturation: 0

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 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
ISO Speed Ratings: 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 1 0 0 0 2 130 0 0 255 128 255 255 255
ScanID: 3292
ImageAdjustment: NORMAL
Flash Setting:
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 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 538859999/100000000 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,



Image analysis: d5d5c4c868f21bf2f307075551120e0f

★ 🖨️ ✖

Dashboard Static EXIF **Thumb** ELA Signatures

Previews



Size: 5342 bytes
Mime type: image/jpeg
Extension: jpg
Dimension: [160L, 120L]

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.

Dashboard Static EXIF Thumb **ELA** Signatures

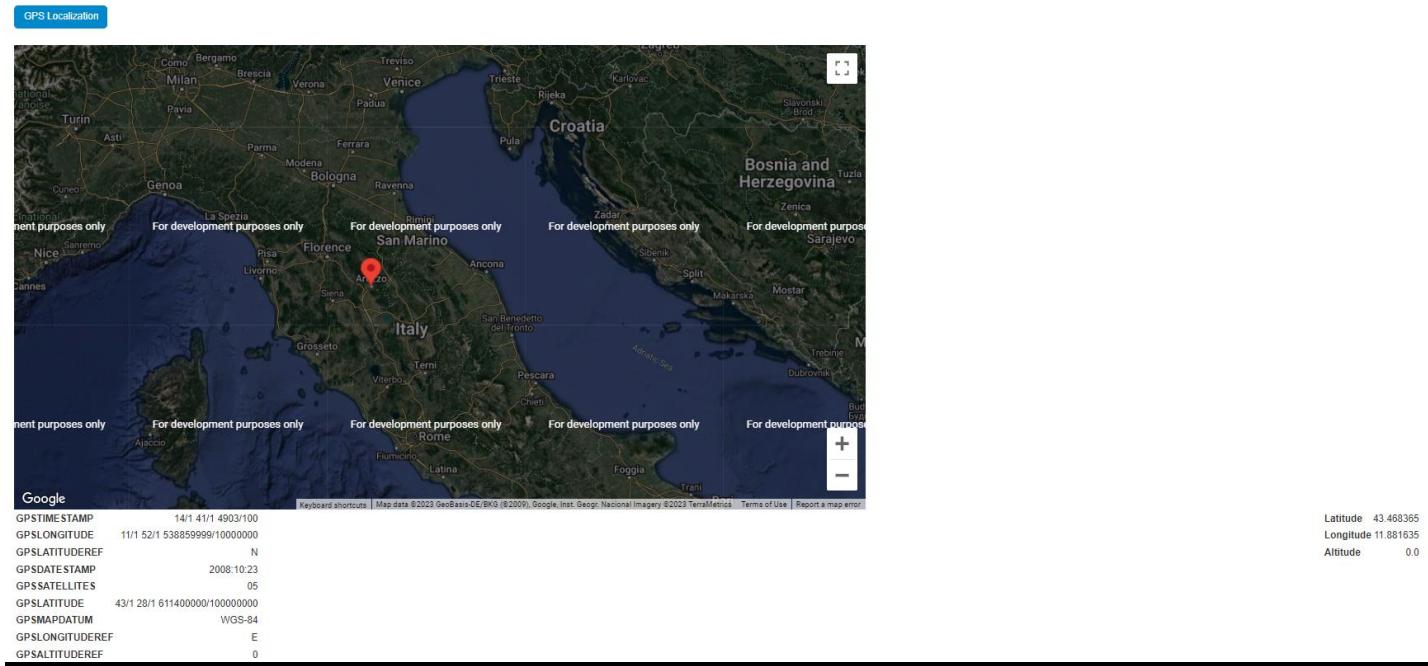
ELA



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,



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 -

File name	Owner	Submitted at	Actions
DSCN0025.jpg	ghiro	Feb. 9, 2023, 6:16 a.m.	

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

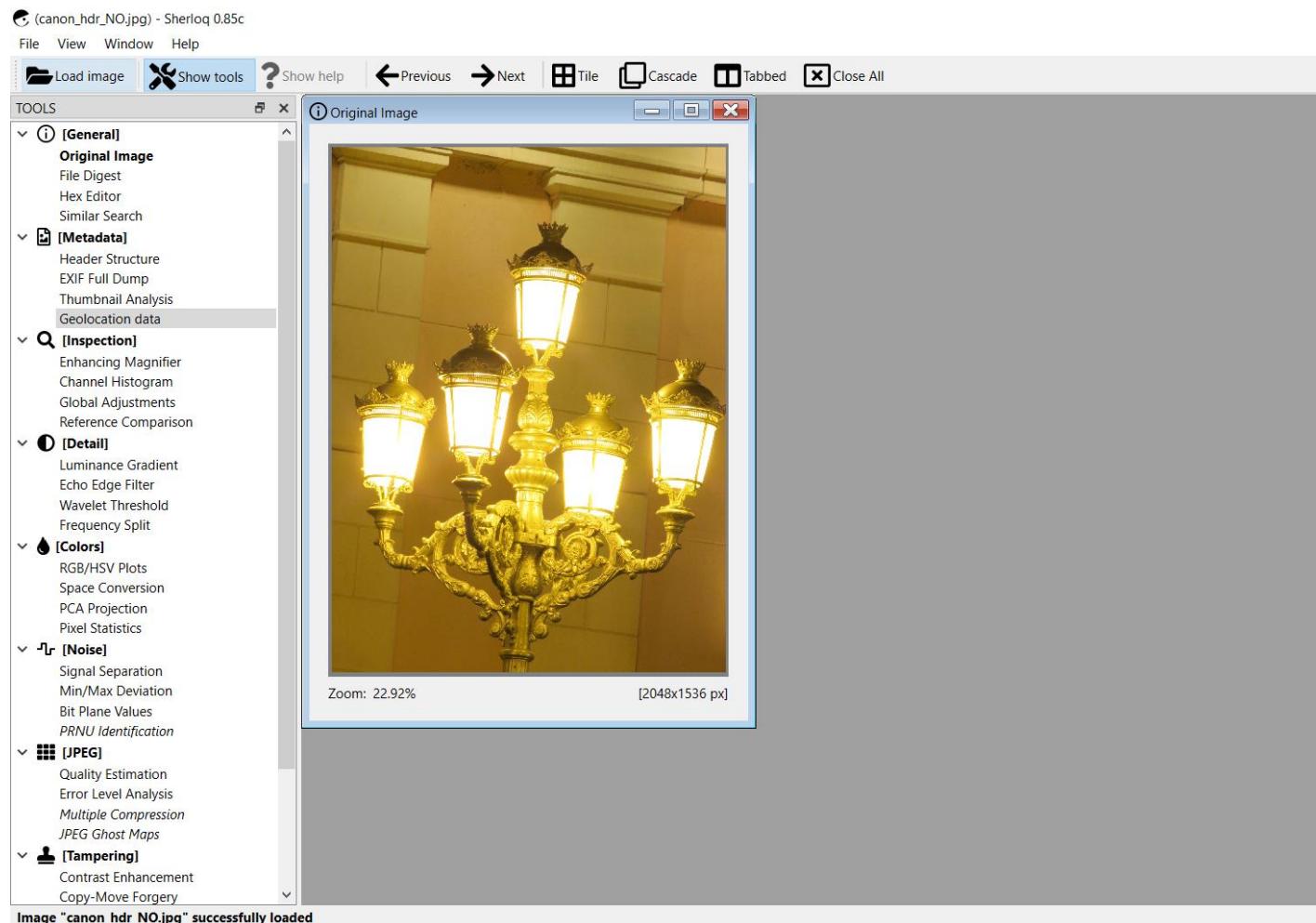
Export both visual and textual results of the analysis

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

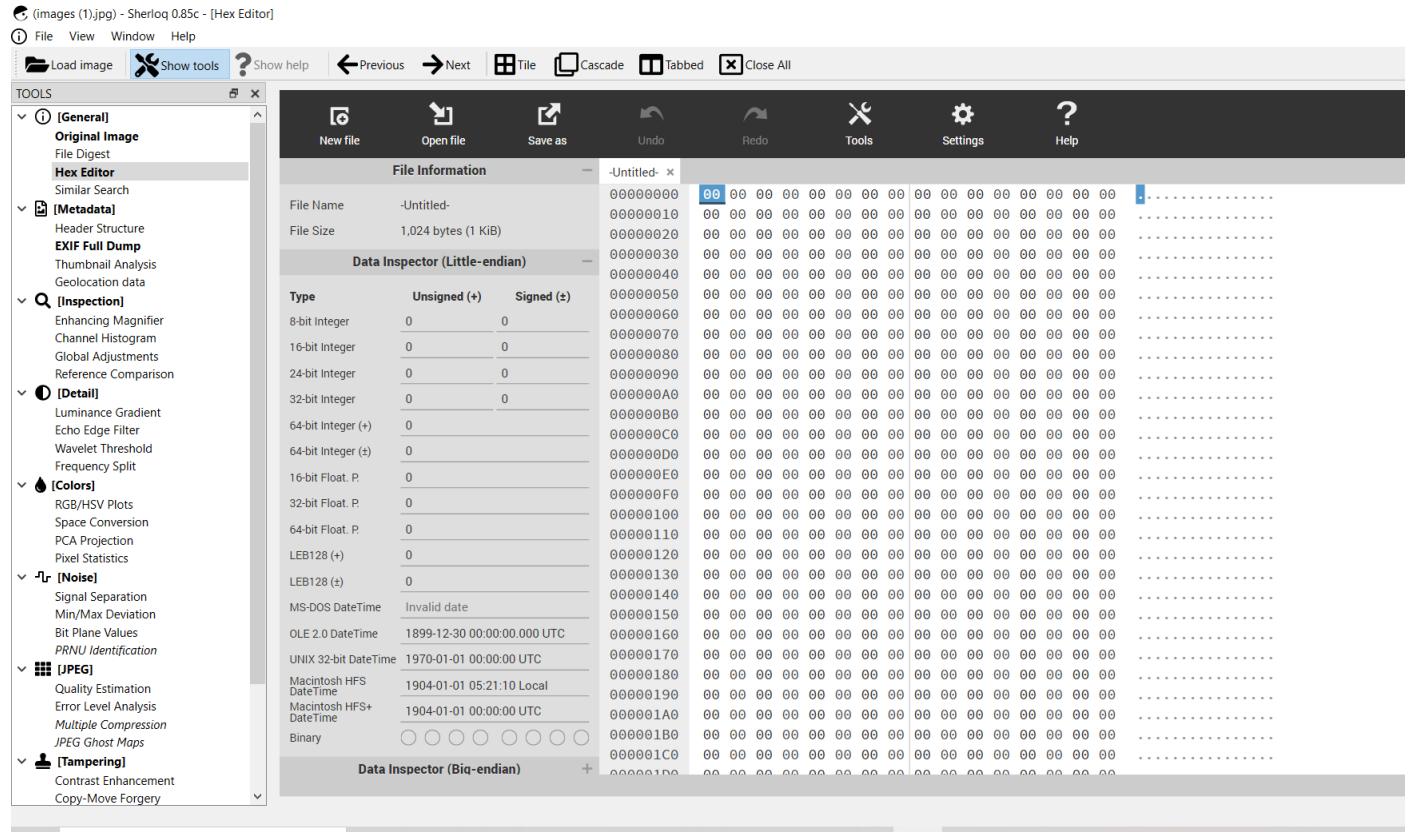
<https://github.com/GuidoBartoli/sherloq>

