www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2024.3.5

УДК 340.6:004
ББК 67.539

МЕТАДАННЫЕ КАК ФОРМИРОВАНИЕ ЦИФРОВОГО СЛЕДА ПРИ ИССЛЕДОВАНИИ ВМЕШАТЕЛЬСТВ В ЦИФРОВЫЕ ФОТОИЗОБРАЖЕНИЯ

Татьяна Викторовна Кислова

Старший преподаватель,
кафедра судебной экспертизы и физического материаловедения,
Волгоградский государственный университет
kislova.tatyana@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Константин Олегович Смирнов

Старший преподаватель,
кафедра судебной экспертизы и физического материаловедения,
Волгоградский государственный университет
smirnov@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Петр Сергеевич Иванов

Аспирант,
кафедра судебной экспертизы и физического материаловедения,
Волгоградский государственный университет
fna-241_846589@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В данной статье рассматривается важность формирования цифровых следов при изменении метаданных в контексте судебной фототехнической экспертизы. В свете роста компьютерных преступлений, цифровые следы становятся актуальным объектом исследования, что подчеркивается анализом достижений судебной фотографии. В исследовании определяются такие метаданные как: автор файла, устройство фотосъёмки, название файла, дата и место съемки, дата изменения или редактирования файла, название программы-редактора, а также другие данные, которые могут использоваться для проведения судебного расследования. Для редактирования фотоснимков использовали программу Adobe Photoshop. Для анализа уровня ошибок использовали сайт Foto Forensics. Для вычисления hash-значений использовали программное обеспечение MD5&SHAChecksumUtility 2.1. В результате работы было выявлено, что метаданные оригинальных фотоснимков не совпадают с метаданными редактированных изображений. Важно продолжать исследовать и развивать подходы к работе с метаданными, учитывая, как их потенциал, так и риски, связанные с их использованием.

Ключевые слова: метаданные, цифровой след, обработка цифровых фотоизображений, файл, судебная фототехническая экспертиза.

Введение

Е.Р. Россинская и И.А. Рядовский считают, что «...цифровой след представляет собой криминалистически значимую компьютерную информацию о событиях или действиях, отраженную в материальной среде, в процессе ее возникновения, обработки, хранения и передачи» [7; 8]. Сегодня такими следами являются содержимое оперативной памяти, файлы и их обрывки, создаваемая программными и аппаратным средствами. Также это может быть служебная информация об этих файлах, располагающихся на материальных носителях в виде цифровых кодированных последовательностей [9; 10]. Только посредством использования специализированных программных и аппаратных средств, осуществляющих декодирование и визуализацию в привычной графической, текстовой или звуковой форме такая информация доступна восприятию человеком. Здесь важно отметить, что ввиду своей подвижности и сложной структуры хранения подобного рода данные могут быть получены и интерпретированы в полном объеме.

Цифровые следы обладают своей специфичностью и представляют собой след, запечатленный в виде цифрового образа, изменяющий состояние информации в памяти абонентского устройства. Следует отметить, что отыскание цифровых следов является сложным процессом и требует привлечения специальных экспертов, обладающих определенным образованием в сфере цифровых технологий и опытом. Преимуществами появления цифровых следов является их объективное и последовательное отражение преступной деятельности лица, поскольку, используя данный вид следов, правоохранительные органы могут проследить порядок событий и действий лиц, участвующих в совершении преступления посредством применения информационных технологий [2; 9; 11].

Цифровые следы, возникающие в результате взаимодействия человека с цифровыми устройствами и интернет-пространством, становятся важным объектом исследования в контексте судебной фототехнической экспертизы. В условиях роста компьютерных преступлений и киберугроз, актуальность изучения цифровых следов не вызывает сомнений, так как они могут служить ключевыми доказательствами в расследовании преступлений.

Метаданные представляют собой важные данные, которые формируют цифровой след пользователя в сети [5; 6]. Они могут включать информацию о файлах, таких как автор, дата создания, использованные приложения, а также геолокационные данные. Эти метаданные становятся критическими для проведения расследований, позволяя отслеживать действия пользователей и выявлять паттерны их поведения. Кроме того, правовая основа для работы с цифровыми следами продолжает развиваться, и в 2022 г. в России был принят стандарт для специалистов по анализу данных цифрового следа.

В современном мире, где цифровые технологии проникают во все сферы жизни, понятие метаданных и их роль в формировании цифрового следа пользователя становятся все более актуальными.

