

УДК 343.98

КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМАЯ ИНФОРМАЦИЯ В ОПЕРАЦИОННОЙ СИСТЕМЕ WINDOWS

А.В. Караваева

karlova_av@bmstu.ru

SPIN-код: 8696-6670

Е.В. Извальцева

izvaltsevaev@student.bmstu.ru

SPIN-код: 9956-4150

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

Рассмотрены компоненты операционной системы Windows, которые потенциально могут содержать важную для работы судебного компьютерно-технического эксперта информацию, и приведены примеры программного обеспечения, упрощающего поиск необходимой эксперту информации. Поскольку преступления, связанные с технологиями, выходят на новый уровень, специалисту в данной области необходимо оперативно находить информацию, способную помочь в раскрытии дела. Показаны способы изучения содержимого компонентов операционной системы средствами самой системы. Приведен список утилит, помогающих автоматизировать процесс поиска информации на компьютере, показаны их главные окна. Проверка информации в одной программе не гарантирует достоверность и полноту полученных данных, поэтому эксперту в области судебной компьютерно-технической экспертизы необходимо уметь пользоваться несколькими программами и утилитами.

Ключевые слова: судебная экспертиза, операционная система Windows, реестр, журнал событий, служебные каталоги, информационные технологии

Введение. Научно-технический прогресс не стоит на месте. Информационные технологии охватывают широкий спектр устройств, которые применяются в различных сферах деятельности, включая бизнес, образование, науку, здравоохранение, развлечения и другие. Информационные технологии играют важную роль в современном мире, обеспечивая автоматизацию и оптимизацию процессов, улучшение коммуникации и обмена информацией, а также повышение эффективности работы организаций и улучшение качества жизни людей в целом. Однако данные технологии также активно используются и преступниками, модернизируя традиционные преступления (преступления с использованием информационных технологий) и создавая новые (киберпреступления). Именно поэтому судебным экспертам в области компьютерно-технической экспертизы (СКТЭ) необходимо улучшать свои навыки для помощи в раскрытии, расследовании и предупреждении таких преступлений. Объектами исследования данной экспертизы является категория предметов,

обладающих общими признаками и относящихся к компьютерным средствам. К таким объектам можно отнести персональные компьютеры, мобильные устройства, операционные системы, прикладное программное обеспечение, текстовые и графические файлы и др. [1]. В данной статье рассмотрена криминалистически значимая информация, которую можно получить посредством исследования объектов с операционной системой (ОС) Windows.

Актуальность данной темы обусловлена тем, что устройства с ОС Windows до сих пор являются одним из часто встречаемых объектов СКТЭ, несмотря на ограничение в использовании лицензий.

Windows — это компьютерная операционная система от корпорации Microsoft с закрытым исходным кодом. Запущенная в 1985 г., эта ОС на данный момент является одной из самых популярных систем во всем мире. Изначально она была запущена как графическая ОС, построенная на MS-DOS (Microsoft Disk Operating System) — однозадачной дисковой ОС. На данный момент последней выпущенной версией является Windows 11, релиз которой состоялся в 2021 г.

Постановка задачи. В рамках данной работы рассмотрим следующие компоненты ОС Windows, содержащие криминалистически значимую информацию:

- реестр ОС Windows;
- журналы событий ОС Windows;
- служебные каталоги.

1. **Реестр Windows** является основным компонентом ОС Windows и содержит значительную информацию о конфигурации системы. Кроме того, в реестре хранится историческая информация о деятельности пользователя; реестр содержит подробные сведения об установленных и открытых приложениях, а также о подключаемых устройствах [2]. Таким образом, системный реестр — иерархически построенная база данных параметров и настроек ОС Windows.

Данная база данных хранит настройки и параметры большинства компонентов и приложений компьютера: конфигурацию аппаратных компонентов, программного обеспечения, профилей пользователя.

Вся эта информация может быть чрезвычайно ценной для судебного эксперта. Однако данная информация может быть полезна только в том случае, если судебный компьютерно-технический эксперт знает об ее существовании и о том, как ее найти или использовать.

