МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Кафедра Системы информационной безопасности

«ДОПУЩЕН К ЗАЩИТЕ»
Заведующий кафедрой
к.т.н. доцент Бердибаев Р.Ш.
(ученая степень, звание, Ф.И.О.)
_____ «___» _____2018 г.
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Метод гарантированного удаления данных в коммерческих банках

Специальность 5В100200 Системы информационной безопасности
Выполнил(а) Советтурсын Әсем Айдосқызы (Ф.И.О.) Группа СИБ-14-2
Научный руководитель профессор Ахметов Б.С.
(ученая степень, звание, Ф.И.О.)
_____ «31» 05 2018 г.
(подпись)
Рецензент: _____
(ученая степень, звание, Ф.И.О.)
_____ «____» _____2018 г.
(подпись)

Консультанты:
по экономической части:
Сомбаева Р.О. к.э.н., доцент
(ученая степень, звание, Ф.И.О.)
_____ «25» 05 2018 г.
(подпись)
по безопасности жизнедеятельности:
д.т.н. Бекбасаров Ш.Ш.
(ученая степень, звание, Ф.И.О.)
_____ «10» 05 2018 г.
(подпись)
по применению вычислительной техники:
проф. Ахметов Б.С.
(ученая степень, звание, Ф.И.О.)
_____ «31» 05 2018 г.
(подпись)
Нормоконтролер: ст.преп. Шкротунова Е.А.
(ученая степень, звание, Ф.И.О.)
_____ «31» мая 2018 г.
(подпись)

Алматы 2018

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Институт Систем управления и информационных технологий

Кафедра Системы информационной безопасности

Специальность Системы информационной безопасности

ЗАДАНИЕ

на выполнение дипломного проекта

Студенту Советтурскому Асету Адгезовичу
(Ф.И.О)

Тема проекта Метод гарантированного удаления данных в коммерческих банках

Утверждена приказом по университету № 155 от «__» 23.10.17 2018 г.

Срок сдачи законченного проекта «06» 05 2018 г.

Исходные данные к проекту (требуемые параметры результатов исследования (проектирования) и исходные данные объекта):
Цель данного дипломного проекта является подобрать наилучший метод гарантированного удаления данных для жестких дисков

Перечень вопросов, подлежащих разработке в дипломном проекте, или краткое содержание дипломного проекта:
Исследование существующего бесплатного и условно-бесплатного ПО для удаления данных
Исследование и сравнительный анализ эффективности существующих методов удаления данных
Разработка авторской программы удаления данных и ее тестирование

Перечень графического материала (с точным указанием обязательных чертежей): Рисунок 3.5 – Раздел 1 диска с данными с разными форматами, Рисунок 3.12 – Раздел незанятое пространство, 3.13 – Остатки документа формата dx, Рисунок 3.14 – Метаданные формата jpg на ячейки 02767622, 3.15 – Метаданные формата mp4 на ячейки 02767622, 3.18 – остатки документа на ячейки 07729898. 3.21 – Все пустые ячейки с размером 102 420 Рисунок 3.25 – Чистый НД после процедуры стирания 7-проходами, 3.42 – Все удаленные файлы 3.44 – Содержимое удаленных файлов при виде HEX формате, Рисунок 3.46 – Восстановление удаленных файлов. Рисунок 3.56 – Просмотр раздела диска 1 в двоичном коде, Рисунок 3.62 – Смотрим содержимое диска после стирания в 1 проход. Рисунок 3.64 – Информация о файле TOOL by Confiser. Рисунок 3.73 – Окно программы Delphi 7, программная часть, Рисунок 3.74 – реализация программы, Рисунок 3.75 – документ удален, Рисунок 3.77 – удален формат Exe, Рисунок 3.78 – Удален формат Mp3, 3.79 – Удален формат Mp4, 3.80 – Удален формат jpg

Основная рекомендуемая литература: Кэрри Б. Криминалистический анализ файловых систем / Кэрри Б. – СПб.: Питер, 2013. Гумаев А.К. Восстановление данных / А.К. Гумаев. – Питер СПб 2014. Боборыкин С.Н., Рожков С.С. Оценка эффективности средств уничтожения информации, хранящейся в накопителях на жестких магнитных дисках // «Специальная техника», №3, 2010. Богдарев А.И., Смаленков С.Е. Надежное стирание информации – миф или реальность? // «Защита информации», №1, 2011. Аширова К.Б., Айтпева С.А. Экономика предприятия телекоммуникации. Учебное пособие. – Алматы: АИЭС 2007. Кармиенко А.В. Естественное и искусственное освещение. – М.: изд. М, 2004.

