SKOPENOW

THE DEFINITIVE GUIDE:
Image-Based OSINT Investigations
<table>
<thead>
<tr>
<th><strong>INTRODUCTION</strong></th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reverse Image Searching</td>
<td>4</td>
</tr>
<tr>
<td>Facial Recognition</td>
<td>18</td>
</tr>
<tr>
<td>Deepfakes</td>
<td>24</td>
</tr>
<tr>
<td>Metadata</td>
<td>28</td>
</tr>
<tr>
<td>Brand Logo Identification</td>
<td>31</td>
</tr>
<tr>
<td>Automating Your Image-Based Investigations</td>
<td>33</td>
</tr>
</tbody>
</table>
INTRODUCTION

The old adage goes that “A picture is worth a thousand words”. 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 guide will show you how to conduct image-based OSINT investigations. We’ll discuss reverse image searching, facial comparison, deepfakes, brand logo identification, and metadata, showing you how to get the most value from your image-based OSINT investigations.
1

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 is characterized by an image being searched and can be done without any text-based search parameters, however, these can be used in addition to the image to provide better quality results.

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.

Investigators use Reverse Image Searching to locate the original source of an image or to identify the approximate date that the picture was first published on the Internet. Reverse image searching also enables Investigators to discover content that is related to their source image, as well as the popularity of the image and any manipulated versions of the image.

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](https://www.bing.com/visualsearch)

Bing states that its Visual Search enables you to “search the web using an image instead of text. You can use Visual Search to find similar images, products, pages that include an image, and even recipes”. To use Bing Visual Search, access the website and select either the ‘Paste Image or URL’ button if the image is browser-based, or the ‘Browse’ button if the image is saved to your device.

Great for: Flipped and Altered Images, and Faces

Yandex enables image-based searches on any image that is uploaded from a device or image URL, including entire images or a fragment of an image. Yandex’s image search is based on computer vision algorithms, which may result in exact copies of the source image and/or images that differ in minor ways from the original, such as different images of the same building. To find more images similar to the selected image, click Other sizes and similar to the right of the image. To see additional similar images, click More similar images on the search results page in the Similar images section.

Great for: Faces, Buildings, and Locations

Recent updates to Yandex now enable you to search for images on specific sites and add text with the image, similar to Google’s image search functionality.
Google Images Search by Picture - https://www.google.com/imghp

Google's Search by Image feature uses reverse image search to identify related images by uploading an image from a device or using an image URL. Google analyzes a submitted picture and constructs a mathematical model of it using advanced algorithms, which is then compared with billions of other images in Google's databases to identify matching and similar results. When available, Google also uses metadata about the image such as a description of the contents of the image.

Great for: Buildings, Locations, and Logos
Tineye - https://tineye.com/

TinEye is a search engine designed specifically for reverse image searching. When an image is uploaded from a device or image URL, TinEye creates a “unique and compact digital signature or fingerprint” of that image and matches it with other indexed images. TinEye identifies alternate sizes and edited versions of the submitted image, but will not usually return similar images of the same subject. TinEye may find different versions of logos due to their strong similarity.

Great for: Logos and Alternate sized versions of the same image.
PimEyes - https://pimeyes.com/en

PimEyes is a search engine designed specifically for facial recognition. PimEyes searches the Internet to find pictures containing given faces that match an image uploaded from a device or image URL. PimEyes markets itself as a platform to search your own face, a “self-monitoring, self-protection, and self-image management tool” that enables users to “find a face and protect your privacy”, stating that their platform is “a great tool to audit copyright infringement”. PimEyes uses the self-use argument in an attempt to circumvent laws relating to the use of facial recognition. However, PimEyes is used extensively in the Investigative world due to its powerful facial recognition capabilities, which outperform other reverse image searching platforms for the majority of images.

PimEyes states that it exclusively crawls websites for images and does not return any images that have been scraped, separating it from services like Clearview AI that search for facial matches against scraped images held in a database. According to PimEye’s website, images uploaded to the site are not saved or indexed, however, a ‘fingerprint’ of the features of a face within images is encoded and temporarily saved on its servers.

