УДКУ 34

Основы компьютерной криминалистики (форензика): теоретические и практические аспекты

Баранников Сергей Николаевич

Кандидат военных наук,
доцент кафедры технологического менеджмента
и социально-экономических дисциплин,
Региональный институт в г. Темрюке,
Московский государственный университет технологий и управления
им. К.Г. Разумовского (Первый казачий университет),
353500, Российская Федерация, Темрюк, Советская, 4;
e-mail: bsn53@bk.ru

Абесалашвили Маринэ Зауровна

Кандидат юридических наук, доцент,
заместитель директора по научной работе и дополнительному образованию,
Региональный институт в г. Темрюке,
Московский государственный университет технологий и управления
им. К.Г. Разумовского (Первый казачий университет),
353500, Российская Федерация, Темрюк, Советская, 4;
e-mail: abesala_m@mail.ru

Колодий Александр Сергеевич

Ректор,
Научно-исследовательский институт судебной экспертизы,
127006, Российская Федерация, Москва, ул Краснопролетарская, 7;
e-mail: rector@dpo1.ru

Аннотация

В статье рассматриваются теоретические и практические аспекты компьютерной криминалистики (форензики), а также актуальные проблемы и вызовы, с которыми сталкиваются специалисты в данной области. Проводится анализ методов и инструментов, используемых для сбора, сохранения, анализа и представления цифровых доказательств. Особое внимание уделяется развитию технологий, включая использование мобильных криминалистов и специализированных образов операционных систем, и их влиянию на методы работы в цифровой криминалистике. В заключении показано, что компьютерная криминалистика является важным инструментом в борьбе с киберпреступностью и злоупотреблениями в цифровой сфере. Постоянное развитие технологий и появление новых угроз требуют от специалистов глубоких знаний и постоянного совершенствования методов и инструментов. Использование мобильных криминалистов и

специализированных образов операционных систем позволяет исследователям эффективно и безопасно проводить анализ цифровых доказательств. Совместные усилия ученых и практиков в данной области позволят обеспечить более высокий уровень кибербезопасности и правопорядка в цифровом мире.

Для цитирования в научных исследованиях

Баранников С.Н., Абесалашвили М.З., Колодий А.С. Основы компьютерной криминалистики (форензика): теоретические и практические аспекты // Вопросы российского и международного права. 2024. Том 14. № 7А. С. 475-481.

Ключевые слова

Компьютерная криминалистика, цифровые доказательства, форензика, сетевой форензик, мобильный криминалист.

Введение

Компьютерная криминалистика, также известная как цифровая криминалистика или форензика, представляет собой область знаний и практической деятельности, направленную на изучение, восстановление и анализ цифровых данных с целью их использования в судебных разбирательствах и расследованиях. В условиях стремительного развития информационных технологий и роста количества киберпреступлений данная область науки приобретает всё большее значение. Сфера применения компьютерной криминалистики включает расследование инцидентов, связанных с кибератаками, утечками данных, мошенничеством и другими правонарушениями в цифровом пространстве. На современном этапе развития компьютерной криминалистики наблюдается интеграция с различными технологиями, такими как искусственный интеллект, облачные вычисления и блокчейн, что расширяет возможности исследователей в выявлении и анализе цифровых доказательств. Однако с этим также возрастают и вызовы, связанные с безопасностью данных, их объемами и юридическими аспектами использования цифровых доказательств.

Основное содержание

Компьютерная криминалистика опирается на междисциплинарные знания, включая информатику, криминалистику и юриспруденцию. Основные задачи дисциплины включают:

1) Обнаружение и сбор цифровых доказательств. Сбор информации с различных цифровых устройств и сетей, которая может иметь отношение к расследуемому событию. Это могут быть жесткие диски, мобильные устройства, сетевые устройства, облачные сервисы и другие носители информации. Сбор данных проводится с учетом сохранения их целостности и неизменности. Для этого применяются такие методы, как создание образов жестких дисков, копирование данных в режиме "только для чтения" и сбор сетевых логов.
2) Сохранение целостности доказательств. Этот этап необходим для того, чтобы собранные доказательства могли быть использованы в судебных разбирательствах. Любые изменения в данных могут привести к их недействительности. Для обеспечения целостности используются такие методы, как создание хэш-сумм, которые позволяют

проверять подлинность данных на всех этапах их обработки.