Реестр Windows состоит из пяти ветвей (рис. 1):

– HKEY_CLASSES_ROOT — сведения, необходимые для запуска установленных в системе программ;

– HKEY_CURRENT_USER — сведения о конфигурации для работающего на данный момент пользователя. Здесь хранятся личные настройки и файлы конкретного профиля пользователя;

– HKEY_LOCAL_MACHINE — сведения об аппаратной части компьютера, подключенных устройствах и их драйверах. Содержит сведения о конфигурации, относящиеся к компьютеру вне зависимости от того, какой пользователь заходит в систему;

– HKEY_USERS — данные обо всех профилях пользователей на компьютере;

– HKEY_CURRENT_CONFIG — сведения о профиле оборудования, используемом локальным компьютером при запуске операционной системы [3, с. 2].

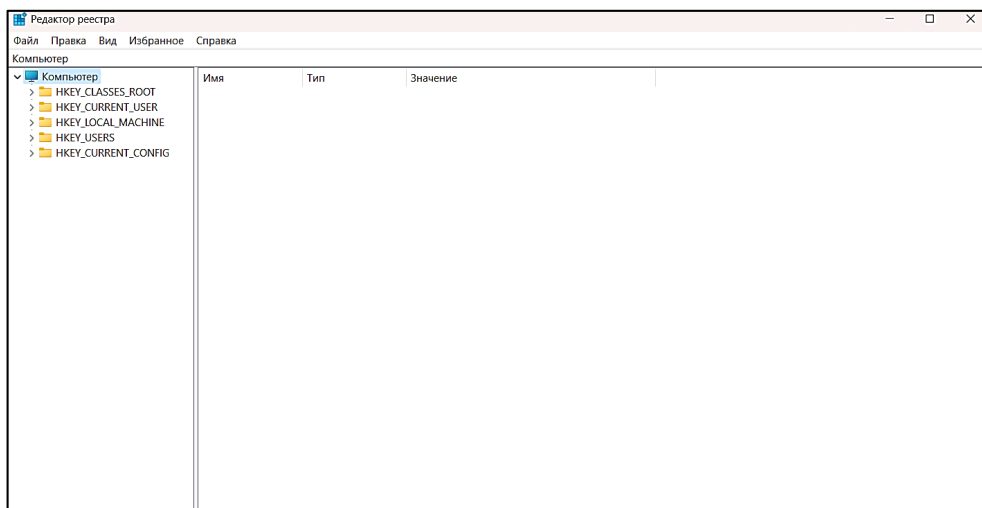


Рис. 1. Окно редактора реестра Windows

2. Журналы событий — это стандартный для приложений и ОС способ записи и централизованного хранения информации о важных программных и аппаратных событиях. Данная служба сохраняет события от различных источников в едином журнале, а программа просмотра событий позволяет пользователю наблюдать за журналом событий.

Журналы событий ОС Windows используются ОС для регистрации общесистемных событий, связанных с работой приложений, системных компонентов, безопасностью и запуском [4].

Журналы ОС Windows можно просмотреть с помощью утилиты «Просмотр событий» (рис. 2):

– приложение — хранит важные события, связанные с конкретным приложением;

– **безопасность** — хранит события, связанные с безопасностью, такие как вход в систему и выход из нее, использование привилегий и обращение к ресурсам;

– **установка** — в этот журнал записываются события, возникающие при установке и настройке операционной системы и ее компонентов;

– **система** — хранит события операционной системы или ее компонентов, например неудачи при запусках служб или инициализации драйверов, общесистемные сообщения и прочие сообщения, относящиеся к системе в целом.

