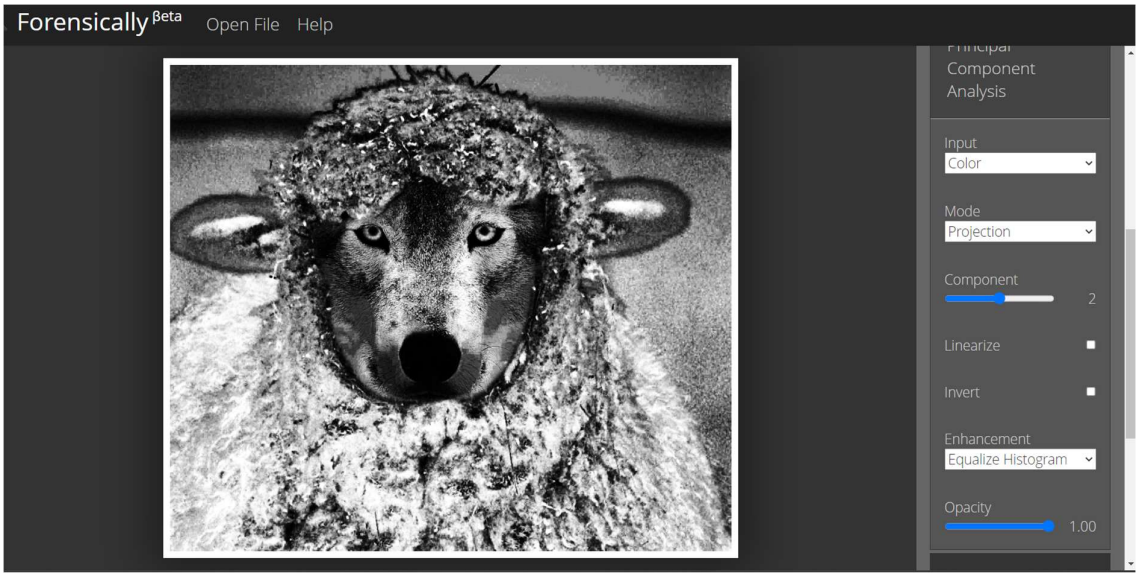
IMAGE FORENSICS

Go to Forensically website and upload the picture

Forensically link : https://29a.ch/photo-forensics/#forensic-magnifier

Clone Detection

Principle component analysis

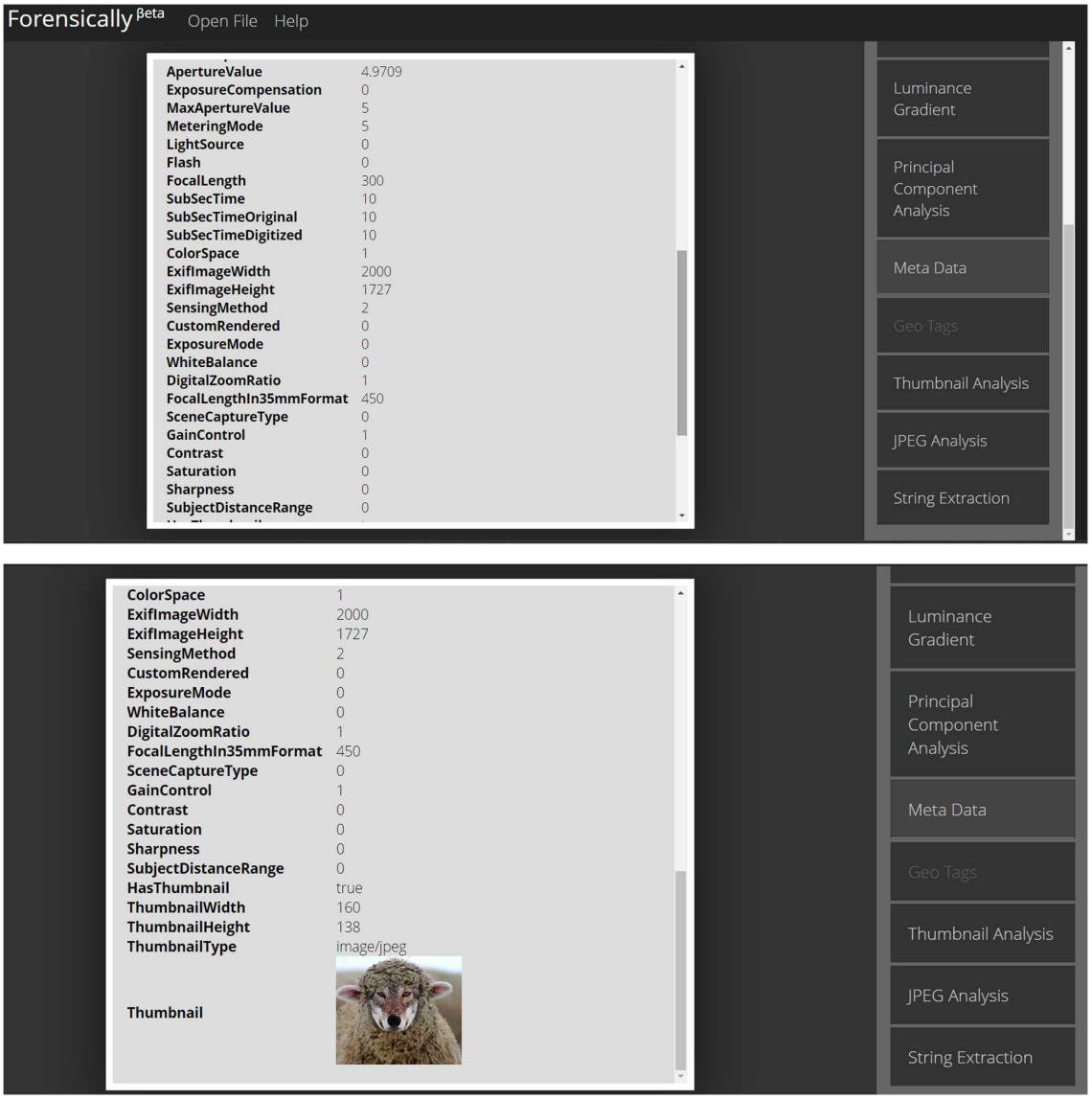


META DATA :

Check modify date and compare with original date

Check software such that to know which software it edited and in which os

ImageWidth	2000
ImageHeight	1727
BitsPerSample	8,8,8
PhotometricInterpretation	2
Make	NIKON CORPORATION
Model	NIKON D50
Orientation	1
SamplesPerPixel	3
XResolution	96
YResolution	96
ResolutionUnit	2
Software	Adobe Photoshop CC 2015 (Windows)
ModifyDate	Sat Apr 06 2019 15:17:32 GMT+0530 (India Standard Time)
YCbCrPositioning	2
ExposureTime	0.0025
FNumber	5.6000
ExposureProgram	0
DateTimeOriginal	Thu Dec 20 2007 17:06:17 GMT+0530 (India Standard Time)
CreateDate	Thu Dec 20 2007 17:06:17 GMT+0530 (India Standard Time)
CompressedBitsPerPixel	4
ShutterSpeedValue	8.6439
ApertureValue	4.9709



Go to FotoForensics and Upload Image then go to metadata so that you can see entire Data of the particular photo which you uploaded

FotoForensics link : https://fotoforensics.com/

Photoshop	
IPTC Digest	2fa07d2f4446a72118a7e9ada4207db2
Displayed Units X	inches
Displayed Units Y	inches
Print Style	Centered
Print Position	0 0
Print Scale	1
Global Angle	30
Global Altitude	30
Copyright Flag	False
URL List	
Slices Group Name	woldf sheep edit
Num Slices	1
Pixel Aspect Ratio	1
Photoshop Thumbnail	(Binary data 7288 bytes)
Has Real Merged Data	Yes
Writer Name	Adobe Photoshop
Reader Name	Adobe Photoshop CC 2015
Photoshop Quality	8
Photoshop Format	Standard
Progressive Scans	3 Scans

