

УДК 004.056.53

А. С. КОНОВАЛОВ, Н. Ю. НОВИКОВ (ЭМ-21)

Научные руководители: старшие преподаватели *В. Е. МИНИН,*
С. С. ТАТУР

ИНСТРУМЕНТЫ ФОРЕНЗИКИ

Проведён анализ инструментальных средств компьютерной форензики, применяемых на различных этапах цифрового расследования – от создания побитовой копии носителя до формирования итогового отчёта. Рассмотрены ключевые принципы форензического исследования (неизменность данных, протоколирование, научная обоснованность, непрерывность цепочки владения) и соответствующие им инструменты с открытым исходным кодом: Guymager для создания образов дисков, The Sleuth Kit и Autopsy для анализа файловых систем, RegRipper для исследования реестра Windows, BrowsingHistoryView для извлечения артефактов веб-браузеров. На практическом примере восстановления удалённого документа с USB-накопителя продемонстрирована методика карвинга и корреляции артефактов.

Компьютерная форензика представляет собой прикладную дисциплину, посвящённую выявлению, сбору, анализу и сохранению цифровых улик для судебных разбирательств. Её деятельность основывается на четырёх ключевых принципах. Первый принцип заключается в неизменности данных, что подразумевает работу исключительно с побитовой копией образа носителя. Вторым принципом является протоколирование, при котором каждое действие эксперта документируется. Третий принцип акцентирует внимание на научной обоснованности методик и профессионализме эксперта. Четвёртый принцип касается непрерывности цепочки владения. Это означает, что улика не должна подвергаться подмене или повреждению [1].

Первым этапом работы является сбор данных и создание образа диска. Образ представляет собой побитовую копию всех секторов носителя, включая скрытые области, неразмеченное пространство и удалённые данные. Для создания образа используются инструменты dd в Linux или графическая утилита Guymager. Обязательной процедурой при этом является расчёт хеш-сумм MD5, SHA-1 или SHA-256. Эти суммы вычисляются сразу после создания образа и повторно по окончании исследования. Совпадение хеш-сумм подтверждает неизменность данных. При подключении оригинального носителя применяется аппаратный блокиратор записи.

Второй этап включает автоматизированный анализ файловой системы. Основным инструментарием служат консольный набор The Sleuth Kit (TSK)

и его графическая оболочка Autopsy. TSK работает напрямую с файловыми системами, такими как NTFS, FAT или EXT, без зависимости от операционной системы исследуемого компьютера. Autopsy предоставляет веб-интерфейс и автоматизирует стандартные задачи. Платформа восстанавливает структуру каталогов, индексирует содержимое, выявляет удалённые записи, извлекает временные метки создания, изменения и доступа, а также проводит анализ сигнатур файлов для обнаружения маскировки. В результате получается целостная картина активных и удалённых файлов, временная шкала событий и ключевые аномалии.

Третий этап предполагает углублённый анализ артефактов операционной системы и приложений. Для анализа реестра Windows применяется утилита RegRipper, которая автоматически извлекает ключевые артефакты из кустов реестра SAM, SYSTEM, SOFTWARE, NTUSER.DAT. RegRipper выявляет сведения о USB-устройствах, включая серийные номера и время подключения. Инструмент определяет список программ автозагрузки, что важно для обнаружения вредоносного ПО. Утилита восстанавливает пути к недавно открывавшимся документам, а также извлекает сетевые параметры, IP-адреса, историю подключений Wi-Fi и информацию об учётных записях пользователей. В таблице 1 приведены основные категории, извлекаемые RegRipper.

