Как вас могут вычислить по фотографии? Удаляем метаданные

Метаданные — это дыра в безопасности по которой вас могут вычислить. Любой снимок сделанный на iPhone/Android содержит данные EXIF – это стандарт добавления к снимку метаданных, включающих в себя самые разные сведения от модели устройства, на которое велась съемка, дата, время и координаты местности, где была сделана та или иная фотография.

Именно поэтому крайне небезопасно выгружать в Сеть снимки, не удалив предварительно метаданные, позволяющие определить места, в которых вы бываете, как часто вы их посещаете, каким именно смартфоном пользуетесь и так далее. Прежде чем говорить о том, как и что можно извлечь из вашей фотографии, давайте подумаем, что такое EXIF-метка.

Стандарт EXIF.

EXIF (англ. Exchangeable Image File Format) — стандарт, с помощью которого описывается какая дополнительная информация (метаданные) могут быть добавлены к изображениям и прочим медиафайлам. Эти данные комментируют этот файл, описывают условия и способы его получения, авторство и т. п.

Данный стандарт получил широкое распространение в связи с появлением цифровых фотокамер. Информация, записанная в этом формате, может использоваться как пользователем, так и различными устройствами, например, принтером. Стандарт EXIF является чрезвычайно гибким (например, позволяет сохранить полученные с приёмника GPS координаты места съёмки) и допускает широкое развитие — как правило, фотоаппараты добавляют к файлу информацию, специфичную только для данной конкретной камеры. Правильно интерпретировать такую информацию могут только программы от изготовителя фотоаппарата.

Разработчик формата — Japan Electronics and Information Technology Industries Association (JEITA).

Версия Exif 2.2 (известная также как Exif Print) введена в 2002 году. Наиболее существенные дополнения касаются данных, описывающих условия съемки, нужных для корректной печати таких изображений. Эти данные могут потребоваться, например, при печати ночных снимков, для которых обилие темноты не является ошибкой фотографа, автоматика принтера может пытаться «спасти» такие снимки, но не должна этого делать. Последняя версия — 2.31.

Использование в цифровой фотографии

Большинство современных цифровых фотокамер записывает параметры съёмки в файлы изображений. Также при обработке изображений в EXIF может записываться дополнительная информация.

В качестве примера информации, записываемой в EXIF, можно указать следующее:

- производитель камеры,
- модель,
- информация о правообладании
- выдержка
- диафрагма
- светочувствительность в ед. ISO
- использование вспышки
- разрешение кадра

- фокусное расстояние
- размер матрицы
- эквивалентное фокусное расстояние
- дата и время съёмки
- ориентация камеры (вертикально/горизонтально) для камер со встроенным акселерометром
- тип баланса белого
- географические координаты и адрес места съёмки

Прочитать/обработать эти параметры можно в программах просмотра изображений (фотоорганайзерах), графических программах и специальных программах для работы с метаданными.

Поиск метаданных в файлах фотографий — одно из звеньев доксинга (англ. «doxing», от «docs»), ставшей уже весьма популярной практики сбора сведений об интересующем человеке в интернет-источниках в тех или иных целях.

Давайте подумаем, чем это может вам угрожать?

1. Вы отправляете фотографии по электронной почте или загружаете в облачное хранилище вроде Google Drive или Dropbox. В этом случае файл остается в неизменном виде, и пользователи, с которыми вы этими файлами поделитесь, при желании увидят все метаданные.
2. Вы загружаете фотографии в соцсети и фотохостинги. В этом случае вероятно выполнение условий, создающих угрозу приватности: а) вы вообще не знаете про метаданные файлов; б) вы тем более не знаете, что ваш сервис их не удаляет.
3. Вы фотографируете старинную вазу или слегка подержанный велосипед и выставляете объявление о продаже на сайте онлайн-барахолки. Дальше все как в пункте 2. В одном из интернет-обсуждений метаданных EXIF упомянута история в духе «у меня от этого друг умер». То есть друг, конечно, жив, но, если верить рассказчику, хороший велосипед у друга все же украли — вскоре после размещения в Интернете объявления о его продаже.

Программы, поддерживающие EXIF

В настоящее время EXIF повсеместно, в большей или меньшей степени, поддерживается программами просмотра изображений и даже штатными средствами операционных систем. Степень поддержки может быть разная, возможно искажение или даже полное удаление данных EXIF из-за неполной поддержки формата. ExifTool и ShowExif обладают наиболее полной поддержкой.

