www.volsu.ru

DOI: https://doi.org/10.15688/lc.jvolsu.2024.3.26

UDC 343.983
LBC 67.53

Submitted: 15.05.2024
Accepted: 20.06.2024

SOFTWARE AND DATA SUPPORT FOR COMPUTER FORENSIC ANALYSIS

Alexey Yu. Stebivko

JSC "Rosselkhozbank", Moscow, Russian Federation;
Russian State University of Justice, Moscow, Russian Federation

Introduction: the paper highlights the role of software and data support for computer forensic analysis carried out at the stage of judicial investigation and preliminary investigation, emphasizing its importance in the era of digitalization. **Purpose:** disclose the questions that modern technologies of computer-technical expertise are able to answer, and necessary data sets for research. **Methods:** the methodological framework for the study is based on the methods of consistency and analysis. **Results:** the paper presents a methodology for auditing computer equipment (CE) and information and communication technologies (ICT) in the context of criminal investigations. It also elucidates the techniques and methods employed in the study of CE and ICT hardware and software. **Conclusions:** the author analyzes the state of crime related to the use of computer technology in telematics networks and information and communication technologies, identifies ways to commit crimes related to the use of malware and legal software, the functioning of a dynamic system representing the mechanism of these crimes, as well as systemic aspects of the emergence and investigation of threats of this type.

Key words: software and data support, computer forensic analysis, digital data, data recovery, malware, unauthorized access, cybersecurity.

Citation. Stebivko A.Yu. Software and Data Support for Computer Forensic Analysis. *Legal Concept = Pravovaya paradigma*, 2024, vol. 23, no. 3, pp. 189-194. (in Russian). DOI: https://doi.org/10.15688/lc.jvolsu.2024.3.26

УДК 343.983
ББК 67.53

Дата поступления статьи: 15.05.2024
Дата принятия статьи: 20.06.2024

ИНФОРМАЦИОННО-ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СУДЕБНЫХ КОМПЬЮТЕРНО-ТЕХНИЧЕСКИХ ЭКСПЕРТИЗ

Алексей Юрьевич Стебивко

АО «Россельхозбанк», г. Москва, Российская Федерация;
Российский государственный университет правосудия, г. Москва, Российская Федерация

Введение: в статье освещается роль информационно-программного обеспечения в судебных компьютерно-технических экспертизах, производимых на стадии судебного следствия и предварительного расследования, подчеркивается его важность в эпоху цифровизации. **Цель:** раскрыть вопросы, на которые способны дать ответ современные технологии компьютерно-технической экспертизы, наборы данных, которые требуются для исследования. **Методы:** методологическую основу данного исследования составили методы системности и анализа. **Результаты:** определены порядок и инструменты аудита средств вычислительной техники (СВТ) при расследовании преступлений, совершенных с использованием СВТ, а также информационно-коммуникационных технологий (ИКТ); охарактеризованы приемы и методы, используемые при исследовании аппаратного и программного обеспечения. **Выводы:** проанализировано состояние преступности, связанной с использованием СВТ в телематических сетях и ИКТ, выделены способы совершения преступлений, связанных с использованием вредоносного и легального программного обеспечения, функционирование динамической системы, представляющей механизм данных преступлений, а также системные аспекты возникновения и расследования угроз данного вида.

Ключевые слова: информационно-программное обеспечение, судебные компьютерно-технические экспертизы, цифровые данные, восстановление данных, вредоносное программное обеспечение, несанкционированный доступ, кибербезопасность.

Цитирование. Стебивко А. Ю. Информационно-программное обеспечение судебных компьютерно-технических экспертиз // Legal Concept = Правовая парадигма. – 2024. – Т. 23, № 3. – С. 189–194. – DOI: https://doi.org/10.15688/lc.jvolsu.2024.3.26

Введение

Информационно-программное обеспечение судебных компьютерно-технических экспертиз – это область, где юридическая экспертиза сочетается с передовыми технологиями для анализа и интерпретации цифровых данных в контексте правовых вопросов. Важность этой области возрастает в эпоху цифровизации, где большое количество дел связано с цифровыми данными.