Таблица 1 – Ключевые артефакты, извлекаемые RegRipper

Категория	Извлекаемые сведения	Значение для расследования
USB-устройства	Серийные номера, время первого/последнего подключения	Установление факта подключения внешнего накопителя
Автозагрузка	Список программ, запускаемых при старте системы	Обнаружение вредоносного ПО, закрепляющегося в системе
Последние документы	Пути к недавно открывавшимся файлам	Выявление файлов, с которыми работал пользователь
Сетевые интерфейсы	IP-адреса, параметры адаптеров, история Wi-Fi-подключений	Определение сетевого окружения и точек доступа
Учётные записи	Информация о профилях пользователей, времени входа в систему	Идентификация активных учётных записей

Для проведения форензического анализа браузеров применяется лёгкая утилита BrowsingHistoryView, которая функционирует без необходимости запуска самих браузеров. Она поддерживает такие браузеры, как Chrome, Firefox, Edge, Opera и их производные. BrowsingHistoryView извлекает полную историю посещений с временными метками, поисковые запросы, историю загрузок файлов, данные автозаполнения форм, а также закладки и

cookie-файлы. Наибольшую ценность представляет не отдельный просмотр каждого источника данных, а их взаимная корреляция. Связывание временных меток из различных источников, включая системный реестр, файловую систему и кэш браузера, позволяет восстановить последовательность действий пользователя. Так, эксперт может установить, что пользователь вошёл в систему, затем подключил USB-накопитель с определённым серийным номером, скопировал на него документ и после этого посетил сайт облачного хранилища [2].

В качестве практического примера рассмотрено восстановление удалённого документа. Исходным материалом служит USB-флеш-накопитель с файловой системой FAT32. Пользователь удалил документ Microsoft Word с названием «Финансовый отчет.docx» и очистил корзину. Первым этапом эксперт создаёт побитовый образ флешки с помощью утилиты Guymager, сохраняя файл образа и вычисляя контрольную сумму SHA-256. Далее образ загружается в систему Autopsy. Несмотря на отсутствие файла в видимой структуре каталогов, система обнаруживает запись об удалённом объекте в журнале. На следующем этапе запускается поиск по сигнатурам файлов с помощью утилиты sigfind из состава The Sleuth Kit, что позволяет выявить заголовки документов формата DOCX в незатронутой области диска. После этого выполняется карвинг и восстановление файла с помощью утилит icat или tsf_recover, в результате чего извлекается файл с целостной внутренней структурой. Финальным шагом является верификация содержимого: эксперт открывает документ в MS Word, проверяет соответствие содержания ожидаемому и анализирует метаданные. При отсутствии перезаписи кластеров файл восстанавливается полностью.

На заключительном этапе происходит формирование итогового отчёта, который включает несколько обязательных разделов. В вводной части указывается основание исследования, сведения об эксперте, дата, время и место проведения работы. Описание исследуемых объектов содержит характеристики носителя: модель, серийный номер, объём, контрольные суммы оригинала и образа, а также информацию о применённых блокировщиках записи [3]. Раздел методики и инструментария перечисляет используемые программы с указанием версий (Guymager, Autopsy, RegRipper, BrowsingHistoryView, The Sleuth Kit) и описывает последовательность действий. Далее приводится поэтапное описание хода исследования с иллюстрациями ключевых находок и данными корреляции артефактов и временных меток. Раздел результатов и выводов содержит краткое резюме обнаруженных цифровых следов, ответы на поставленные вопросы и анализ причинно-следственных связей между артефактами. В таблице 2 приведено краткое представление отчёта на каждом этапе.

Таблица 2 – Соответствие этапов исследования и содержимого отчёта

Этап исследования	Что фиксируется в отчёте	Форма представления
Создание образа (Guymager)	Хеш-суммы, модель носителя, время копирования	Скриншот окна программы, текстовый протокол
Анализ в Autopsy	Найденные удалённые файлы, таймлайн событий	Выдержки из интерфейса, экспортированные списки
Анализ реестра (RegRipper)	Записи о USB-устройствах, автозагрузке, сетевых параметрах	Текстовый отчёт утилиты, сводная таблица
Форензика браузеров	История посещений, поисковые запросы, загрузки	Экспортированные CSV-файлы, скриншоты

Законодательство Республики Беларусь признаёт электронные цифровые доказательства в правовой системе. Новый Кодекс гражданского судопроизводства (КГС), который вступил в силу с 1 января 2026 года, впервые выделяет электронные доказательства как отдельную категорию. К ним относятся электронные документы, текстовые, мультимедийные и голосовые сообщения, базы данных, а также информация, распространяемая через интернет. В статье 199 КГС подробно регламентированы процедуры представления, исследования, хранения и возврата таких доказательств. В уголовном процессе нормы, касающиеся цифровых следов, распределены между Уголовно-процессуальным кодексом и подзаконными актами МВД и Следственного комитета.

