**ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ**

**«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ**

**Студенттер мен жас ғалымдардың**
# «ǴYLYM JÁNE BILIM - 2024»
**XIX Халықаралық ғылыми конференциясының**
**БАЯНДАМАЛАР ЖИНАҒЫ**

**СБОРНИК МАТЕРИАЛОВ**
**XIX Международной научной конференции**
**студентов и молодых ученых**
# «ǴYLYM JÁNE BILIM - 2024»

**PROCEEDINGS**
**of the XIX International Scientific Conference**
**for students and young scholars**
# «ǴYLYM JÁNE BILIM - 2024»

**2024**
**Астана**

**УДК 001**
**ББК 72**
**G99**

**«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.**

**ISBN 978-601-7697-07-5**

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

**УДК 001**
**ББК 72**
**G99**

**ISBN 978-601-7697-07-5**

3. 2020-2021 жылдардағы веб-қосымшалардың осалдықтары мен қауіптері , www.ptsecurity.com – 2022. - https://www.ptsecurity.com/ru-ru/research/analytics/web-vulnerabilities-2020-2021/
4. Хабр. [SIEM: жиі қойылатын сұрақтарға жауаптар]. [Электрондық ресурс]. Кіру режимі: https://habrahabr.ru/post/172389
5. Securitylab. [SIEM дегеніміз не?]. [Электрондық ресурс]. Кіру режимі: http://www.securitylab.ru/analytics/430777.php

УДК 004.056.5

## ИСПОЛЬЗОВАНИЕ МЕТОДОВ И ИНСТРУМЕНТОВ ЦИФРОВОЙ КРИМИНАЛИСТИКИ ДЛЯ ВОССТАНОВЛЕНИЯ ПОТЕРЯННЫХ ДАННЫХ

**Балташева Назерке Төлегенқызы**
Nazerke2810@gmail.com,
студент III курса образовательной программы 6B06306 «Системы информационной безопасности», Евразийский национальный университет им. Л.Н. Гумилева
**Баж Мансия Уразбайқызы**
mansiya.orz@gmail.com
студент III курса образовательной программы 6B06306 «Системы информационной безопасности», Евразийский национальный университет им. Л.Н. Гумилева
Научный руководитель Аймичева Гаухар Ислямовна

В эпоху цифровизации обеспечение целостности данных является одной из актуальных задач. Зачастую необходимые файлы могут быть удалены с компьютера или USB-носителя, как случайно, так и злоумышленно. Это особенно актуально в образовательной среде, где как обучающиеся, так и преподаватели могут столкнуться с потерей важных данных. По результатам проведенного опроса среди участников академической среды 80% респондентов сталкивались с необходимостью восстановления удаленных данных (рис.1). И всего лишь около 20% смогли восстановить удаленные файлы с использованием специального инструментария (рис.2). Предположительно это студенты, изучавшие инструменты криминалистического анализа, участвовавших также в опросе. В связи с этим, рассмотрение методов и инструментов восстановления потерянных данных, рассматриваемых в данной статье, является актуальным для участников образовательной среды и других пользователей цифровых устройств.

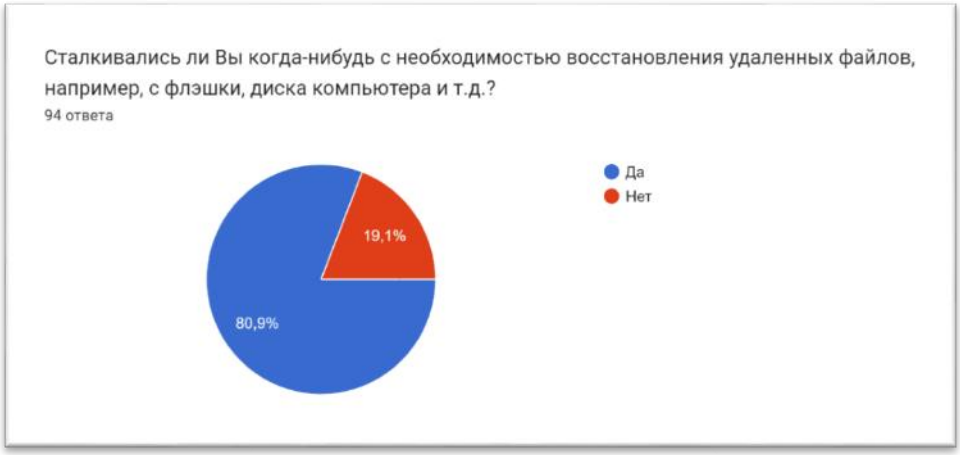



Рисунок 1. Результаты опроса 94-х респондентов на предмет выяснения факта необходимости восстановления удаленных данных


Рисунок 2. Результат опроса 94-х респондентов для выяснения «Смогли ли восстановить удаленные данные?»

