УДК 343.983 DOI: 10.18698/2541-8009-2019-07-501

НЕКОТОРЫЕ ОСОБЕННОСТИ ИССЛЕДОВАНИЯ ГРАФИЧЕСКИХ ФАЙЛОВ В ШЕСТНАДЦАТЕРИЧНОМ ФОРМАТЕ

А.В. Карлова carlova.anastasia@yandex.ru
SPIN-код: 8696-6670

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация

Статья посвящена созданию нового способа выявления координат места съемки цифровых изображений с мобильных устройств с помощью шестнадцатеричного редактора WinHex. При открытии графического файла в шестнадцатеричном виде можно исследовать его структуру. В ходе исследования был выявлен шаблон, в котором закодированы координаты места съемки фотоизображения. После проведения ряда вычислений можно получить координаты долготы и широты, которые позволяют идентифицировать точное место съемки того или иного изображения. Разработаны и сформулированы методические рекомендации для выявления геоданных посредством исследования графических файлов вручную с помощью шестнадцатеричного редактора.

Ключевые слова

Судебная экспертиза, мобильное устройство, задачи геопозиционирования, геоданные, геолокация, фотоизображения, шестнадцатеричный редактор, методические рекомендации

Поступила в редакцию 18.06.2019

Актуальность статьи обусловлена тем, что исследование данных с мобильных устройств для решения задач геопозиционирования всегда рассматривалось в совокупности с исследованием и других данных с устройств. Однако очень часто необходимо выявить, находилось ли устройство в определенном месте, поскольку исходя из ответа на этот вопрос будет строиться доказательственная база. По совокупности всех имеющихся доказательств можно говорить о том, находилось ли само лицо — обладатель устройства в тот или иной момент времени в конкретном месте.

Графические файлы являются одним из источников данных геопозиционирования [1].

Геотегированное изображение — это изображение, которое содержит метаданные географической идентификации. Эти данные состоят из координат широты и долготы (иногда также высоты). Хотя существует несколько специальных инструментов для извлечения информации о геоданных из изображений, но знание того, как инструмент действительно работает и где на уровне кодировки изображения хранятся такие данные, также необходимо [2].

Самый простой и быстрый способ проверить географическое положение изображения в операционной системе Windows — щелкнуть правой кнопкой мыши на изображение и выбрать из выпадающего меню пункт «Свойства». Необходимая информация находится на вкладке «Сведения». Можно также ис-

пользовать инструмент для извлечения геоданных и других метаданных, например, бесплатный инструмент Exiftool. Но есть случаи, когда требуется ручной анализ изображения, который мы далее и рассмотрим [3].

На всех устройствах, которые использовались в этом эксперименте, был обнаружен стандарт ведения журнала метаданных EXIF (Exchangeable Image File Format) [3].

Поскольку длина и содержание метаданных (например, марка и модель камеры, программное обеспечение, автор, время и т. п.) варьируются от устройства к устройству, неудивительно выявлять различные начальные смещения данных геотега. Другими словами, нам не удалось найти согласованность в смещении местоположения геотега на изображении [4]. Однако мы получили образец (шаблон), необходимый для вычисления координат. Были созданы и сформулированы рекомендации для выявления геоданных посредством исследования графических файлов вручную с помощью шестнадцатеричного редактора, которые рассмотрены далее.

В проведенном анализе использован следующий подход:

1) находим две буквы направления, т. е. N, S, E или W;

2) практическим путем устанавливаем образец (шаблон): 00 00 xxxx **00 00 00 01** 00 00 xxxx **00 00 00 01** 00 0000 xxxx **00 00 64** (поскольку предопределенного местоположения смещения не обнаружено). Для этого используем шестнадцатеричный редактор WinHex, а также стандартное приложение для операционной системы Windows — «Калькулятор».

Для начала откроем исследуемые изображения в программе WinHex (рис. 1).