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

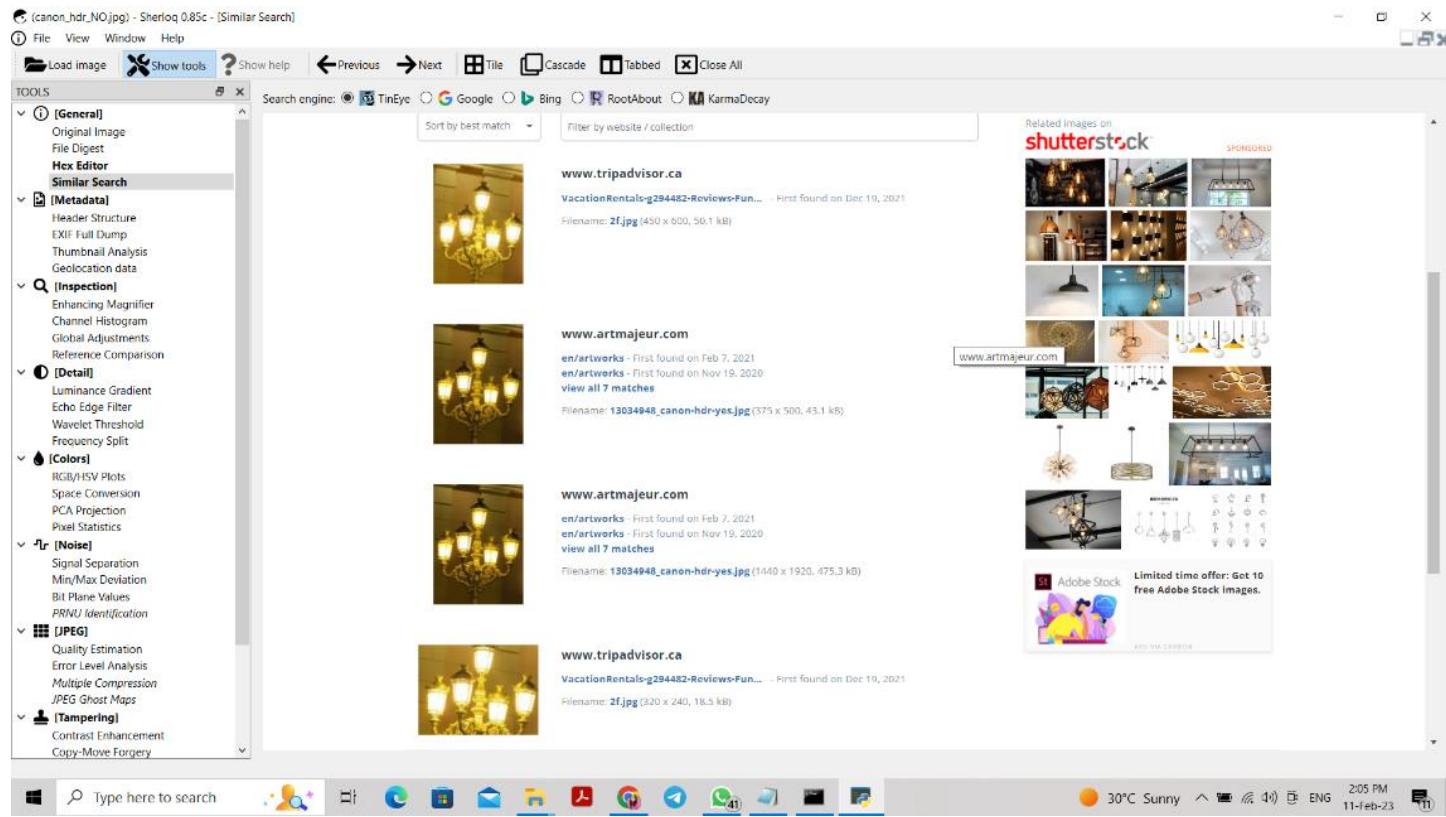
Load the image in the working interface –



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

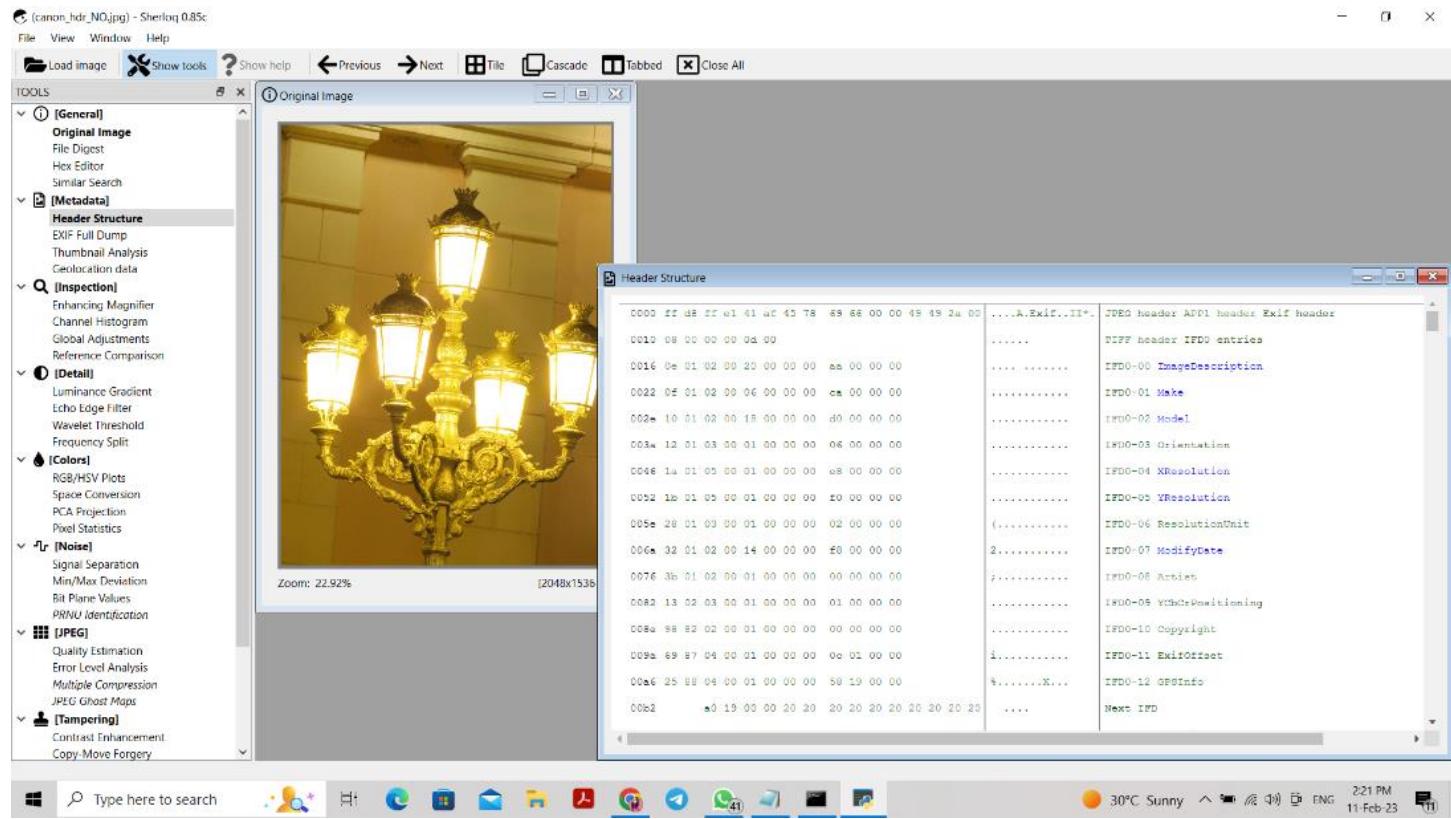


Similar search tool where can find similar images from web –



Under Meta data,

Header structure-



Exif full Dump-

(canon_hdr_NO.jpg) - Sherloq 0.85c - [EXIF Full Dump]

File View Window Help

Load image Show tools ? Previous Next Tile Cascade Tabbed Close All

TOOLS

[General] Original Image File Digest Hex Editor Similar Search

[Metadata] Header Structure EXIF Full Dump Thumbnail Analysis Geolocation data

[Inspection] Enhancing Magnifier Channel Histogram Global Adjustments Reference Comparison

[Detail] Luminance Gradient Echo Edge Filter Wavelet Threshold Frequency Split

[Colors] RGB/HSV Plots Space Conversion PCA Projection Pixel Statistics

[Noise] Signal Separation Min/Max Deviation Bit Plane Values PRNU Identification

[JPEG] Quality Estimation Error Level Analysis Multiple Compression JPEG Ghost Maps

[Tampering] Contrast Enhancement Copy-Move Forgery

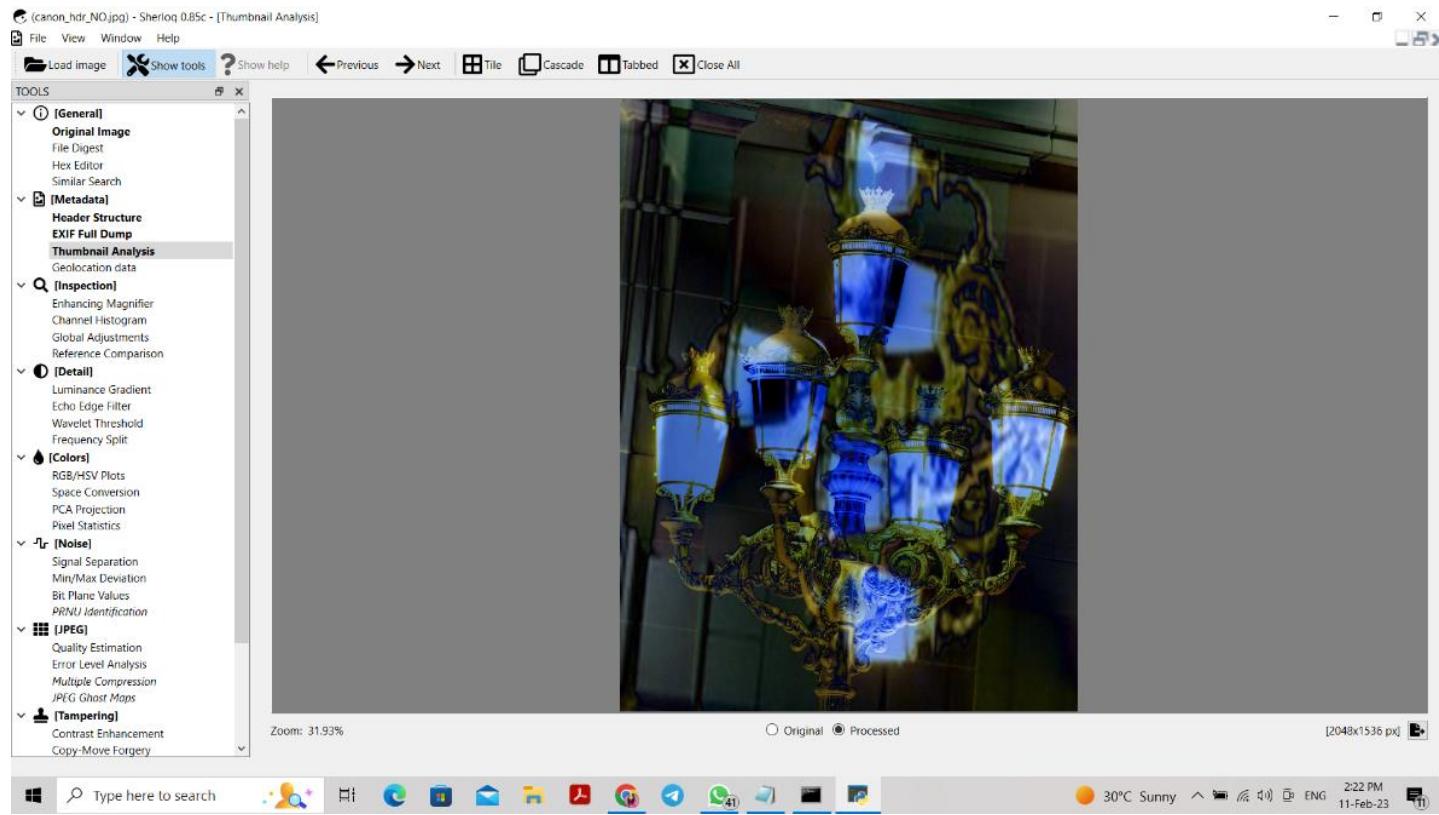
Group	Description	Value
1	ExifTool	Warning [minor] Adjusted MakerNotes base by -128
2	File	ZoneIdentifier
3		Exists
4		FileCreateDate
5		2023:02:08 18:42:59+05:30
6		ExifByteOrder
7		II
8		CurrentIFTUDigest
9		3d11bd32a4f9bd1e994037f6cc6008d1
10		ImageWidth
11		2048
12		ImageHeight
13		1536
14		BitsPerSample
15		8
16		ColorComponents
17		3
18		YCbCrSubSampling
19		2 1
20	EXIF	ImageDescription
21		
	Make	Canon
	Model	Canon PowerShot SX60 HS
	Orientation	6
	XResolution	180
	YResolution	180
	ResolutionUnit	2
	ModifyDate	2015:02:28 04:20:03
	YCbCrPositioning	1
	ExposureTime	0.0166666667
	FNumber	5.6

Search: Export...