3) Анализ и интерпретация. В рамках этого этапа проводится детальный анализ собранных данных с целью выявления важных фактов и связей. Включает восстановление удаленных файлов, анализ временных меток и сетевой активности, а также выявление следов работы вредоносного ПО. Используются такие методы, как восстановление файлов, анализ логов и метаданных, а также исследование аномалий в сетевом трафике.
4) Документирование и представление доказательств. Документирование включает создание детализированных отчетов о проведенных действиях и полученных результатах. Это важный этап, так как позволяет представить результаты расследования в суде. Отчеты должны быть ясными, четкими и не вызывать сомнений в точности и полноте представленных данных.

Форензика файловых систем. Анализ файловых систем играет ключевую роль в восстановлении удаленных данных и исследовании структуры данных на носителях информации. Этот процесс включает изучение файловой системы на наличие скрытых или удаленных данных, а также анализ временных меток файлов и их изменений. Среди популярных инструментов для анализа файловых систем можно отметить:

1) EnCase. Это один из наиболее мощных инструментов, используемых для анализа файловых систем и данных на жестких дисках. Он позволяет создавать образы дисков, восстанавливать удаленные файлы, а также анализировать метаданные и события в файловой системе. EnCase часто используется как в правоохранительных органах, так и в корпоративной среде.
2) FTK Imager. Программа для создания образов жестких дисков и предварительного анализа данных. Она позволяет быстро получать доступ к файлам и папкам, даже если они были удалены или повреждены.
3) Специализированные образы операционных систем. Для проведения криминалистического анализа могут использоваться специальные операционные системы, такие как CAINE (Computer Aided INvestigative Environment) и DEFT (Digital Evidence & Forensics Toolkit). Эти дистрибутивы включают набор инструментов для анализа данных и предоставляют безопасную среду для работы с подозрительными файлами и системами.

Сетевой форензик. Сетевой форензик предполагает сбор и анализ сетевых пакетов для выявления подозрительной активности и восстановления хронологии событий. Этот метод важен для расследования инцидентов, связанных с несанкционированным доступом к сетям, взломами и утечками данных. Основные инструменты, используемые для сетевого форензика, включают:

– Wireshark. Это мощный инструмент для анализа сетевого трафика, который позволяет перехватывать и анализировать пакеты данных. Wireshark используется для выявления аномалий в трафике, обнаружения атак и анализа работы сетевых протоколов.
– tcpdump. Консольный инструмент для захвата и анализа сетевых пакетов. Он позволяет в реальном времени перехватывать пакеты и сохранять их для дальнейшего анализа. Tcpdump используется в основном для диагностики сетевых проблем и расследования инцидентов безопасности.
– NetFlow-анализаторы. Эти инструменты позволяют собирать и анализировать информацию о потоках данных в сети, что может помочь в выявлении аномальной активности и попыток вторжений.

Форензика мобильных устройств. С увеличением использования мобильных устройств в повседневной жизни, они становятся важным источником цифровых доказательств. Мобильные устройства могут содержать информацию о звонках, сообщениях, местоположении и активности в интернете. Для анализа мобильных устройств используются специализированные инструменты и методики, такие как:

– Cellebrite UFED. Инструмент, предназначенный для извлечения данных с мобильных устройств. Он позволяет получать доступ к контактам, сообщениям, фотографиям и другим данным, хранящимся на смартфонах и планшетах. Cellebrite также поддерживает восстановление удаленных данных, что делает его незаменимым инструментом в криминалистике мобильных устройств.
– XRY. Программное обеспечение для криминалистического анализа мобильных устройств, поддерживающее широкий спектр моделей и операционных систем. XRY позволяет извлекать данные с устройств на базе Android, iOS и других платформ, а также восстанавливать удаленные файлы и сообщения.
– Мобильные криминалисты. Это специализированные устройства, которые позволяют проводить экспресс-оценку данных мобильных телефонов на месте преступления. Такие устройства могут быстро извлекать данные без необходимости долгого подключения и анализа на стационарных системах.