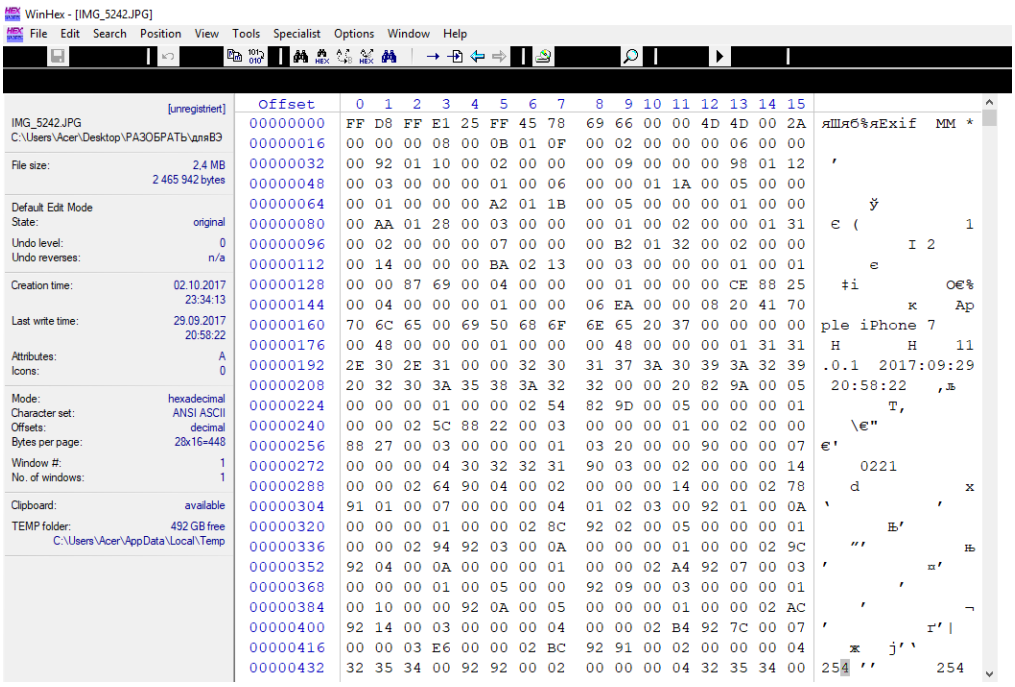

Рис. 1. Файл IMG_5242.JPG. Окно программы WinHex

Данные о местоположении съемки обычно присутствуют рядом с отметкой даты/времени.

Находим шаблон 00 00 00 01 00 00 xxxx 00 00 00 01… 00 00 00 64. Как только шаблон будет идентифицирован, найдем 4 байта перед первым набором 00 00 00 01 (выделено синим цветом на рис. 2), т. е. здесь смещение байта составляет 1968.

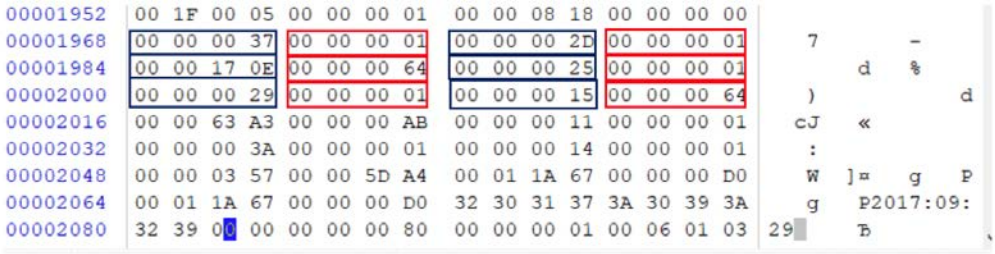

Рис. 2. Фрагмент файла IMG_5242.JPG, содержащий геометку в шестнадцатеричном виде. Окно программы WinHex

Далее необходимо провести расчеты, а именно преобразовать шестнадцатеричную систему счисления в десятичную (hex в dec).

Начнем преобразовывать со смещения 1968 с помощью стандартного приложения «Калькулятор» (табл. 1).

Таблица 1

Преобразование шестнадцатеричной системы счисления в десятичную (hex в dec) с помощью программы «Калькулятор»

hex	dec	Окно программы «Калькулятор»
Широта		
00 00 00 37	55	HEX 37 DEC 55
00 00 00 01	1	HEX 1 DEC 1
00 00 00 2D	45	HEX 2D DEC 45
00 00 17 0E	5902	HEX 170E DEC 5 902
00 00 00 64	100	HEX 64 DEC 100
Долгота		
00 00 00 25	37	HEX 25 DEC 37
00 00 00 29	41	HEX 29 DEC 41
00 00 00 15	21	HEX 15 DEC 21

Полученные значения необходимо поделить: 00 00 00 37 = 55 делим на следующие 4 байта 00 00 00 01 = 1, получаем 55/1 = 55. Таким образом выполняем вычисления со следующими парами по 4 байта:

- 45/1 = 45;
- 5902/100 = 59.02.

Это завершает вычисление широты, значение которой по результатам проведенных вычислений получилось равным 55:45:59.02.