Type here to search

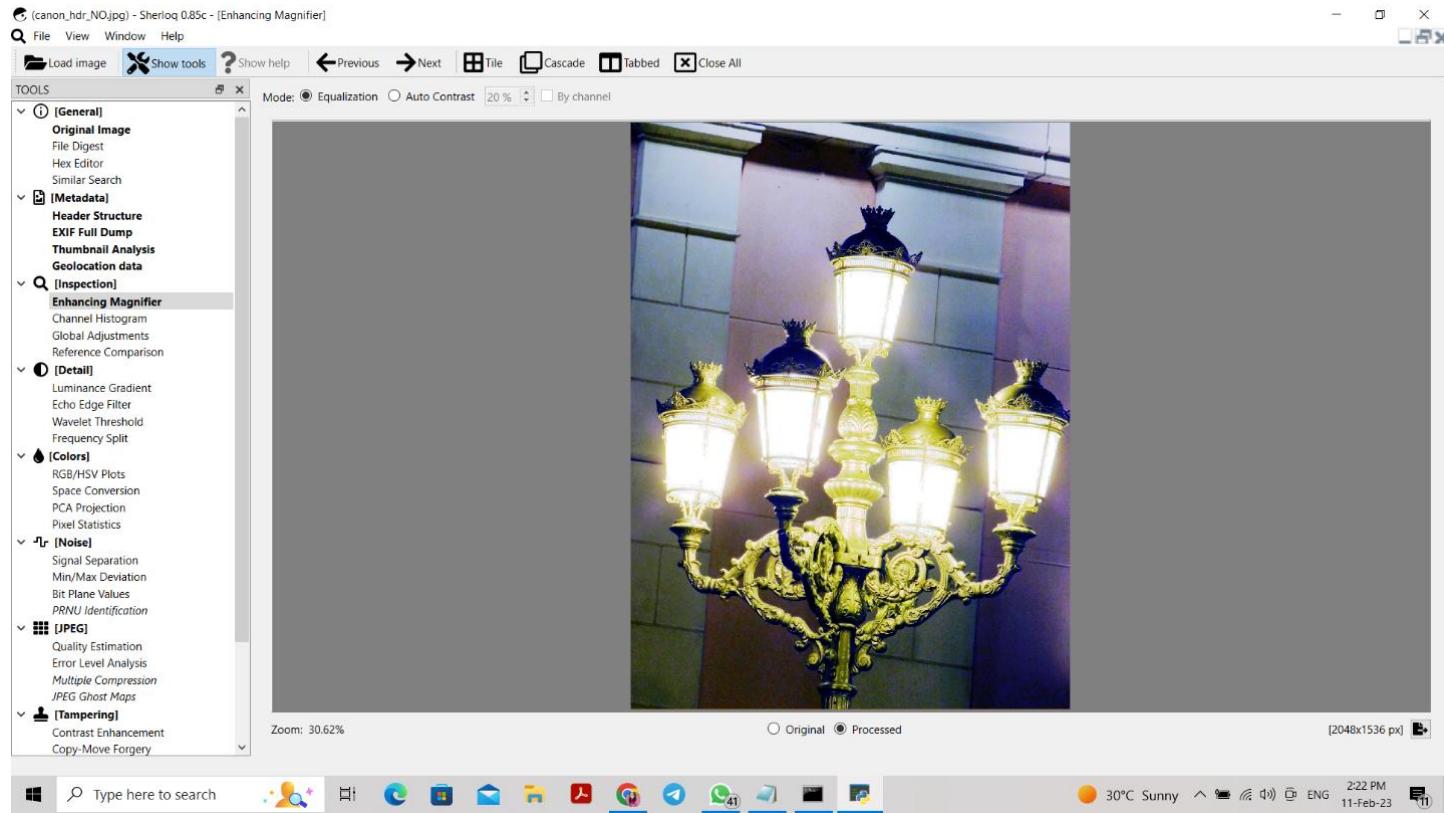
30°C Sunny 2:22 PM 11-Feb-23

Thumbnail analysis-

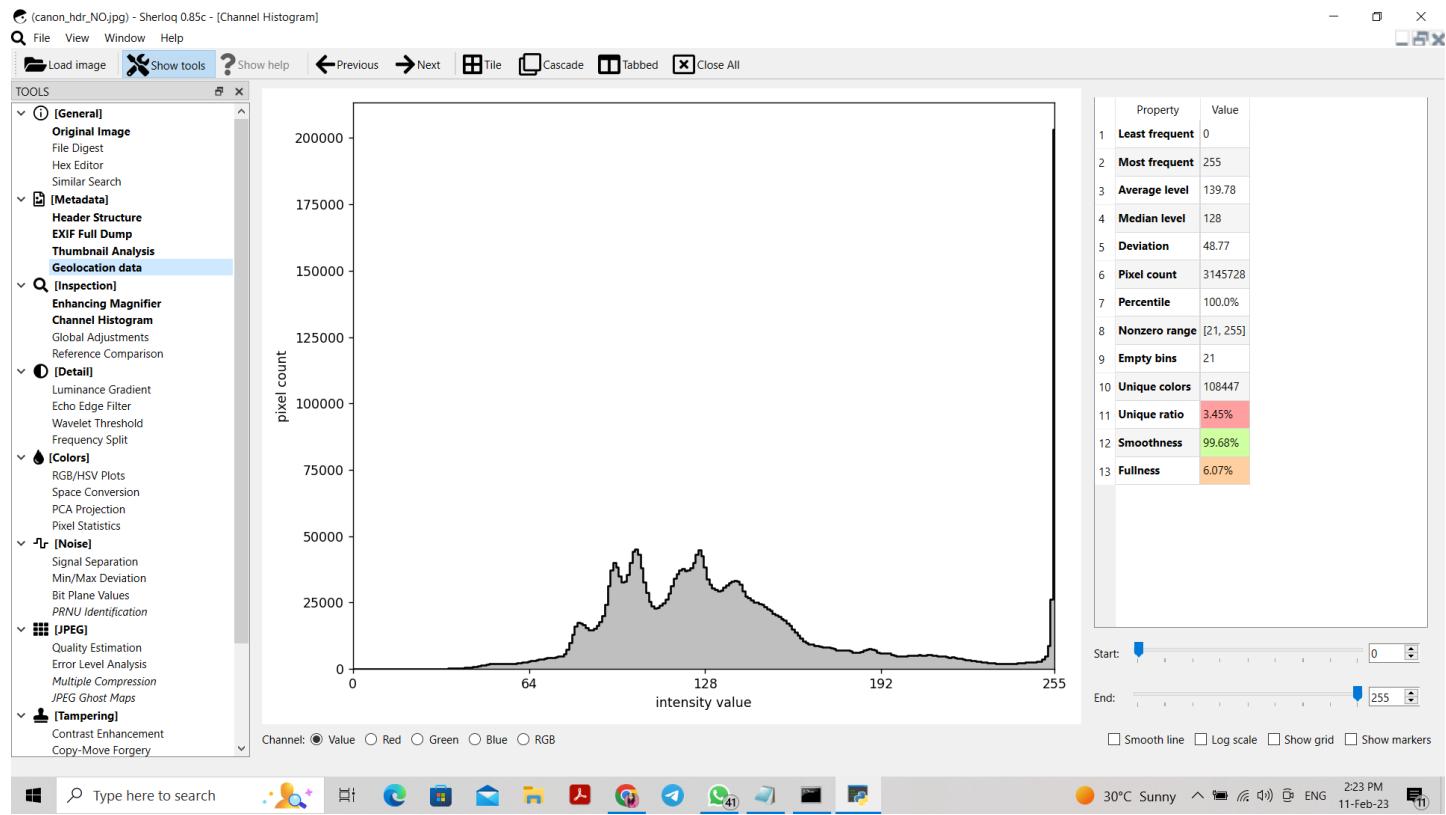


Under Inspection,

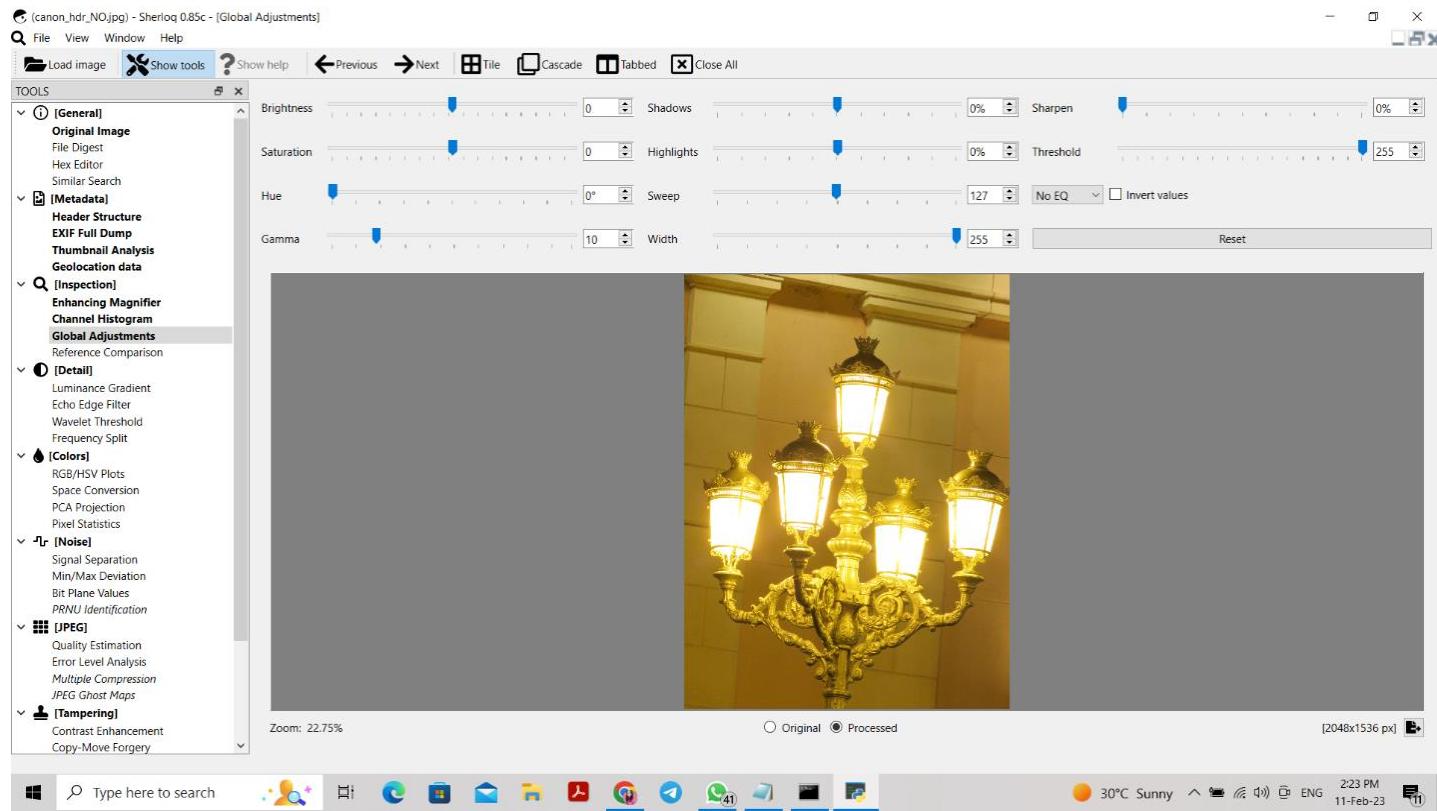
Enhancing magnifier-



