JAISHREE S **231901011**

EXP NO: 10

Extract Exchangeable image file format

Aim:

How to Extract Exchangeable image file format (EXIF) Data from Image Files using Exifreader Software.

Introduction:

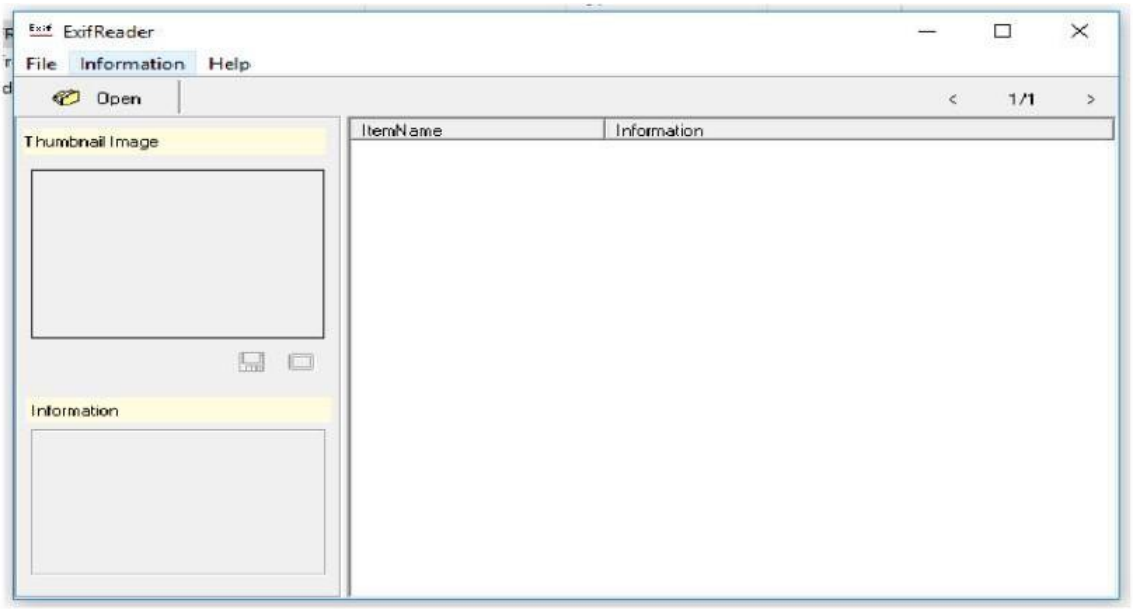
In many cases when a computer, phone, or mobile device is seized for evidence, the system will have graphic images that might be used as evidence. Obviously, in some cases, these graphic images may be evidence such as in child pornography cases. Most digital devices "stamp" information on these graphic images that can tell us a lot about the who, what, when, and where the pictures were taken. This information is known as EXIF data and can very often be useful to the forensic investigator. Exchangeable image file format (EXIF) is a standard set by the digital camera industry to identify formats for digital images and sound files. This information includes camera settings, time, date, shutter speed, exposure, whether a flash was used, compression, the name of the camera, and other information critical to viewing and editing the image in image-editing software. This information can be useful to the forensic investigator.

There are numerous applications that can extract this EXIF data from graphic files. Nearly every one of the major forensic suites (EnCase, FTK, Oxygen, etc.) has this capability built-in. For this lab, we will be using a simple, Windows-based tool called ExifReader (free).

Extract EXIF Data from Image Files

Step-01:

Download the ExifReader from the above link and click on the .exe file (ExifRead.exe) and it will open a clean and simple GUI Wizard as shown below:



Now, simply click on the "Open" button and browse to the pictures from the system or media. Normally, JPEG and JPG contain the maximum information, so let's use a JPEG file

Step-02: Open a Picture File

Once the selected picture opens the picture, it will load the picture into the thumbnail to the left and display the EXIF data to the right down the page as shown below.

There are lots of information you can collect in the EXIF data, but most are related to the technical specifications of the camera and photography. GPS coordinates of where the picture was taken. Most of this is of limited value to the forensic investigator.

Result:

Thus, the forensic tools executed successfully, and the evidence was captured and analyzed accurately.