XMP	
XMP Toolkit	Adobe XMP Core 5.6-c111 79.158325, 2015/09/10-01:10:20
Creator Tool	Adobe Photoshop CS3 Windows
Metadata Date	2019:04:06 09:47:32+05:30
Format	image/jpeg
Legacy IPTC Digest	E8F15CF32FC118A1A27B67ADC564D5BA
Date Created	2007:12:20 11:36:17-05:00

you got to know that photoshop software used for this photo

String Extraction :

It works same as meta data it shows all the written and modified ,It gives all meta data in simple string formate ,String foramte inckudes Time Stamp , Sofware edited and all the written information etc

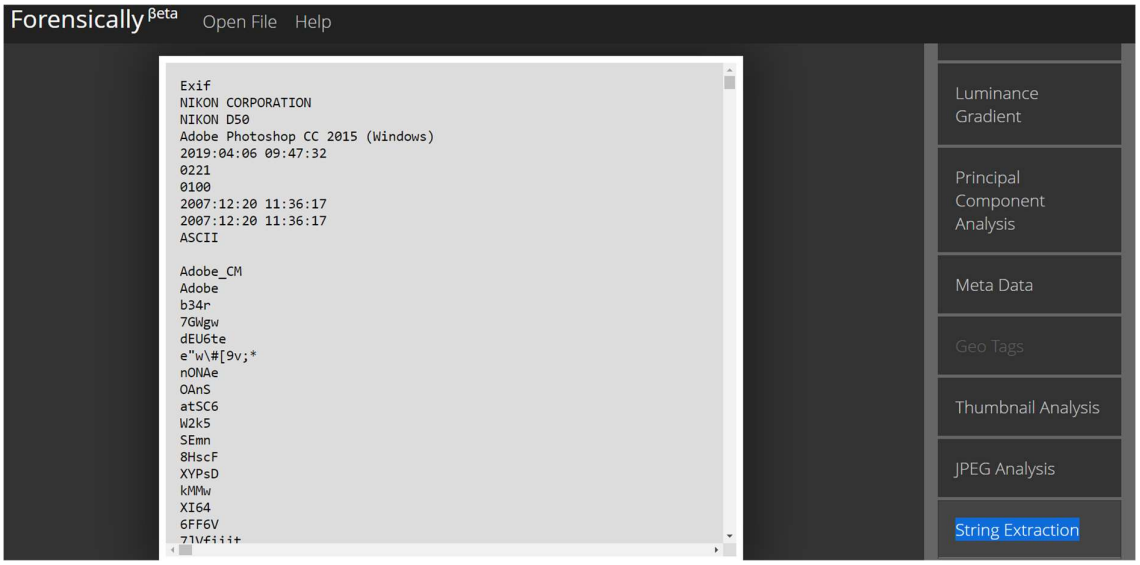
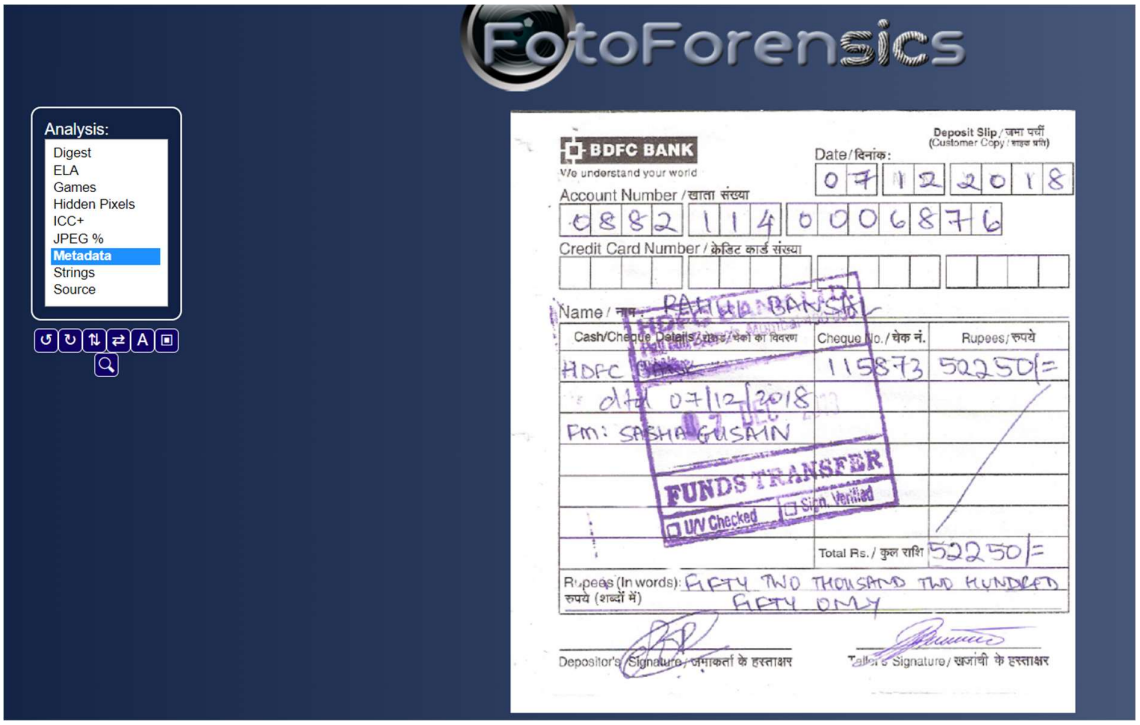