Судебные дела, касающиеся метаданных, становятся все более распространенными. Например, в делах, связанных с уголовными преступлениями, применяются метаданные для отслеживания действий подозреваемых. Такие случаи подчеркивают необходимость четкого определения границ между легитимным использованием данных для обеспечения безопасности и незаконным вмешательством в частную жизнь граждан.

Цифровые следы, возникающие в результате взаимодействия человека с цифровыми устройствами и интернет-пространством, становятся важным объектом исследования в контексте судебной фототехнической экспертизы. В условиях роста компьютерных преступлений и киберугроз, актуальность изучения цифровых следов не вызывает сомнений, так как они могут служить ключевыми доказательствами в расследовании преступлений.

Актуальность данной работы обусловлена не только увеличением числа преступлений, связанных с использованием цифровых технологий, но и необходимостью совершенствования методов и подходов к их расследованию. В условиях, когда традиционные методы криминалистики сталкиваются с новыми вызовами, цифровые следы открывают новые горизонты для правоохранительных

органов. Важно отметить, что цифровые следы могут быть использованы не только для идентификации преступников, но и для восстановления хода событий, что делает их незаменимыми в судебной экспертизе. В условиях постоянного изменения законодательства и появления новых технологий исследование метаданных и их правового статуса становится важной задачей для специалистов, работающих в области информационных технологий и права.

Методика проведения исследования

При исследовании цифровых фотоизображений следует иметь точное представление о том, какие изменения могли быть внесены в данный объект. Существуют несколько областей, которым следует уделить особое внимание. Первая область – это именно та информация, которая находится в самом снимке. Для исправления таких данных используют графические редакторы, одним из часто использованных является Adobe Photoshop. Вторая область исследования фотоснимка – стандарт, позволяющий добавлять к изображениям специальную информацию, комментирующую данный файл, то есть EXIF (англ. Exchangeable Image File Format). EXIF-файлы предоставляют такую информацию о фотоснимке, как обстоятельства и методы его получения, авторство, модель камеры, время получения снимка. Метаданным так же свойственно подвергаться изменению и это может усложнить выполнение экспертного исследования. К примеру, есть вероятность того, что перед экспертом возникнет вопрос отождествления фотоизображений и камеры, благодаря, которой они были сделаны. Для того чтобы исследование было выполнено наиболее точно, необходимо максимально изучить описанные выше области и возможности внесения в них изменений и корректировок [1].

При просмотре фотографий в интернете, можно заметить, как некоторые сайты предоставляют важную информацию, которая относится к этим изображениям, такую как время, параметры экспозиции, бренд камеры и т. д. Эта информация, называемая EXIF, позволяет рассказать о том, какими настройками пользовался фотограф, на какое оборудование была запечатлено изображение.

Возможность видеть эти метаданные имеет большое значение в фототехнической экспертизе, так как именно они позволяют узнать, какие настройки и инструменты использовались для создания или корректировки конкретной фотографии. К сожалению, единственным для веб-сайта форматом файла, который может обрабатывать EXIF, является JPEG, поэтому увидеть данные таких форматов, как GIF и PNG, невозможно. Кроме того, чтобы скрыть следы преступления, в рамках уголовного дела, мошенники предпочитают удалять EXIF-данные со своих фотографий. Они скрывают свой стиль съемки, корректируют изображения с помощью фоторедакторов или удаляют все метаданные, тем самым усложняя работу эксперта.

Изображения, полученные при помощи различных цифровых устройств, могут стать вещественными доказательствами по уголовному делу [1]. В этом случае могут возникнуть вопросы о подлинности этих снимков, на которые будет необходимо ответить эксперту в рамках фототехнической экспертизы [3; 4].

Существует несколько возможностей вносить изменения в полученные цифровые изображения. Одна из них – это внесение изменений в само изображение при помощи графических редакторов, либо с помощью стандарта EXIF – добавить или изменить информацию о файле, содержащем графическое изображение. Теги с метаданными, включенные в стандарт EXIF, позволяют:

– увидеть съемочные настройки фотоаппарата для файла изображения; целостность изображения;

– точные координаты места съемки при наличии данной функции у фотокамеры;

– установить в случае вмешательства в целостность изображения программное обеспечение, которым оно было произведено [11].

Одной из важных особенностей метаданных является их упорядоченная структура. Информация точно отнесена к категории и содержит конкретный формат. Так, категорию времени создания можно заполнить только с помощью формата записи даты и времени.