Консультации по проекту с указанием относящихся к ним разделов проекта

Раздел	Консультант	Сроки	Подпись
БЖД	д.т.н. Бекбасаров Ш.И.	11.05	[подпись]
ТЭО	к.э.н. Саккинбаева Р.О.	04.04.18 25.05.18	[подпись]
Научный руководитель	проф. Ахметов Б.С.	31.05.18	[подпись]

График
подготовки дипломного проекта

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Сбор информации по удалению данных	05.03 - 10.03	
Ознакомление с литературой по удалению данных	11.03 - 30.03	
Составление плана по методу гарантир. удал. данных	1.04 - 02.04	
Покупка нужных срезов для исследования метода гар.уд.дан	03.04 - 06.04	
Список программ для метода гарантир. удал. данных	07.04 - 10.04	
Среда разработки ПО и алгоритм программ	11.04 - 19.04	
Практическая часть	20.04 - 25.04	
Программа Eraser	26.04 - 30.04	
Программа DBD SAFE Erase	31.04 - 04.05	
Программа Disk WipE	05.05 - 09.05	
Программа CCleaner	10.05 - 13.05	
Реализация авторского ПО	14.05 - 20.05	
Тестирование ПО	21.05 - 23.05	
Технико-экономическое обоснование. Расчет	24.05 - 26.05	
Безопасность жизнедеятельности. Расчет.	27.05 - 28.05	
Анализ работы и заключение.	29.05 - 29.05.	

Дата выдачи задания «10» 01 2018 г.

Заведующий кафедрой _____ (_____)
(подпись) (Ф.И.О)

Научный руководитель проекта _____ (Ахметов С.С)
(подпись) (Ф.И.О)

Задание принял к исполнению студент _____ (Совоттурсун А.А)
(подпись) (Ф.И.О)

Содержание

Введение

В нашем современном мире тема о безопасности и доступности данных на цифровых носителях каждым годом становиться все более актуальнее. Весь мир охвачен компьютерными технологиями, что сейчас является абсолютно нормальным, что у каждой ячейки семьи есть свой по крайней мере один компьютер, не считая уже новых, навороченных мобильных телефонов, у которых возможности как у компьютеров. Инфотехнологии постоянно развиваются, а с этим и растет необходимость в умелом обращении с данными.

Развитие технологии изменили путь общения людей и ведение бизнеса. Мир умных технологии, процессоров, таблиц, сообщений стало частью повседневной жизни людей. В наше время возможность пользоваться программами больше не требует особенных познаний в информационных технологиях. Интерфейс приложений стал на много интуитивным, познав одну из программ, можно без труда разобраться в других. Огромные коммерческие банки, компаний, учебные заведение и.т.д, ежесекундно пользуются многими программами и ежедневно сохраняют больше тысячи данных в своих носителях жесткого диска и прочих накопителях.

Тем самым пришли к выводу, что данные надо защищать и внедрять технические средства, обеспечить безопасность информации при обработке, вводе, хранения и передачи, но к сожалению последнему этапу утилизация информации особо не уделяют многого внимания.

Когда наши компьютерные оборудования устаревают или же ломаются, в большинство случаях они требует замену на новую. Тем самым, старое железо выкидывают или передают вместе с носителями информации в другие организации, а значит и со всеми данными, которые на защиту были потрачены деньги, труд, время, и это происходит в крупных организациях все чаще. Этим наиболее пользуются заинтересованные лица, злоумышленники, перекупая старое оборудование от известной компании на открытых рынках восстанавливая с цифровых носителей конфиденциальные данные, служебные записи, рабочие документы, бухгалтерские отчеты, истории сообщений, пороли, секретные досье и тому подобные важные данные, что почти это делается на его основаниях совершенно законно, так как он теперь владелец этого оборудование.