Image2 - Deposit Slip

Open Foto Forensics website

FotoForensics link : https://fotoforensics.com/

and upload the photo



go to metadata so that you can see entire Data of the particular photo which you uploaded

IPTC	
Coded Character Set	UTF8
Application Record Version	101
Time Created	14:32:43+00:00
Photoshop	
IPTC Digest	d4f0c7de4b4ea5033797a962fedcd5ae
Displayed Units X	inches
Displayed Units Y	inches
Print Style	Centered
Print Position	0 0
Print Scale	1
Global Angle	30
Global Altitude	30
URL List	
Slices Group Name	Healthy-Living-India-Cheque-Deposit-Slip
Num Slices	1
Pixel Aspect Ratio	1
Photoshop Thumbnail	(Binary data 8840 bytes)
Has Real Merged Data	Yes
Writer Name	Adobe Photoshop
Reader Name	Adobe Photoshop CC 2015
Photoshop Quality	12
Photoshop Format	Progressive
Progressive Scans	3 Scans
XMP	
XMP Toolkit	Adobe XMP Core 5.6-c111 79.158325, 2015/09/10-01:10:20
Create Date	2010:12:07 14:32:43

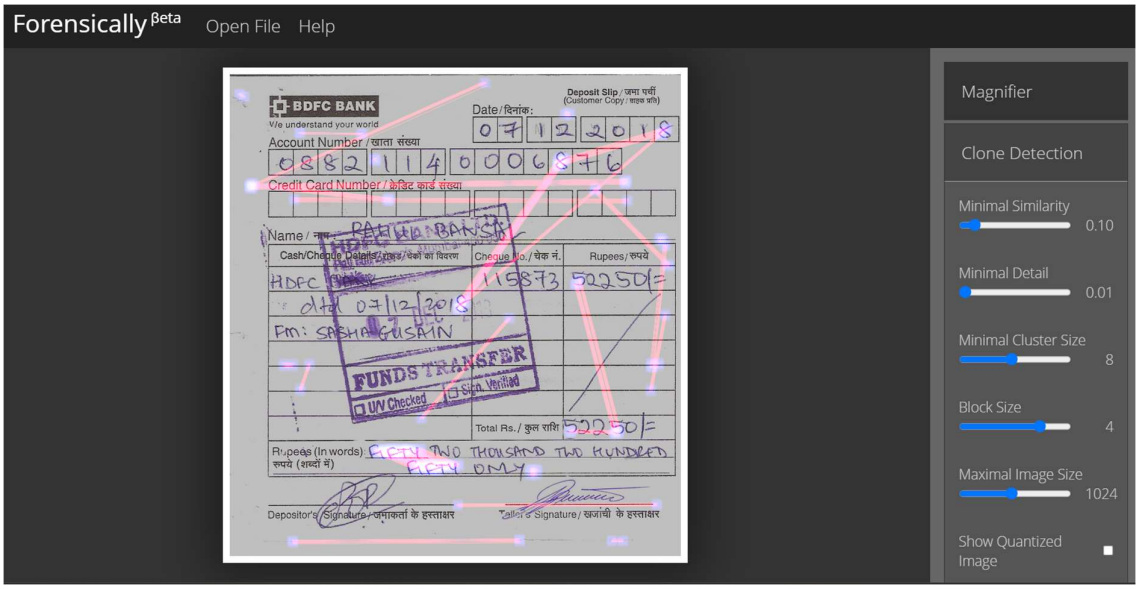
You got to known that IT is Edited by Adobe and Encoded by UTF-8

In EXIF you got to known that Modyfied Date and Original date , where that photo is edited and by which Os (Windows)

EXIF	
Photometric Interpretation	RGB
Make	HP
Camera Model Name	HP oj5600
Orientation	Horizontal (normal)
Samples Per Pixel	3
X Resolution	200
Y Resolution	200
Resolution Unit	inches
Software	Adobe Photoshop CC 2015 (Windows)
Modify Date	2019:05:04 08:43:19
Y Cb Cr Positioning	Co-sited
Reference Black White	0 255 128 255 128 255
Exif Version	0220
Date/Time Original	2010:12:07 14:32:43

Clone Detection :

By Clone detection you got to known which got manipulated and which got added



For example in this Sample you got to see that in top date section and Account number section 8 is manipulated , down in rupees Section that 5's got manipulated and in bottom portion FIFTY got added (Marked by all those red Marks you got to known which got manipulated)