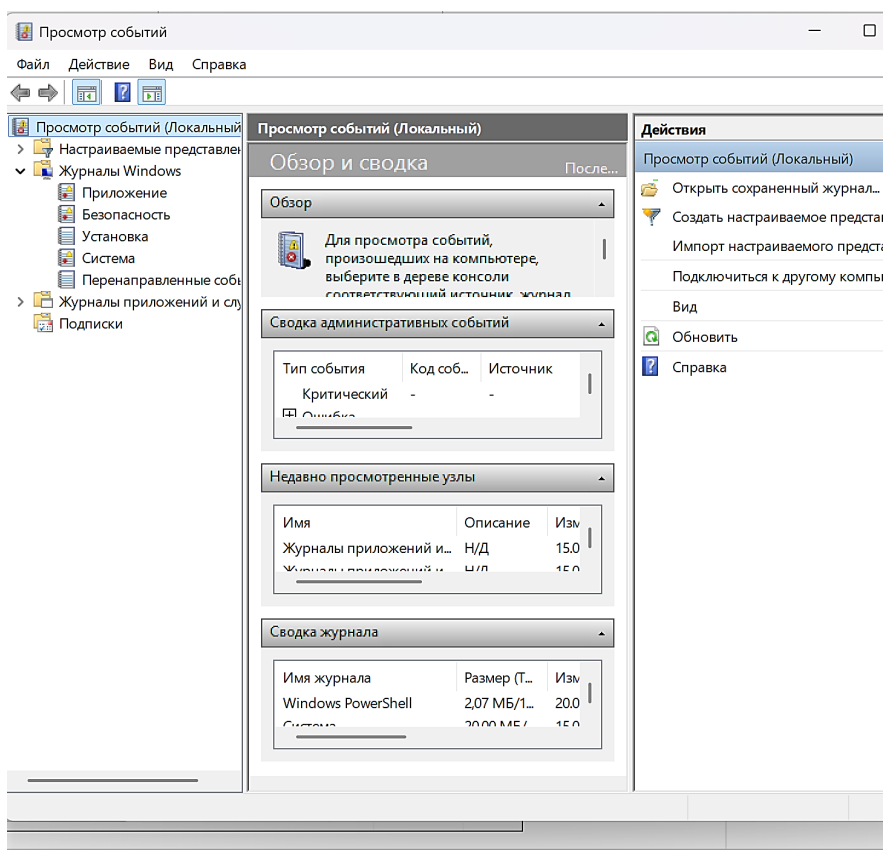


Рис. 2. Окно просмотра событий ОС Windows

Все записи из журнала событий хранятся в реестре событий HKLM. В нем находятся три различных журнала, отвечающие за журналы приложений, безопасности и системы. Они являются базовыми, однако у пользователей есть возможность создавать дополнительные журналы.

3. Служебные каталоги. Каталог — объект в файловой системе, упрощающий организацию файлов. Типичная файловая система содержит большое количество файлов, и каталоги помогают упорядочить ее путем их группировки [5]. Существует два типа каталогов: системный (служебный) и пользовательский. Рассмотрим некоторые служебные каталоги и их содержимое:

– каталог Program Files (рис. 3) содержит папки с программами, установленными как в процессе инсталляции Windows, так и пользователями компьютера. Для каждой программы отведена отдельная папка;

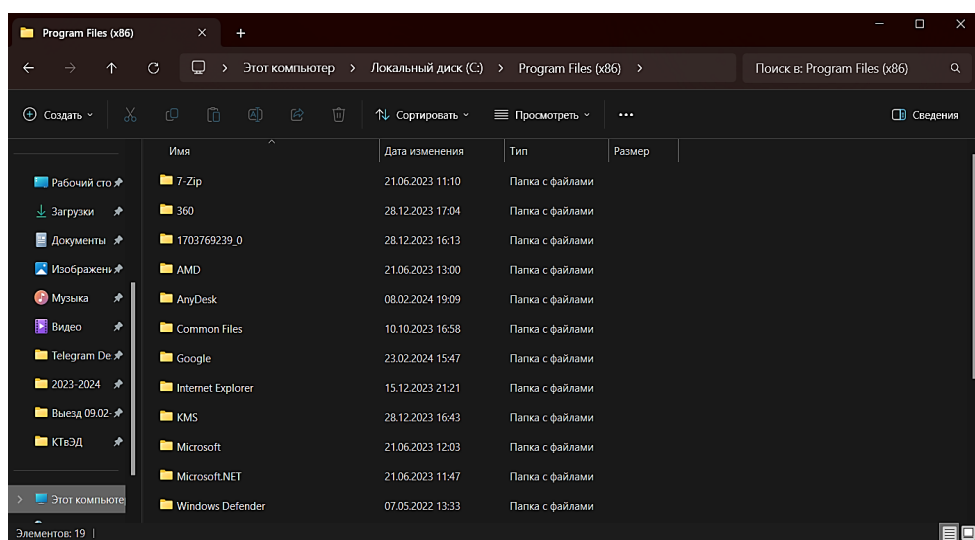


Рис. 3. Окно проводника, содержащее каталог Program Files

– каталог Windows (рис. 4) содержит все исполняемые файлы операционной системы, драйвера, модули и пр.;

– каталог «Пользователи» (рис. 5) содержит профили пользователей;

– каталог ProgramData (рис. 6) содержит установленные данные, установочные файлы приложений;

– каталог Recovery (рис. 7) содержит образ, необходимый для входа в среду восстановления;

