

Image-Based OSINT Investigations Tips & Techniques

Images can provide a wealth of value to an OSINT investigation, they can show what a subject looks like, locations where the subject has been, and any vehicles used. Identifying this information can facilitate actions like surveillance or arrests, which would otherwise be reliant on text-based descriptions.

Using search engines and free tools, investigators can utilize images to develop the intelligence picture, identify devices used to take images, identify where and when images were taken, and identify if a social media account belongs to a subject.

This article will detail reverse image searching, facial comparison, deepfakes, and metadata, showing you how to get the most value from your image-based OSINT investigations.

This is an introduction to Image-Based OSINT investigations. To view the full webinar and handout, which includes advanced techniques and analysis, [click here](#).

Reverse Image Searching

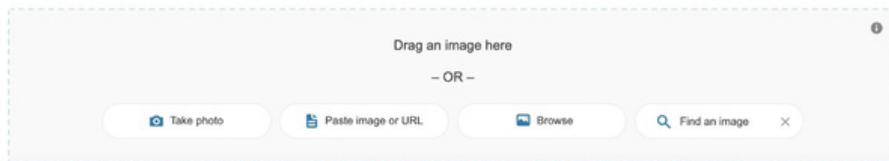
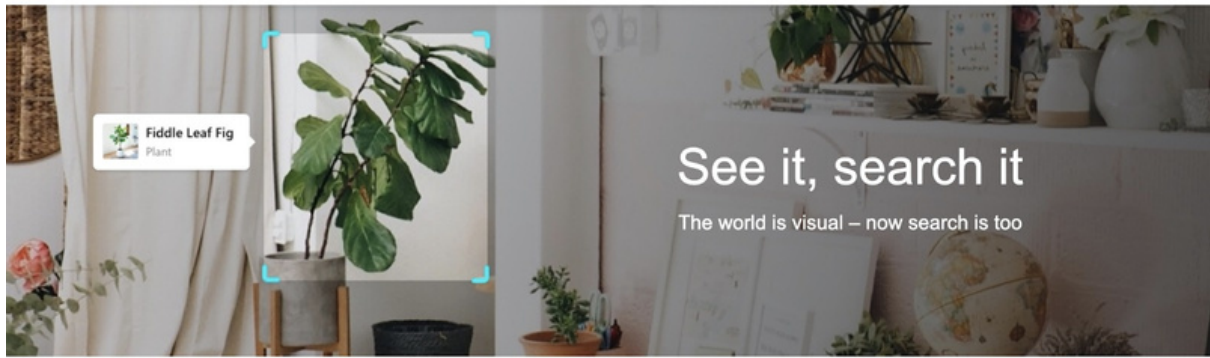
Using Search Engines, you can quickly discover visually similar photos from around the web using Reverse Image Searching technology, utilizing content-based image retrieval (CBIR) query techniques. Uploading a photograph from your device or inputting the URL of an image, you can ask a search engine to locate and show you related images used on other websites, either those images that are exactly the same or the same but a different size, or those that contain similar looking items or people.

Reverse Image Searching can be used as part of an investigation to identify related images relating to images that contain statues, buildings, places, people, and logos. Using Search Engines, you may be able to identify where an image was taken by recognizing a statue or building in the background that can be identified by the Search Engine. Similarly, Search Engines may be able to locate other images of your subject or logos on sites that identify them.

Reverse Image Searching can be conducted on most search engines, as well as on sites dedicated to Reverse Image Searching. Some of the best sites for Reverse Image Searching include:

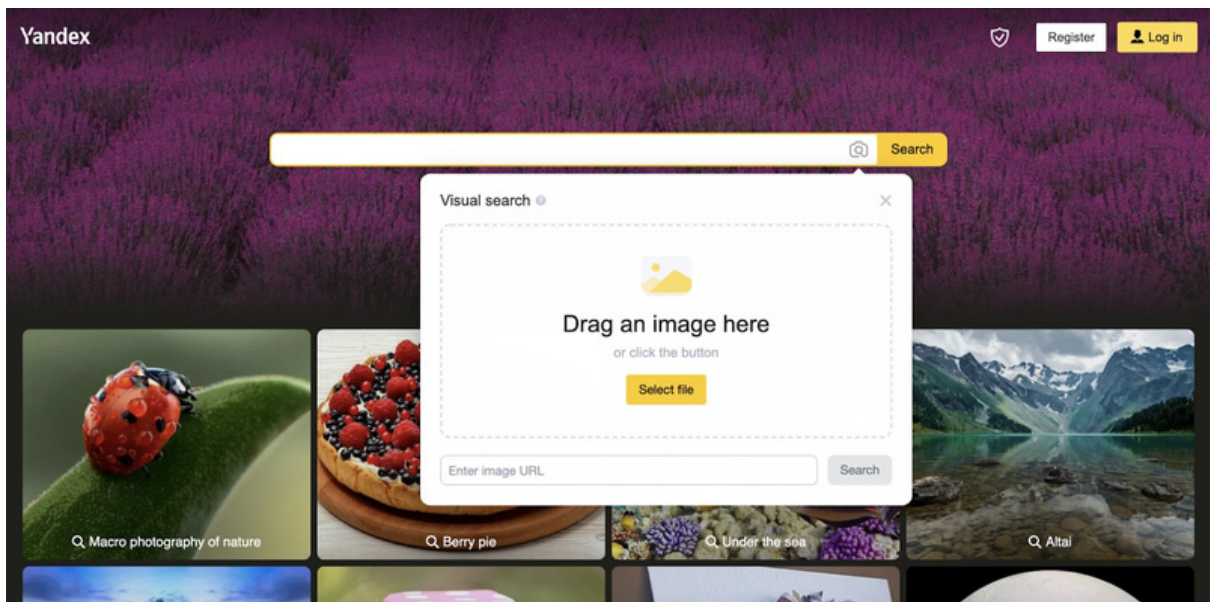
Bing Visual Search - <https://www.bing.com/visualsearch>

Great for: Flipped and Altered Images, and Faces



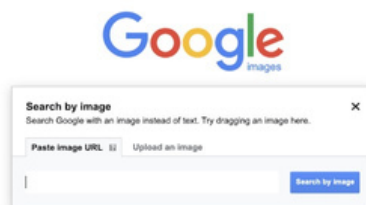
Yandex Visual Search - <https://yandex.com/images/>

Great for: Faces, Buildings, and Locations



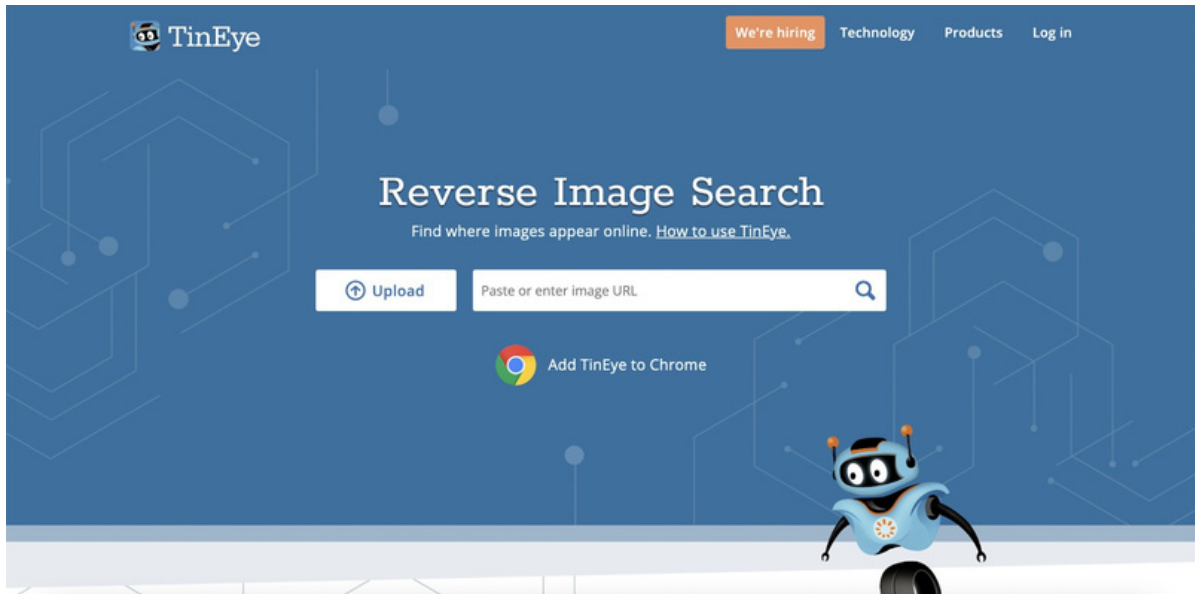
Google Images Search by Picture - <https://www.google.com/imghp>