Great for: Faces

Until October 2021, PimEyes provided users with 10 free searches per day, which would display a number of blurred results. Unfortunately, PimEyes is now behind a paywall, which means that users have to pay at least $23.99 per month to access search results.

Each search engine has its own strengths and weaknesses with regard to its reverse image searching capabilities. When searching by images containing different contents, whether statues, buildings, locations, faces, and logos, each platform will deliver different results and results of varying quality.
Searching for Statues
When searching with images containing statues, Google is the platform most likely to be able to identify the statue and bring back similar photos.

The below image of the Fontaine Saint-Michel was searched on all four search engines.

Google was able to identify the fountain and locate many similar images taken of it.
Bing was also able to identify the fountain and locate similar images taken of it.

Yandex was able to locate similar images of the fountain, however, it identified the statues as Warrior Angel, a monument to Czechoslovak prisoners of war.

TinEye was able to find many identical copies of the same photo from different sources in a range of sizes.
Google was able to identify the statue and provide the location of the statues, the Accademia Gallery. Google also found similar images of the same statue.

Bing was unable to identify the statue or locate similar images of the statue.

Yandex was able to identify the statue and was able to locate similar images of the same statue.

Again, TinEye was able to locate multiple copies of the same image of the statue in varying sizes.
Searching for Buildings
When searching with images containing buildings, Yandex and Google are the platforms most likely to be able to identify the building and bring back similar photos, however, Bing is also a strong contender and may occasionally bring back results that Yandex cannot.

The below image of a cathedral in Malaga, Spain, was searched on all four search engines.

Google was able to identify the building and provide very similar photos of the building from the same location, as well as photos from different angles.

Bing was able to identify the building and sites that contain the specific image. Bing also located other images of the same building but did not bring back images from the same location, as Google did.

Yandex was able to locate similar images of the same building and similar looking buildings but mislocated the building as the bell tower of Kazan Cathedral in Nerecht.

TinEye was able to locate the same image from different sources and in different sizes.
Searching for Locations
When searching with images containing locations, such as parks, Yandex and Google are the platforms most likely to be able to identify the location and bring back similar photos.

The below image taken from Lincoln Park, Chicago, was searched on all four search engines.

Google correctly identified the image was taken at Lincoln Park and brought back images taken from a similar location of the same view.

Bing identified web pages containing the same image and brought back images taken at a similar location of the same point of view. One of these images currently identifies the location as Lincoln Park, however, this is likely based on the similarity of the images rather than Bing itself identifying the location.

Yandex also identified images taken at a similar location from the same point of view. Yandex provided an article that misidentified the area as Austin, Texas, however, in the ‘Images appears to contain’ section, the location was correctly identified as “skyline chicago lincoln park”

TinEye successfully located multiple copies of the same image in different sizes from a variety of sources.
Searching for Faces
When searching with images containing faces, Yandex and Bing are the platforms most likely to be able to identify the face and bring back photos containing the same person.

The below stock image of a man was searched on all four search engines.

Google located only different sized versions of the same image. Google assigned the phrase ‘looplight portrait’ to the image, bringing back sites containing loolights.

Bing identified web pages containing the specific image, located different images that contain the same stock photo flipped vertically, and also identified some other images containing another stock image of the same person.

Yandex identified a range of different images that all contain the same photo minus the background, which has been digitally removed and replaced with a plain background.

TinEye successfully located multiple copies of the same stock photo in different sizes from a variety of sources. TinEye also found cropped versions of the same photo in different images.
Searching for Logos
When searching with images containing logos, TinEye is the platform most likely to be able to bring back images containing the same or similar logos. If a logo contains text, then Bing is most likely to be able to recognize the text in the image and use it as a search parameter.

The below logo from Watches of Wales, extracted from the company’s Instagram account, was searched on all four search engines.

Google located a number of images that also contained W’s, however, these were images containing black text on a white background, rather than the white text on a black background found in the source image.

