

O'ZBEKISTON RESPUBLIKASI
OLIIY TA'LIM, FAN VA INNOVATSIYALAR VAZIRLIGI
FARG'ONA DAVLAT UNIVERSITETI

**FarDU.
ILMIY
XABARLAR**

1995-yildan nashr etiladi
Yilda 6 marta chiqadi

3-2024

**НАУЧНЫЙ
ВЕСТНИК.
ФерГУ**

Издаётся с 1995 года
Выходит 6 раз в год

N.N.Tashatov, M.K.Onarkulov, Askarbekkizi Akbota Axborot xavfsizligi xavflarini tahlil qilish va baholash usullari	7
G.S.Uzoqova, J.N.Xo'jamberdiyeva Fizika ta'limida o'quv-tadqiqot faoliyatini shakllantirish tamoyillari	12
B.K.Abduraimova, Sh.A.Ro'zaliyev, Kayrat Dinara Kayratkizi Axborot xavfsizligini tekshirish usullarini tahlil qilish	19
N.N.Tashatov, Orazymbetova Aidana Zhandoskyzy, I.N.Tojimatov Ma'lumotlarni yaxlitligi buzilishi xavfining matematik modellari	24
Sh.A.Yuldashev, R.T.To'lanova Xalkogenid yupqa pardalarining mikroparametrlarini aniqlash.....	30
K.O.Rakhimov, Z.X.Mamatova, Tazhikenova Nurzhanar Kabikenkizi Common phishing attacks in Kazakhstan and ways to protect citizens from internet scammers	37
K.O.Рахимов, К.Б.Буланов, Ш.М.Ибрагимов Изучение эффективности инструментов с открытым исходным кодом для восстановления нетрадиционно удаленных данных	43
K.O.Рахимов, M.K.Онаркулов, Д.Б.Каримова Использование облачных технологий в анализе уязвимостей программного обеспечения	47
M.K.Онаркулов, Ш.А.Рузалиев, Камбар Нортилеу Сейтказиули Способы защиты информации от компьютерных вирусов	52

A.B.Yulchiev, Sh.Yuldashev, I.R.Askarov Development of the oil base of cream-perfumed soaps with the help of blended oil compositions	61
M.I.Payg'amova, G'M.Ochilov Uglerodli xomashyolar asosida ko'mir adsorbentlar olish va ularning fizik-kimyoviy xossalari	67
S.A.Mamatkulova, I.R.Askarov Studying the flavonoid composition of the biological supplement of anice and cilorant.....	72
D.G'.Xamidov, S.F.Fozilov, M.Y.Ismoilov, M.Q.To'raqulova Gossipol qatroni asosida olingan surkov materialining sifat ko'rsatkichlari	76
S.A.Mamatkulova, T.E.Usmanova, I.R.Askarov Determination of the amount of flavonoids in paulownia and rosmarinus plant leaves	82
Д.А.Мансуров, А.Х.Хаитбаев, Х.Х.Хайитбоэв, Д.Г.Омонов, Ш.Ш.Тургунбоев Изучение биологической активности цитраля с помощью методов виртуального скрининга	85
З.А.Хамракулов Агрохимическая эффективность хлора кальций – магниевое дефолианта	92
A.A.Ibroximov, N.B.Ibroximova, I.J.Jalolov Oqchangal (<i>Nitraria sp</i>) o'simligining bargi va urug'i makro va mikroelement tarkibini ICP-MS usulida o'rganish.....	103
O.A.Abduhamidova, O.M.Nazarov Yerqalampir o'simligining makro va mikroelement tarkibini o'rganish	111
M.K.Saliyeva, O.E.Ziyadullayev, G.Q.Otamuxamedova Molekulasida geteroatom saqlagan atsetilen spirtlari ishtirokida murakkab efirlar sintezi	118
D.T.Khasanova, I.R.Askarov, A.B.Yulchiev Production of yogurt on the basis of expressed wheat malt.....	124