Анализ вредоносного ПО. Вредоносное ПО (malware) представляет собой один из главных инструментов киберпреступников для проникновения в системы и кражи данных. Анализ вредоносного ПО позволяет выявить его функциональность, понять методы работы и разработать меры защиты. Существует два основных подхода к анализу вредоносного ПО:

1) Статический анализ. Изучение кода вредоносного ПО без его запуска. Статический анализ включает декомпиляцию и исследование кода для выявления функциональных возможностей программы. Основные инструменты для статического анализа включают IDA Pro, которая позволяет исследовать бинарные файлы, и Hex-Rays для декомпиляции.
2) Динамический анализ. Запуск вредоносного ПО в контролируемой среде (песочнице) для наблюдения за его поведением. Для этого используются виртуальные машины и специализированные программные среды, такие как Cuckoo Sandbox, которые позволяют отслеживать изменения в системе и сетевой активности.

Заключение

Современная компьютерная криминалистика сталкивается с рядом сложных задач и вызовов, которые затрудняют проведение расследований и анализ цифровых доказательств:

1) Шифрование данных. Использование сильных алгоритмов шифрования делает практически невозможным доступ к данным без соответствующих ключей. В условиях, когда все больше пользователей защищают свои данные шифрованием, специалисты по компьютерной криминалистике сталкиваются с проблемой доступа к потенциально важным доказательствам.
2) Объемы данных. С каждым годом объемы данных, подлежащих анализу, увеличиваются. Это требует использования мощных вычислительных ресурсов и новых подходов к автоматизации анализа данных, таких как применение машинного обучения и искусственного интеллекта.

3) Правовые аспекты. В разных странах существуют различные законодательные ограничения на сбор и использование цифровых доказательств. Это создает сложности в проведении международных расследований и обмене информацией между правоохранительными органами разных государств.
4) Облачные технологии. Использование облачных сервисов для хранения данных создает дополнительные сложности в их обнаружении и извлечении. Доступ к данным в облаке требует дополнительных разрешений и соблюдения юридических процедур, что может затруднить расследование.
5) Искусственный интеллект и машинное обучение. С развитием технологий искусственного интеллекта преступники начинают использовать его для создания более сложных и адаптивных угроз. Например, вредоносное ПО, использующее методы машинного обучения, может изменять свое поведение в зависимости от окружения, что затрудняет его обнаружение и анализ.

С учетом вышеуказанных вызовов, компьютерная криминалистика находится на этапе активного развития и интеграции новых технологий. Среди перспективных направлений можно выделить:

1) Автоматизация анализа данных. Использование технологий искусственного интеллекта и машинного обучения для автоматизации анализа больших объемов данных и выявления аномалий.
2) Облачные криминалистические платформы. Разработка инструментов для анализа данных, хранящихся в облачных хранилищах, и интеграция с облачными сервисами для упрощения доступа к цифровым доказательствам.
3) Киберфорензика. Развитие методов анализа данных, связанных с кибератаками и сетевыми угрозами, включая исследование методов проникновения и анализа вредоносного трафика.
4) Интернет вещей (IoT) и криминалистика. Анализ данных с устройств интернета вещей, которые все чаще используются как часть цифрового пространства и могут содержать важные доказательства.
5) Юридические аспекты. Разработка и гармонизация международных стандартов и протоколов для проведения цифровых расследований и обмена информацией между различными юрисдикциями.