Вот что показала говорят специалисты Kaspersky Lab:

- Facebook, Twitter, «ВКонтакте» — метаданные из фотографий **удаляют**;
- Google+ — **не удаляет**;
- Instagram — **удаляет**;
- Flickr, Google Photo, Tumblr — **не удаляют**;
- eBay, Craigslist — **удаляют**;
- ЦИАН — **не удаляет**.

Кстати, с помощью геометок на ЦИАН можно вычислять нечестных риелторов, размещающих в объявлении фотографии других квартир (конечно, если они не удалили EXIF самостоятельно)

Сервисы из тех, что не удаляют метаданные, имеют, как правило, настройку конфиденциальности, позволяющую отключить их отображение. Но именно отображение: сервис все равно может эти данные сохранить отдельно. И эта тема заслуживает отдельного обсуждения.

Например, именно так поступает Facebook. Убедиться в этом весьма просто — достаточно воспользоваться штатной функцией загрузки копии своих данных. Пройдя несложную процедуру, вы получаете архив, содержащий помимо прочего загруженные в соцсеть фотографии вместе с аннотацией в виде HTML-файла. В эту аннотацию входят и координаты места съемки, и IP-адрес, с которого фотографии отправлялись.

Список хранимых Facebook пользовательских данных есть в справочной системе соцсети.

Взглянуть на взаимодействие правоохранительных органов и соцсети с непривычной стороны позволяет появившаяся в Сети инструкция, в которой описывается процедура запроса у Facebook данных пользователей. В качестве автора документа, опубликованного на сайте netzpolitik.org, указан сотрудник Департамента шерифа Сакраменто. Это уже вторая версия руководства: обновление потребовалось из-за модификации механизма архивирования пользовательских данных, произведенной Facebook, отмечается в самом документе.

Подробности взаимодействия госорганов и онлайн-сервисов в части персональных данных выходят за рамки этой заметки. Наше же дело — просто предупредить вас о том, что соцсети сохраняют значительно больше данных о фотографиях, чем может показаться, — и в определенных обстоятельствах могут ими поделиться с другими людьми.

Кстати, в метаданных хранится не только текстовая информация, но и миниатюра той картинки, в которой они содержатся. И иногда проблемы могут возникать с ними.

В 2003 году американская телеведущая Кэтрин Шварц (Catherine Schwartz) разместила в блоге свои безобидные, казалось бы, фотографии. Однако в метаданных этих файлов хранились миниатюры оригинальных снимков, показывающие полное изображение до процедуры кадрирования. И да, на двух из них Шварц предстала в обнаженном виде.

Но ведь с тех пор прошло больше десяти лет, разработчики наверняка уже совладали с очевидной угрозой приватности, так ведь? Что ж, невредно будет проверить — просто на всякий случай.

По данным Kaspersky Lab, испытав Adobe Photoshop Express, GIMP, Windows Paint, Microsoft Office Picture Manager, IrfanView и XnView, специалисты удостоверились: при редактировании изображения миниатюра обновляется.

Еще одним подопытным стал редактор Corel PHOTO-PAINT версии X8. Внезапно выяснилось: при сохранении JPG-файла миниатюра не обновляется, показывая хоть и в уменьшенном виде, но исходное изображение!

Безусловно, вся совокупность этих данных может использоваться для идентификации человека, проводившего съемку. Но наиболее интересны, безусловно, геокоординаты.

Если вы используете Windows 10, то вы можете очень просто увидеть метаданные вашей фотографии.

Рисунок 1 Пример фотографии

Для этого нажмите правой клавишей мыши на файле и выберите **Свойства.** В появившемся окне выберите вкладку **Подробно** (Рис 2).