Bing identified a number of images containing white text on a black background, however, these images did not contain any W’s or the word Watch. Bing utilizes OCR and did recognize the phrase Watches of Wales in the source image.

Yandex successfully identified one exact match and a number of images containing white text on a black that contained W’s and appeared visually similar to the source image.

TinEye successfully identified several exact matches for the source image in a range of sizes as well as the same logo with gold lettering. TinEye was the only platform to successfully find multiple copies of the correct logo.
RevEye Reverse Image Search

Reverse Image Searching can be assisted with a Chrome extension, RevEye Reverse Image Search. Installing RevEye within Chrome enables you to right-click on any image within the Chrome browser and open up the Reverse image search dropdown list, from which you can reverse search the chosen image on Google, Bing, Yandex, and TinEye, or you can choose to search all four at once.
FACIAL RECOGNITION
Facial Recognition systems use AI algorithms to detect, identify and analyze faces in images and videos. When conducting an investigation into a person, an Internet Investigator is responsible for collecting all relevant data and information related to that individual from social networks, the surface web, the deep web, and the dark web. The Investigator needs to identify the relevant social media profiles belonging to the subject, which is commonly done based on a name, location, and photo.

Frequently, a subject may use different photos on different social media sites as their profile photo. If the account is locked down or few images are posted, then it may not be possible to identify the same image throughout social media sites. Images posted on some social media sites may also be historical depending upon how frequently they are used and the age of the account.

When identifying social media accounts, it may be necessary for the Investigator to compare the images associated with each social media account to identify if the individual in the images is the same person. When the images are taken decades apart, this process can be difficult.

Fortunately, facial features, including eyes, nose, mouth, and face shape can be used to devise a mathematical formula for a person’s face. In adults, these features do not naturally change, which means that despite age or habits, such as drinking or tiredness, the formula can be used to identify if the same individual is present in different photographs.

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 is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through Microsoft-managed data centers. One of the features of Azure is a face verification tool, which 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.

The Azure Face service provides AI algorithms that detect, recognize, and analyze human faces in images that enable organizations to use the service for identity verification, touchless access control, and face blurring for privacy. The Detect API detects human faces in an image and returns the rectangle coordinates of their locations and a unique ID that represents the stored face data. Face detection can also extract a set of face-related attributes, such as head pose, age, emotion, facial hair, and glasses. The verification determines if the rectangle coordinates of two faces belong to the same person.

The Azure Face service can be utilized during OSINT investigations to determine that images on different social media profiles include the same person or to determine if a social media profile belongs to a missing person based upon an old image.

The Azure Face service can be demoed for free, which enables you to manually upload 2 images at a time to search for facial matches. Utilizing Microsoft Azure’s Cognitive Services Face demo, you can upload two images, which can both either be uploaded from a device or image URL. Upload two images and select submit, which will return a Verification result below the images, scoring the likelihood that the faces belong to the same person between 0 and 1.
Amazon Rekognition - http://aws.amazon.com/rekognition

Amazon Rekognition is a cloud-based software as a service computer vision platform that enables users to conduct image and video analysis using proven, highly scalable, deep learning technology. Amazon Rekognition can identify objects, people, text, scenes, and activities in images and videos, as well as provide facial analysis and facial search capabilities to detect, analyze, and compare faces for a wide variety of user verification, people counting, and public safety use cases.

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. Amazon Rekognition recognizes a face in the image, analyzes the facial attributes of that face, and returns a percentage confidence or probability score for the face and the facial attributes that are detected in the image to determine the likelihood that each image contains the same person. Amazon Rekognition Face makes a prediction of whether the faces match regardless of facial expressions, facial hair, and age.

After signing up for AWS, search for ‘Rekognition’ within the search bar at the top of the page, clicking on ‘Amazon Rekognition’ on the drop-down results.

To analyze a face with Amazon Rekognition, click on Facial Analysis on the left-hand menu. This feature allows you to analyze faces in an image and receive a JSON response.
Click the orange Upload button and select the image that you want to analyze.

Within the Results drop-down on the right-hand side, you can click through and see quick results for each face that was detected in the image.