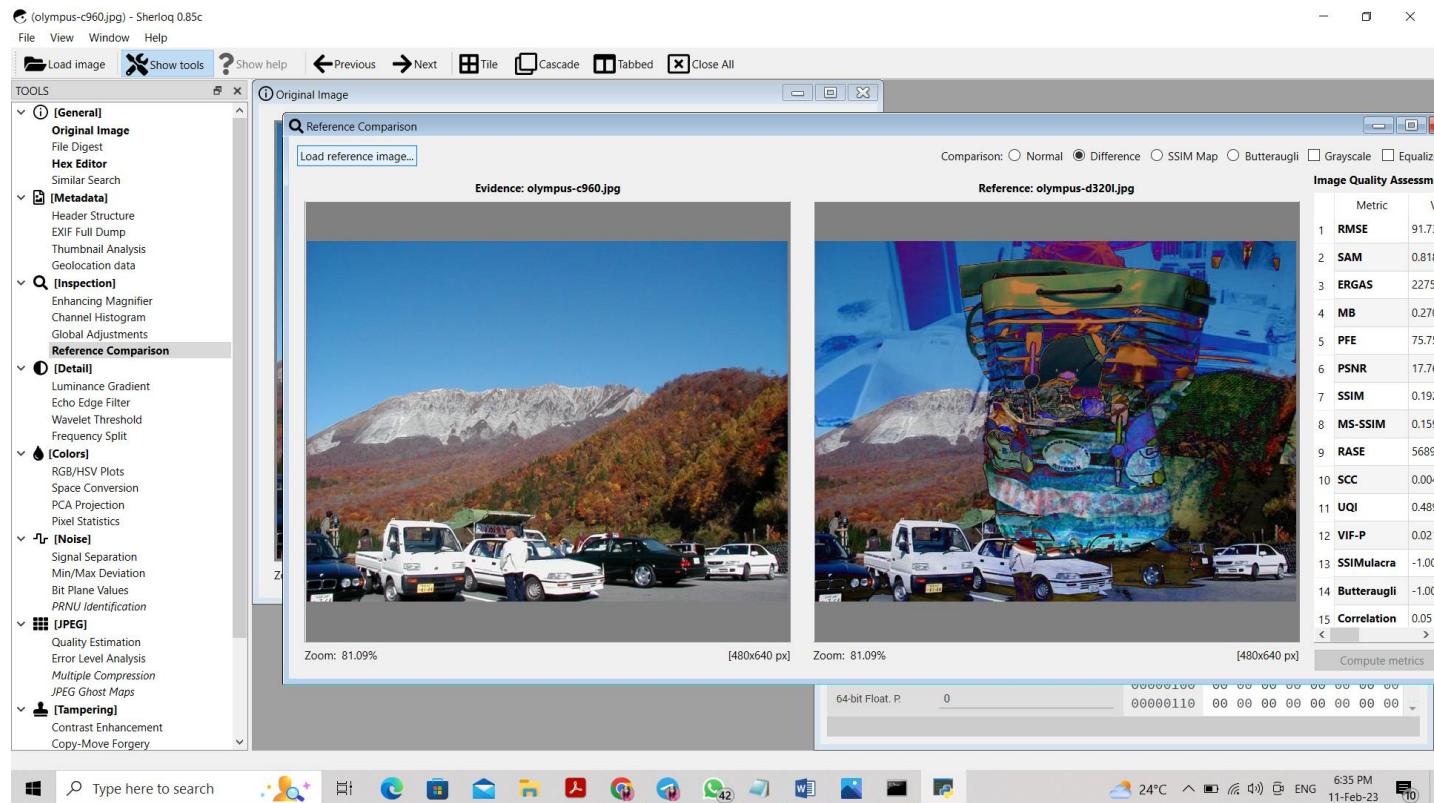
Channel histogram-



Global adjustments-

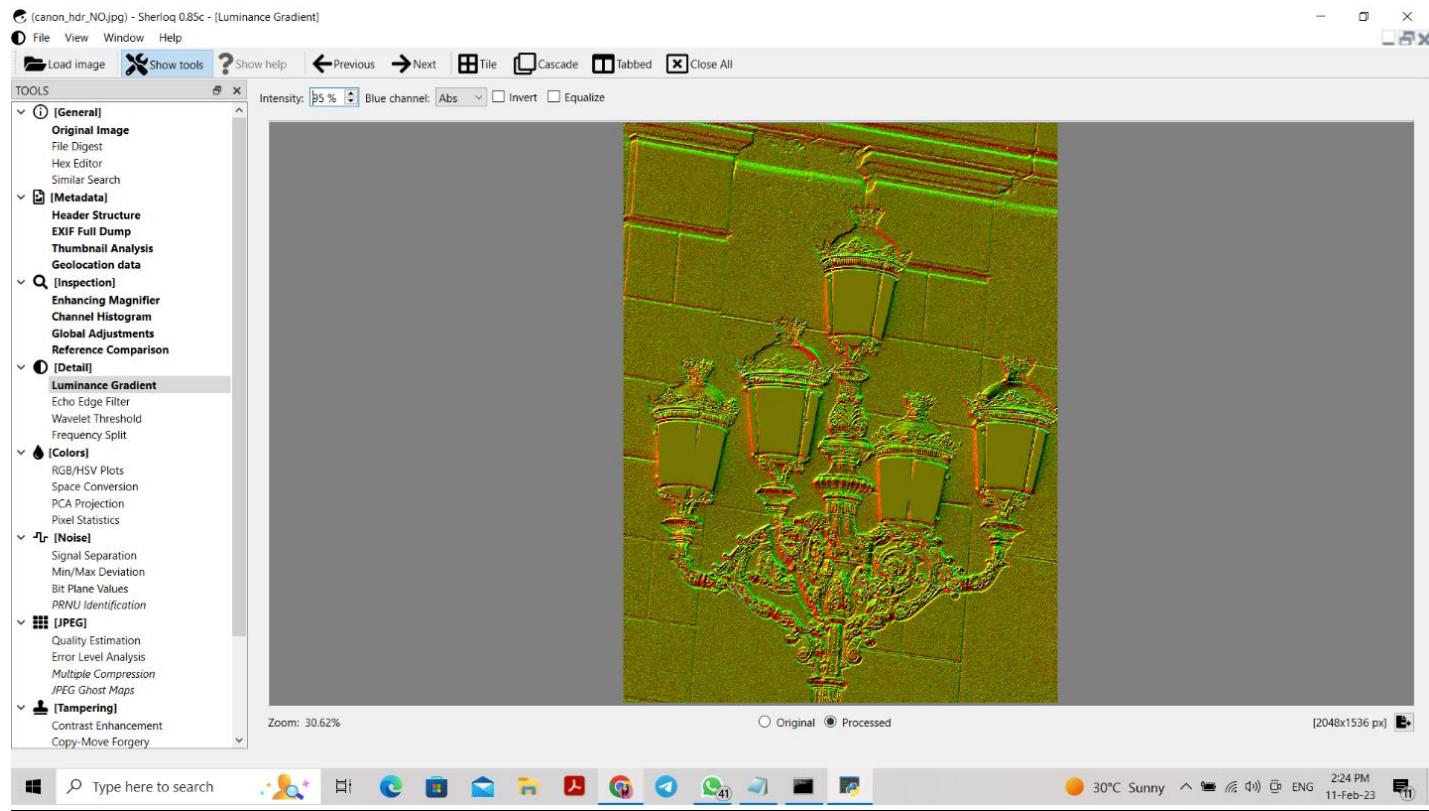


Reference Comparison-

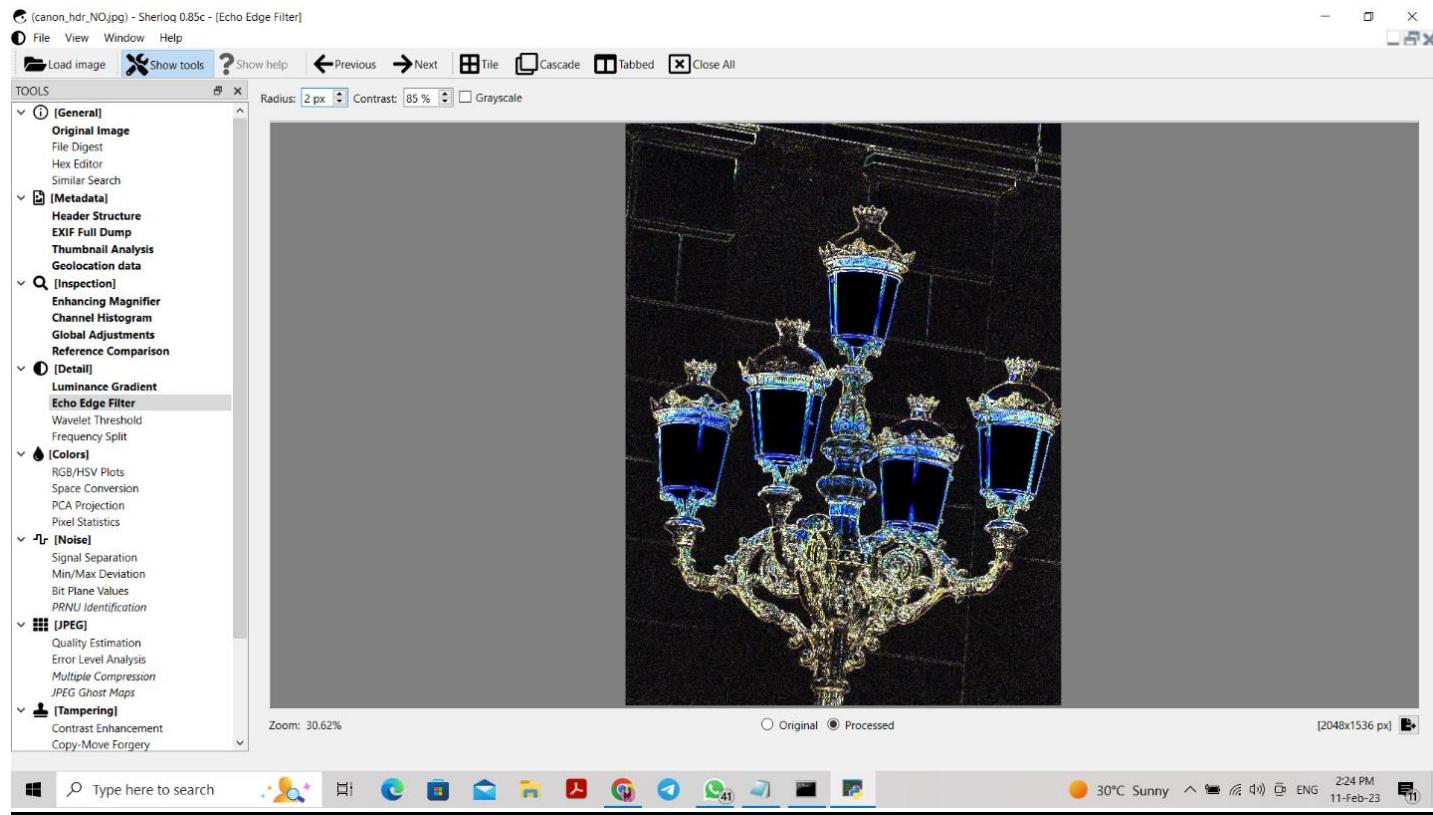


Under detail,