Great for: Buildings, Locations, and Logos



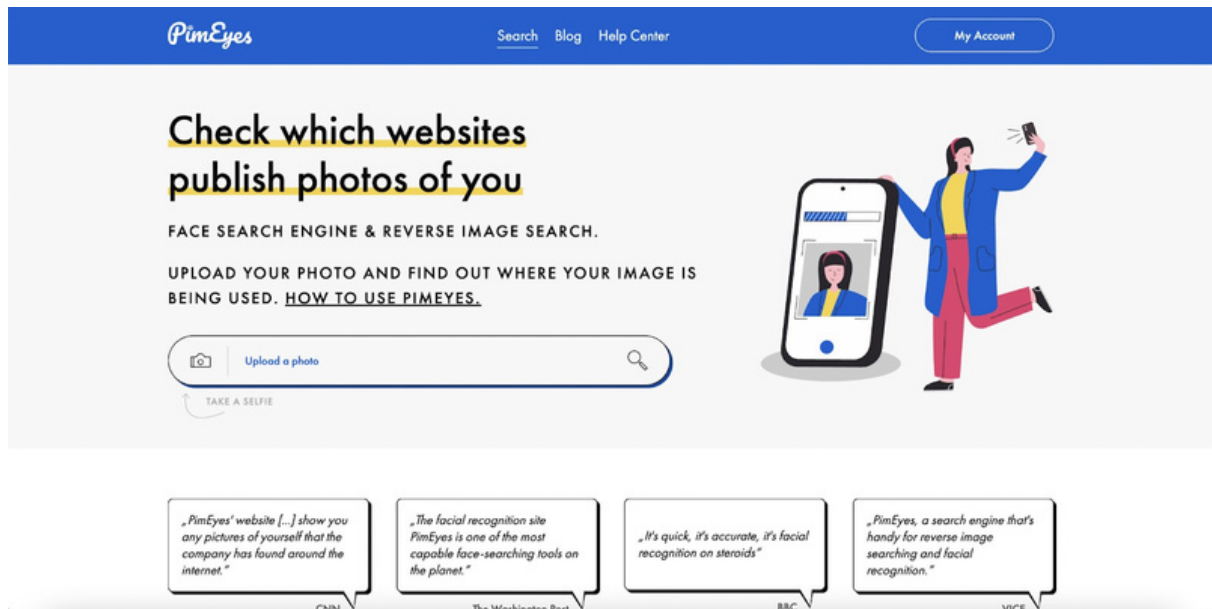
Tineye - <https://tineye.com/>

Great for: Logos and Alternate sized versions of the same image.



PimEyes - <https://pimeyes.com/en>

Great for: Faces



Facial Recognition

Facial Recognition systems use AI algorithms to detect, identify and analyze faces in images and videos. Facial features, including eyes, nose, mouth, and face shape can be used to devise a mathematical formula for a person's face.

Facial recognition systems analyze photographs to determine the face's geometry and develop this formula based upon a range of parameters. The system can then match the image to other images using the same technique, comparing if the formulas calculated are similar enough to denote a facial match.

Microsoft Azure - <https://azure.microsoft.com/en-au/services/cognitive-services/face/>

Microsoft Azure's face verification tool enables users to determine the likelihood that two uploaded images containing faces include faces that belong to the same person, which is expressed through a confidence score.