По данным отчета SciVal международной библиометрической платформы Scopus за 2020 – 2023 гг. проблеме восстановления данных посвящены публикации 32 стран мира, среди которых США, Малайзия, Иран, Китай, Ирак, Индия, Саудовская Аравия, ОАЭ и др. страны, однако Казахстана в этом списке нет (рис. 3).

| | Countries/Regions | Scholarly Output | Views Count | Field-Weighted Citation Impact | Citation Count |
|---|---|---|---|---|---|
| 1. | United States | 18 | 153 | 1.20 | 69 |
| 2. | Malaysia | 11 | 276 | 1.73 | 42 |
| 3. | Iran | 9 | 95 | 0.32 | 25 |
| 4. | China | 8 | 112 | 0.58 | 7 |
| 5. | Iraq | 7 | 127 | 1.48 | 15 |
| 6. | India | 4 | 48 | 1.73 | 4 |
| 7. | Saudi Arabia | 4 | 78 | 1.32 | 9 |
| 8. | United Arab Emirates | 4 | 113 | 1.42 | 14 |
| 9. | Hong Kong | 3 | 19 | 2.00 | 2 |
| 10. | Indonesia | 3 | 70 | 2.78 | 7 |
| 11. | Russian Federation | 3 | 20 | 0.18 | 1 |
| 12. | Singapore | 3 | 19 | 2.00 | 2 |

Рисунок 3. Количество публикаций в разрезе стран (источник Scopus, 2020-2023гг.)

Известно, что удаленные данные можно восстановить в случае если кластер, в котором был записан файл не перезаписан новыми данными [1,2]. Выбор метода восстановления файлов зависит от наличия метаданных [3,4]. В случае если метаданные не уничтожены, то удаленный файлы можно восстановить с помощью инструментов AutoPsy, PhotoRec, бибилиотеки The Sleuth Kit и других специальных утилит. В случае же, если метаданные файла специально удалены или файлы повреждены, и файлы нельзя восстановить стандартным способом, то используется методика Carving files, согласно которой файл восстанавливается с помощью сигнатур в заголовке или конце файла, в этом случае потребуются инструменты для чтения шестнадцатеричного кода файлов Hexinator или специальные инструменты Foremost, Scalpel и др. [3,4,5].

Рассмотрим процесс восстановления файлов для стандартного случая, когда метаданные файлов не уничтожены и файлы не повреждены, а всего лишь удалены с диска или флэш-носителя.

*Структура файловых систем*. Флеш-накопители используют файловые системы для организации и хранения данных. Одной из наиболее распространенных файловых систем для флеш-накопителей является FAT (File Allocation Table) или его более новая версия, exFAT. Файловая система FAT состоит из таблицы файловой системы (File Allocation Table), каталога корневого каталога (Root Directory) и кластеров данных (Data Clusters). Каждый файл на флеш-

накопителе имеет запись в таблице файловой системы, указывающую на его расположение на носителе [2,3].

*Удаление файлов с USB-носителя.* Ключевым моментом является понимание того, что файлы, удаленные с USB-носителя, не удаляются навсегда. При удалении файла с флеш-накопителя, операционная система помечает соответствующую запись в таблице файловой системы как "удаленную", но не удаляет непосредственно данные файла с носителя. Это означает, что фактически данные остаются на носителе, пока они не будут перезаписаны другими данными [3,4].

*Алгоритм восстановления удаленных файлов.* В первую очередь необходимо создать образ USB-носителя. Это позволит работать с копией информации без риска повредить оригинальные файлы. Для создания образа носителя можно использовать специализированные программы, такие как FTK Imager, Autopsy, которые представляют собой мощные системы цифровой криминалистики, позволяющие автоматически анализировать образы носителей и находить утерянные данные. После того как создан образ можно приступить к его анализу и восстановлению удаленных файлов.

Рассмотрим детально процедуру создания образа носителя и восстановления файлов с помощью инструмента Autopsy.

**1-шаг.** Выбор типа источника доказательств (Source Evidence Type)

В главном меню выбираем команду Add data source, после чего в диалоговом окне Select Source из списка доступных типов источников доказательств выбираем "Physical Drive" потому, что мы работаем с физическим USB-накопителем, а не с логическим диском, образом файла или содержимым папки (рис. 4).