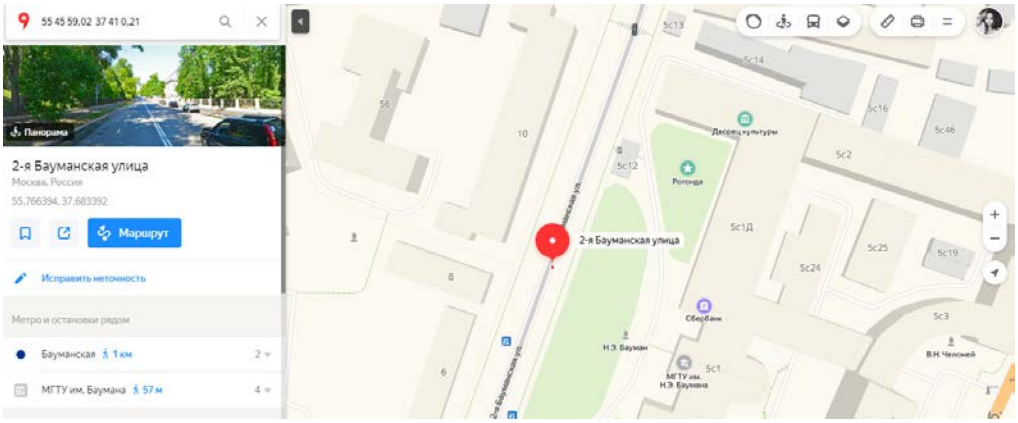

Рис. 3. Визуализация координат, извлеченных из файла IMG_5242.JPG, с помощью онлайн-сервера «Яндекс.Карты»

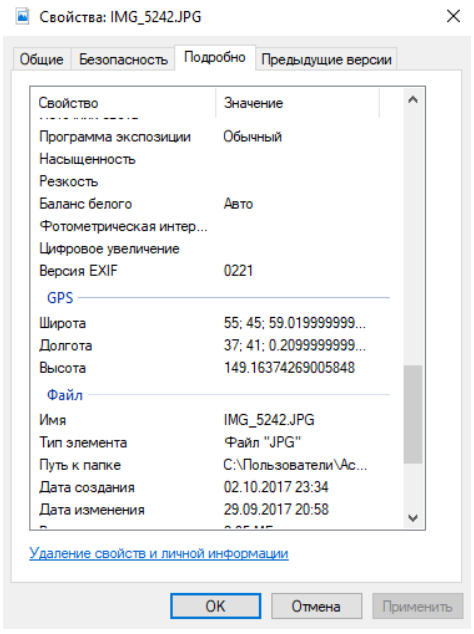

Рис. 4. Свойства файла IMG_5242.JPG

Продолжим вычислять значение долготы:

- 37/1 = 37;
- 41/1 = 1;
- 21/100 = 0.21.

Таким образом, долгота составляет 37:41:0.21.

Исходя из полученных вычислений выявлены координаты съемки исследуемого изображения: 55:45:59.02; 37:41:0.21.

Используем онлайн-ресурс «Яндекс.Карты», чтобы визуализировать полученные координаты (рис. 3).

Сравниваем полученные результаты с координатами, указанными в пункте «Свойства» исследуемого файла (рис. 4), и значения, полученные с помощью программы ExifTool, и видим, что они идентичны.

Проведем аналогичные исследования для файла IMG_5209.JPG. Находим необходимый шаблон, выбираем 4 байта перед первым набором 00 00 00 01 (выделено синим цветом на рис. 5), здесь уже информация о геоданных начинается со смещения 1936.

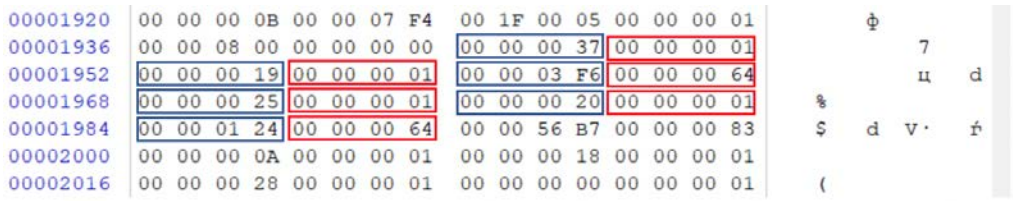

Рис. 5. Фрагмент файла IMG_5209.JPG, содержащий геометку в шестнадцатеричном виде. Окно программы WinHe

Также преобразовываем значения со смещения 1936 с помощью стандартного приложения «Калькулятор» (табл. 2).

Таблица 2

Преобразование шестнадцатеричной системы счисления в десятичную (hex в dec) с помощью программы «Калькулятор»

hex	dec
Широта	
00 00 00 37	55
00 00 00 19	25
00 00 03 F6	1014
Долгота	
00 00 00 25	37
00 00 00 20	32
00 00 01 24	292

Проводим аналогичные вычисления для определения широты и долготы:

- 55/1 = 55;
- 25/1 = 25;
- 1014/100 = 10.14;
- 37/1 = 37;
- 32/1 = 32;
- 292/100 = 2.92.

На основе полученных вычислений мы выявили координаты съемки исследуемого изображения: 55:25:10.14; 37:32:2.92.

