Секция «Криминалистика»

Метаданные изображения как объект компьютерной экспертизы

Научный руководитель – Жидков Дмитрий Николаевич

Вайберт Наталия Антоновна

Студент (специалист)

Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, Санкт-Петербург, Россия

E-mail: tasha.vaybert@mail.ru

В современном обществе с высокой скоростью развиваются новые информационные технологии, нередко именно они становятся предметом преступления. В связи с этим в России и по всему миру начали своё развитие компьютерные экспертизы. На сегодняшний день именно они являются одними из самых перспективных и развивающихся экспертиз, помимо этого, обладают огромным объёмом объектов для исследования, который увеличивается с появлением новых технологий.

В настоящей работе мы будем изучать информационно-компьютерную экспертизу графических файлов. В ходе экспертизы исследованию подвергаются файлы с расширениями графических форматов (.bmp, .jpg, .tif, .cdr и другие). Целью такой экспертизы является поиск, обнаружение и анализ информации, подготовленной пользователем или созданной программой. Суть информационно-компьютерной экспертизы представляет собой извлечение и анализ ряда специфических атрибутов, благодаря которым система распознает данный пакет информации и размещает его в хранилище данных, а также данные о пользователе, сгенерировавшем файл, о размере, типе, времени создания файла, помимо этого, можно получить информацию о последнем обращении к данному файлу, о дате последних внесенных изменений.

Приведем в пример несколько программ, используемых для анализа метаданных графических файлов, которые могут применяться в рамках компьютерной экспертизы:

- Exiftool-10.12;
- Opanda IExif;
- ShowExif.

Основным современным программным обеспечением для проведения компьютерной экспертизы графических файлов являются:

- «Мобильный криминалист Эксперт»;
- «Мобильный криминалист Десктоп»;
- Belkasoft Evidence Center 2020.;
- Porn Detection Stick.

При проведении исследований метаданных изображений мы можем получить много криминалистически важной информации, например, геолокация, дата и время, технические характеристики и модель устройства, на которое было сделано фотоизображение. Эти сведения могут являться источниками информации о самом противоправном деянии или лицом, его совершившем.

Так, для получения и проведения в дальнейшем анализа, полученной информации перед экспертом ставятся следующие основные вопросы, касающиеся обстоятельств создания и использования файлов, являются:

1. Когда был создан исследуемый файл?
2. Кто именно из пользователей, имевших доступ к компьютерной системе, является создателем исследуемого файла?

3. Какого числа и во сколько (относительно времени компьютерной системы) были внесены изменения в файл?
4. Какие пользователи имели полномочия на внесение изменений в исследуемый файл?
5. Возможен ли доступ по сети к исследуемому файлу?
6. Какое количество пользователей получают сетевой доступ к исследуемому файлу?
7. Сколько раз производились обращения к данному файлу?
8. Когда был удален исследуемый файл (для восстановленных файлов)?
9. Какой пользователь удалил данный файл?
10. Когда, в какое время и с какого компьютера был осуществлен несанкционированный доступ к файлам?
11. Был ли исследуемый файл распространен посредством сетевых технологий?
12. Кто являлся распространителем данного файла?
13. Какое количество конечных пользователей получили исследуемый файл?
14. Производилось ли копирование файла или его части?
15. Был ли исследуемый файл создан на представленном для анализа компьютере или скопирован в него с внешнего носителя?
16. Был ли исследуемый файл разослан по локальной сети? С какого именно компьютера это было осуществлено?[1]

В настоящее время мы можем проследить, на сколько актуальна компьютерная экспертиза графических файлов. Многие пользователи не задумываются о том, что скрыто за простой фотографией, но в то же время именно она может раскрыть много информации о самом пользователе, его устройстве, а также о том, изменял ли пользователь файл, на каком устройстве и когда.

Источники и литература

1) Экспертиза обстоятельств создания и использования файлов и баз данных URL: https://sudexpa.ru/expertises/ekspertiza-obstoiatelstv-sozdaniia-i-ispolzovaniia-failov-i-baz-dannykh/ (дата обращения 01.03.2021).