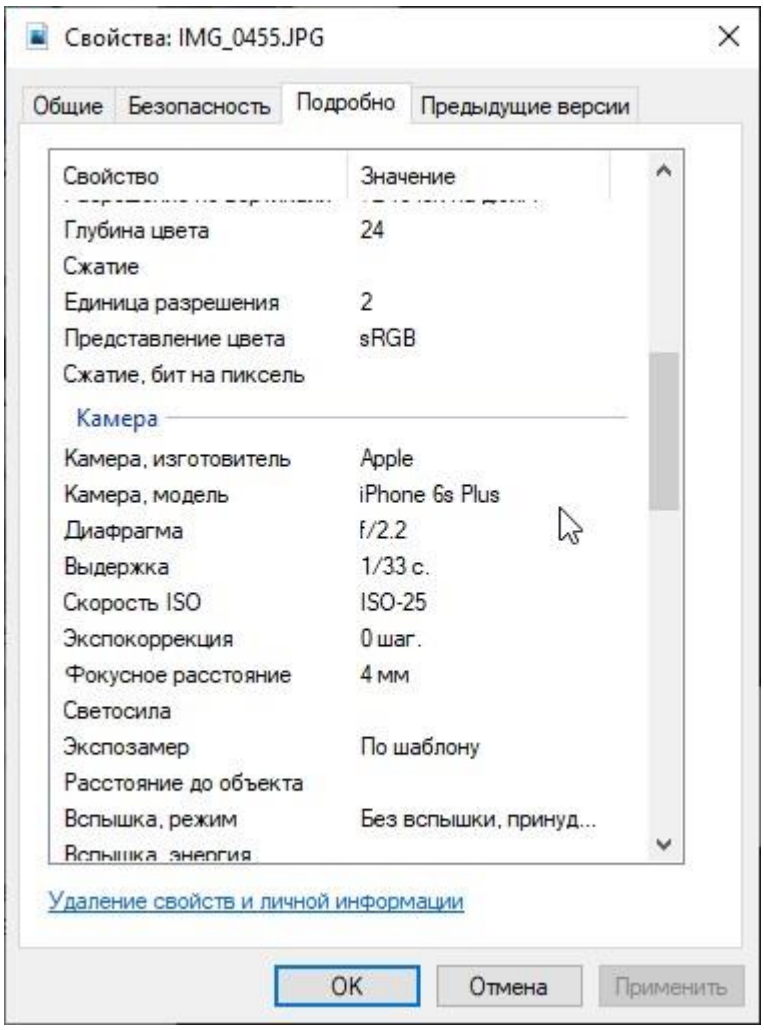

Рисунок 2 Свойства Подробно

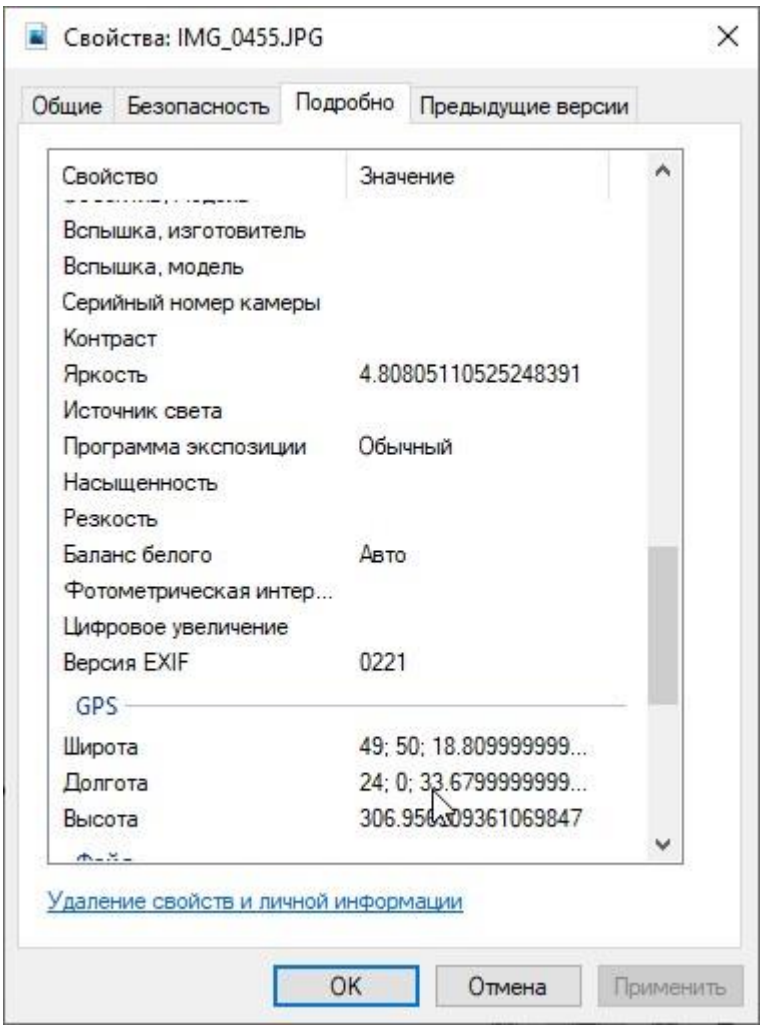

Рисунок 3 Свойства Геокоординаты

Используя Google Maps ,вы сможете установить что это (рис.4).