Используем онлайн-ресурс «Яндекс.Карты», чтобы визуализировать полученные координаты (рис. 6).

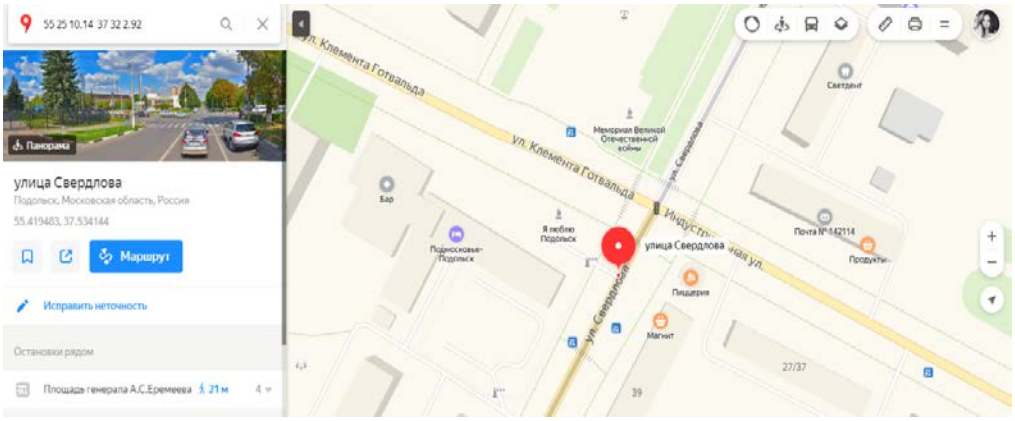

Рис. 6. Визуализация координат, извлеченных из файла IMG_5209.JPG, с помощью онлайн-сервера «Яндекс.Карты»

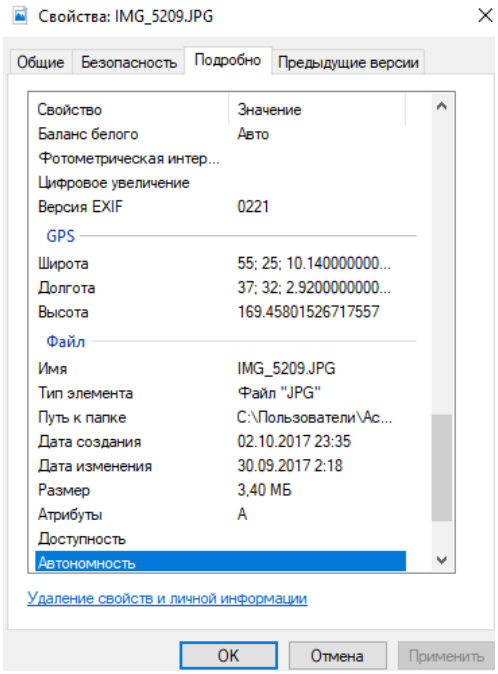

Рис. 7. Свойства файла IMG_5209.JPG

Сравниваем полученные результаты с координатами, указанными в пункте «Свойства» исследуемого файла (рис. 7), и значения, полученные с помощью программы ExifTool, и видим, что они идентичны.

Проведем аналогичные исследования для файла IMG_5246.JPG. Находим необходимый шаблон, выбираем 4 байта перед первым набором 00 00 00 01 (выделено синим цветом на рис. 8), здесь информация о геоданных начинается со смещения 1952.

Также преобразовываем значения со смещения 1952 с помощью стандартного приложения «Калькулятор» (табл. 3).

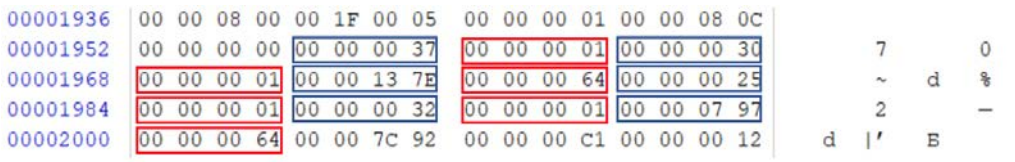

Рис. 8. Фрагмент файла IMG_5246.JPG, содержащий геометку в шестнадцатеричном виде. Окно программы WinHex

Таблица 3

Преобразование шестнадцатеричной системы счисления в десятичную (hex в dec) с помощью программы «Калькулятор»

hex	dec
Широта	
00 00 00 37	55
00 00 00 30	48
00 00 13 7E	4990
Долгота	
00 00 00 25	37
00 00 00 32	50
00 00 07 97	1943

Проводим аналогичные вычисления для определения широты и долготы:

- 55/1 = 55;
- 48/1 = 48;
- 4990/100 = 49.9;
- 37/1 = 37;
- 50/1 = 50;
- 1943/100 = 19.43.