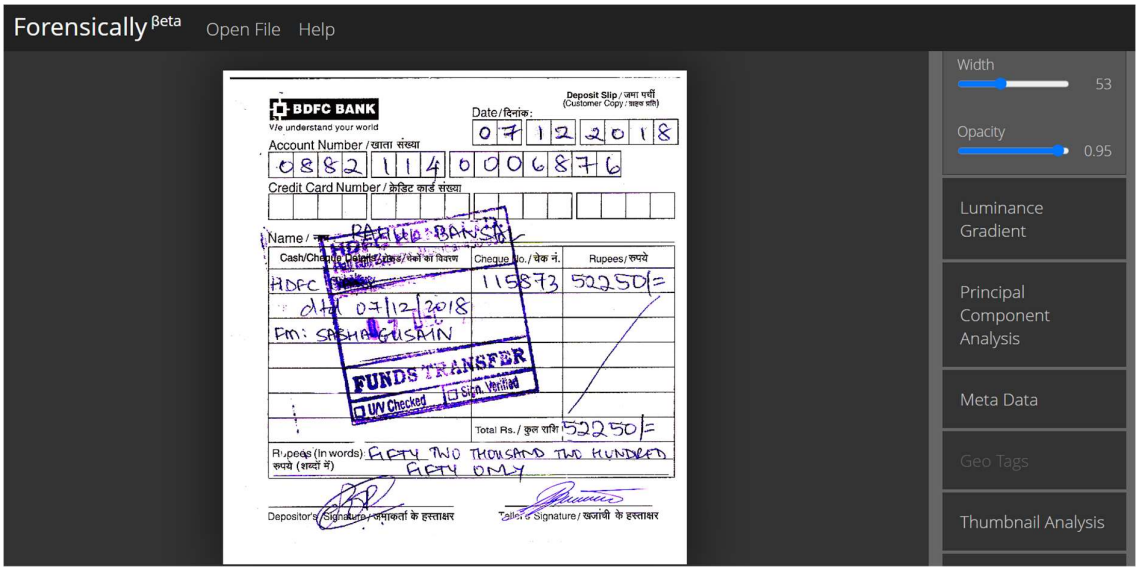
Error Level Analysis

Error Level Analysis is a forensic method to identify portions of an image with a different level of compression. The technique could be used to determine if a picture has been digitally modified.Error level analysis (ELA) is the analysis of compression artifacts in digital data with lossy compression such as JPEG.Error level analysis is used to improve the efficiency of distinguishing copy-move images produced by Deep Fake from the real ones. Error Level Analysis is used on images in-depth for identifying whether the photograph has long passed through changing.

Here signature is got added as it shown in different shade

Level Sweep

This tool allows you to quicky sweep through the histogram of an image. It magnifies the contrast of certain brightness levels.



Go to **Meta Data** :

Gives All the Information of Image

ImageWidth	720
ImageHeight	768
BitsPerSample	8,8,8
PhotometricInterpretation	2
Make	HP
Model	HP oj5600
Orientation	1
SamplesPerPixel	3
XResolution	200
YResolution	200
ResolutionUnit	2
Software	Adobe Photoshop CC 2015 (Windows)
ModifyDate	Sat May 04 2019 14:13:19 GMT+0530 (India Standard Time)
YCbCrPositioning	2
ReferenceBlackWhite	0,255,128,255,128,255
DateTimeOriginal	Tue Dec 07 2010 20:02:43 GMT+0530 (India Standard Time)
ColorSpace	1
ExifImageWidth	720
ExifImageHeight	768

ModifyDate	Sat May 04 2019 14:13:19 GMT+0530 (India Standard Time)
YCbCrPositioning	2
ReferenceBlackWhite	0,255,128,255,128,255
DateTimeOriginal	Tue Dec 07 2010 20:02:43 GMT+0530 (India Standard Time)
ColorSpace	1
ExifImageWidth	720
ExifImageHeight	768
Saturation	0
Sharpness	0
HasThumbnail	true
ThumbnailWidth	150
ThumbnailHeight	160
ThumbnailType	image/jpeg
Thumbnail	

String Extraction –

Sometimes images contain (meta) data in odd places. A simple way to find these is to scan the image for sequences of sensible characters. A traditional tool to do this is the strings program in Unix-like operating systems

```
Exif
HP oj5600
Adobe Photoshop CC 2015 (Windows)
2019:05:04 08:43:19
0220
0100
2010:12:07 14:32:43
   0A0   7A0   8A0HPSI0002
  11A0   0A0   0A0       0
  21A0   0A0   0A0       0
  31A0   0A0   0A0       0
  32A0   0A0   0A0       0
  41A0   0A0   0A0       0
  42A0   0A0   0A0       0
  43A0   0A0   0A0       0
  44A0   0A0   0A0       0
  51A0   0A0   0A0       0
  61A0   1A0   1A0       0
  62A0   0A0   0A0       0
  63A0   0A0   0A0       0
  64A0   0A0   0A0       0
  71A0   1A0   1A0       0
  81A0   4A0   1A0       0
  82A0   4A0   1A0       0
  83A0   4A0   1A0       0
  84A0   4A0   1A0       0
Adobe CM
```

Image 3 :

Go to Foto Forensics Site : https://fotoforensics.com/

Upload Image

You get Meta Data :