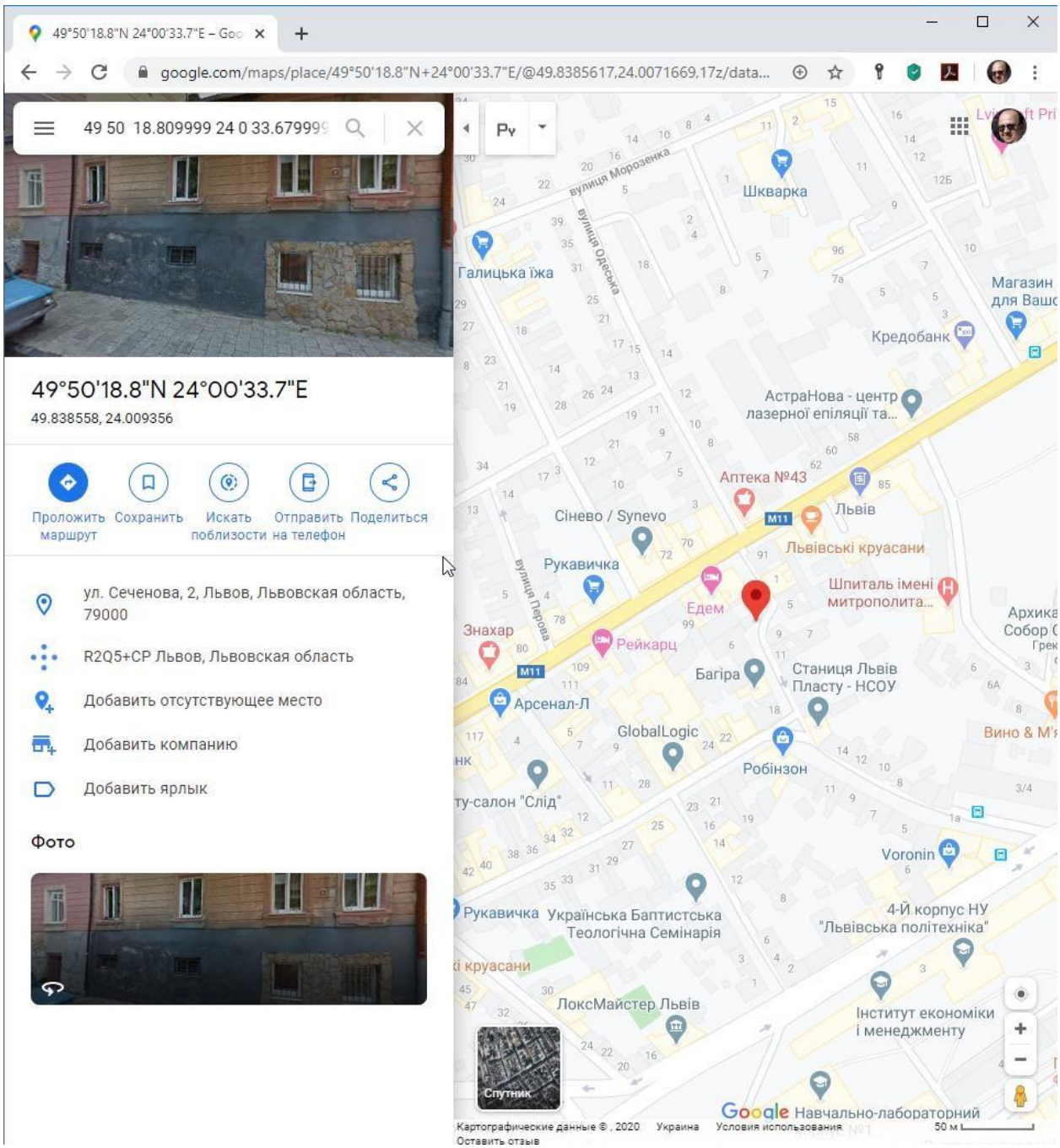

Рисунок 4 То же место на картах Google

Таким образом вы сможете понять не только когда сделано фото, но и увидеть, какой именно это город, улица и даже номер дома.

Существуют сайты, на которых вы можете загрузить изображение и увидеть развернутые метаданные, например:

- http://exif.regex.info/exif.cgi
- http://metapicz.com/

С их помощью можно найти информацию обо всех параметрах съёмки, вплоть до того, на какую дистанцию был сфокусирован объектив.

Существует расширение для браузера Google Chrome, позволяющее просмотреть EXIF любой картинки на открытой вами веб-странице.

Через EXIF вы можете узнать, сколько снимков было сделано на камеру. К примеру, это полезно при покупке б/у фототехники. Приём работает с камерами Nikon. Камеры других производителей не всегда прописывают в EXIF этот параметр, и его приходится извлекать, прибегая к дополнительным ухищрениям.

Чтобы получить полные данные EXIF, лучше не редактировать кадр на ПК. Загрузим выбранный снимок на сайт http://exif.regex.info/exif.cgi и найдём графу Shutter Count. Здесь мы увидим «пробег» фотоаппарата.