С точки зрения пользователя, данные которые он удаляет в своем внешнем накопителе убежден, что удаленного файла уже не существует. Однако это не так, даже переформатирование накопителя гарантированно не удаляет информацию полностью.

Таким образом гарантированное удаления данных используется для защиты информации от утечек, которые могут возникнуть в связи с неправильной утилизацией запоминающих устройств и их последующим использованием злоумышленником. Может происходить как с уничтожением носителя, так и без.

Гарантированное уничтожение информации без уничтожения носителя актуально в случаях: продажи или дарения носителя, передачи носителя в другое подразделение или организацию, если возможна потеря носителя (вследствие потери или хищения).

Целью данного дипломного проекта является подобрать наилучший метод гарантированного удаление данных для жестких дисков.

Для достижения вышеуказанной цели необходимо выполнить следующие задачи:

– исследование существующего бесплатного и условно-бесплатного программного обеспечения для удаления данных;

– исследование и сравнительный анализ эффективности существующих методов удаления данных;

– разработка авторской программы удаления данных и ее апробация.

В дипломном проекте буду использовать квалитативные методы — это анализ и наблюдение, разработка программы.

После выбора эффективного метода гарантированного удаления данных, попробовать восстановить информацию в специализированных лабораторных местах, где услуги считаются платными. Проанализировать и сделать отчет после восстановления данных, сделать выводы, был ли выбранный метод эффективным.

1 Методы гарантированного удаления данных

1.1 Метод разрушения носителя

С появлением мощных накопителей многое изменилось в компьютерном мире, объем хранение информаций стало просто колоссальным, легче стало хранить информацию в своем компьютере, быстродействие конечно же также увеличилось, все стало удобнее и круче по вверх развития технологии. Чем быстрее развивались технологии, тем сложнее их стало защищать от угроз злоумышленников. Все что мы храним в компьютере – будь это данные от коммерческих банков, крупных предприятии или даже наши собственные личные данные могут быть скомпрометированы против нас самих же. В цифровом мире, все данные мы как это положено храним либо в компьютере жесткого диска, старые диски как CD/DVD-R, USB флешках, если еще остались старые кассеты, то и в них тоже могут храниться данные. Но сейчас 2018 год и мир технологии сильно изменился в сильную сторону. Сейчас каждый человек почти с нулевыми познаниями в технологиях IT, программирования и.т.д, может легко изучить любую нужную ему программу, потому что сейчас все программы стали очень понятными с удобным интуитивным интерфейсом, что позволяет легко обучится неопытному пользователю. Но даже не смотря на все эти тонкости, многие люди совершают одну большую ошибку и не учитывают простые вещи, которые случаются повседневно в их жизни, связанные с их данными, которые они хранят в накопителях.

Многие пользователи думают, что компьютер создает файлы и сохраняет эти данные на жестком диске, но, когда приходит время и пользователь считает, что эти данные больше ему не нужны он их удаляет, думая, что эти же удаленные данные уже не существует.[1] Однако это не так, опытный квалифицированный пользователь ПК знает, что, удалив данные с накопителей они вовсе не удаляются, потому что та же операционная система образует свои системные файлы хранящеюся информацию об удаленных данных по которым легко можно восстановить и получить метаданные, а что если говорит о самом жестком диске, то от удаленных данных или даже форматирование твердого накопителя остается остаточная намагниченность предыдущих записей. Можно привести такую легкую аналогию и объяснить на простом жизненном примере. Запись данных на разных накопителях можно сравнить с записью какой-либо информации с обычной ручкой на бумаге. Например, мы пишем на бумаге письмо, написали имя человека, затем вместо этого имени решили записать другое, мы берем ластик и стираем предыдущее имя, записываем поверх новое. Что с этого мы получаем? То, что стирание ластиком не идеальное, если приглядеться можно увидеть остатки стертой записи и восстановить их выдавливанием бумаги грифеля. Конечно, твердый накопитель работает иначе, но принцип тот же. А что взять USB флешки, смарт памяти, то от них остаются остаточный заряд, на компакт дисков остаточная яркость. Потому что были не мало случаев, когда с такими методами злоумышленники делали свои «грязные» дела, законно. В большинство случаях

