silo
By Authentic8

What is Exif Data?

When a digital image is captured, metadata specific to that image is stored. This information is called Exchangeable Image File Format data, or Exif data. Some examples of Exif data are date, time, and file size. This information can be extremely useful when conducting image analysis. Analysts can exploit Exif data to find the location of the image, camera make and model, and other information that is valuable to the intelligence production cycle.

Incorporating Exif Data

To find Exif data, an analyst can use a number of different tools. FotoForensics is the service used for the workflow described here. An analyst can take the image of the cargo ship and upload it into FotoForensics to analyze the available Exif data. This image was found in a ship-spotting forum.

User-uploaded images to forums will likely have their Exif data. However, if the analyst tries to pull Exif data from an image on social media, there will likely be little to no data present. Social media platforms have begun to strip Exif data off of user images to protect user privacy.

Once on FotoForensics, the analyst will have two options for image analysis. The analyst can paste an image URL or upload a file for analysis.

For this workflow, the analyst can save the above image of the cargo ship, and then upload the .jpg file into FotoForensics.

When the upload is complete the analyst should select the metadata field (#1). The analyst can then scroll down and begin to review information pertinent to the investigation.
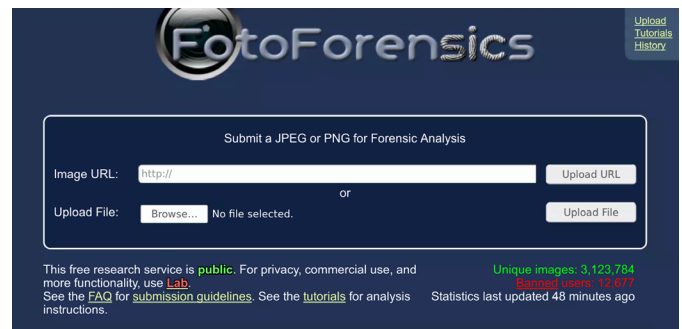
FotoForensics user interface: http://fotoforensics.com

FotoForensics, post image upload with metadata selected.

After reviewing the Exif data collected by FotoForensics, a few pieces of information stand out. In the above images, the analyst can glean what type of device was used to capture this image (#2). This information can be useful when investigating a party of interest that may have a standard issue camera for reconnaissance.

FotoForensics also provides the analyst with an approximate latitude and longitude coordinate (#3). This coordinate can be further incorporated into a targeting packet or a reconnaissance mission.

Overall, the information captured from Exif data can greatly enhance a unit's analytic ability. The exploitation of images, whether of an adversarial object or person or of a location, can help the analyst to further understand their battlespace or objective.

Conclusion

This workflow covers how to extract and incorporate Exif data into the intelligence product. The analyst found a .jpg file of a cargo ship and leveraged FotoForensics to conduct Exif data analysis. Results from the analysis included key identifiers such as equipment used and location data that can then be incorporated further into a finished intelligence product.

For more information please contact osint@authentic8.com.

PROTECT THE THINGS YOU CARE ABOUT FROM THE THINGS YOU CANNOT TRUST

Authentic8 enables anyone, anywhere, on any device to experience the web without risk. The Silo Web Isolation Platform by Authentic8 separates the things you care about like apps, data and devices, from the things you cannot trust like public websites, external users and unmanaged devices. Silo executes all web code in a secure, isolated environment that is managed by policy, to provide protection and oversight.

Today, the world's most at-risk organizations rely on Silo to deliver trust where it otherwise cannot be guaranteed.

CONNECT WITH US

+1 877-659-6535
www.Authentic8.com