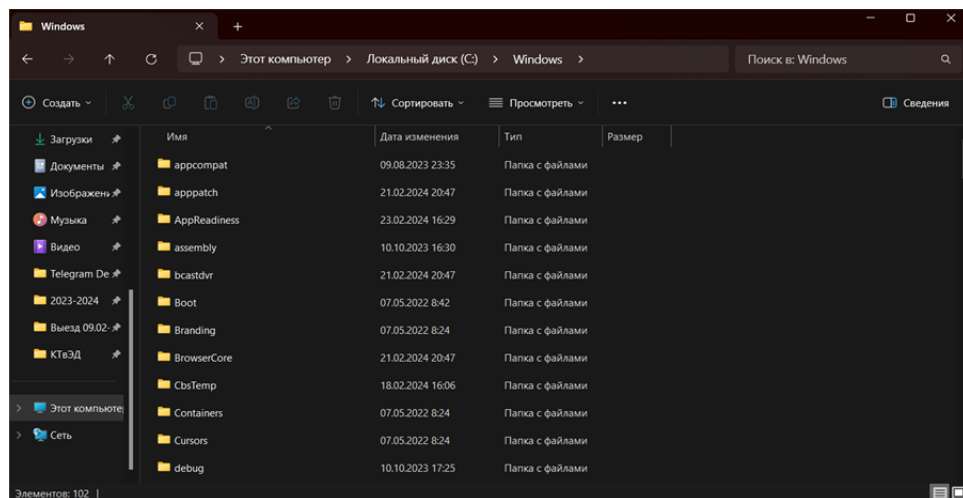


Рис. 4. Окно проводника, содержащее каталог Windows

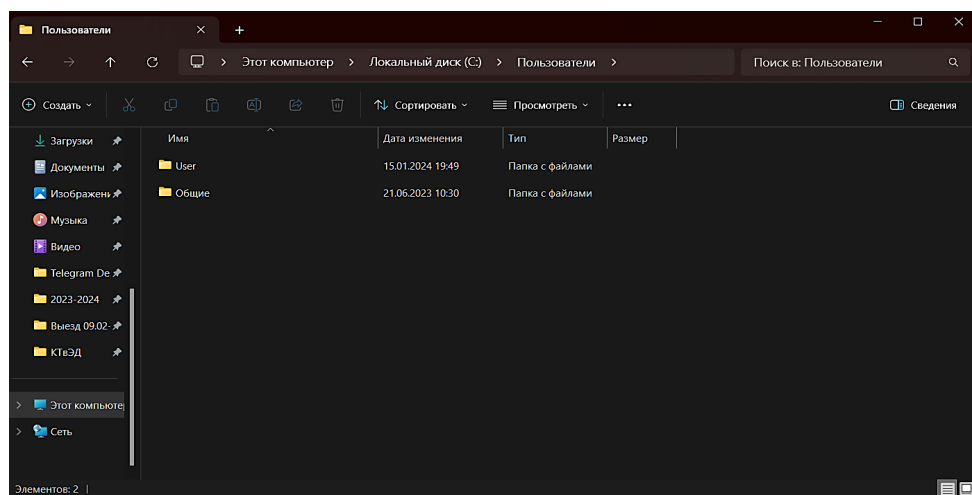


Рис. 5. Окно проводника, содержащее каталог «Пользователи»

Далее необходимо рассмотреть ПО для поиска и исследования криминалистически значимой информации из перечисленных компонентов ОС Windows:

– Windows Registry Recovery (рис. 8) — утилита для просмотра файлов реестра ОС Windows, содержимое открытого файла отображается в виде стандартного оформления программы RegEdit;