Компьютерная криминалистика является важным инструментом в борьбе с киберпреступностью и злоупотреблениями в цифровой сфере. Постоянное развитие технологий и появление новых угроз требуют от специалистов глубоких знаний и постоянного совершенствования методов и инструментов. Использование мобильных криминалистов и специализированных образов операционных систем позволяет исследователям эффективно и безопасно проводить анализ цифровых доказательств. Совместные усилия ученых и практиков в данной области позволят обеспечить более высокий уровень кибербезопасности и правопорядка в цифровом мире.

Библиография

1. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press, 2011.
2. Nelson B., Phillips A., Steuart C. Guide to Computer Forensics and Investigations. Cengage Learning, 2014.
3. Bunting S., Weihrich W. EnCase Computer Forensics: The Official EnCE: EnCase Certified Examiner Study Guide. John Wiley & Sons, 2012.

4. Carrier B. File System Forensic Analysis. Addison-Wesley Professional, 2005.
5. Luttgens J., Pepe A., Mandia K. Incident Response & Computer Forensics. McGraw-Hill Education, 2014.
6. Altheide C., Carvey H. Digital Forensics with Open Source Tools: Using Open Source Platform Tools for Performing Computer Forensics on Target Systems. Syngress, 2011.
7. Sammons J. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. Syngress, 2012.

Fundamentals of computer forensics: theoretical and practical aspects

Sergei N. Barannikov

PhD in Military Sciences,
Associate Professor of the Department of Technological Management and Socio-Economic Disciplines,
Moscow State University of Technology and Management named after K.G. Razumovsky (First Cossack University),
Regional Institute in Temryuk,
353500, 4 Sovetskaya str., Temryuk, Russian Federation;
e-mail: bsn53@bk.ru

Marine Z. Abesalashvili

PhD in Law, Associate Professor,
Deputy Director for Research and Additional Education,
Moscow State University of Technology and Management named after K.G. Razumovsky (First Cossack University),
Regional Institute in Temryuk,
353500, 4 Sovetskaya str., Temryuk, Russian Federation;
e-mail: abesala_m@mail.ru

Aleksandr S. Kolodii

Rector,
Research Institute of Forensic Science,
127006, 7, Krasnoproletarskaya str., Moscow, Russian Federation;
e-mail: rector@dpo1.ru

Abstract

The article discusses the theoretical and practical aspects of computer forensics (forensics), as well as current problems and challenges faced by specialists in this field. An analysis of the methods and tools used to collect, preserve, analyze and present digital evidence is conducted. Particular attention is paid to the development of technologies, including the use of mobile forensic experts and specialized operating system images, and their impact on the methods of work in digital forensics. In conclusion, it is shown that computer forensics is an important tool in the fight against cybercrime and abuse in the digital sphere. Constant technological development and the emergence of new threats require specialists to have deep knowledge and constantly improve their methods and

tools. Using mobile forensics and specialized operating system images allows researchers to effectively and safely analyze digital evidence. Joint efforts of scientists and practitioners in this field will ensure a higher level of cybersecurity and law and order in the digital world.

For citation

Barannikov S.N., Abesalashvili M.Z., Kolodii A.S. (2024) Osnovy komp'yuternoi kriminalistiki (forenzika): teoreticheskie i prakticheskie aspekty [Fundamentals of computer forensics (forensics): theoretical and practical aspects]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 14 (7A), pp. 475-481.

Keywords

Computer forensics, digital evidence, forensics, network forensic, mobile forensic.

References

1. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press, 2011.
2. Nelson B., Phillips A., Steuart C. Guide to Computer Forensics and Investigations. Cengage Learning, 2014.
3. Bunting S., Weihrich W. EnCase Computer Forensics: The Official EnCE: EnCase Certified Examiner Study Guide. John Wiley & Sons, 2012.
4. Carrier B. File System Forensic Analysis. Addison-Wesley Professional, 2005.
5. Luttgens J., Pepe A., Mandia K. Incident Response & Computer Forensics. McGraw-Hill Education, 2014.
6. Altheide C., Carvey H. Digital Forensics with Open Source Tools: Using Open Source Platform Tools for Performing Computer Forensics on Target Systems. Syngress, 2011.
7. Sammons J. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. Syngress, 2012.