В этом контексте особое внимание уделяется программному обеспечению и инструментам, которые используются для анализа данных с компьютеров, мобильных устройств и других цифровых платформ. Поскольку результаты экспертизы часто используются на этапе досудебного расследования, в судебных процессах, эти инструменты должны быть точными, эффективными и обеспечивать высокую степень надежности.

Эксперты, которые работают в этой области, обязаны обладать техническими знаниями и навыками и понимать юридические аспекты работы с цифровыми носителями. К ним относится знание программного обеспечения, правоприменительной практики, а также приемов и методов работы с соответствующим набором информации, которая может повлиять на результаты расследования или судебное дело.

Судебные компьютерно-технические экспертизы охватывают широкий спектр задач, каждая из которых требует уникального подхода и специализированного программного обеспечения, например:

– восстановление удаленных данных;

– анализ сетевых взаимодействий;

– идентификация и анализ вредоносных программ;

– выявление следов несанкционированного доступа к системам.

Результаты

В целом, успешное проведение компьютерно-технических экспертиз требует не только глубоких технических знаний, но и способности использовать специализированное программное обеспечение (далее – ПО) для обработки и анализа больших объемов данных. Это позволяет экспертам выявлять скрытую информацию, которая может быть критически важной на этапе досудебного следствия и в судебном процессе.

Информационно-программное обеспечение при проведении судебных компьютерно-технических экспертиз включает следующие области [4]:

1. Операционная система. Для поиска цифровых улик информация извлекается из операционной системы, определяются подозрительные действия через сопоставление хэш-сумм и анализа сигнатур жесткого диска, примером служит инструмент OS Forensics [6].

2. Файловая система. Для поиска цифровых улик производится извлечение и восстановление данных на разделах жесткого диска.

3. Энергозависимая память. Используется для поиска цифровых улик, отсутствующих на жестком диске, а также для анализа происходящего на компьютере в фиксированный момент времени. В энергозависимой памяти обычно хранятся руткиты, которые скрывают свои процессы, файлы, ключи реестра, и даже сетевые соединения, позволяя найти то, что скрыто. Одним из способов ее снятия является копирование с помощью инструментов LiveKd – linux kernel crush dump (LKCD), подключение к ядру специальных модулей ядра, перевод компьютера в режим гибрентации, через подключение последовательной высокоскоростной шины. Следует иметь в виду, что снятие данных энергозависимой памяти возможно только при включенном средстве вычислительной техники (далее – СВТ), в противном случае данные обычно теряются.

4. Веб-браузеры. Для поиска цифровых улик производится извлечение данных просмотра веб-страниц, их количество, продолжительность, загруженных файлов с каждой страницы, файлов cookie, а также другой информации.

5. Сетевая криминалистика. Для поиска цифровых улик осуществляется монито-

ринг трафика и анализ сетевых пакетов на разных уровнях модели OSI с помощью таких инструментов, как Tcpdump, NetFlow Traffic Analyzer, «ГАРДА Монитор», ntoping, PT Network Attack Discovery, Malcolm [3]. Большинство ПО не имеет открытого кода, что не позволяет создать универсальную систему для ретроспективного анализа. Наиболее подходящим решением стала система Malcolm, которая позволяет не только с высокой скоростью анализировать большой объем данных, но и визуализировать полученную информацию.

При обнаружении сбоя в первую очередь компьютер отключается от сети, фиксируется его состояние и анализируются сохранившиеся данные.

Далее определяется характер сбоя, который условно делится на случайный и умышленный [3].

Случайный возникает по ошибке пользователя, вследствие использования нелицензионного ПО, наличия ошибок в программном или аппаратном обеспечении, превышения полномочий пользователя в операционной системе, предоставления доступов третьим лицам. Умышленный возникает в результате кибератаки (фишинг, DoS-атаки, вредоносное ПО), хищения документов и техники, нарушения политик безопасности.