По тому же принципу работает и более простой в использовании сервис https://www.camerashuttercount.com/.

Вместе с тем нужно учесть, что данные EXIF можно подделать. Ведь EXIF легко поддаётся редактированию. Существуют даже онлайн-сервисы для изменения съёмочных параметров. Поэтому данные EXIF могут выступать справочной, но не абсолютно объективной информацией.

Если же вы хотите удалить эти данные, то проще всего в Windows воспользоваться следующей ссылкой (Рис.5).

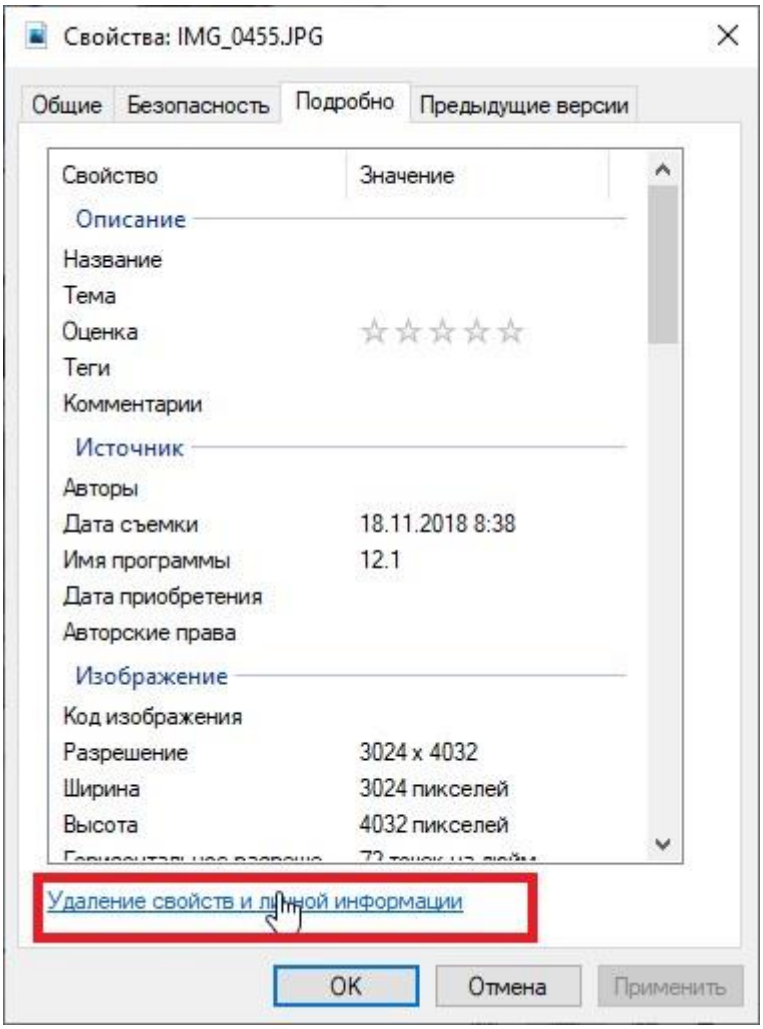

Рисунок 5 Удаление свойств и личной информации

Безусловно, приложения для удаления/изменения метаданных существуют и для Android.

https://play.google.com/store/apps/details?id=apps.syrupy.metadatacleaner&hl=ru

И для IPhone (https://apps.apple.com/us/app/metapho/id914457352)

Рекомендации

Чтобы не «засветить» вместе с фотографиями что-то лишнее, не предназначенное для чужих глаз, предлагаем подборку самоочевидных, в общем-то, советов.

- Отключайте сохранение местоположения на устройстве (только для камеры или для всех приложений сразу).
- Удаляйте метаданные из файлов перед публикацией в Сети. Например, это умеет делать бесплатный для личного некоммерческого использования XnView. А вот встроенный в Windows механизм «Удаление свойств и личной информации» (вызывается в окне свойств файла на вкладке «Подробно») на поверку оставляет и миниатюру, и блоки EXIF.
- Удалять метаданные фотографий перед отправкой в Сеть можно и прямо на мобильном устройстве. Вот, например, приложения для iOS, Android и Windows Phone.
- В настройках приватности сетевых сервисов запретите им сохранять метаданные фотографий.

Полезный совет для тех, кому действительно есть что терять: вовсе не отправляйте в Сеть фотографии и данные, которые могут пригодиться вашим недоброжелателям. То есть не публикуйте вообще ничего такого, что в определенных обстоятельствах может быть использовано против вас.