**Image Validator**

**Scope**

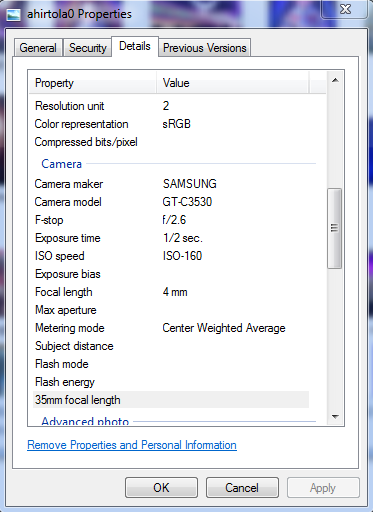
* While uploading image files using the HTML element **<input>**, there is a chance of bypassing the accept attribute by changing the extension manually. The example below:

<input type="file" id="img" name="img" accept="image/jpeg" />

illustrates that the input element should only accept a *jpeg* file but if a *gif* file extension is renamed as *jpeg* file, the element will accept it.

In order to validate a file, **File Signature** (magic number) can be used in order to identify or verify the contents of a file. The Magic number technique uses bytes within a file used to identify the format of the file; generally a short sequence of bytes (most are 2-4 bytes long) placed at the beginning of the file.

* Another problem that occurs for especially image files is the exposure of private info. When a picture is taken, along with the picture, meta data is also stored in the file which can be viewed from "Details".



Now often there are information that might contain sensitive information and should not be exposed. In order to remove them before even processing and storing the file, the EXIF data should be cleared by manipulating the bytes of the file.

**Future Scope**

* The code can be expanded to different file types.
* The different hex codes are hardcoded into the program, this can be extracted from an excel or web service.
* Rotation information is also being removed, need to be skipped when clearing off the EXIF data.