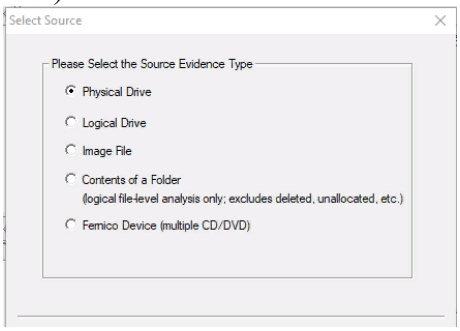



Рисунок 4. Выбор типа источника доказательств

**2-шаг.** Выбор источника диска (Source Drive Selection)

На втором шаге указываем наш USB-накопитель, с которого мы хотим создать образ (рис. 5).

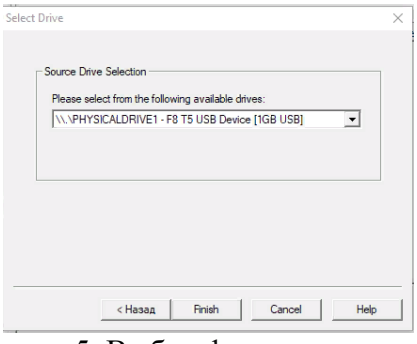



Рисунок 5. Выбор физического диска

**3-шаг.** Выбор типа образа (Destination Image Type)

На следующем шаге нам представлен список доступных типов образа: Raw (dd), SMART, E01, AFF. Мы выбрали тип "Raw (dd)" (рис. 6), поскольку этот формат обеспечивает полный и точный образ всего содержимого диска, включая неиспользуемое пространство и удаленные файлы.

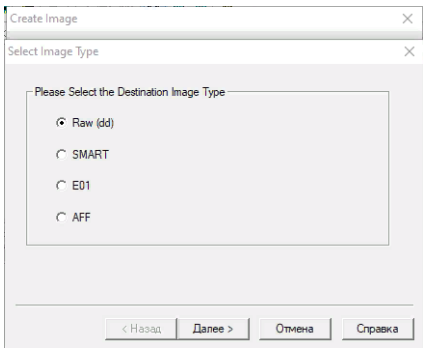


Рисунок 6. Выбор тип образа

**4-шаг.** Вывод информации о результате создания образа

После выбора источника и типа образа начался процесс создания образа. Выводится информация о процессе, включая прогресс, затраченное время и оценку времени до завершения (рис. 7).

*В поле Destination (Путь назначения)* указан путь к месту, где был сохранен созданный образ. В данном случае, образ был сохранен в папку C:\Users\mansi\Desktop\FTK\usb_image.

*Поле Status (Статус)* показывает, что образ был создан успешно.

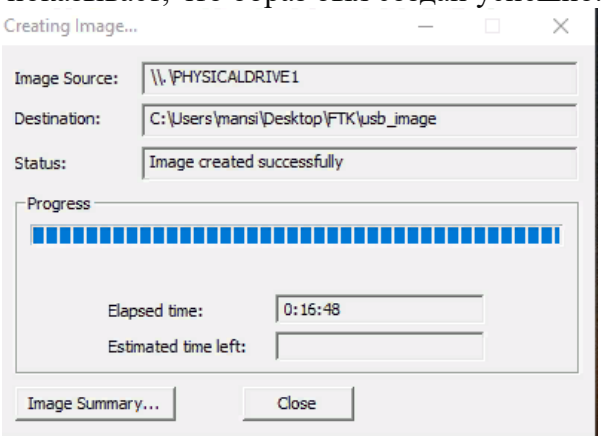


Рисунок 7. Завершение создания образа в «AutoPsy»

**5-шаг.** Восстановление удаленного файла

После выбора в программе Autopsy созданного нами образа открывается окно с его полным содержимым. Autopsy определяет удаленные файлы и отображает их список в папке Deleted files с указанием метаданных, таких как имя файла, размер, дата удаления и другие параметры.

Мы решили восстановить текстовый документ «документ1.docx» (рис. 8). Для восстановления выбранного файла необходимо выполнить следующие действия:

1. Выбираем файл "документ1.docx" из списка удаленных файлов.
2. Нажимаем правой кнопкой мыши на выбранный файл, чтобы открыть контекстное меню.
3. В контекстном меню выбираем пункт "Extract File(s)".
4. Указываем место для сохранения восстановленного файла. Рекомендуется выбрать другой носитель данных или диск, чтобы избежать перезаписи данных.
5. После завершения процесса восстановления проверяем полученный файл на целостность и правильность восстановления.