Злоумышленник может быть определен по цифровым следам, оставшимся после совершения противоправных действий на многих устройствах, в связи с чем производится идентификация и изъятие всех устройств, на которых может находиться необходимая для расследования информация, в том числе смартфонов, персональных компьютеров, ноутбуков, умных устройств, карт памяти, камер, биометрических сканеров, серверов, систем контроля и управления доступом (СКУД), маршрутизаторов, коммутаторов, систем GPS и «Глонасс».

Перед изъятием устройств определяется план сбора устройств, устанавливается их приоритет и осуществляется съем изменчивых данных, которые теряются после выключения СВТ. Одним из криминалистических инструментов для съема изменчивых данных является программное обеспечение Volatility Framework, которое позволяет снять образ оперативной памяти устройства, извлечь из образа цифровые артефакты, дату и время, список запущенных процессов, список открытых и конечных сетевых соединений, загруженные библиотеки процессов, имена открытых файлов каждым из процессов и др. Для исследования жестких дисков и энергозависимой памяти, создания отчетов о пользовательских и системных действиях также может быть использовано программное обеспечение в виде Digital Forensics Framework.

Алгоритм сбора устройств выглядит следующим образом:

1) определение устройств, на которых произошел (вероятно, произошел) компьютерный инцидент (далее – КИ);

2) разбивка устройств по их пользователям.

При изъятии каждый носитель информации помещается в отдельную упаковку, снабженную индивидуальным номером и местом выемки, необходимыми для экспертов-криминалистов.

Исследование сбоев, анализ вычислительных устройств, программного обеспечения, сетевого трафика, активности пользователей производится непосредственно экспертами-криминалистами с помощью различного программного обеспечения, в том числе открытого (PyFlag, Xplico, NetworkMiner), проприетарного (Netintercept, NetWitness, Iris, NetDetector, DeepSee), а также встроенных утилит операционной системы для проведения сетевой экспертизы, таких как nslookup, traceroute, tcpslice, netstat, nbtstat, whois, ping, dig [7].

Для идентификации КИ может использоваться программный код, который собирает значения атрибутов на устройстве, после чего происходит объединение атрибутов всех устройств на основе совпадения названия атрибутов, далее осуществляется идентификация файла на основе метрических алгоритмов.

В качестве примера ПО, используемого при исследовании вычислительных устройств, можно привести инструмент bulk_extractor, который позволяет автоматически извлекать из больших массивов информации на диске полезную информацию – адреса электронной почты, номера банковских карт и телефонов, метаданные (GPS-координаты, время и дату, автора, номер камеры) видеозаписей и фотографий, списки слов для подбора паролей, удаленные фай-

лы, пользовательскую активность, а также производить поиск по ключевым словам.

При осмотре истории браузера в компьютерах пользователей следует иметь в виду, что отсутствующие сведения зачастую продолжают храниться даже после очистки в приложении. Так, любой современный браузер (Internet Explorer, Google Chrome, Safari, Mozilla Firefox, Opera) хранит историю поиска на устройстве даже после ее удаления в приложении, удаленная история продолжает храниться в скрытом файле, который невозможно удалить неосведомленному пользователю. Internet Explorer хранит данный файл в index.dat, браузеры на технологии Mozilla Firefox в файле history.dat.

Криминалистические методы сбора информации о посещенных веб-сайтах реализуются с помощью программного обеспечения WebHistorian [2], которое позволяет сформировать отчет о посещенных страница всех браузеров, открыть кэшированные (находящиеся в памяти устройства) страницы и просмотреть их содержание, даже если доступ к указанным страницам отозван (требуется аутентификация). Другим инструментом является AnalyzerIndex.dat, с помощью которого можно просматривать и редактировать файлы index.dat, просматривать файлы cookie и кэшированные страницы, ориентирован на использование в браузере Microsoft Edge.