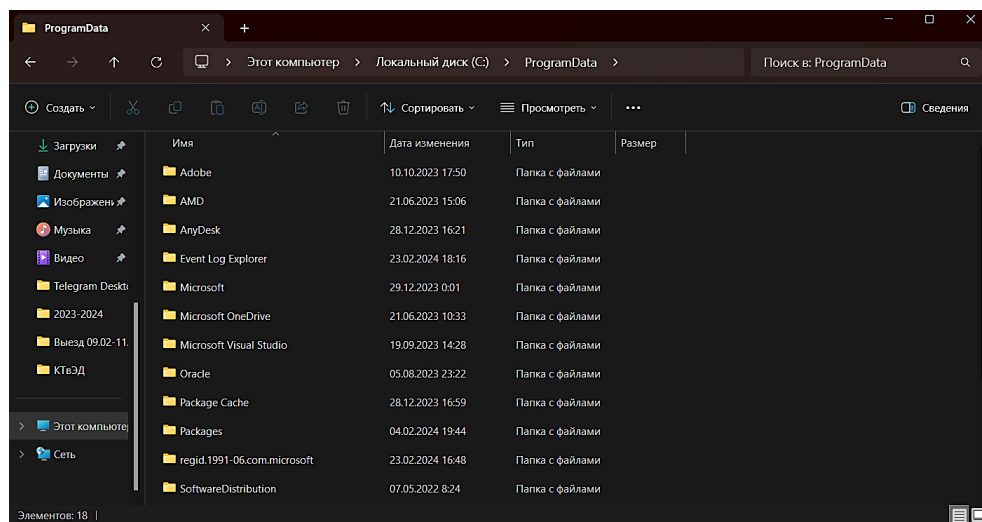


Рис. 6. Окно проводника, содержащее каталог ProgramData

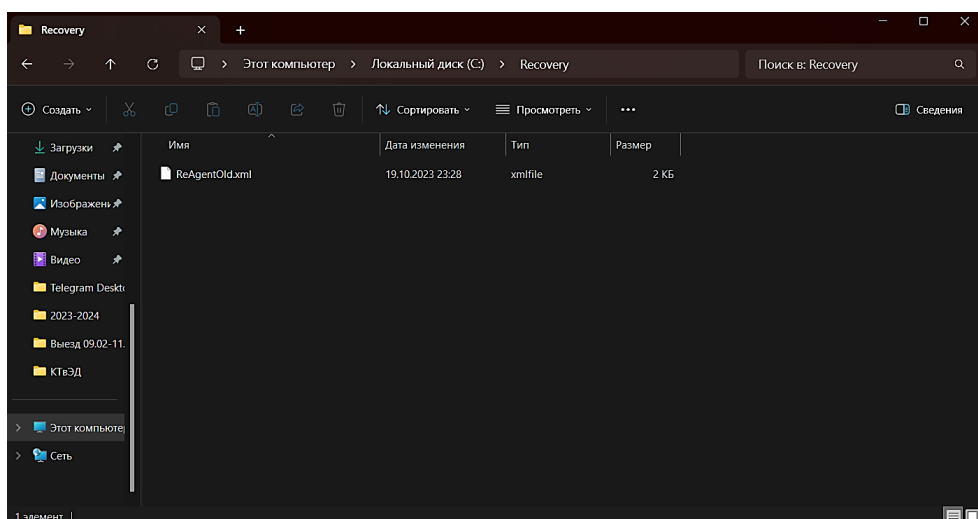


Рис. 7. Окно проводника, содержащее каталог Recovery

– Hetman Partition Recovery (рис. 9). Данная утилита позволяет восстановить удаленную историю браузера [6]. Все, что необходимо, — это знать, где в служебных каталогах находится файл истории браузера, историю которого необходимо восстановить;