Основными государственными органами, участвующими в регулировании и использовании цифровых доказательств, являются Главное управление по противодействию киберпреступности МВД (Управление К), Следственный комитет Республики Беларусь и Государственный комитет судебных экспертиз (ГКСЭ). Управление К отвечает за раскрытие киберпреступлений, оперативно-розыскные мероприятия и сбор цифровых доказательств. Следственный комитет проводит расследования уголовных дел и компьютерно-технические экспертизы. ГКСЭ осуществляет проведение судебных экспертиз, в том числе экспертиз компьютерной информации. Оперативно-аналитический центр при Администрации Президента отвечает за защиту государственных информационных систем и обеспечение их безопасности.

В условиях санкционных ограничений белорусские государственные ведомства сосредоточены на сотрудничестве с российскими производителями специализированного программного обеспечения. В 2025 году на базе Института Следственного комитета был проведён международный семинар КИБЕР-КРИМ 2025, на котором демонстрировались новейшие разработки и достигнуты соглашения о внедрении перспективных программно-аппаратных комплексов. Подготовка специалистов в этой области осуществляется совместно Академией МВД и Белорусским государственным университетом информатики и радиоэлектроники (БГУИР), где курсанты обучаются по специально-

стям «компьютерные системы и сети» и «защита информационных систем». Выпускники пополняют кадры Оперативно-аналитического центра, Комитета государственной безопасности и Главного управления по противодействию киберпреступности МВД.

Использование программ с открытым исходным кодом, таких как Autopsy, The Sleuth Kit и RegRipper, в белорусской экспертной практике допускается при соблюдении ряда условий. Во-первых, применяемые алгоритмы должны быть методически обоснованы и описаны в экспертной методике. Во-вторых, необходимо обеспечить контроль целостности данных, включая фиксацию хеш-сумм образа до и после анализа. В-третьих, требуется воспроизводимость результатов: другой эксперт при использовании того же инструментария должен получить идентичные выводы. В-четвёртых, каждый этап анализа должен документироваться с помощью скриншотов и логов, включаемых в итоговый отчёт.

Анализ нормативной базы указывает на устойчивую тенденцию цифровизации судебного процесса в Беларуси. Новый Кодекс гражданского судопроизводства расширяет возможности извещения участников через SMS и интернет, допускает электронную подачу процессуальных документов. Совместно с модернизацией технического оснащения следственных подразделений это формирует условия для внедрения инструментов цифровой forensики в практику правоприменения.

Основные выводы состоят в следующем. Во-первых, эффективное форензическое исследование строится на строгой последовательности этапов от создания побитового образа до оформления заключительного отчёта. Инструменты Guymager, Autopsy, RegRipper, BrowsingHistoryView и другие покрывают весь цикл и при правильном применении обеспечивают решение типовых экспертных задач. Во-вторых, современные методы карвинга и корреляции артефактов из реестра, браузеров и файловой системы позволяют восстанавливать даже намеренно удалённые данные и выстраивать хронологию действий пользователя. В-третьих, в Беларуси наблюдается тренд на легализацию цифровых доказательств: принятие нового Кодекса, обновление технического оснащения и подготовка кадров создают предпосылки для интеграции рассмотренных инструментов в судебную практику.

СПИСОК ЛИТЕРАТУРЫ

1 **Carrier, B.** File System Forensic Analysis / B. Carrier. – Boston : Addison-Wesley, 2005. – 592 с.

2 **Carvey, H.** Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry / H. Carvey. – 2nd ed. – Syngress, 2016. – 216 с.

3 Nir Sofer. BrowsingHistoryView // NirSoft. – URL: https://www.nirsoft.net/utils/browsing_history_view.html (date of access: 28.05.2026).

Получено 28.05.2026