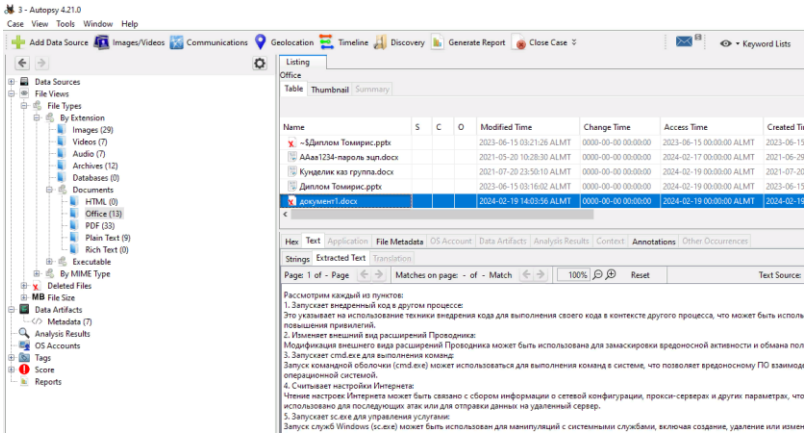
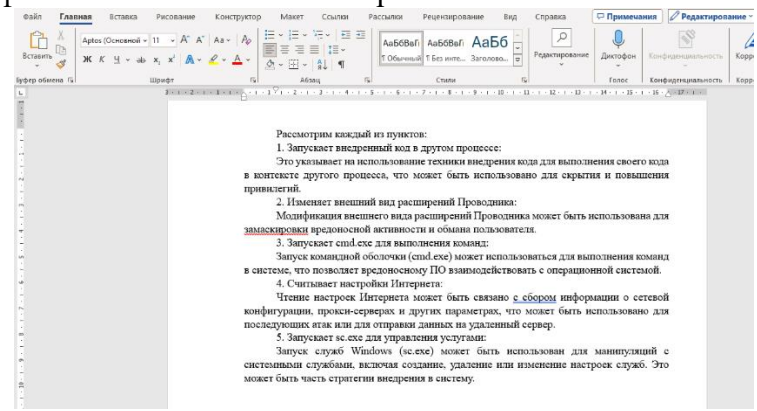


Рисунок 8. Список удаленных файлов и их метаданные

**6-шаг.** Отображение содержимого восстановленного файла

После выполненных шагов можно открыть восстановленный файл из папки, указанной при сохранении файла. На рисунке 9 показан результат восстановления удаленного файла «документ1.docx». Содержимое восстановленного файла проверяем в программе Microsoft Word. Мы видим, что файл восстановлен без потерь.



Рассмотрим каждый из пунктов:

1. Запускает внедренный код в другом процессе:

Это указывает на использование техники внедрения кода для выполнения своего кода в контексте другого процесса, что может быть использовано для скрытия и повышения привилегий.

2. Изменяет внешний вид расширений Проводника:

Модификация внешнего вида расширений Проводника может быть использована для замаскировки вредоносной активности и обмана пользователя.

3. Запускает cmd.exe для выполнения команд:

Запуск командной оболочки (cmd.exe) может использоваться для выполнения команд в системе, что позволяет вредоносному ПО взаимодействовать с операционной системой.

4. Считывает настройки Интернета:

Чтение настроек Интернета может быть связано с сбором информации о сетевой конфигурации, прокси-серверах и других параметрах, что может быть использовано для последующих атак или для отправки данных на удаленный сервер.

5. Запускает sc.exe для управления услугами:

Запуск служб Windows (sc.exe) может быть использован для манипуляций с системными службами, включая создание, удаление или изменение настроек служб. Это может быть часть стратегии внедрения в систему.

Рисунок 9. Содержимое восстановленного файла «документ1.docx».

В заключении работы хотелось подчеркнуть практический результат восстановления удаленных файлов в классической ситуации, когда не уничтожены метаданные, что имеет место при обычном удалении файлов. В частности, с помощью инструмента Autopsy нам удалось эффективно восстановить удаленный документ с USB-носителя. Этот опыт подтверждает, что использование специализированных инструментов восстановления данных, таких как Autopsy и другие инструменты имеет большое значение для обеспечения безопасности и сохранности важных учебных материалов и проектов в образовательной среде. Считаем, что данная работа будет полезна для всех участников академической среды.

## Список использованных источников


1. W. Xu, L. Deng, and D. Xu, "Towards Designing Shared Digital Forensics Instructional Materials," in *Proceeding of the 46st Annual International Computer Software and Applications Conference (COMPSAC 2022),* pp. 117-122, July 2022.
2. Fairbanks K. D. An analysis of Ext4 for digital forensics //Digital investigation. – 2012. – Т. 9. – С. S118-S130.
3. Easttom C. Digital Forensics, Investigation, and Response. – Jones & Bartlett Learning, 2021.
4. Digital Forensics Essentials. EC-Council official curricula. EC-Council, 2021
5. Nikkel B. Practical Linux Forensics: A Guide for Digital Investigators. – no starch Press, 2021.