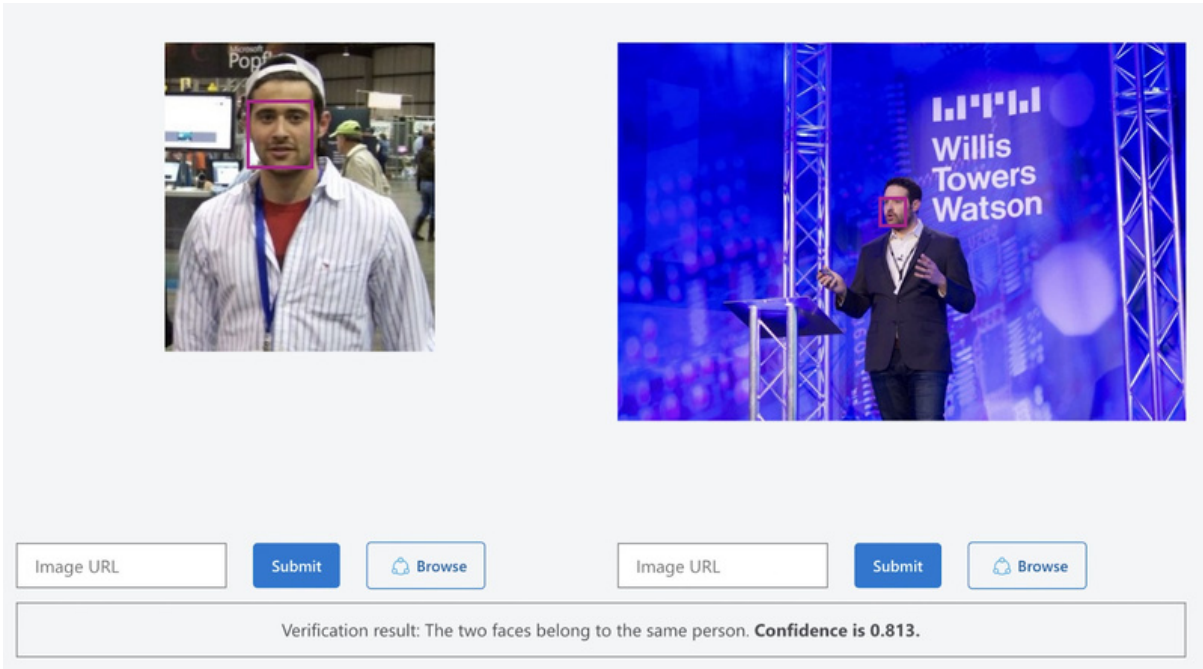


Image URL

Image URL

Verification result: The two faces belong to the same person. **Confidence is 0.813.**

Amazon Rekognition - aws.amazon.com/rekognition

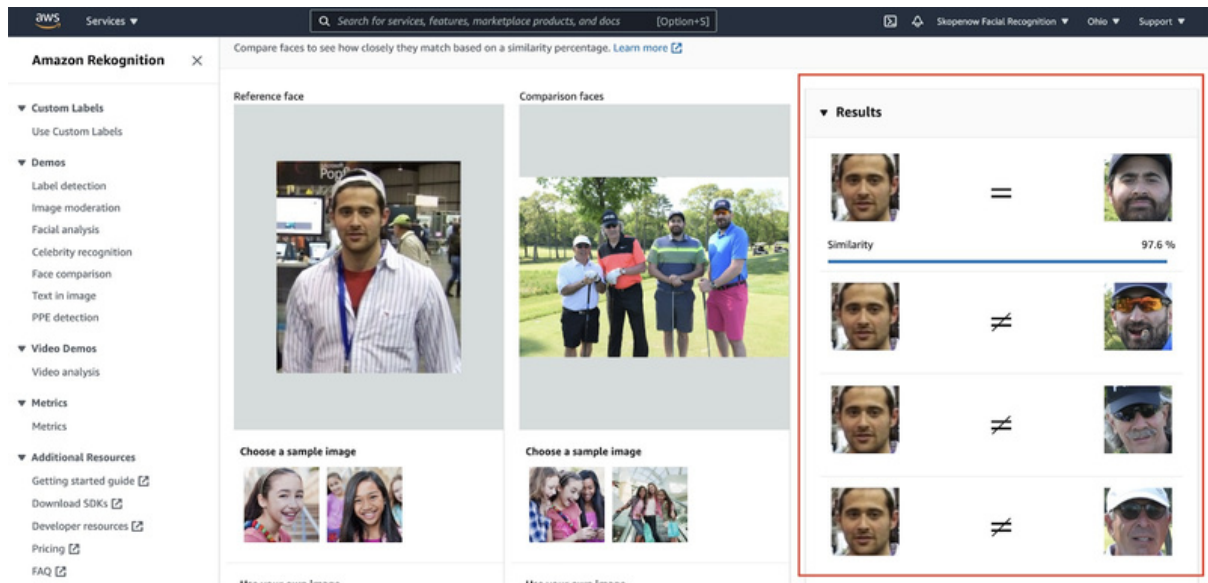
Amazon Rekognition can detect faces in images and videos. With Amazon Rekognition, you can get information about where faces are detected in an image or video, facial landmarks such as the position of eyes, and detected emotions. You can also compare a face in an image with faces detected in another image.