В вычислительной технике криминалистический анализ позволяет выявлять различные цифровые улики через атрибуты операционной системы, к примеру:

– последние открытые файлы, пути к файлам, их позицию в кэше;

– время последнего открытия по артефакту файла через атрибут операционной системы Shimcahe;

– название, дату и время выполнения приложения, количество запусков и путь через атрибут Prefetch;

– историю, к каким папкам обращался пользователь через набор ключей реестра Shellbags;

– историю изменения всех файлов на разделе жесткого диска, внесенную в файлы и папки через атрибут UsnJrnl;

– историю и расположение приложений, выполнявшихся на устройстве, в том числе имя запустившего пользователя, список сетей, к которым было подключено устройство, длительность соединений и объем переданной по ним информации, нагрузку процессора и ресурс батареи через атрибут System Resource Usage Monitor;

– все приложения, которые использовал конкретный пользователь через атрибут User Assist [5].

Выводы

Таким образом, криминалистический анализ служит для получения широкого круга ответов по цифровым следам на устройстве [1], включая идентификацию людей, мест, предметов и событий, а также определение того, как эти элементы связаны. Отчет по результатам компьютерно-технической экспертизы может быть положен в основу принятия решения при расследовании преступлений, совершенных с использованием средств вычислительной техники.

Компьютерно-техническая экспертиза является видом инженерно-технических экспертиз [8], цель которой заключается в исследовании компьютерной техники и носителей информации на предмет содержания в них цифровых улик, которые могут применяться при расследовании компьютерных инцидентов. Объектами компьютерно-технической экспертизы могут являться абсолютно любые объекты информационной инфраструктуры – от персональных компьютеров и переносных носителей информации до программного обеспечения и различных текстовых и графических файлов.

В заключение стоит подчеркнуть, что на досудебном и судебном следствии компьютерно-технические судебные экспертизы в большинстве случаев выступают в качестве основополагающего элемента, особо значимого для принятия решения. С учетом растущего присутствия цифровых данных эффективность и достоверность такого обеспечения приобретают новый уровень значимости. Это наиболее важно в случаях, когда дела включают анализ цифровой информации, требующий глубокого и точного подхода.

Специалисты, работающие в этом направлении, сталкиваются с задачей интегра-

ции высокотехнологичных инструментов с нормами материального и процессуального права, совмещают техническую компетентность с правовыми знаниями, что необходимо для достижения объективных результатов в судебных разбирательствах и на досудебном следствии.

Используемое в таких исследованиях программное обеспечение должно отвечать строгим критериям в плане функциональности, безопасности и сохранения конфиденциальности. С учетом непрерывных изменений в цифровом пространстве и развития киберугроз постоянное обновление технологий и знаний является необходимостью.

В этом контексте информационно-программное обеспечение занимает центральное место в достижении правосудия в цифровую эпоху, предоставляя экспертам инструменты для точного и эффективного изучения цифровых данных, что критически важно для формирования справедливых и обоснованных решений на досудебном следствии и в судебных процессах.

СПИСОК ЛИТЕРАТУРЫ

1. Ловцов, Д. А. Информационно-математическое обеспечение имитационного моделирования интегрированных логистических систем / Д. А. Ловцов, А. В. Васенов // Известия Института инженерной физики. – 2009. – № 4. – С. 30–36.

2. Майорова, Е. В. Использование методов форензики при расследовании инцидентов компьютерной безопасности / Е. В. Майорова, А. В. Черток // Технико-технологические проблемы сервиса. – 2019. – № 4. – С. 36–41.

3. Пантюхин, И. С. Основы компьютерно-технической экспертизы / И. С. Пантюхин, Д. Н. Шидакова // Вестник полиции. – 2016. – № 1. – С. 20–29.

4. Пырьев, М. С. Средства анализа сетевого трафика локальной вычислительной сети в ретроспективе / М. С. Пырьев, А. С. Коллеров // Вестник УрФО. – 2019. – № 4. – С. 58–62.