как показывает статистика за 2018 год в журнале сайта «Хакер.ру», злоумышленники скупали старые парки ПК от крупных компаний в рынках, и восстанавливали таким образом все метаданные с носителей и использовали для своих целей. Таким образом НСД сплывали все чаще от крупных банков, компаний. Все данные, что включают в себя, пороли, счета, текстовые данные, письма, переписки деловых лиц – все это злоумышленники брали от скупленных ими компьютеров на рынке, поэтому можно сказать они это сделали почти что законно.

Поэтому тема моей дипломной работы актуальна и нужно научить пользователей, работающих в коммерческих банках, крупных компаний и других сферах, правильно удалять данные, а именно выбрать эффективный метод удаления данных.

На настоящий момент существуют три уровня удаления или, так сказать, уничтожения данных [2]:

– метод физического разрушения носителя уничтожение;

– аппаратные средства уничтожения;

– программные средства уничтожения данных.

Метод разрушения носителя – самый простой и самый проверенный годами метод уничтожения данных. Рассмотрим все тонкости этого метода и сделаем анализ метода по эффективности.

Что нужно знать перед тем, как уничтожать твердые накопители воздействием силы? Первое что надо понять, это то, что просто взять и ударить молотком по ЖД и выкинуть его. Не рекомендуется, потому что даже при сломанных блинах можно восстановить часть информации на остаточных целых местах, по ферромагнитной пленке. Да и еще под словом «разрушение» еще не означает сломать руками или молотком. Эту категорию метода я разделяю на три способа:

– механическое, пиротехническое;

– химия;

– тепловое воздействие;

Первый способ – это как можно сильно и круче измельчить все блины винчестера или другие накопители, так чтобы не остались кусочки целых участков для восстановления информации. К примеру, взять мясорубку, которая крутит мясо, думаю принцип понятен как должен выглядит накопитель после этих воздействий. Пиротехническое, кратко скажу опасен для самого человека, ведь под термином «пиротехническое», имеется ввиду взрыв.

Второй способ – химия, уничтожение накопителей с помощью агрессивных химических воздействии на сам предмет. Например, кислота.

Третьи способ – тепловое воздействие, то есть просто жечь накопитель, но и здесь есть свои условия в технике безопасности, которые нужно соблюдать. Для этого нужно довести разогрев носителя до точки Кюри, а это около 800-1000 градусов по С. Только таким методом восстановление абсолютно становится невозможным, потому что рабочий магнитный материал проходит через слой точки Кюри. Этот метод довольно опасен так же для

самого человека, но этот способ многие используют при уничтожении данных носящие государственные тайны, оно и понятно почему выбрали такой способ.

Вывод всего выше сказанного таков: метод данных очень быстр по скорости уничтожения и надежность высока. Но также может возникнуть опасность для самого человека. Для некоторых уничтожении по условиям процедур – нужны специальные навыки или дорогостоящие оборудования. После этого метода повторно использовать накопитель невозможно, метод финансово затратный. [2][3]

1.2 Аппаратные методы

Цель аппаратного метода – уничтожение информаций без физического воздействия и не подвергнуть к разрушению конструкций самого носителя. То есть перестройка структуры рабочего магнитного устройства носителя. Чтобы этого достичь нужно устранить векторы, намагниченные в самом жестком диске. Для этого существуют несколько способов:

– размагничивание поверхности носителя;

– намагничивание поверхности носителя до максимальных возможных значений – это называется «насыщение».