Исходя из полученных вычислений мы выявили координаты съемки исследуемого изображения: 55:48:49.9; 37:50:19.43.

Используем онлайн-ресурс «Яндекс.Карты», чтобы визуализировать полученные координаты (рис. 9).

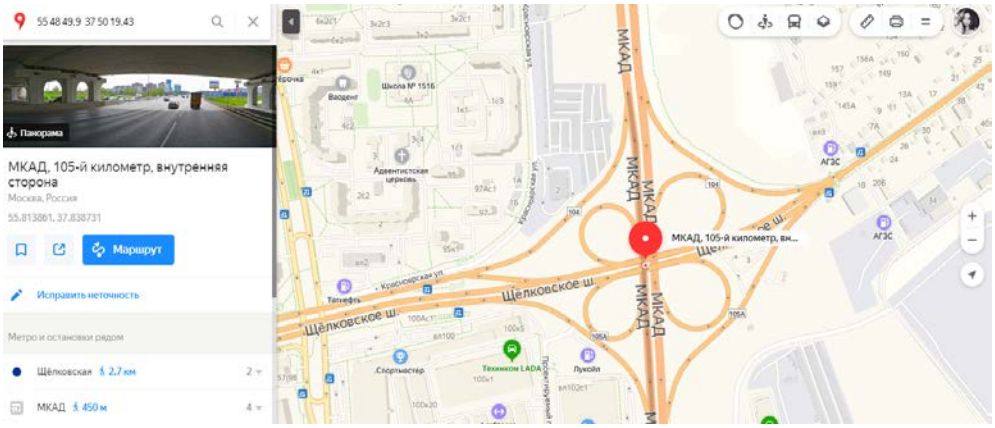

Рис. 9. Визуализация координат, извлеченных из файла IMG_5246.JPG, с помощью онлайн-сервера «Яндекс.Карты»

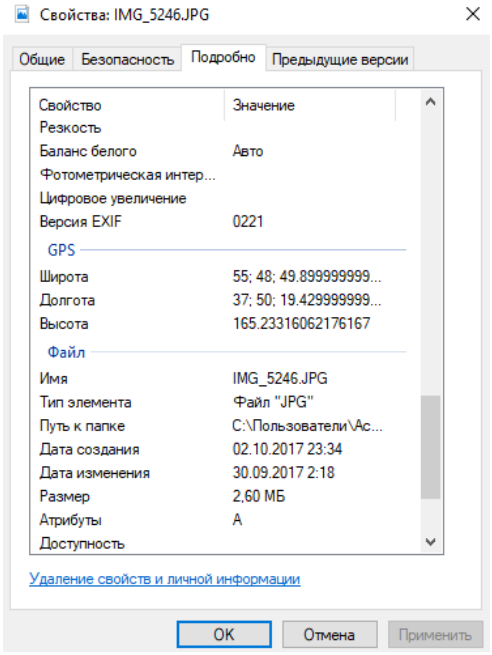

Рис. 10. Свойства файла IMG_5246.JPG

Сравниваем полученные результаты с координатами, указанными в пункте «Свойства» исследуемого файла (рис. 10), и значения, полученные с помощью программы ExifTool, и видим, что они идентичны.

Рассмотрим вариант определения местоположения в случае, когда координаты были удалены. Удаляем информацию о координатах съемки в пункте «Свойства» файла IMG_5209.JPG (рис. 11).

При исследовании данного изображения с помощью ExifTool координаты не были выявлены (рис. 12).

Однако при использовании программы WinHex обнаружено, что информация в шестнадцатеричном виде сохранилась без изменений (рис. 13).