Благодаря структурированному виду, метаданные доступны для чтения не только человеком, но и компьютерами. Таким образом,

метаданные могут быть обработаны машинным методом и использованы для различных целей: индексация, поиск, объединение [3; 5].

Существует множество онлайн-сервисов и программ для просмотра и изменений данных EXIF, которые были более подробно описаны в практической части данной статьи.

При анализе будут использоваться изображения, сделанные при помощи смартфона iPhone XR и сохраненные в формате JPG.

Далее цифровые изображения были перемещены на персональный компьютер. Затем были созданы копии оригинальных изображений, которые подверглись обработке в Adobe Photoshop 2018 версии CC 20.0.3.

Исследуемый объект, пятиэтажное кирпичное здание (рис. 1), фиксируем с помощью смартфона iPhone XR.

Выполнен вырез и заливка с последующей заменой, проведена штампом, увеличено облако, данное увеличение заметно при увеличении масштаба. Результат отражен на рисунке 2.

Рис. 1. Цифровое изображение до изменений

Рис. 2. Цифровое изображение после изменения в программе Photoshop

Открываем свойства цифрового изображения, затем вкладку «Подробно» (рис. 3), для того чтобы ознакомиться с метаданными изображения, представленного на рисунке 1.

Размер изображения: 694 × 635, а именно, ширина – 694 пикселей, высота – 635 пикселей.

Горизонтальное разрешение составляет 220 точек на дюйм, по вертикали – 220 точек на дюйм с глубиной цвета 24 бит.

То же самое проделываем с цифровым изображением после изменения (рис. 4).

Размер изображения: 588 × 537, а именно, ширина – 588 пикселей, высота – 537 пикселей. Горизонтальное разрешение составляет 96 точек на дюйм, по вертикали – 96 точек на дюйм с глубиной цвета 24 бит.

Исходное цифровое изображение обрабатываем с помощью сайта Foto Forensics.

Для сравнения рассмотрим другой вид модификаций фотоизображений и иной способ их выявления.

С помощью инструментов, предлагаемых программой FotoForensics, воспользуемся инструментом ELA (Error Level Analysis), который идентифицирует внутри самого изображения области с различной степенью сжатия. Дело в том, что формат JPEG использует систему сжатия с потерями. Каждая последующая перезапись (сохранение) в этом формате увеличивает потери качества. Далее рассматривая изображения после изменения выборочно увеличивая нужную область изображения (см. рис. 5–7).

Таким образом, можно сделать вывод о том, что EXIF-стандарт позволяет находить вмешательства в цифровое фотоизображение по метаданным, отображенным в свойствах файла. В формате же ELA области с изменениями в цифровом фотоизображение будут определяться по их различной степени сжатия.

К сожалению, метаданные, полученные после обработки цифровых фотоизображений с помощью инструментов, предлагаемых программой FotoForensics, не всегда могут дать информацию о том, что в данный файл произошло вмешательство (см. рис. 8).

Далее проиллюстрируем работу hash-функции. Она обладает возможностью обеспечения достоверности информации, генерируемой, передаваемой и хранящейся в цифровом виде. Возьмем оригинал фотографии, изменим размер, обрезав часть информации,

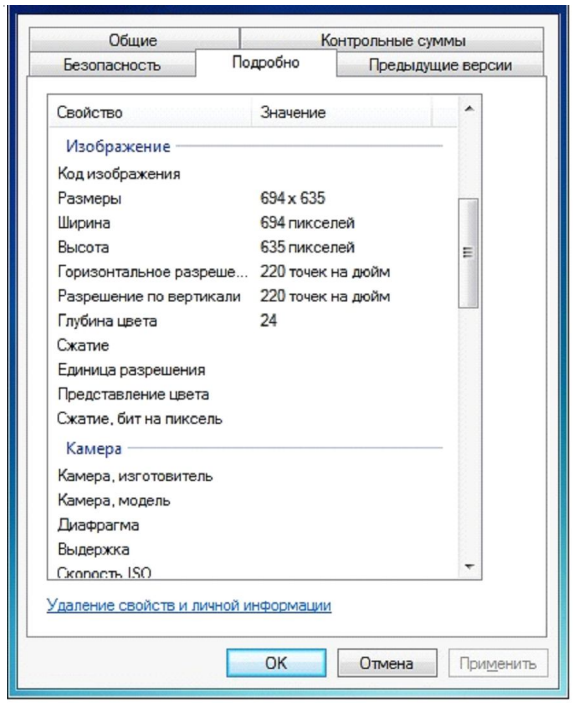

Рис. 3. Метаданные цифрового изображения до их изменения в разделе «Подробно»