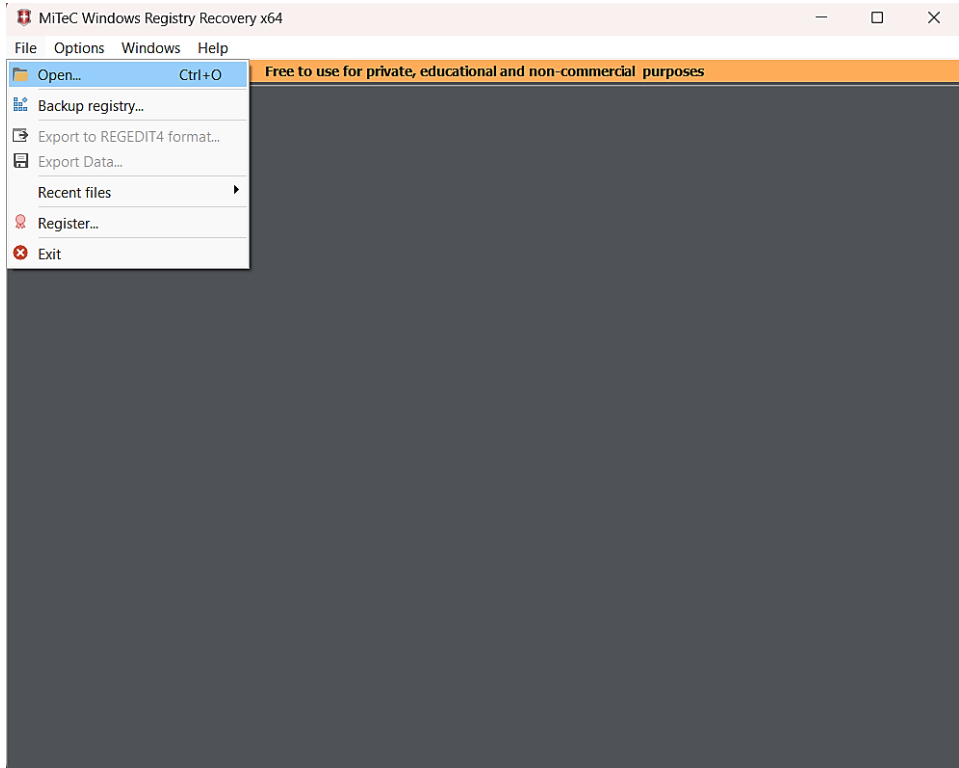


Рис. 8. Окно программы Windows Registry Recovery

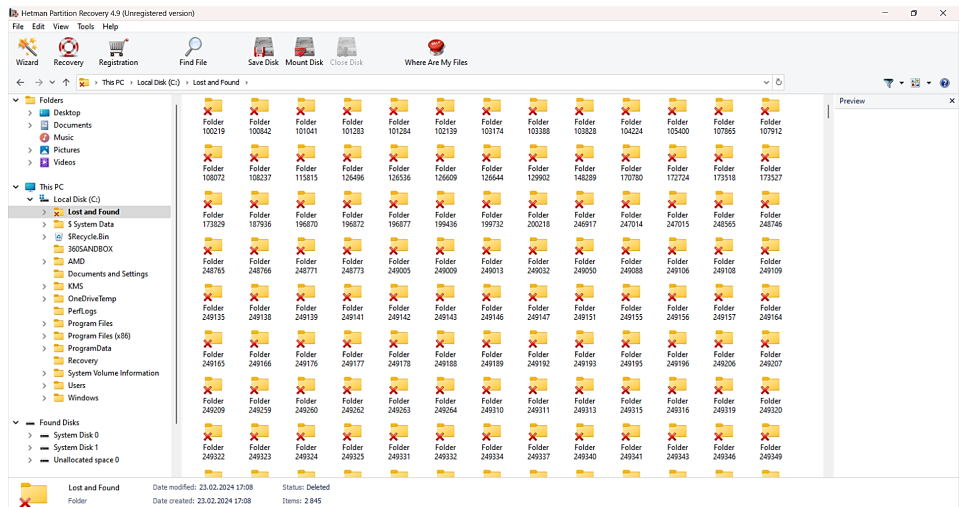


Рис. 9. Окно программы Hetman Partition Recovery

– поисковая утилита AVSearch (рис. 10). Благодаря данной утилите можно найти файлы форматов TXT, HTML, RTF, архивных и бинарных файлов по конкретным словам или словосочетаниям [7];

– Event Log Explorer — это эффективное средство для просмотра и анализа событий, хранящихся в журналах ОС семейства Microsoft Windows (рис. 11). Утилита позволяет существенно ускорить и упростить решение задач анализа журналов событий, таких как журнал безопасности, журнал приложений, журнал системы, журнал установки и др. [8];