5. Leslie, F. Packet Analysis for Network Forensics: A Comprehensive Survey / F. Leslie // Forensic Science International: Digital Investigation. – 2020. – DOI: 10.1016/j.fsidi.2019.200892

6. Roussev, V. Digital Forensic Science: Issues, Methods, and Challenges / V. Roussev. – Cham : Springer, 2016. – 155 p. – (Synthesis Lectures on Information Security, Privacy, and Trust ; vol. 8, № 5).

7. Sachdeva, S. Analysis of Digital Forensic Tools / S. Sachdeva, B. Raina, A. Sharma // Journal of Computational and Theoretical Nanoscience. – 2020. – Vol. 17. – P. 2459–2467.

8. Sudhakar, K. An Emerging Threat Fileless Malware: A Survey and Research Challenges / K. Sudhakar // Cybersecurity. – 2022. – Vol. 3. – DOI: https://doi.org/10.1186/s42400-019-0043-x

REFERENCES

1. Lovcov D.A., Vasenov A.V. Informacionno-matematicheskoe obespechenie imitacionnogo modelirovaniya integrirovannyh logisticheskih system [Information-Mathematical Support for Simulation Modeling of Integrated Logistics Systems]. *Izvestiya Instituta inzhenernoj fiziki*, 2009, no. 4, pp. 30-36.

2. Majorova E.V., Chertok A.V. Ispolzovanie metodov forenziki pri rassledovanii incidentov kompyuternoj bezopasnosti [Using Forensic Methods in Investigating Computer Security Incidents]. *Tekhniko-tekhnologicheskie problemy servisa*, 2019, no. 4, pp. 36-41.

3. Pantyuhin I.S., Shidakova D.N. Osnovy kompyuterno-tekhnicheskoj ekspertizy [Fundamentals of Computer Forensics]. *Vestnik policii*, 2016, no. 1, pp. 20-29.

4. Pyryev M.S., Kollerov A.S. Sredstva analiza setevogo trafika lokalnoj vychislitelnoj seti v retrospektive [Tools for Analyzing Network Traffic of a Local Computer Network in Retrospect]. *Vestnik UrFO*, 2019, no. 4, pp. 58-62.

5. Leslie F. Packet Analysis for Network Forensics: A Comprehensive Survey. *Forensic Science International: Digital Investigation*, 2020. DOI: 10.1016/j.fsidi.2019.200892

6. Roussev V. *Digital Forensic Science: Issues, Methods, and Challenges.* Cham, Springer, 2016. 155 p. (Synthesis Lectures on Information Security, Privacy, and Trust; vol. 8, no. 5).

7. Sachdeva S., Raina B., Sharma A. Analysis of Digital Forensic Tools. *Journal of Computational and Theoretical Nanoscience*, 2020, vol. 17, pp. 2459-2467.

8. Sudhakar K. An Emerging Threat Fileless Malware: A Survey and Research Challenges. *Cybersecurity*, 2022, vol. 3. DOI: https://doi.org/10.1186/s42400-019-0043-x

Information About the Author

Alexey Yu. Stebivko, Leading Counsel, JSC "Rosselkhozbank", Proyezd Krasnogvardeysky 1-y, 7, Bld. 1, 123100 Moscow, Russian Federation; Postgraduate Student, Russian State University of Justice, Novocheremushkinskaya St, 69, 117418 Moscow, Russian Federation, a.stebivko@yandex.ru, https://orcid.org/0000-0001-5152-5315

Информация об авторе

Алексей Юрьевич Стебивко, ведущий юрисконсульт, АО «Россельхозбанк», проезд Красногвардейский 1-й, 7, стр. 1, 123100 г. Москва, Российская Федерация; аспирант, Российский государственный университет правосудия, ул. Новочеремушкинская, 69, 117418 г. Москва, Российская Федерация, a.stebivko@yandex.ru, https://orcid.org/0000-0001-5152-5315