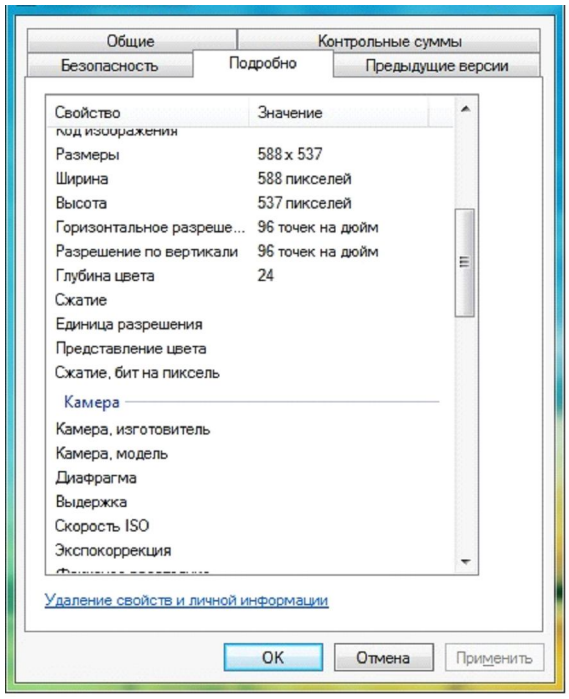

Рис. 4. Метаданные цифрового изображения после их изменения в разделе «Свойства»

и модифицируем изображение. Затем сравним результат хеширования файлов. Для вычисления hash-значений используем свободно распространяемое программное обеспечение MD5&SHA Checksum Utility 2.1 (см. рис. 9–15).

Результаты вычисления hash-значений программы MD5&SHA Checksum Utility 2.1 отражены на рисунке 15.

Так как hash-данные двух образцов не соответствуют оригиналу, можно сделать вывод о недостоверности информации.

Рис. 5. ELA-анализ уровня ошибок изображения до изменения

Рис. 6. ELA-анализ уровня ошибок изображения после его изменения

Рис. 7. ELA-анализ изображения после его изменения

File:	**1,180** × **1,080** JPEG (**1.3** megapixels) 364,802 bytes (356 kilobytes)
Color Encoding:	**WARNING:** No color-space metadata and no embedded color profile: **Windows and Mac web browsers treat colors randomly**. Images for the web are most widely viewable when in the sRGB color space and with an embedded color profile. See my Introduction to Digital-Image Color Spaces for more information.

Рис. 8. Метаданные, полученные с помощью сайта Foto Forensics

Рис. 9. Оригинал изображения

File:	C:\Users\Матвей\Downloads\IMG_1218.heic
MD5	91FBABDFC327D987ADA76C8BCBE872DE
SHA-1	0EB8AB7D13ADD1E065C284AD5A2563AFCDB10F2B
SHA-256	6031C809B5A364BD75F0F30DCB37463CF20C7F6B9671C5BEB87ACC0D97AF321F

Рис. 10. Hash-значения для оригинала изображения

Рис. 11. Обрезанное изображение

File:	C:\Users\Матвей\Downloads\IMG_1218.heic
MD5	731BF75B59F5E33BC0F9DEAF9A4D1AE5
SHA-1	3AD97E207092FA872B477B4CFCC44E7D6F13CA75
SHA-256	D2EDE4C4BB91FB1156BFD952F7BDEA395129A2CB5D212F2C94FDAE3C5CA54D9B

Рис. 12. Hash-значения для обрезанного изображения

Рис. 13. Редактированное изображение (скопирован столб)

Рис. 14. Hash-значения для редактированного изображения

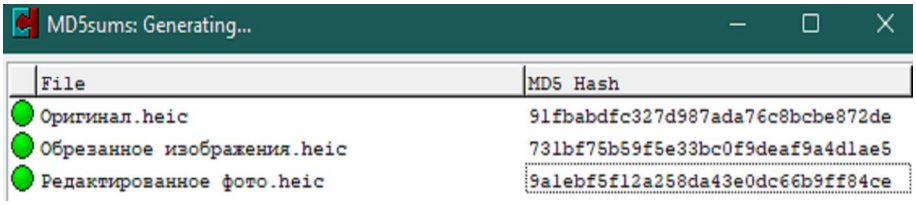

Рис. 15. Результаты вычисления hash-значений

Аналогичным образом можно провести сравнение hash-значений SHA1, sha256 и убедиться в том, что hash-значения оригинала не совпадают с двумя другими изображениями.