Using Facial Analysis you can analyze faces within an uploaded photograph for analyzed details of the included persons.

The screenshot shows the Amazon Rekognition console interface. On the left is a navigation menu with categories like Custom Labels, Demos, Video Demos, Metrics, and Additional Resources. The main area displays a photograph of four men on a golf course. Below the photo are options to 'Choose a sample image' or 'Use your own image' with an 'Upload' button. On the right, the 'Results' panel shows a list of attributes and their confidence scores:

Attribute	Confidence Score
looks like a face	99.9 %
appears to be male	99.7 %
age range	32 - 48 years old
smiling	58 %
appears to be happy	70.4 %
not wearing glasses	96.4 %

Using Face comparison, Rekognition will express a confidence score that the persons in two photos are the same person.



Deepfakes

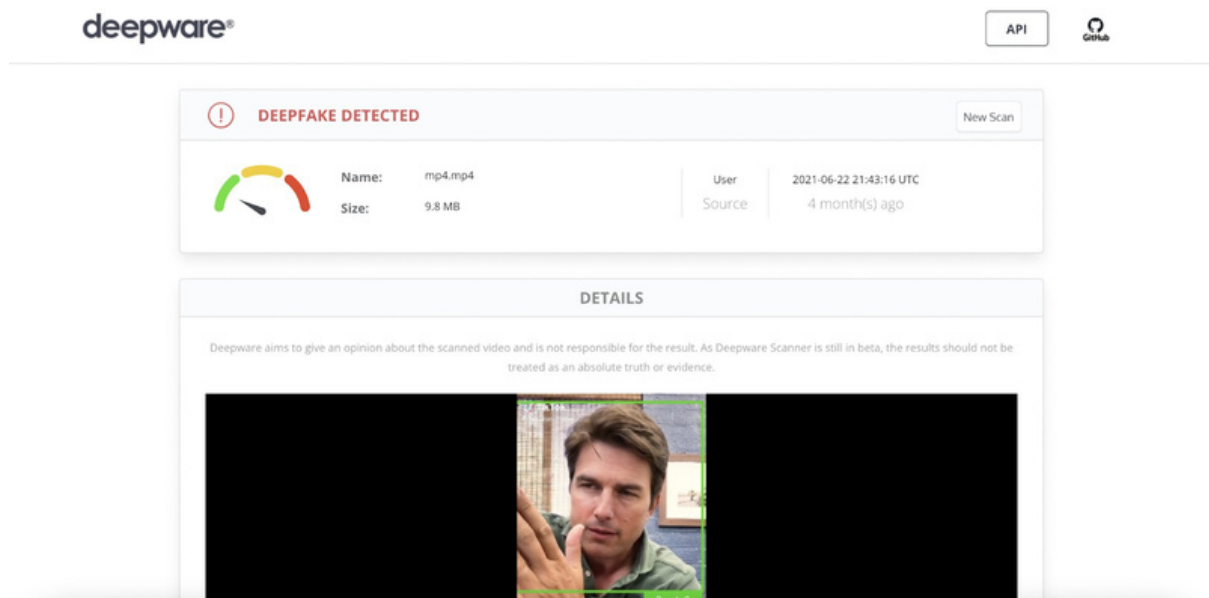
Deepfakes are convincing simulations of audio and video media created by AI using deep learning algorithms to make media that depicts fake events that have not occurred. Deepfakes enable media to be created that can depict politicians and celebrities making statements that they have never made and crimes being committed by innocent members of the public. Deepfakes can also be used to commit crimes, such as voices being replicated to access bank accounts via phone lines or to convince family members to transfer money.