You can get entire information image Where it edited and when It modified

File	
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Exif Byte Order	Little-endian (Intel, II)
Current IPTC Digest	641c991ccc1d480b8b674174ccf41146
Image Width	5184
Image Height	3456

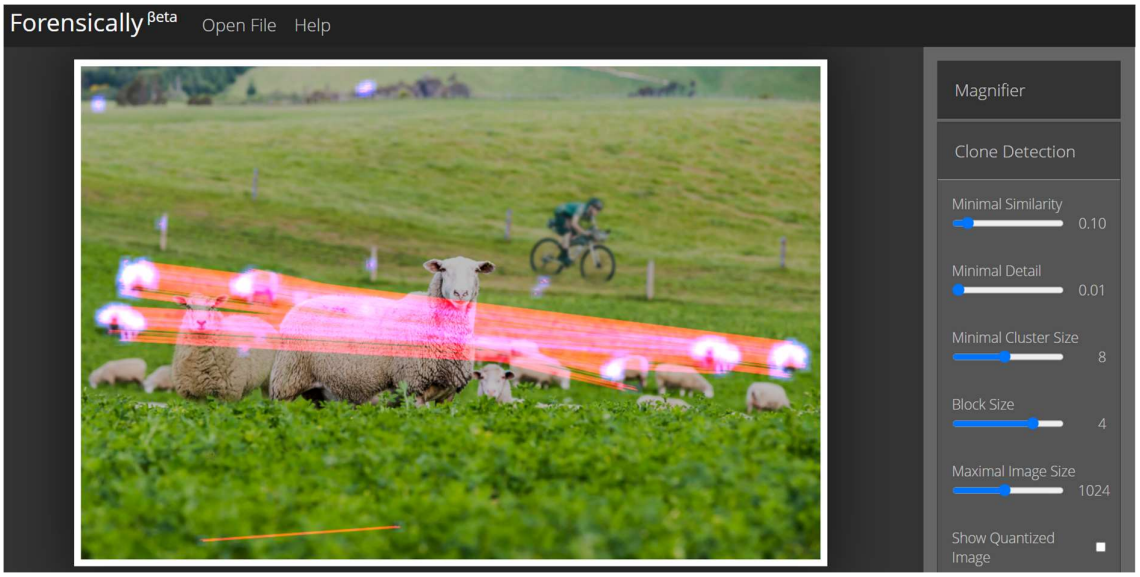
EXIF	
Photometric Interpretation	RGB
Orientation	Horizontal (normal)
Samples Per Pixel	3
X Resolution	300
Y Resolution	300
Resolution Unit	inches
Software	Adobe Photoshop CC 2015 (Windows)
Modify Date	2019:04:06 10:53:33
Exif Version	0230
Color Space	sRGB
Exif Image Width	5184
Exif Image Height	3456
Compression	JPEG (old-style)
Thumbnail Offset	398
Thumbnail Length	6844
Thumbnail Image	(Binary data 6844 bytes)

IPTC	
Coded Character Set	UTF8
Application Record Version	101

Photoshop	
IPTC Digest	641c991ccc1d480b8b674174ccf41146
Displayed Units X	inches
Displayed Units Y	inches
Print Style	Centered
Print Position	0 0
Print Scale	1