Цифровая природа информации делает применение hash-функций независимым от содержания информации. В данном пункте работы описано использование hash-функций для установления неизменности файла, содержащего цифровой фотоснимок.

Выводы

В заключение данной работы можно подвести итоги, касающиеся значимости метаданных как важного элемента цифрового следа пользователя в сети. Метаданные, представляющие собой структурированную информацию о данных, играют ключевую роль в формировании цифрового следа, который, в свою очередь, становится основой для идентификации и отслеживании действий пользователей, но и в определенных случаях может служить важным инструментом для проведения фототехнической экспертизы.

Таким образом, метаданные как цифровой след представляют собой важный и многогранный инструмент, который требует внимательного и ответственного подхода. Важно продолжать исследовать и развивать подходы к работе с метаданными, учитывая, как их потенциал, так и риски, связанные с их использованием.

СПИСОК ЛИТЕРАТУРЫ

1. Анализ модифицированных цифровых фотоизображений с помощью открытого программного обеспечения / Е. В. Борознина [и др.] // НБИ технологии. – 2023. – Т. 17, № 4. – С. 36–46. – DOI: 10.15688/NBIT.jvolsu.2023.4.5

2. Закиян, А. А. Цифровые следы в криминалистике / А. А. Закиян // Молодой ученый. – 2023. – № 23 (470). – С. 326–328.

3. Иванов, В. Ю. О теоретических аспектах использования в криминалистике понятия электронно-цифрового следа / В. Ю. Иванов // Юридические исследования. – 2020. – № 7.– С. 75–80. – DOI: 10.25136/2409-7136.2020.7.33682

4. Кузнецова, Е. Ф. Метаданные и их роль в системах поиска информации / Е. Ф. Кузнецова// Научные исследования в цифровую эпоху. – 2022. – № 1. – С. 5–12.

5. Лебедев, П. Р. Этика цифрового следа: правовые и моральные аспекты / П. Р. Лебедев // Право и информационные технологии. – 2021. – № 2. – С. 30–36.

6. Петрова, А.С. Цифровой след пользователя: методы анализа и применения / А. С. Петрова // Журнал информационной безопасности. – 2021. – № 4. – С. 25–30.

7. Россинская, Е. Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации / Е. Р. Россинская // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2019. – № 5 (57). – С. 31–44. – DOI: 10.17803/2311-5998.2019.57.5.031-044

8. Россинская, Е. Р. Современные способы компьютерных преступлений и закономерности их реализации / Е. Р. Россинская, И. А. Рядовский // Lex Russica (Русский закон). – 2019. – № 3 (148). – С. 87–99. – DOI: 10.17803/1729-5920.2019.148.3.087-099

9. Семикаленова, А. И. Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики / А. И. Семикаленова, И. А. Рядовский // Актуальные проблемы российского права. – 2019. – № 6 (103). – С. 178–185. – DOI: 10.17803/1994-1471.2019.103.6.178-185

10. Семикаленова, А. И. Цифровые следы: назначение и производство экспертиз / А. И. Семикаленова // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2019. – № 5. – С. 115–120. – DOI: 10.17803/2311-5998.2019.57.5.115-120

11. Яковлев, С. Ю. Метаданные как инструмент обеспечения информационной безопасности / С. Ю. Яковлев // Информационная безопасность. – 2019. – № 3. – С. 15–20.

REFERENCES

1. Boroznina E.V., Smirnov K.O., Kakorina O.A., Kislova T.V. Analysis of Modified Digital Photographic Images Using Open Source Software. *NBI technologies*, 2023, vol. 17, no. 4, pp. 36-46. DOI: 10.15688/NBIT.jvolsu.2023.4.5

2. Zakiyan A.A. Cifrovye sledy v kriminalistike [Digital Traces in Criminology]. *Molodoj uchenyj* [Young Scientist], 2023, vol. 23, no. 470, pp. 326-328.

3. Ivanov V.Yu. O teoreticheskih aspektah ispol'zovaniya v kriminalistike ponyatiya elektronno-cifrovogo sleda [On the Theoretical Aspects of the Use of the Concept of an Electronic Digital Footprint in Criminology]. *Yuridicheskie issledovaniya* [Legal Research], 2020, no. 7, pp. 75-80. DOI: 10.25136/2409-7136.2020.7.33682

4. Kuznetsova E.F. Metadannye i ih rol' v sistemah poiska informacii [Metadata and Their Role in Information Retrieval Systems]. *Nauchnye issledovaniya v cifrovuyu epohu* [Scientific Research in the Digital Age], 2022, no. 1, pp. 5-12.