Click on the Response drop-down to see the JSON results.
To compare faces with Amazon Rekognition, select Face comparison in the panel navigation on the left-hand menu.

Click on the orange Upload button for the comparison face and select the image that you want to analyze.

The results will show whether the reference face was a match for any of the detected faces in the comparison faces image.

Click on the Response drop-down to see the JSON results.
DEEP FAKES
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. Frequently used to create pornography, deepfakes also enable media to be created that depicts 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.

Deepfake images and videos are created by running thousands of images of the faces of two people through an AI encoder. The AI encoder identifies the similarities between the two faces and compresses them to the shared features. A second algorithm, an AI decoder, is then used to recover the faces from the compressed images. Feeding the ‘wrong’ compressed image into the decode, the decoder can replace the original face with the intended face, reconstructing the image or frames within a video with the features, movements, and expressions of the new individual in the place of the originals.

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

The University at Buffalo’s DeepFake-o-meter (http://zinc.cse.buffalo.edu/ubmdfl/deep-o-meter/) is a free tool that enables you to upload a video for analysis to determine if it is a deepfake, using up to 11 different detection methods.

Images generated by artificial intelligence, including generative adversary network (GAN) images, fail to accurately or consistently depict the reflections in the eyes of the subjects of videos, possibly due to the many photos combined to generate the deepfake. The DeepFake-o-meter exploits this shortcoming by spotting tiny deviations in reflected light in the eyes of deepfakes, allegedly with 94% efficiency with portrait-like photos.
To use the DeepFake-o-meter, access the website and upload a video from your device or using a video URL. Select from any of the 11 detection methods, or all of them, and then enter your email address and a 4-6 digit passcode. Hit the submit button and you will receive an email to the entered email address.

Once the video has been processed, which may take several hours, you will receive an email with a hyperlink containing a file to be downloaded to your device. Within this download, you will find graphs for the selected detection methods that score the authenticity of the submitted video.

If the submission is successful, you will be directed to a new web page telling you to wait.
Deepware Scanner - https://scanner.deepware.ai/

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. Click the checkbox to agree to the ToS and Privacy Policy and then hit the submit button.

Using a deepfake of Tom Cruise from TikTok, the Deepware Scanner identified the video as being a deepfake.

Using a real video of Terry Crews from TikTok, the Deepware Scanner identified the video as being genuine.
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. Metadata can be written into a photograph taken digitally, which can be used to identify information like copyright, camera make and model, shutter speed, and keywords. Metadata in digital photos is often created by the device, either a camera or phone, however, it can also be manually input by the photographer or software. Most digital cameras and smartphones write metadata within an image, including model number, shutter speed, and sometimes even the location that the image was taken.

Metadata then can provide a range of information to an investigator, sometimes identifying the coordinates that the photo was taken, or otherwise identifying which device they own or confirming who took the photo. 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).

Accessing the Jeffrey’s Image Metadata Viewer website, you can enter an image URL or select an image file from your device. You will then need to complete a CAPTCHA, which will make the ‘View Image Data’ button active, enabling you to search the uploaded image through the platform.

Jeffrey’s Image Metadata Viewer

![Image](http://exif.regex.info/exif.cgi)

The EXIF data for the uploaded image will be presented below the upload box. A Basic information section will detail the Camera and Lens used, Image Taken Date, and Location if this information is available within the image. Further below you may see further tables provided enhanced information.

---

Photo Me — www.photome.de

Photo Me is a device application alternative to Jeffrey’s Image Metadata Viewer that will display the same EXIF data.
BRAND LOGO IDENTIFICATION
World Intellectual Property Organization

The World Intellectual Property Organization Intellectual Property Portal provides a database for you to search international Intellectual Property by keyword and image. Accessing the website, you can enter search criteria within the SEARCH BY section, entering the brand name within the Text field, or describing the contents of a logo within the Image class field. To support your search, you can select the Image tab in the FILTER BY section and upload a logo, to help filter the results. To use the image filter, select a strategy and image type and click the filter button. The image filter will help you to identify logos matching or similar to the one in the uploaded image.
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.