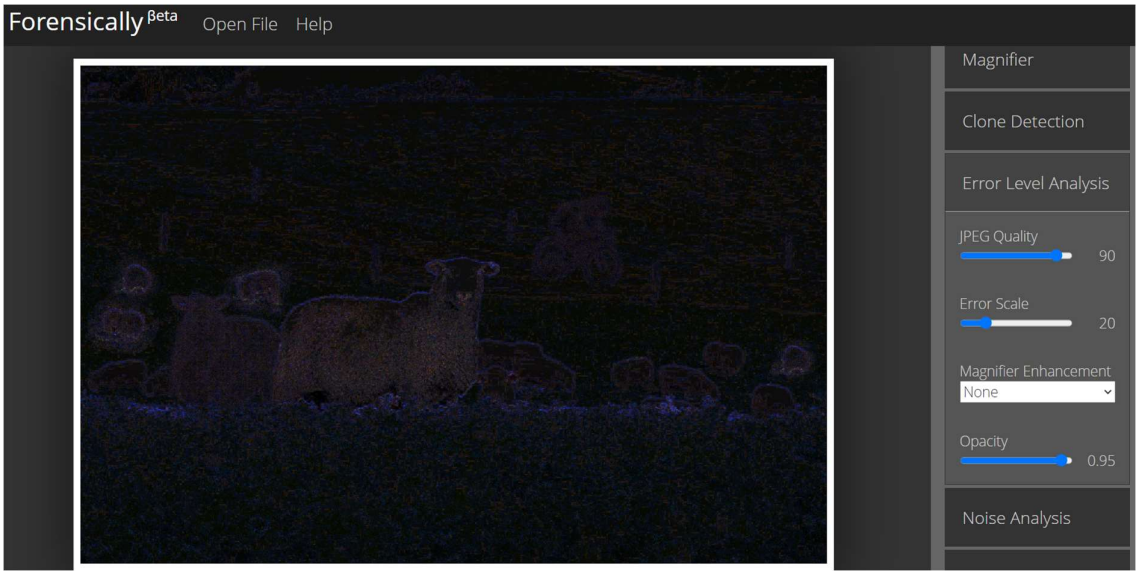
Clone Detection :

If you clone any of Particular item ,It revels what you have added any new



Error Level Analysis :

.The technique could be used to determine if a picture has been digitally modified

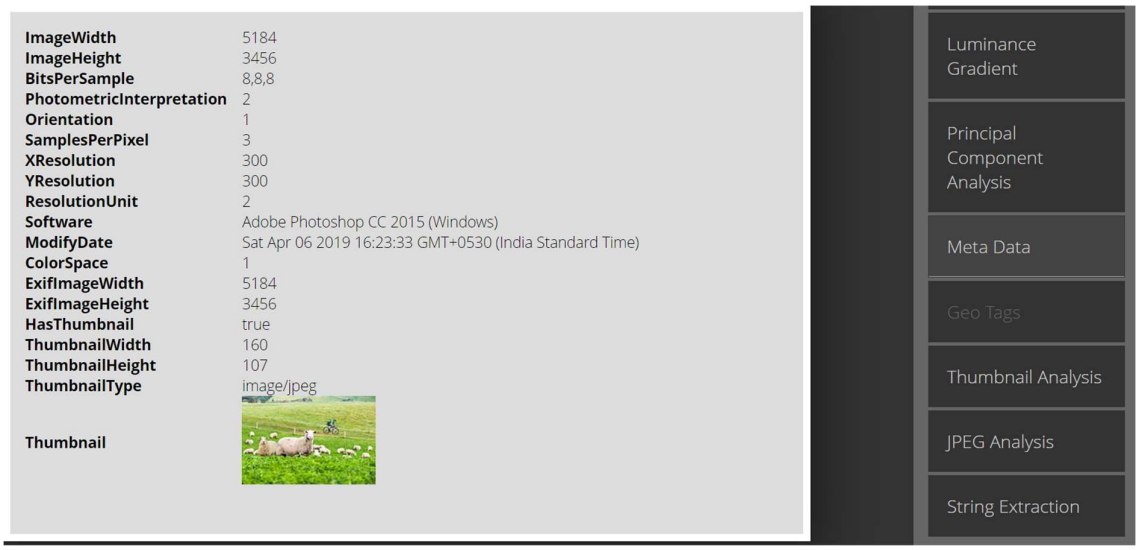


You got to know that there is no cycle rider as It is added

Level Sweep :

Meta Data :

Entire information of photo will be recorded such as Software it got edited and Modify Dae



String Extraction :

Sometimes images contain (meta) data in odd places. A simple way to find these is to scan the image for sequences of sensible characters.