5. Lebedev P.R. Etika cifrovogo sleda: pravovye i moral'nye aspekty [Ethics of the Digital Footprint: Legal and Moral Aspects]. *Pravo i informacionnye tekhnologii* [Law and Information Technology], 2021, no. 2, pp. 30-36.

6. Petrova A.S. Cifrovoj sled pol'zovatelya: metody analiza i primeneniya [The Digital Footprint of the User: Methods of Analysis and Application]. *Zhurnal informacionnoj bezopasnosti* [Journal of Information Security], 2021, no. 4, pp. 25-30.

7. Rossinskaya E.R. Problemy ispol'zovaniya special'nyh znanij v sudebnom issledovanii komp'yuternyh prestuplenij v usloviyah cifrovizacii [Problems of Using Special Knowledge in the Judicial Study of Computer Crimes in the Context of Digitalization]. *Vestnik Universiteta imeni O.E. Kutafina (MGYuA)* [Bulletin of the O.E. Kutafin University (MGUA)], 2019, vol. 5 (57), pp. 31-44. DOI: 10.17803/2311-5998.2019.57.5.031-044

8. Rossinskaya E.R. Sovremennye sposoby komp'yuternyh prestuplenij i zakonomernosti ih realizacii [Modern Methods of Computer Crimes and Patterns of Their Implementation]. *Lex Russica*, 2019, vol. 3 (148), pp. 87-99. DOI: 10.17803/1729-5920.2019.148.3.087-099

9. Semikalenova A.I., Ryadovsky I.A. Ispol'zovanie special'nyh znanij pri obnaruzhenii i fiksacii cifrovyh sledov: analiz sovremennoj praktiki [The Use of Special Knowledge in the Detection and Fixation of Digital Traces: An Analysis of Modern Practice]. *Aktual'nye problemy rossijskogo prava* [Actual Problems of Russian Law], 2019, vol. 6 (103), pp. 178-185. DOI: 10.17803/1994-1471.2019.103.6.178-185

10. Semikalenova A.I. Cifrovye sledy: naznachenie i proizvodstvo ekspertiz [Digital Traces:

Appointment and Production of Examinations]. *Vestnik Universiteta im. O.E. Kutafina (MGYuA)* [Bulletin of the O.E. Kutafin University (MGUA)], 2019, vol. 5, pp. 115-120. DOI: 10.17803/2311-5998.2019.57.5.115-120

11. Yakovlev S.Yu. Metadannye kak instrument obespecheniya informacionnoj bezopasnosti [Metadata as an Information Security Tool]. *Informacionnaya bezopasnost'* [Information Security], 2019, vol. 3, pp. 15-20.

METADATA AS THE FORMATION OF A DIGITAL FOOTPRINT IN THE STUDY OF INTERVENTIONS IN DIGITAL PHOTOGRAPHIC IMAGES

Tatiana V. Kislova

Senior Lecturer,
Department of Forensic Examination and Physical Materials Science,
Volgograd State University
kislova.tatyana@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Konstantin O. Smirnov

Senior Lecturer,
Department of Forensic Examination and Physical Materials Science,
Volgograd State University
smirnov@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Peter S. Ivanov

Postgraduate Student,
Department of Forensic Examination and Physical Materials Science,
Volgograd State University
fna-241_846589@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. This article discusses the importance of forming digital footprints when changing metadata in the context of forensic phototechnical examination. In the light of the growth of computer crimes, digital footprints are becoming an urgent object of research, which is emphasized by the analysis of the achievements of forensic photography. The study identifies metadata such as: the author of the file, the device of photographing, the name of the file, the date and place of shooting, the date of modification or editing of the file, the name of the editing program, as well as other data that can be used to conduct a judicial investigation. The Adobe Photoshop program was used to edit the photos. The Foto Forensics website was used to analyze the error level. MD5&SHAChecksumUtility 2.1 software was used to calculate hash values. As a result of the work, it was revealed that the metadata of the original photographs does not match the metadata of the edited images. It is important to continue to explore and develop approaches to working with metadata, taking into account both their potential and the risks associated with their use.

Key words: metadata, digital footprint, processing of digital photographic images, file, forensic phototechnical examination.