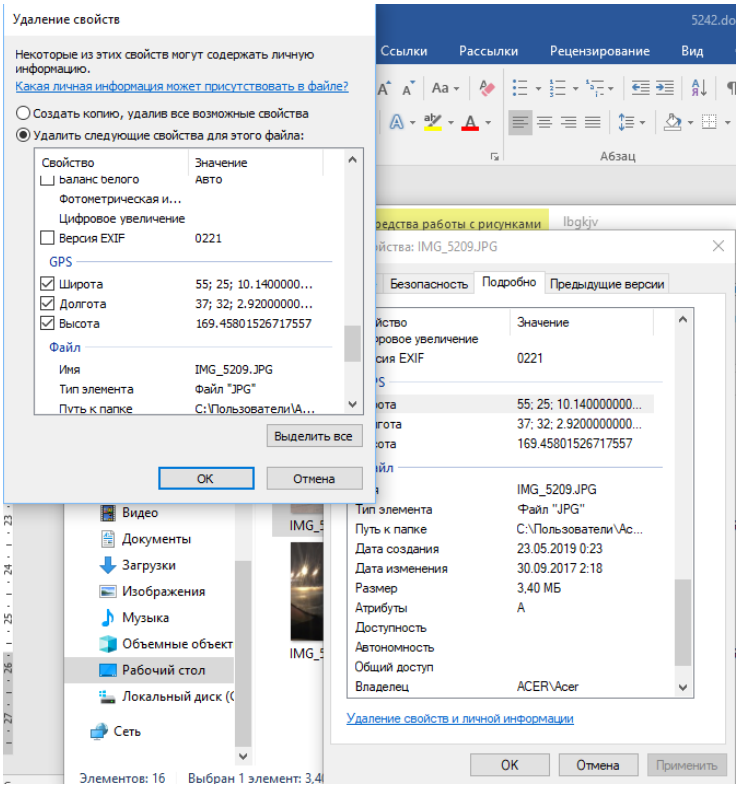

Рис. 11. Удаление GPS-координат файла IMG_5209.JPG

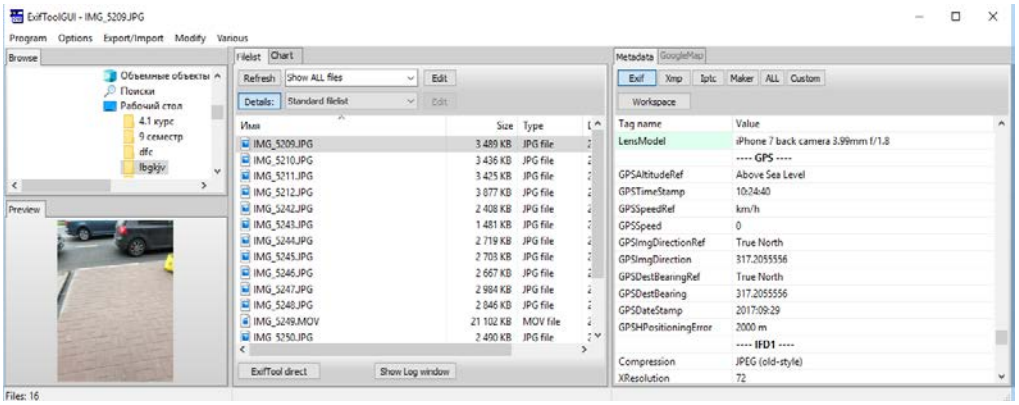

Рис. 12. Метаданные файла IMG_5209.JPG после удаления GPS-координат. Окно программы ExifToolGUI

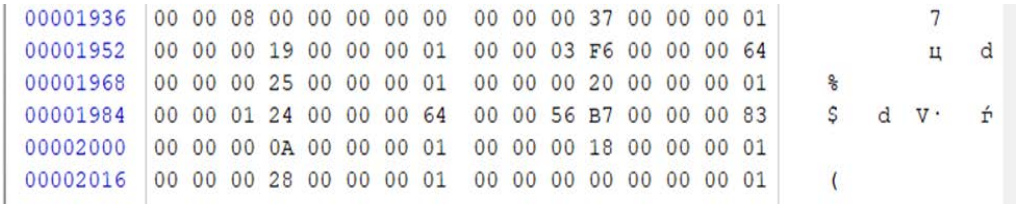

Рис. 13. Фрагмент файла IMG_5209.JPG, содержащий геометку в шестнадцатеричном виде после удаления GPS-координат во вкладке «Свойства» файла. Окно программы WinHex

Ранее были рассмотрены фотоизображения, полученные с мобильного устройства под управлением операционной системы iOS. Далее рассмотрим фотоизображения, полученные с мобильного устройства с операционной системой Android [5]. Исследуем для начала метаданные файла 20190525_135947.JPG в программе ExifToolGUI (рис. 14) и в пункте «Свойства» (рис. 15).