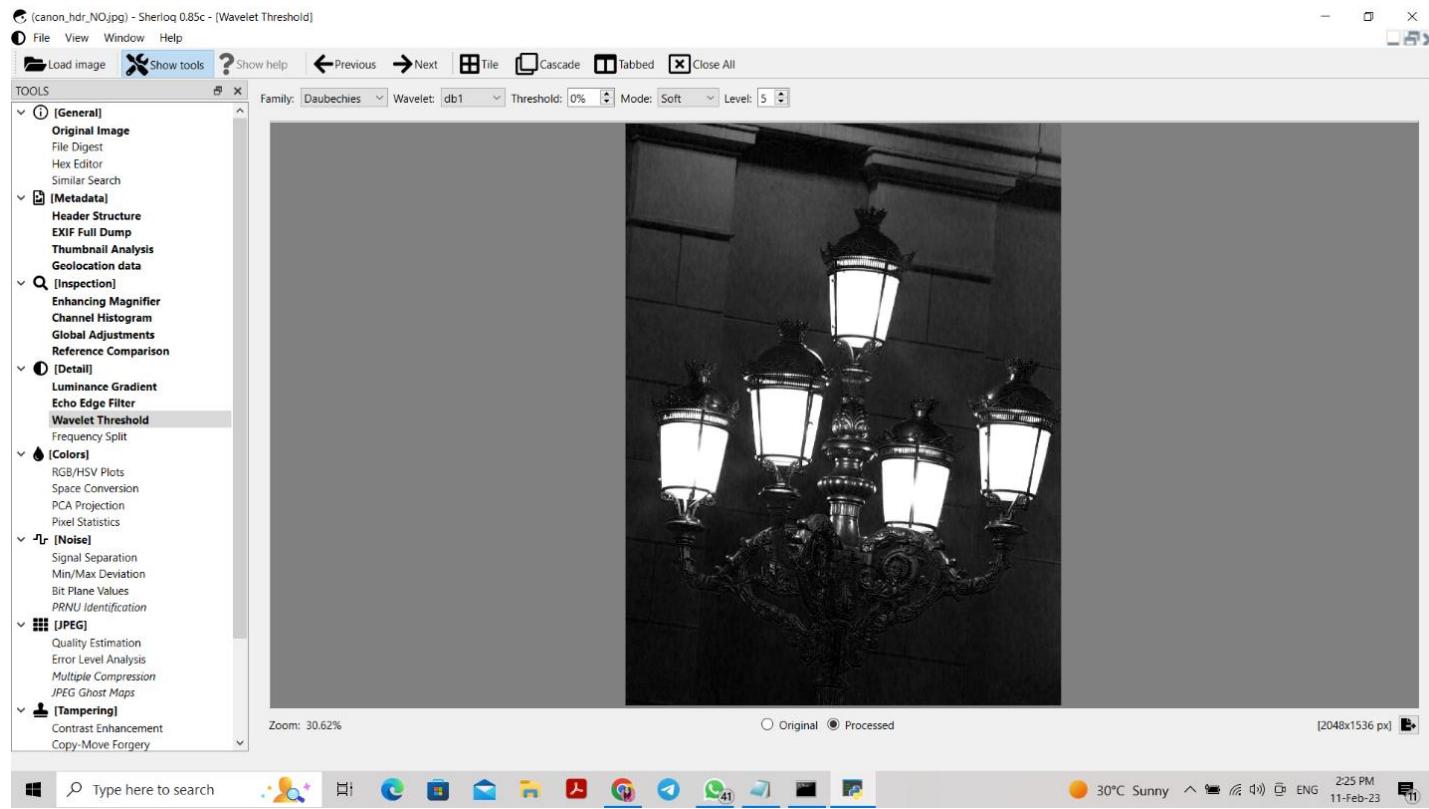
Luminance gradient -



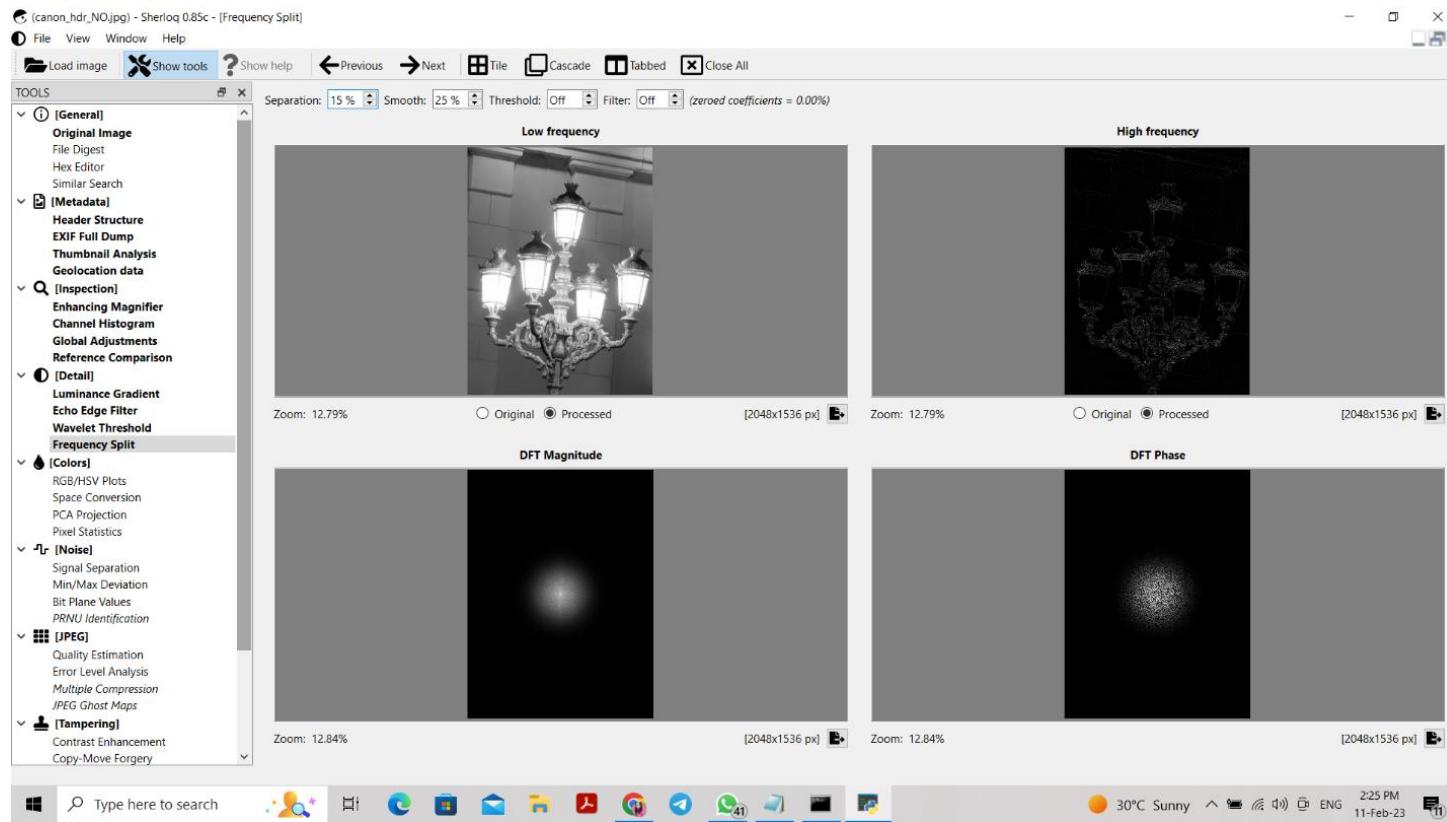
Echo edge filter-



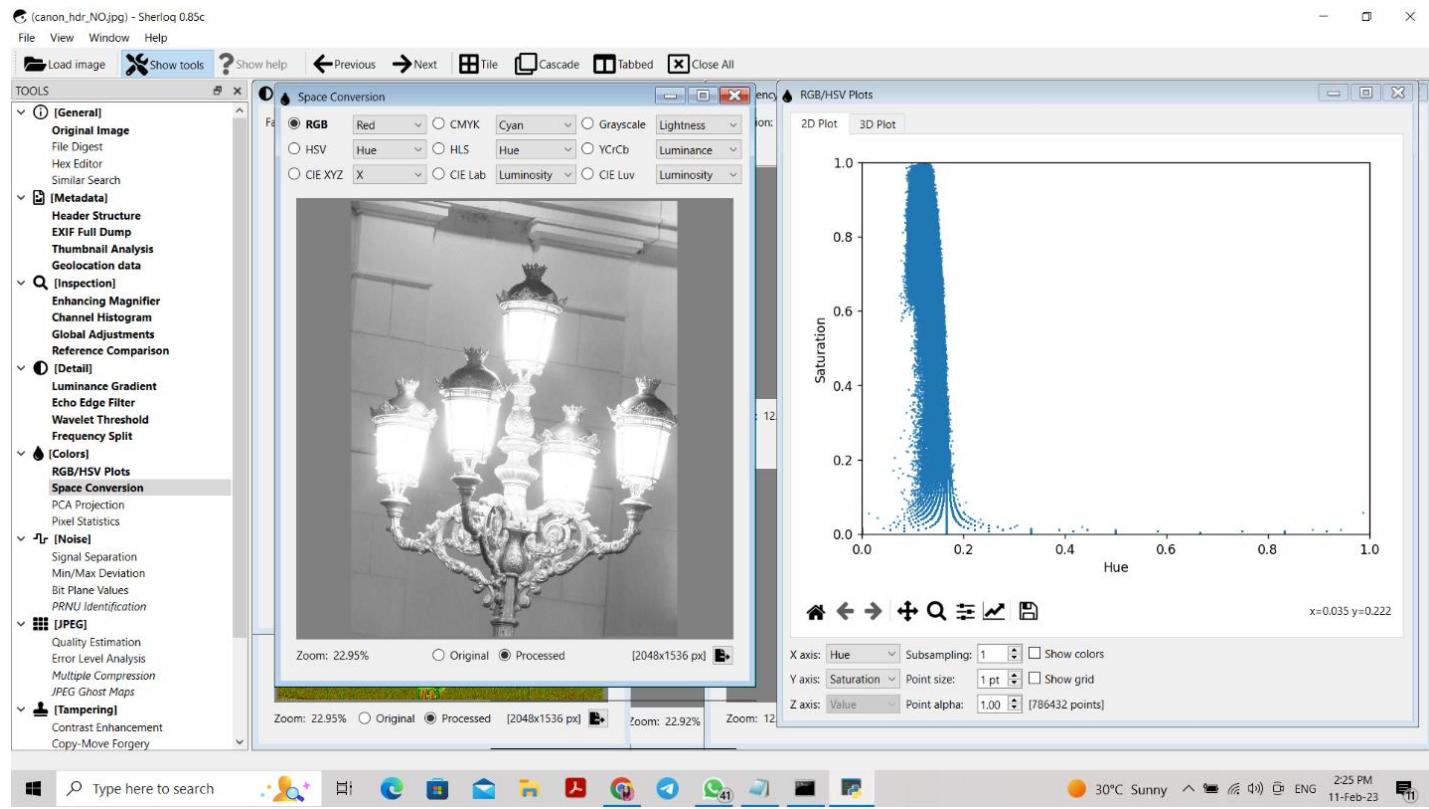
Wavelet Threshold-



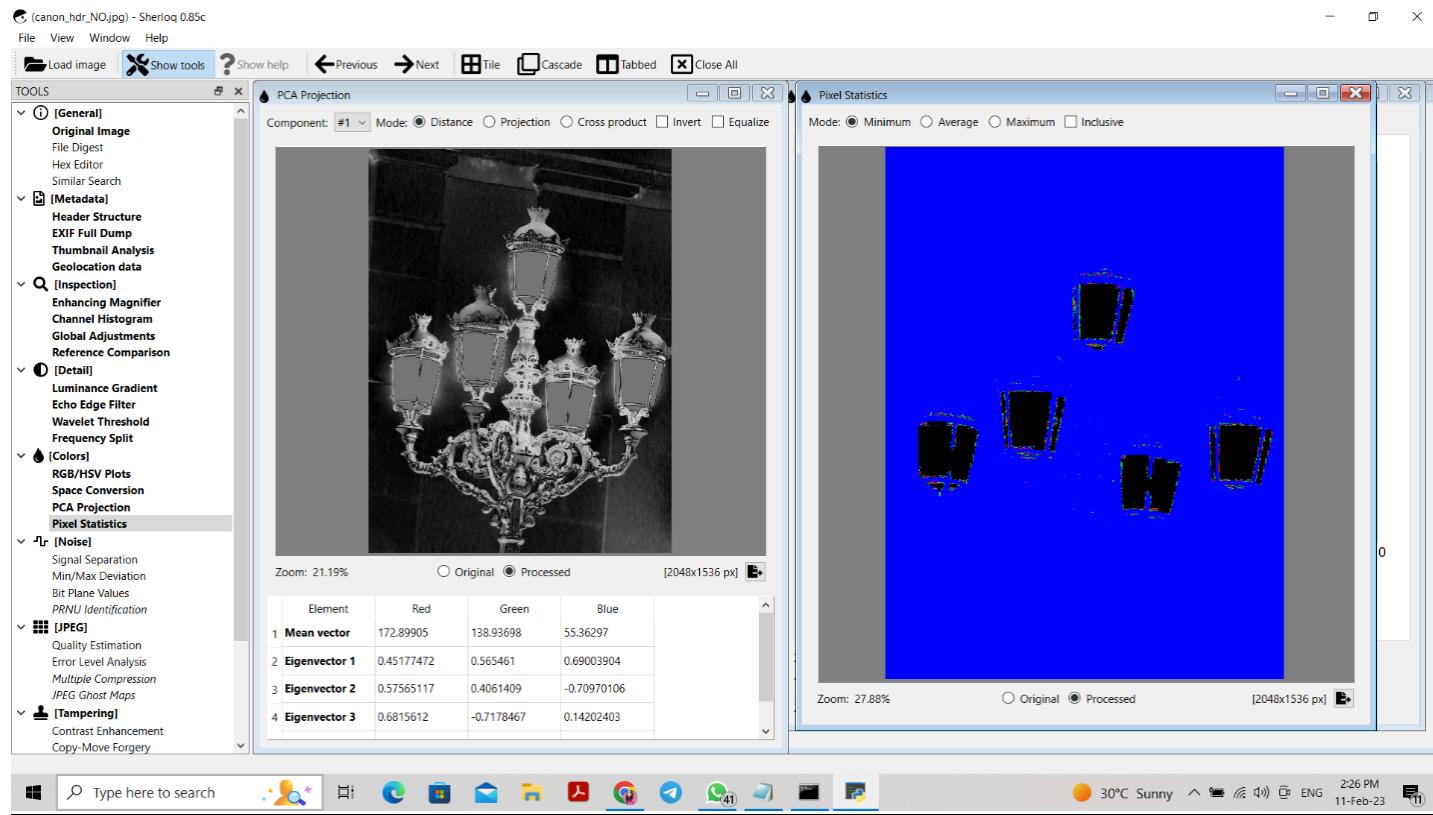