Using OSINT techniques and tools deepfaked images, video, and audio can be identified, verified, and debunked.

The [Deepware Scanner](#) is a deepfake detection tool designed to enable users to analyze a suspicious video to find out if it's synthetically manipulated.

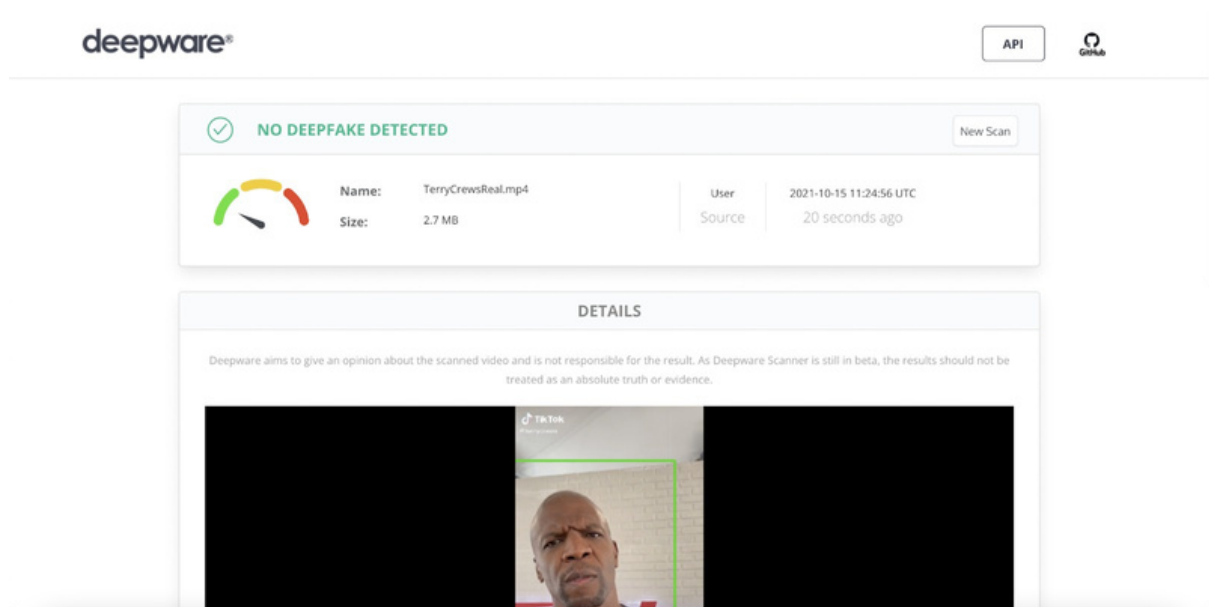
To use the Deepware scanner, access the website and upload a video from your device or using a video URL.

Using a [deepfake of Tom Cruise](#) from TikTok, the Deepware Scanner identified the video as being a deepfake.



The screenshot shows the Deepware Scanner interface. At the top left is the 'deepware' logo. At the top right are 'API' and 'GitHub' buttons. Below the header is a notification bar with a red exclamation mark icon and the text 'DEEFAKE DETECTED'. To the right of this bar is a 'New Scan' button. Below the notification bar is a summary section with a gauge icon showing a red needle. The summary includes: Name: mp4.mp4, Size: 9.8 MB, User Source: 2021-06-22 21:43:16 UTC, and Source: 4 month(s) ago. Below the summary is a 'DETAILS' section with a disclaimer: 'Deepware aims to give an opinion about the scanned video and is not responsible for the result. As Deepware Scanner is still in beta, the results should not be treated as an absolute truth or evidence.' Below the disclaimer is a video player showing a frame of Tom Cruise with a green bounding box around his face.