UO'K: 343.98.064

**AN'ANAVIY BO'LMAGAN O'CHIRILGAN MA'LUMOTLARNI TIKLASH UCHUN OCHIQ
MANBALI VOSITALARNING SAMARADORLIGINI O'RGANISH****ИЗУЧЕНИЕ ЭФФЕКТИВНОСТИ ИНСТРУМЕНТОВ С ОТКРЫТЫМ ИСХОДНЫМ
КОДОМ ДЛЯ ВОССТАНОВЛЕНИЯ НЕТРАДИЦИОННО УДАЛЕННЫХ ДАННЫХ****EXPLORING THE EFFICIENCY OF OPEN-SOURCE TOOLS IN RETRIEVING
UNCONVENTIONAL DELETED DATA****Raximov Quvvatali Ortikovich¹** ¹Farg'ona davlat universiteti, t.f.b.f.d., (PhD)**Bulanov Kaldijan Baurjanovich²**²Evrosiyo milliy universiteti, Qozog'iston, magistrant**Ibragimov Shavkat Ma'mirovich³**³Farg'ona davlat universiteti, katta o'qituvchi**Annotatsiya**

Raqamli ma'lumotlarni qayta yozish raqamli muhitda dalillarni yo'q qilishni anglatadi. Hozirgi vaqtda kompyuter foydalanuvchilarining katta qismi o'chirilgandan so'ng ularning fayllarini tiklash xavfi haqida xabardor. Natijada, ular ko'pincha keraksiz qidiruvlarni oldini olish uchun ularni o'chirishdan ko'ra, fayllarni qayta yozishni afzal ko'rishadi. An'anaviy bo'lmagan usullar bilan o'chirilgan ma'lumotlarni muvaffaqiyatli tiklashga qodir bo'lgan maxsus vositalar mavjudligiga qaramay, ushbu vositalardan foydalanish qimmatga tushmoqda va malakali texnik xodimlarni talab qiladi. Raqamli dalillar spektrini turli senariylarda samarali boshqarish uchun faqat bitta texnologiya yoki metodologiyaga tayanmasdan, keng ko'lamli vositalardan foydalanish kerak. Ushbu maqolada raqamli ma'lumotlarni o'chirish uchun noan'anaviy usullardan foydalanish ma'lumotlarni yo'q qilishning samarali usuli ekanligini isbotlandi. Ushbu tadqiqotning asosiy maqsadi noan'anaviy yondashuvlar yordamida o'chirilgan ma'lumotlarni tiklashda ochiq manbali vositalarning samaradorligini baholashdir.

Аннотация

Перезапись цифровых данных - это процесс устранения улик в цифровой среде. Многие пользователи компьютеров теперь знают о рисках, связанных с восстановлением своих файлов после их удаления. В результате они предпочитают перезаписывать свои файлы, а не просто удалять их, чтобы предотвратить нежелательный поиск. Хотя существуют специализированные инструменты, которые могут успешно восстанавливать данные, удаленные нетрадиционными методами, они являются дорогостоящими и требуют квалифицированного технического персонала. Для эффективного управления цифровыми доказательствами в различных сценариях важно использовать различные инструменты, а не полагаться только на одну технологию или метод. Это исследование показало, что использование нетрадиционных методов удаления цифровых данных может быть эффективным способом уничтожения данных. Целью этого исследования была оценка эффективности инструментов с открытым исходным кодом при восстановлении удаленных данных с помощью нетрадиционных методов.

Abstract

Digital data overwriting is the process of eliminating evidence in a digital environment. Many computer users are now aware of the risks associated with recovering their files after they have been deleted. As a result, they prefer to overwrite their files rather than simply delete them to prevent any unwanted searches. Although there are specialized tools available that can successfully recover data deleted using non-traditional methods, they are expensive and require skilled technical personnel. To effectively manage digital evidence in various scenarios, it is important to use a variety of tools instead of relying on just one technology or method. This study has shown that using non-traditional methods for deleting digital data can be an effective way to destroy data. The aim of this research was to assess the efficiency of open-source tools in retrieving deleted data through unconventional methods.

Kalit so'zlar: ochiq kodli dasturiy ta'minot, ma'lumotlarni tiklash, noan'anaviy ma'lumotlarni o'chirish, ma'lumotlar maxfiyligi, xavfsizlik.

Ключевые слова: программное обеспечение с открытым исходным кодом, восстановление данных, нетрадиционное удаление данных, конфиденциальность данных, безопасность.

Key words: open-source software, data recovery, unconventional data deletion, data privacy, security.