Frequency Split-



RGB/HSV Plots and space conversion-

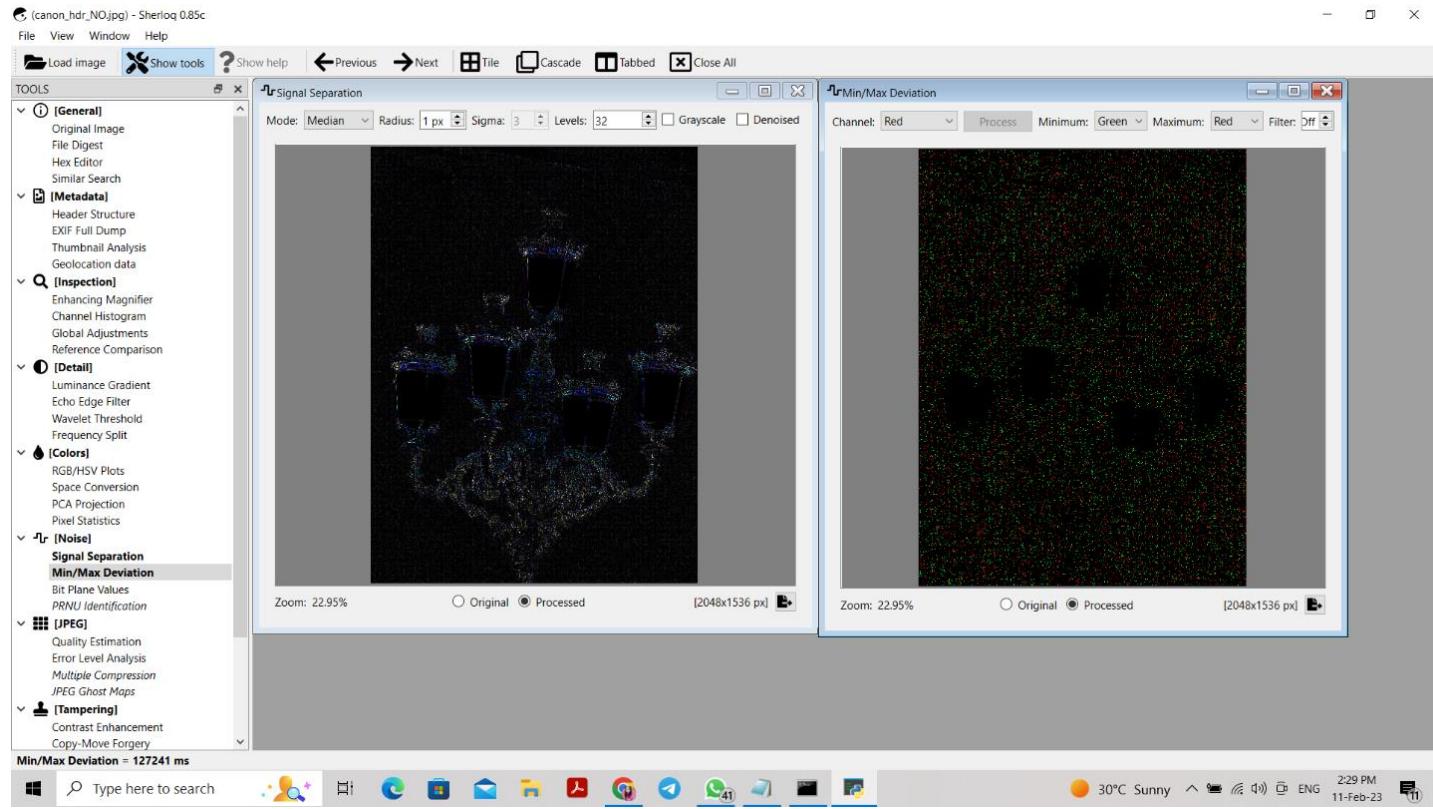


PCA Projection and Pixel statistics-

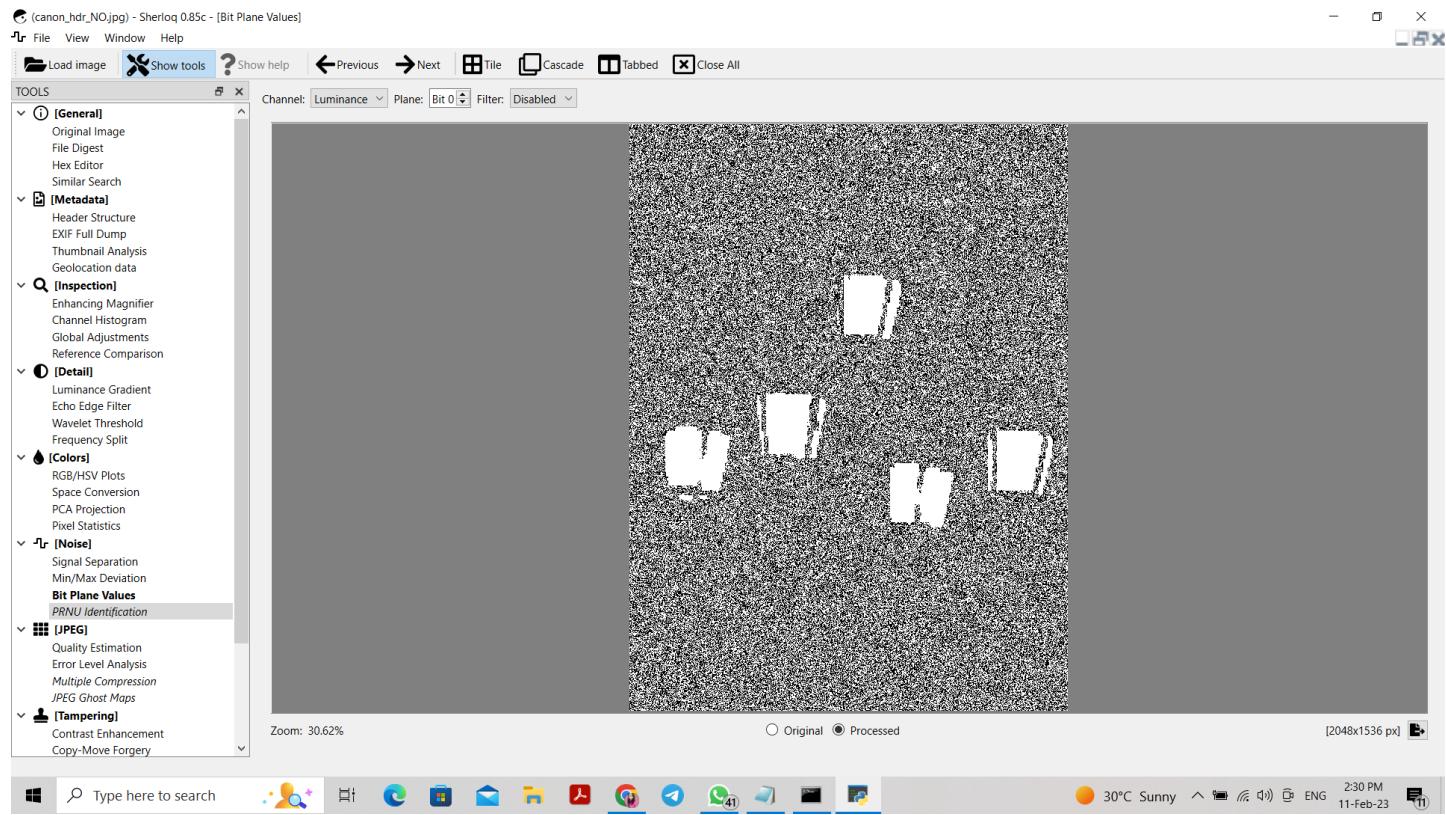


Under Noise,

Signal separation and Min/Max deviation -