Using a [real video of Terry Crews](#) from TikTok, the Deepware Scanner identified the video as being genuine.



The screenshot shows the Deepware Scanner interface. At the top left is the 'deepware' logo. At the top right are 'API' and 'GitHub' buttons. Below the header is a notification bar with a green checkmark icon and the text 'NO DEEFAKE DETECTED'. To the right of this bar is a 'New Scan' button. Below the notification bar is a summary section with a gauge icon showing a green needle. The summary includes: Name: TerryCrewsReal.mp4, Size: 2.7 MB, User Source: 2021-10-15 11:24:56 UTC, and Source: 20 seconds ago. Below the summary is a 'DETAILS' section with a disclaimer: 'Deepware aims to give an opinion about the scanned video and is not responsible for the result. As Deepware Scanner is still in beta, the results should not be treated as an absolute truth or evidence.' Below the disclaimer is a video player showing a frame of Terry Crews with a green bounding box around his face.

Metadata

Metadata is data that provides information about data that is not the content of the data itself, i.e. summarising basic information about data to make it easier to find or work with.

Unfortunately, the majority of social media sites remove metadata from images as they are uploaded, however, if an original digital photo can be sourced then it is likely to provide some information on the photograph. Metadata can be viewed freely using a number of tools.

Jeffrey's Image Metadata Viewer – <http://exif.regex.info/exif.cgi>

Jeffrey's Image Metadata Viewer is a browser-based tool that enables you to upload a photo and view the EXIF data, detailing the time and date the image was taken, the type of camera used, and the location (in the event that location was enabled on the camera).

Jeffrey's Image Metadata Viewer will show all of the Metadata within an image, including Camera, Shutter Speed, Date Captured, and any embedded co-ordinates.

Basic Image Information

Target file: 20180704_172057[7684].jpeg

Camera:	samsung SM-A520F
Lens:	3.6 mm (Max aperture <i>f</i> /1.9) (shot wide open)
Exposure:	Auto exposure, Program AE, 1/25 sec, <i>f</i> /1.9, ISO 250
Flash:	none
Date:	July 4, 2018 5:20:57PM (timezone not specified) (3 years, 3 months, 9 days, 21 hours, 48 minutes, 47 seconds ago, assuming image timezone of GMT)
Location:	Latitude/longitude: 52° 28' 59" North, 1° 54' 51" West (52.483056, -1.914167) Map via embedded coordinates at: Google, Yahoo, WikiMapia, OpenStreetMap, Bing (also see the Google Maps pane below) Timezone guess from earthtools.org: GMT
File:	3,013 × 4,204 JPEG (12.7 megapixels) 2,441,333 bytes (2.3 megabytes)
Color Encoding:	WARNING: Color space tagged as sRGB, without an embedded color profile. Windows and Mac browsers and apps treat the colors randomly. Images for the web are most widely viewable when in the sRGB color space and with an embedded color profile. See my Introduction to Digital-Image Color Spaces for more information.

Extracted 183 × 256 8.3-kilobyte "EXIF:ThumbnailImage" JPG
Displayed here at 200% (1/68 the area of the original)



Click image to isolate; click this text to show histogram

*Please note that the location shown in the above screenshot is not associated with Skopenow or its employees. This location is used to demonstrate the capabilities of the platform.

Automating your Image-Based Investigations

Skopenow's facial recognition capabilities enable facial match searches against the person in an uploaded image that you upload against images that are available on social media profiles to bring back the best results. Skopenow instantly and anonymously locates and archives social media accounts and posts, plots location history, flags actionable behaviors, and reveals hidden connections between individuals. Skopenow's automatic report builder will save you time organizing the analyzed intelligence into a court-ready report. Please reach out to sales@skopenow.com or visit www.skopenow.com/demo to schedule a demo and activate a 7-day free trial for qualified businesses.