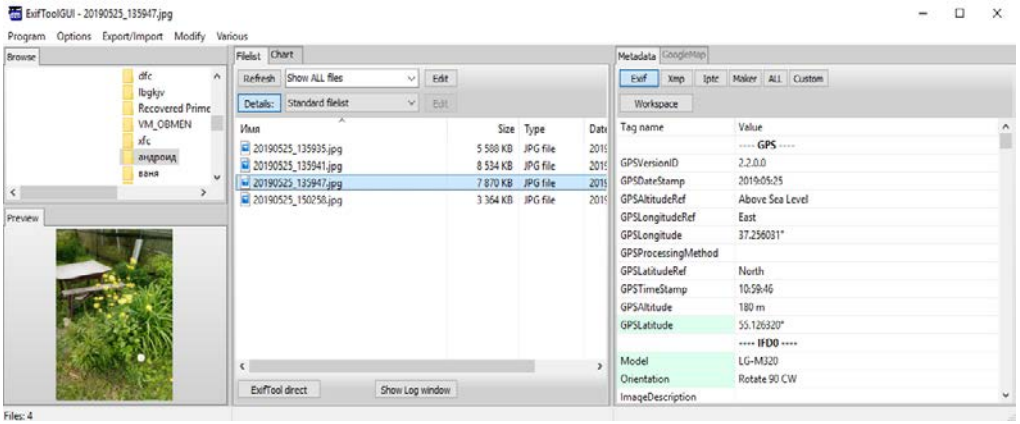

Рис. 14. Метаданные файла 20190525_135947.JPG. Окно программы ExifToolGUI

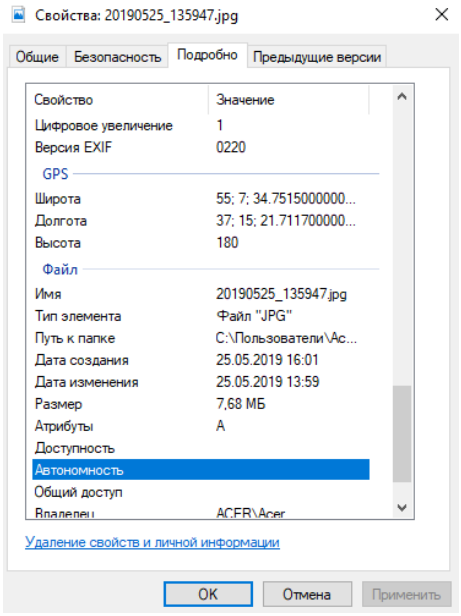

Рис. 15. Свойства файла 20190525_135947.JPG

Для начала откроем исследуемое изображение в программе WinHex. Данные о местоположении съемки обычно присутствует рядом с отметкой даты/времени [6].

Находим шаблон 00 00 00 01 00 00 xxxx 00 00 00 01… 00 00 00 64, который мы выявили в предыдущем исследовании. Однако в данном случае байты расположены в обратном порядке, что является своеобразной особенность для операционной системы Android. Как только шаблон будет идентифицирован, найдем 4 байта со смещения 983 (долгота) и со смещения 1098 (широта).

Также преобразовываем значения с помощью стандартного приложения «Калькулятор» (табл. 4).

Рис. 16. Фрагмент файла 20190525_135947.JPG, содержащий геометку в шестнадцатеричном виде. Окно программы WinHex

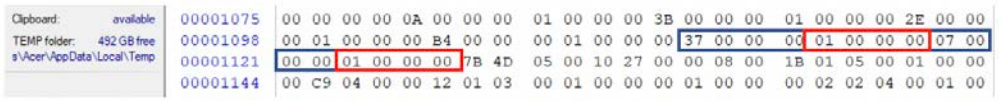

Рис. 17. Фрагмент файла 20190525_135947.JPG, содержащий геометку в шестнадцатеричном виде. Окно программы WinHex

Таблица 4

Преобразование шестнадцатеричной системы счисления в десятичную (hex в dec) с помощью программы «Калькулятор»

hex	dec
Широта	
00 00 00 37	55
00 00 00 07	7
Долгота	
00 00 00 25	37
00 00 00 0F	15

Полученные значения необходимо поделить: так, 00 00 00 37 = 55 мы делим на следующие 4 байта 00 00 00 01=1, получаем 55/1 = 55. Таким образом проводим вычисления со следующими парами по 4 байта:

- 7/1=7.

Это завершает вычисление широты, которое в итоге проведенных вычислений получилось равным 55:7.

Продолжим вычислять значение для долготы:

- 37/1 = 37;
- 15/1 = 15.

Получилось, что долгота составляет 37:15.

Исходя из полученных вычислений мы выявили координаты съемки исследуемого изображения: 55:7; 37:15. Это совпадает с координатами, полученными с помощью приложения ExifToolGUI.

Исходя из всего проведенного исследования в отношении цифровых изображений, можно сделать вывод, что на данный момент существует много (в том числе и бесплатных) инструментов для исследования блока EXIF в графических файлах, однако эксперту также необходимо знать, каким образом вручную можно выявить координаты местоположения съемки изображения [7]. Исходя из закономерностей ручного исследования можно также сделать предположение об операционной системе мобильного устройства, с помощью которого было сделано фотоизображение.

По результатам проведенной работы был разработан новый способ определения координат места съемки изображения, а также методические рекомендации по его использованию с помощью шестнадцатеричного редактора WinHex и стандартного приложения «Калькулятор». Этот способ пригодится экспертам в области судебной компьютерно-технической экспертизе для исследования и поврежденных графических файлов, которые не представляется возможным исследовать обычными программами для исследования блока EXIF.