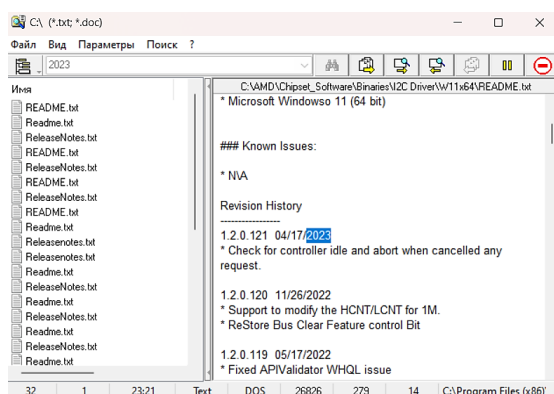


Рис. 10. Окно утилиты AVSearch

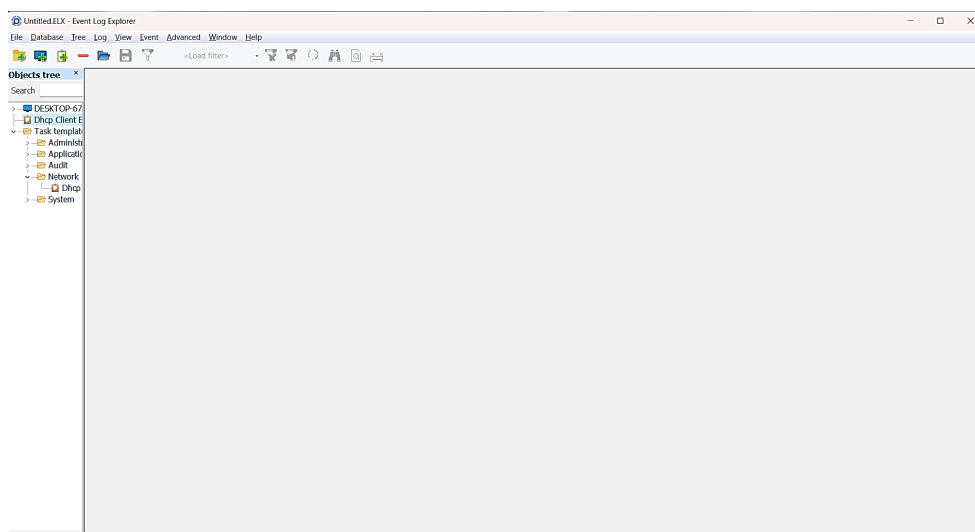


Рис. 11. Окно программы Event Log Explorer

– Bulk_extractor. Благодаря данной утилите можно извлекать из устройства адреса электронной почты, номера телефонов и кредитных карт, определять местоположение (рис. 12) [9].

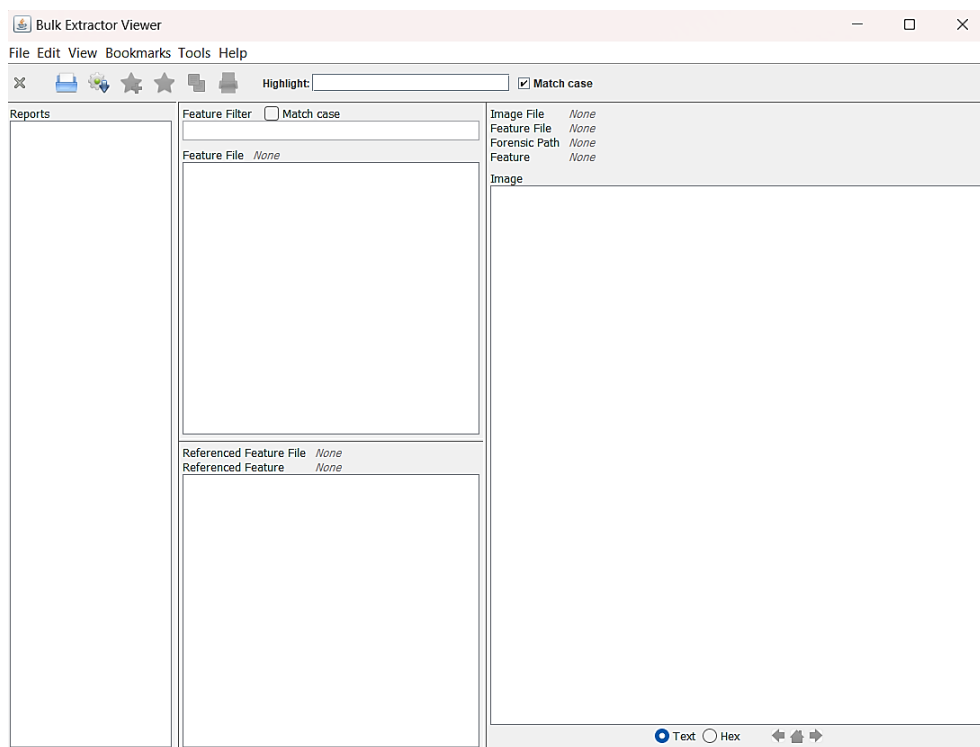


Рис. 12. Окно утилиты bulk_extractor

Закключение. На данный момент компьютерно-техническая экспертиза стоит в самом начале своего развития. Но даже несмотря на это существуют разнообразные программы, которые могут помочь эксперту в его работе. Некоторые из них были рассмотрены в данной статье, но это лишь малая часть того, что существует на данный момент. Зная, где и что искать, а также то, какие программы могут в этом помочь, эксперт сможет быстро и качественно выполнять свою работу, не тратя время на просмотривание данных вручную. Но всегда стоит помнить, что одна программа не гарантирует точный результат — поэтому каждому судебному эксперту следует разбираться как минимум в нескольких программах, нацеленных на поиск конкретных данных, чтобы в итоге получать полную и достоверную информацию.