ВВЕДЕНИЕ

В современном информационном мире вопросы безопасности и конфиденциальности данных играют ключевую роль. Одним из аспектов, требующих особого внимания, является восстановление данных, удаленных в нетрадиционных способах. Отмечается, что многие пользователи компьютеров предпочитают перезаписывать данные, чем просто удалять их, с целью предотвращения возможного восстановления информации. Однако, несмотря на распространенность этой практики, существует недостаточно исследований, посвященных оценке эффективности инструмента с открытым исходным кодом для восстановления таких данных.

Цель настоящего исследования заключается в тщательном изучении эффективности применения программного обеспечения с открытым исходным кодом в процессе восстановления нетрадиционно удаленных данных. В частности, будет проанализирована способность такого программного обеспечения справиться с восстановлением данных, удаленных в различных способах, а также определены его преимущества и ограничения. Это исследование направлено на расширение наших знаний о возможностях и эффективности открытых инструментов в области восстановления данных, что может быть ценным для как бизнес-сферы, так и общества в целом.

МЕТОДЫ И СПОСОБЫ АНАЛИЗА

В ходе этого исследования инструменты с открытым исходным кодом были протестированы на возможность удаления файлов способами, которые обычно не используются обычными пользователями, такими как очистка носителя информации, удаление данных методом перезаписи и использование специализированного программного обеспечения для удаления данных. Методы, обычно используемые для удаления файлов или любых цифровых данных, содержащих ценную информацию, состоят либо из нажатия кнопки «удалить», либо из комбинации «SHIFT+DELETE».

Использованная техника и технологии:

1. Рабочая станция: Процессор - Core i5-8400, ОЗУ - 8 ГБ, Операционная система - Windows 10 Pro, Тип системы - 64-битная операционная система
2. Съёмный носитель информации: Kingston Data Travel 8 GB.
3. Гарантированная программа удаления: Программное обеспечение Гарант.

Для данного исследования был подготовлен уникальный набор данных, который ускорит процесс восстановления информации и поможет классифицировать продукты с открытым исходным кодом для восстановления данных, удаленных нестандартным способом. Известный набор данных включает общие типы файлов (а именно: pptx, xlsx, docx, pdf), как показано в таблице ниже.

Таблица 1

№	Имя файла	Расширения файла размер	Размер файла
1	Test	docx	1,44 КБ
2	Kaldyzhan	docx	13,8 КБ
3	АКТ	pdf	329КБ
4	Презентация	pptx	8МБ
5	Образец	xlsx	7,76КБ
6	ЗС	pdf	121КБ
7	Антивирус лиц	xlsx	5,21КБ
8	приказ	pdf	333КБ
9	Буланов	pptx	5,8МБ
10	БКБ	xlsx	114КБ

Таблица 1. Информация о файлах.

FIZIKA-TEKNIKA

Методология, использованная в этом исследовании, была разделена на четыре части. Они были обозначены как: период стирания, период перезаписи, период программного обеспечения, период восстановления.

Таблица 2

Режим удаления	Названия программы			
	Stellar Windows Recovery	Recuva	Pro Discover	Win- Hex
Традиционное удаление	10/10	10/10	10/10	5/10
Форматирования	10/10	7/10	10/10	5/10
Перезапись	0/10	0/10	0/10	0/10
Программа гарантированного удаления	0/10	0/10	0/10	3/10

Таблица 2. Таблица восстановления по режимам удаления.

В таблице 2 было обнаружено, что восстановление возможно с помощью различных программ, таких как Stellar Windows Recovery, Recuva, Pro Discover и Win-Hex. В соответствии с полученными результатами было обнаружено, что программы успешно восстановили данные, удаленные в ходе традиционного процесса удаления и очистки. Кроме того, было показано, что Pro Discover и Win-Hex не смогли восстановить полную информацию в течение традиционного периода удаления и форматирования.