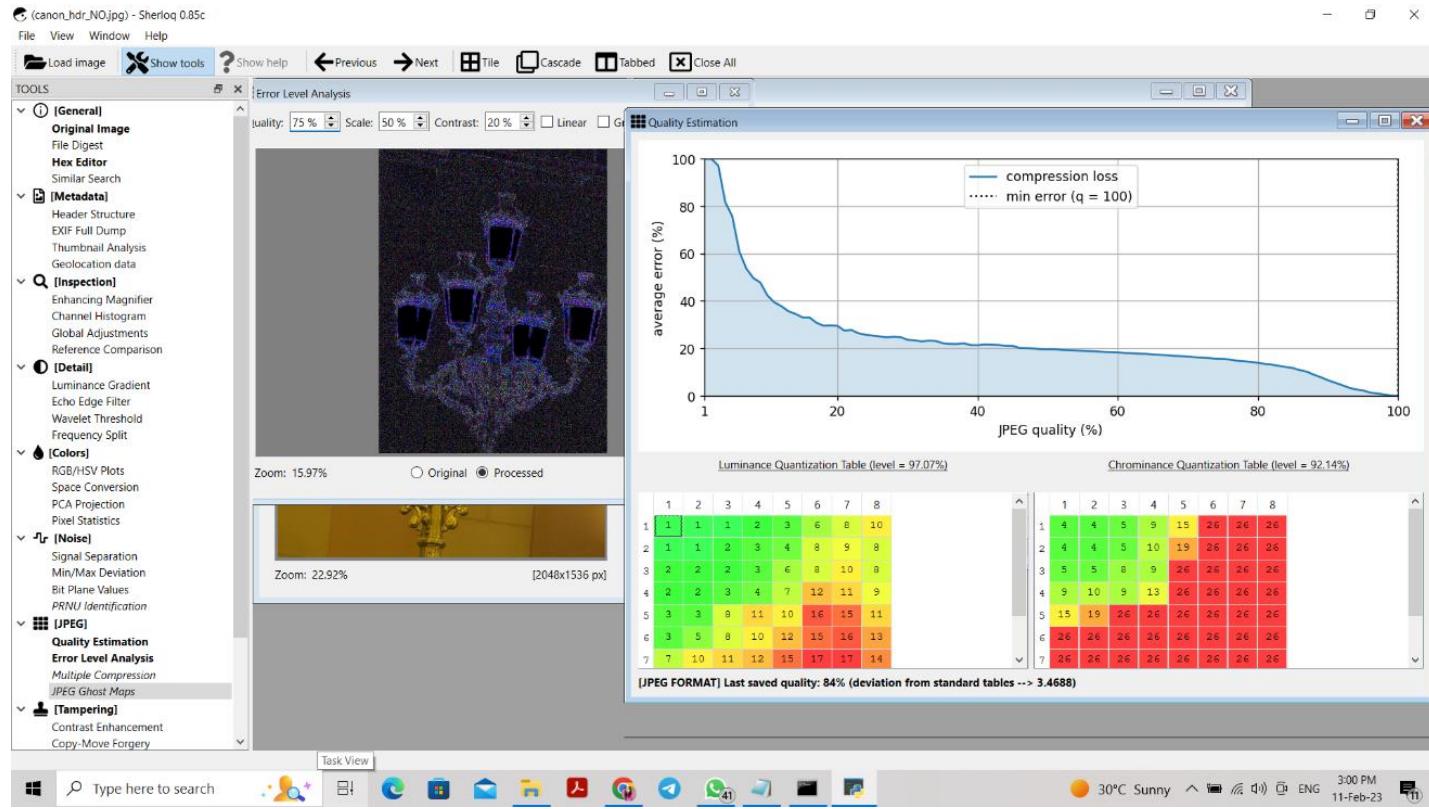


Bit Plane Values-



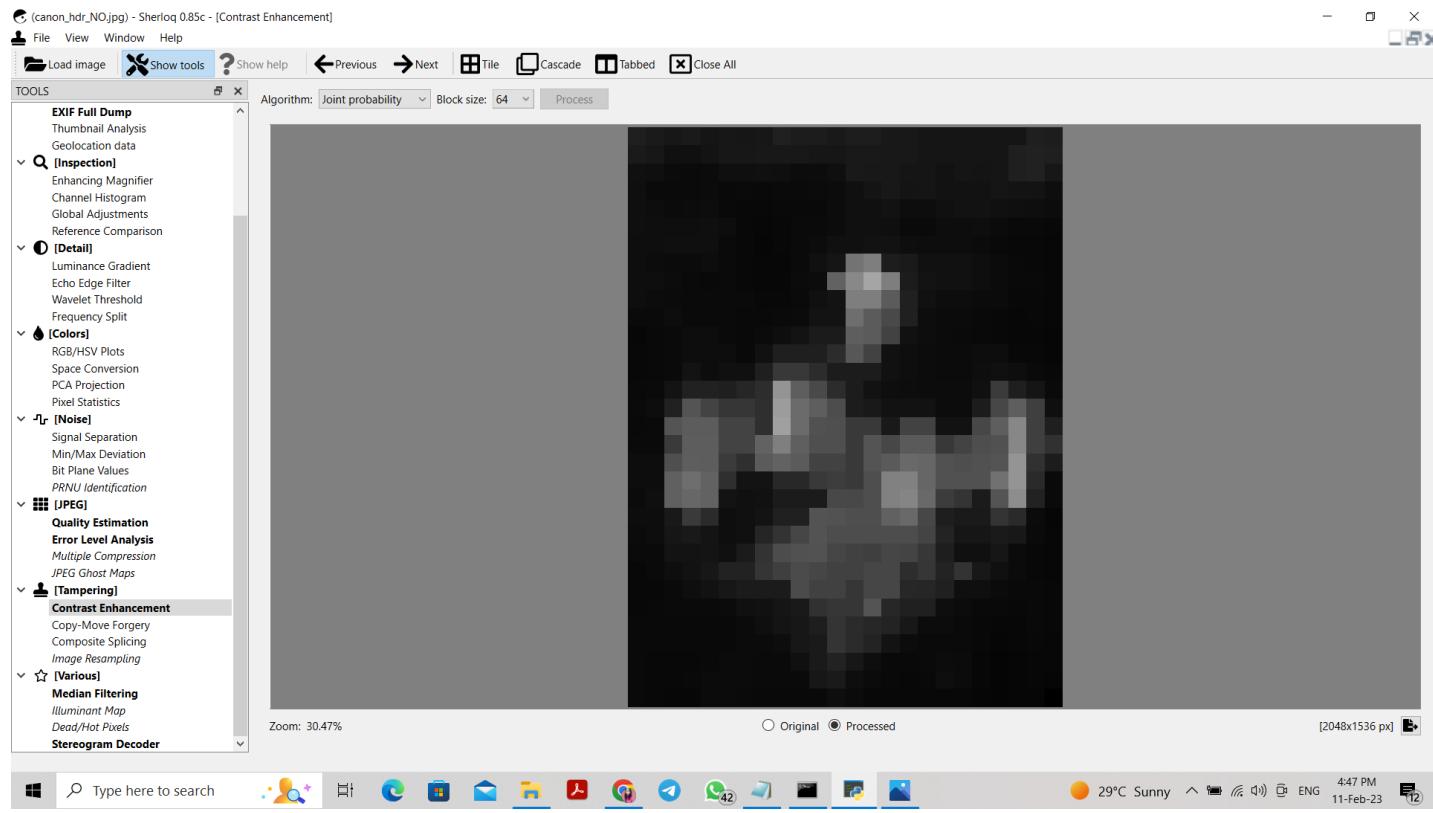
Under JPEG,

Quality Estimation and Error level analysis-

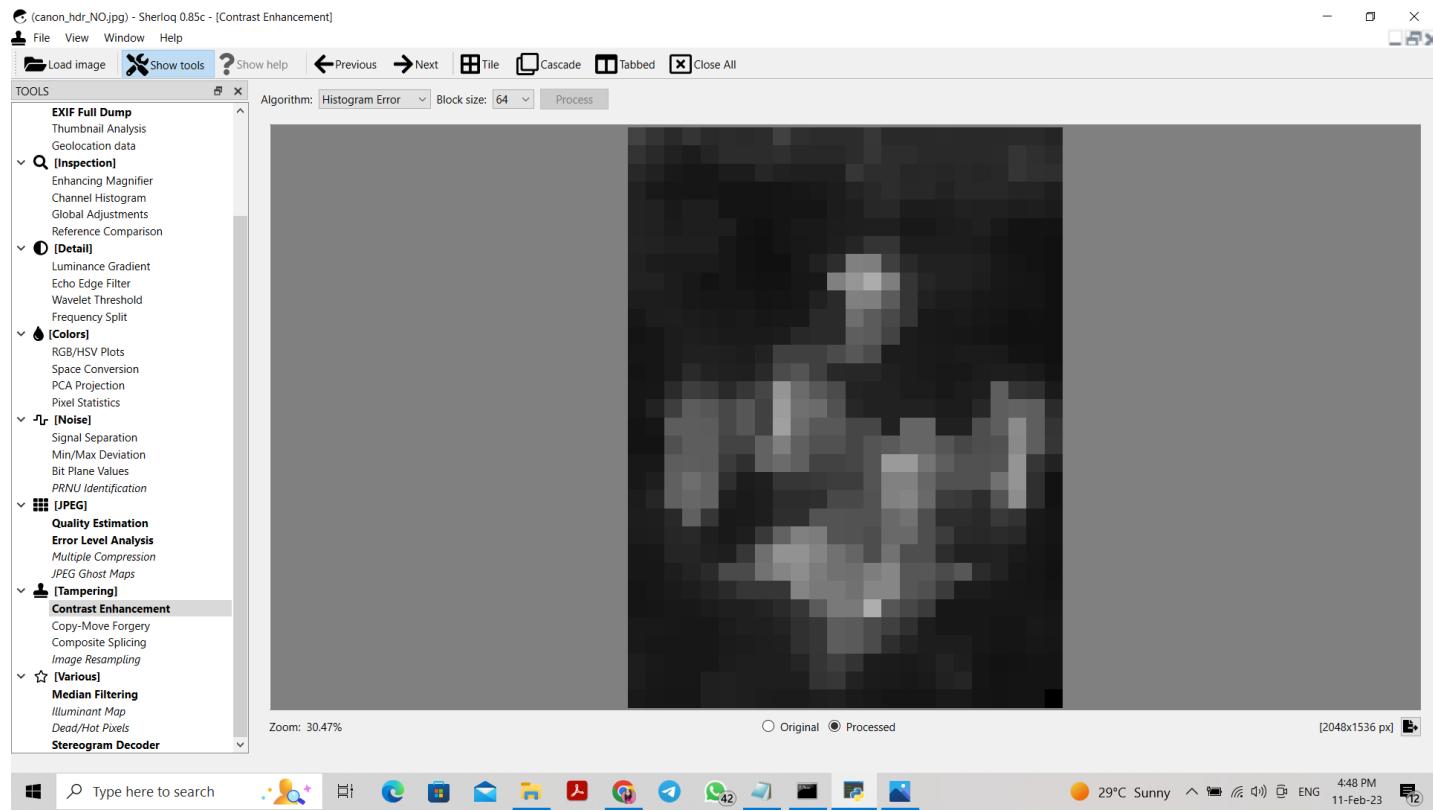


Under Tampering.