Литература

- [1] *Компьютерно-техническая экспертиза*. URL: <http://www.sudexpert.ru/possib/comp.php> (дата обращения 09.04.2024).
- [2] *Microsoft. Сведения о реестре Windows для опытных пользователей*. URL: <https://learn.microsoft.com/ru-ru/troubleshoot/windows-server/performance/windows-registry-advanced-users> (дата обращения 09.04.2024).
- [3] Карлова А.В. Установление обстоятельств работы с USB-устройствами в операционной системе Windows. *Политехнический молодежный журнал*, 2019, № 4(33). URL: <https://ptsj.bmstu.ru/articles/465/465.pdf> (дата обращения 09.04.2024).
- [4] *Обзор Просмотра событий операционной системы Windows 7*. URL: <https://acerfans.ru/faq/1317-obzor-prosmotra-sobytij-operacionnoj-sistemy> (дата обращения 09.04.2024).
- [5] *Основные каталоги Windows и их структура*. URL: <https://windowso.ru/articles/osnovnye-katalogi-windows-i-ih-struktura> (дата обращения 09.04.2024).
- [6] *Microsoft. Просмотр или удаление содержимого журнала браузера в Microsoft Edge*. URL: <https://support.microsoft.com/ru-ru/microsoft-edge/просмотр-или-удаление-содержимого-журнала-браузера-в-microsoft-edge-00cf7943-a9e1-975a-a33d-ac10ce454ca4> (дата обращения 09.04.2024).
- [7] *Утилиты для поиска информации на компьютере*. URL: https://fcenter.ru/online/hardarticles/utilities/7332-Utility_dlya_poiska_informacii_na_komp_jutere (дата обращения 09.04.2024).
- [8] *15 лучших компьютерных (цифровых) инструментов и программного обеспечения для криминалистики в 2024 году*. URL: <https://www.guru99.com/ru/computer-forensics-tools.html> (дата обращения 09.04.2024).
- [9] *15 лучших и бесплатных инструментов компьютерного криминалиста*. URL: <https://habr.com/ru/companies/tomhunter/articles/660773/> (дата обращения 09.04.2024).

Поступила в редакцию 06.02.2026

Караваева Анастасия Владимировна — старший преподаватель кафедры «Безопасность в цифровом мире», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Извальцева Ева Витальевна — студентка кафедры «Безопасность в цифровом мире», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Ссылку на эту статью просим оформлять следующим образом:

Караваева А.В., Извальцева Е.В. Криминалистически значимая информация в операционной системе Windows. *Политехнический молодежный журнал*, 2026, № 04(105). URL: <https://ptsj.bmstu.ru/catalog/jur/crim/1120.html>

FORENSICALLY SIGNIFICANT INFORMATION IN WINDOWS OS

A.V. Karavaeva

karlova_av@bmstu.ru

SPIN-code: 8696-6670

E.V. Izvaltseva

izvaltsevaev@student.bmstu.ru

SPIN-code: 9956-4150

Bauman Moscow State Technical University, Moscow, Russian Federation

This article considers the components of the Windows operating system that may contain important information for the work of a digital forensics expert and provides examples of software that simplifies the search for information required by an expert. Since technology-related crimes are reaching a new level, specialists in this field must promptly identify information that can help solve a case. The article shows methods for studying the contents of operating system components using built-in system tools. It also presents utilities that help automate the process of searching for information on a computer and shows their interfaces. Verifying information with a single program does not guarantee the reliability and completeness of the data obtained. Therefore, an expert in the field of computer forensics should be able to use several programs and utilities.

Keywords: forensic analysis, Windows OS, Windows Registry, Windows Event Log, system directories

Received 06.02.2026

Karavaeva A.V. — Senior Lecturer, Department of Security in the Digital World, Bauman Moscow State Technical University, Moscow, Russian Federation.

Izvaltseva E.V. — Student, Department of Security in the Digital World, Bauman Moscow State Technical University, Moscow, Russian Federation.

Please cite this article in English as:

Karavaeva A.V., Izvaltseva E.V. Forensically significant information in Windows OS. *Politekhnicheskii molodezhnyy zhurnal*, 2026, no. 04(105). (In Russ.). URL: <https://ptsj.bmstu.ru/catalog/jur/crim/1120.html>