Основываясь на этом исследовании, можно сделать вывод, что инструменты с открытым исходным кодом могут быть эффективно использованы в качестве инструмента предварительной проверки на более низком уровне исследования, поскольку они успешно определяют существование файла через его титульный файл, а также дату его создания и изменения. Было высказано предположение, что лучшим преимуществом внедрения таких инструментов в цифровую криминалистику в следственных целях является то, что это снижает нагрузку и обеспечивает высокий уровень отсрочки дел. Таким образом, можно сказать, что, хотя инструменты с открытым исходным кодом не могут восстанавливать данные во всех нестандартных ситуациях, они могут быть эффективно использованы по следующим причинам, отсутствие затрат на приобретение инструментов, можно загрузить с любой платформы с открытым исходным кодом, для работы с программным обеспечением не требуется специального обучения.

Таблица 3

Функция	Названия программы			
	Stellar Windows Recovery	Recuva	Pro Discover	Win- Hex
Традиционное удаление	+	+	+	+
Форматирования	+	+	+	+
Перезапись	-	-	-	-
Программа гарантированного удаления	-	-	-	+
Предварительный просмотр файла перед восстановлением.	+	-	+	+
Информация о файле (Размер, дата создания и дата изменения)	+	-	+	+
Специальные функции для облегчения работы	+	-	+	+
Наличие файла после удаления.	-	-	+	-

Таблица 3. Сравнительная таблица.

Следует отметить следующие результаты из таблицы 3. В контексте эффективности программного обеспечения для восстановления данных, Pro discover продемонстрировал выдающиеся результаты при восстановлении удаленных данных с использованием различных инструментов и методов.

Преимущества использования этого инструмента от других могут быть как удаленные файлы были восстановлены в максимальном состоянии, точная информация о файле была получена из используемого набора тестовых данных, позволяет проводнику открывать и проверять файл перед его восстановлением и в тех случаях, когда файл не может быть восстановлен, он показал, что он существует в системе.

Win Hex можно рассматривать как эффективный инструмент восстановления, поскольку он продемонстрировал способность восстанавливать многие файлы в нестандартных ситуациях. Win Hex, будучи шестнадцатеричным редактором, позволяет исследователю видеть двоичные значения файла, но для этого требуется специальная подготовка.

Программное обеспечение для восстановления с открытым исходным кодом, в частности, Stellar Windows Recovery, Recuva, Pro-Discover и WinHex, рассмотренное в настоящей исследовательской работе, продемонстрировало возможность восстановления удаленных данных.

ЗАКЛЮЧЕНИЕ

В заключении проведенного исследования отмечается, что анализ эффективности инструментов с открытым исходным кодом для восстановления нетрадиционно удаленных данных позволяет выделить несколько ключевых выводов. В частности, такие инструменты предоставляют широкий спектр возможностей для восстановления данных, что делает их привлекательными для различных задач. Однако, необходимо учитывать, что некоторые инструменты обладают более высокой скоростью и точностью восстановления данных, чем другие, что может иметь критическое значение в определенных ситуациях. Кроме того, важным фактором является активность сообщества разработчиков и поддержка инструментов, что обеспечивает быструю реакцию на обнаружение новых типов утерянных данных и обновления инструментов для их эффективного восстановления. В целом, изучение эффективности инструментов с открытым исходным кодом для восстановления нетрадиционно удаленных данных подчеркивает их значимость в области информационной безопасности и восстановления данных, однако для успешного применения таких инструментов необходимо учитывать их особенности и ограничения, а также иметь достаточный уровень знаний и навыков для их эффективного использования.

СПИСОК ЛИТЕРАТУРЫ:

1. Sansurooah, K, Hope, H, Almutairi, H, Alnazawi, F and Jiang, Y, (2013), "An investigation into the efficiency of forensic data erasure tools for removable usb flash memory storage devices", originally published in the Proceedings of the 11th Australian Digital Forensics Conference.
2. Singh, Gurpreet, and Puneet Garg. "Digital forensics investigation using open-source tools: A survey." *Computers & Electrical Engineering* 87 (2020): 106780.
3. Sattar, Atif, et al. "Digital forensic analysis of Internet of Things (IoT): A systematic literature review." *Journal of Network and Computer Applications* 187 (2021): 102942.
4. Chow, Kam-Pui, and Sujeet Sheno. "Cyber forensics." 2020.
5. Форензика. Теория и практика расследования киберпреступлений | Шелупанов Александр Александрович, Смолина Анна 2022
6. Н. Н. Федотов. Форензика-компьютерлік криминалистика, 2007 г.