Литература

[1] Карлова А.В. Криминалистическое исследование следов установки предположительно контрафактных программных продуктов. *Политехнический молодежный журнал*, 2018, № 12. DOI: 10.18698/2541-8009-2018-12-415 URL: http://ptsj.ru/catalog/jur/crim/415.html

[2] Карлова А.В. Установление обстоятельств работы с USB-устройствами в операционной системе Windows. *Политехнический молодежный журнал*, 2019, № 4. DOI: 10.18698/2541-8009-2019-4-465 URL: http://ptsj.ru/catalog/jur/crim/465.html

[3] Карлова А.В. Использование информации мобильных устройств для определения местоположения пользователя. *Аллея Науки*, 2018, № 10(26). URL: https://www.alley-science.ru/ domains_data/files/454November2018/ISPOLZOVANIE%20INFORMACII%20MOBILNYH%20USTROYSTV%20DLYa%20OPREDELENIYa%20MESTOPOLOZhENIYa%20POLZOVATELYa.pdf

[4] Яковлев А.Н. Влияние ошибок трактования нормативно закрепленной IT-терминологии на судопроизводство. *E-Forensics Russia. Мат. конф.* М., 2018.
[5] Геолокация без GPS (часть 1). *habr.com: веб-сайт*. URL: https://habr.com/post/256321/ (дата обращения: 06.06.2019).
[6] Wi-Fi simple geolocation tool. *easycoding.org: веб-сайт*. URL: https://www.easycoding.org/projects/wloc (дата обращения: 05.06.2019).
[7] Геолокация по WI-FI. *cryptoworld.su: веб-сайт*. URL: https://cryptoworld.su/wi-fi-geo/ (дата обращения: 08.06.2019).

Карлова Анастасия Владимировна — студентка кафедры «Юриспруденция, интеллектуальная собственность и судебная экспертиза», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

SOME FEATURES OF STUDY OF IMAGE FILES IN HEXADECIMAL FORMAT

A.V. Karlova
carlova.anastasia@yandex.ru
SPIN-code: 8696-6670

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

The article is devoted to the creation of a new method for identifying the coordinates of a digital image shooting location from mobile devices using the WinHex hexadecimal editor. When opening a graphic file in hexadecimal, you can explore its structure. During the study, a pattern was found in which the coordinates of the place where the photo image was taken were encoded. After a series of calculations, you can get the coordinates of longitude and latitude, which allow you to identify the exact location of the shooting of a particular image. The article contains guidelines for identifying geodata through the manual study of graphic files using a hexadecimal editor.

Keywords

Forensics, mobile device, geolocation tasks, geodata, geolocation of images, hexadecimal editor, guidelines

Received 18.06.2019

References

[1] Karlova A.V. Forensic investigation of the installation of allegedly counterfeit software products. *Politekhnicheskiy molodezhnyy zhurnal* [Politechnical student journal], 2018, no. 12. DOI: 10.18698/2541-8009-2018-12-415 URL: http://ptsj.ru/catalog/jur/crim/415.html (in Russ.).

[2] Karlova A.V. Establishing the circumstances of working with USB-devices in the Windows operating system. *Politekhnicheskiy molodezhnyy zhurnal* [Politechnical student journal], 2019, no. 4. DOI: 10.18698/2541-8009-2019-4-465
URL: http://ptsj.ru/catalog/jur/crim/465.html (in Russ.).

[3] Karlova A.V. Using information of mobile devices for definition user's location. *Alleya Nauki*, 2018, no. 10(26). URL: https://www.alley-science.ru/domains_data/files/454November2018/ISPOLZOVANIE%20INFORMACII%20MOBILNYH%20USTROYSTV%20DLYa%20OPREDELENIYa%20MESTOPOLOZhENIYa%20POLZOVATELYa.pdf (in Russ.).

[4] Yakovlev A.N. [Effect of treating mistakes of statuary IT terminology on legal procedures]. *E-Forensics Russia. Mat. konf.* [Proc. E-Forensics Russia]. Moscow, 2018 (in Russ.).

[5] Geolokatsiya bez GPS (chast' 1) [Geolocation without GPS (part 1)]. *habr.com: website* (in Russ.). URL: https://habr.com/post/256321/ (accessed: 06.06.2019).

[6] Wi-Fi simple geolocation tool. *easycoding.org: website*.
URL: https://www.easycoding.org/projects/wloc (accessed: 05.06.2019).

[7] Geolokatsiya po WI-FI [Geolocation using Wi-Fi]. *cryptoworld.su: website* (in Russ.). URL: https://cryptoworld.su/wi-fi-geo/ (accessed: 08.06.2019).

Karlova A.V. — Student, Department of Law, Intellectual Property and Forensic Examination, Bauman Moscow State Technical University, Moscow, Russian Federation.