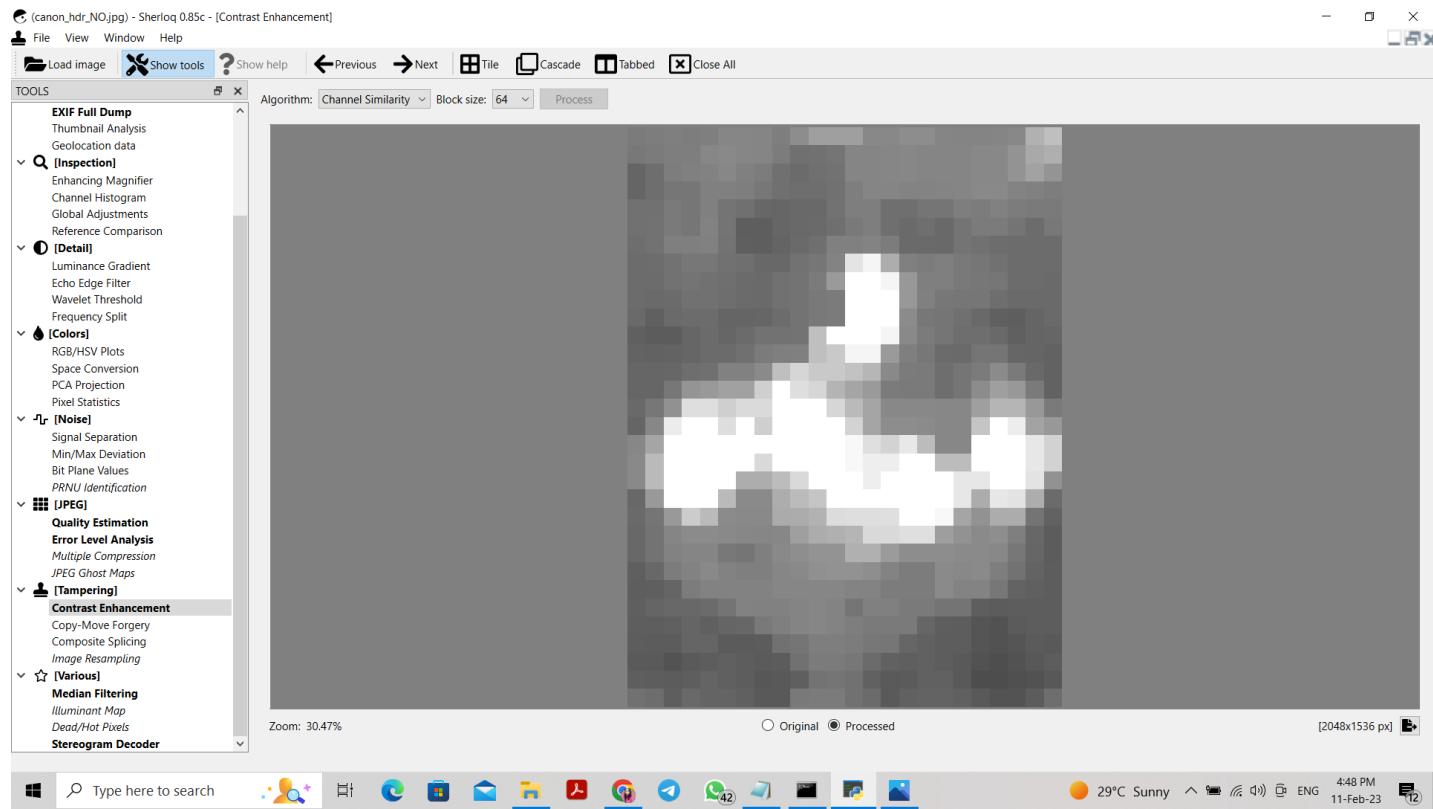
Contrast Enhancement (Joint probability algo)-



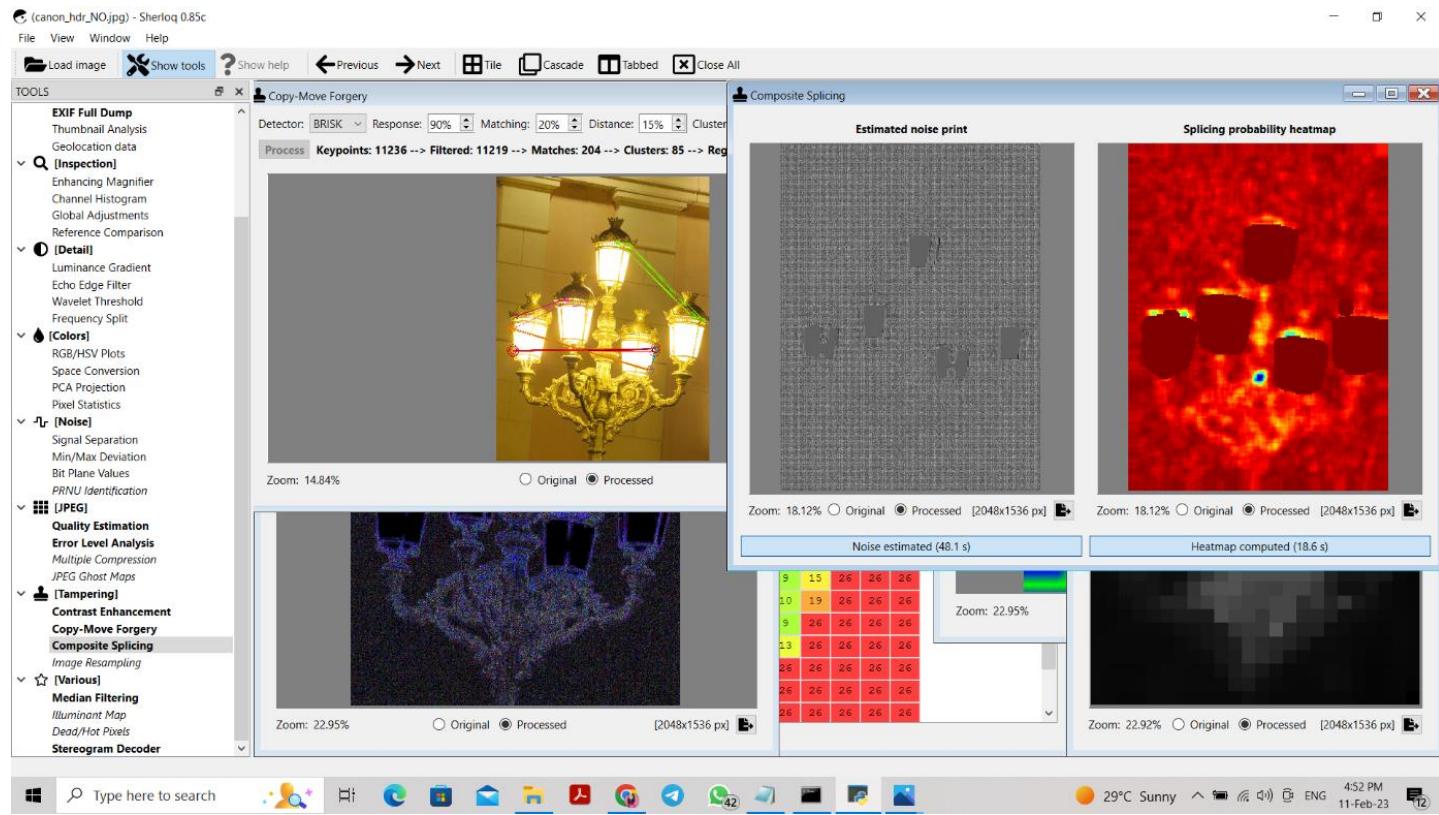
Contrast Enhancement (Histogram Error)-



Contrast Enhancement (Channel Similarity algo)-

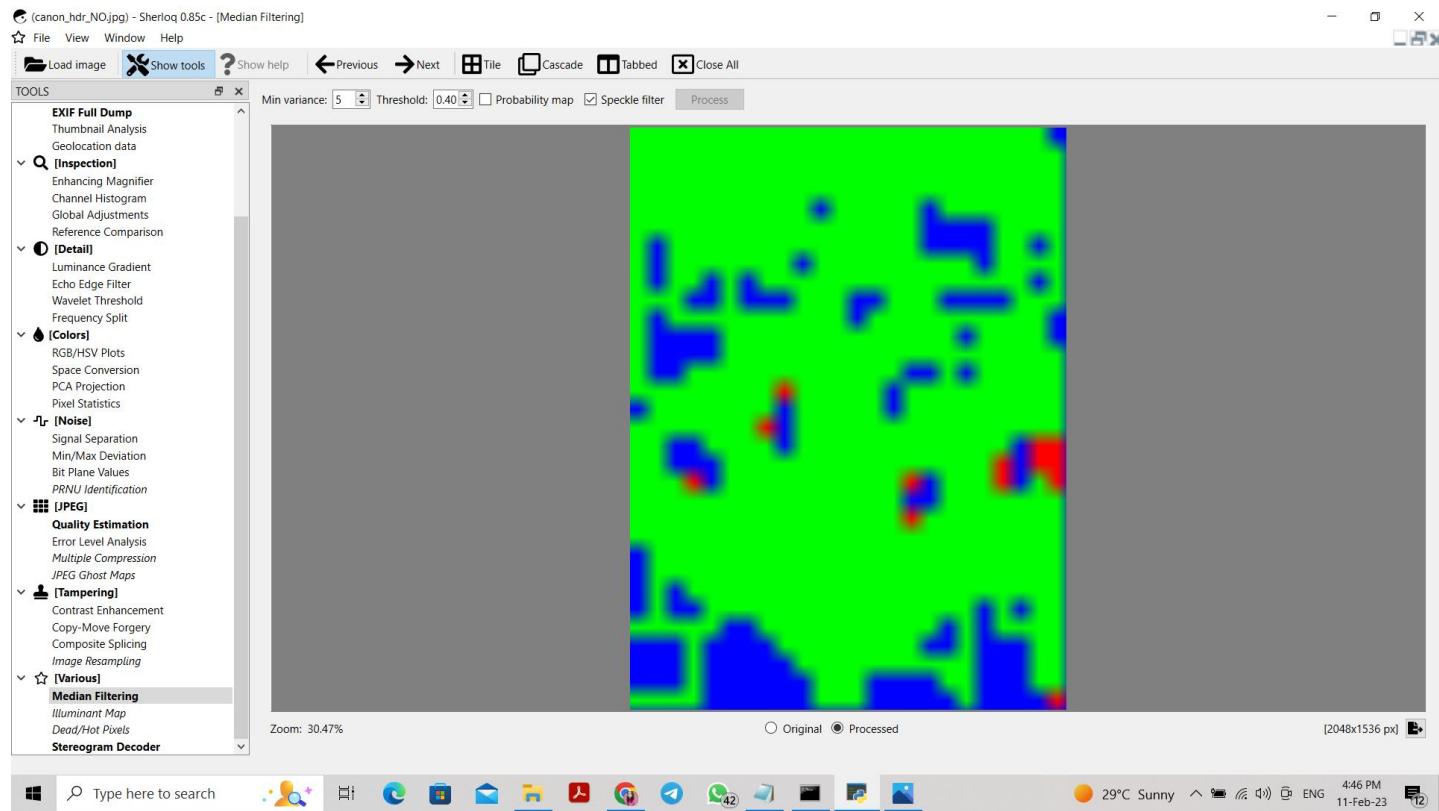


Copy move forgery and Composite Splicing -



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>