Размагнитить ферромагнетик возможно и иным методом – разместить его в долго убывающую, неустойчивую, магнитную область. Но с жестким диском появляются проблемы, сопряженные с огромной коэрцитивной мощью (исчезающей намагниченностью) ферромагнитного возмещения диска. Получение мощных неподвижных полей в проемах электромагнитов потребует трудных промышленных заключений и крупных энергозатрат.

Более лучшим методом является – это намагничивание рабочих поверхностей носителя до максимального значения. При намагничивании магнитное поле работает также, как и магнитные головки жесткого диска при записи на блины. Если усилить внешние поля напряженности, создаваемые головками на величину при которой произойдёт насыщение материала поверхности самого диска, тогда домены магнита будут переориентирована по направлению этого внешнего поля, таким образом все данные на жестком диске будут уничтожены. Самый распространенное оборудование таким методом является – импульсаторы, намагничивающее устройство. К примеру, взять оборудование «Импульс 7В», куда во внутрь эти оборудования можно поместить любой накопитель и вся ваша информацию будет уничтожена за пару секунд. Есть даже версий модели, при которых можно просто поставить в сервера под такие устройства, в случае несанкционированного проникновения на сервер, тогда дистанционно сработает импульс и уничтожит мгновенно все накопители в серверном отделе.

Плюсы этого метода в том, что он дает возможность создания сильных намагничивании полей с малыми энергозатратами, высокую скорость намагничивания, возможность помещение самого носителя в камеру намагничивания, а также возможность срабатывания дистанционно. Но есть также и минусы, это огромные денежные затраты, ведь стоимость одного

такого устройства может превысит свыше миллион тенге. После уничтожения информации носители не могут быть использованы повторно, также требуется специальная подготовка для установки этих устройств и потребуется навыки специалистов. Но не смотря на минусы, эти оборудования стоят того, ради сохранности и нераспространения собственных данных. [2][3]

1.3 Программные методы

Программные методы делятся на три категории: базовая, продвинутая, профессиональная.

Базовая, самая простая и часто применяемая форма уничтожения информации на жестких дисках. Принцип работы уровня очень прост, происходит перезапись жесткого диска в загрузочный сектор, также затрагивает основную и резервную таблицу разделов, тем самым записывается последовательность нулей. Этот способ дает усложнение доступа к данным хранящимся на диске, но сами данные не уничтожаются. Восстановление информации после этого способа возможно с помощью тщательного посекторного чтения. Этот уровень обеспечивает высокую скорость, но эффективность заставляет желать лучшего утечкой информации нежелательна. Можно повторно использовать жёстки диск после этих процедур.

В продвинутом уровне происходит запись последовательности нулей или единиц в секторе, где хранится информация. Последовательность этой операций уничтожает информацию. Восстановить с помощью специальных программ невозможно, но была теория, что есть возможность восстановить данные взяв их из остаточной намагниченности в краях дорожки дисков, что несет информацию о прошлых записях.

Преимущество этого уровня – высокая гарантия, но по сравнению с базовым уровнем, скорость удаление значительно ниже, повторное использование жесткого диска возможна.

Профессиональный уровень – это использование неоднократной перезаписи информации. С увеличением циклов чисел перезаписи данных приводят к усложнению восстановления, точнее сказать дает возможность полного стирание данных, это обосновывается непосредственным дрейфом головки записи жесткого диска во время каждого цикла. После несколько повторов этих процедур вероятность перезаписи краевых дорожек диска возрастает, тем самым повышается сложность самого процесса восстановления уничтоженных данных.

Гарантированное удаление данных на этом уровне очень высока, но сам процесс стирания очень долгий, повторно использовать жесткий диск возможно.

Также были придуманы методы, которых прозвали «маскировкой». Принцип работы данного метода перемагнитить буквально каждый битовый промежуток в записи по максимальной. Перезапись байтами #FF, битовая маска из восьми двоичных единиц и нулей, но также можно использовать

другие произвольные числа, что дает невозможность восстановления программными методами. [2]

Выбрать какой именно метод подходит зависит от уровня секретности данных, которые хранятся в носителях. Во многих странах есть собственные руководящие документы, в которых прописаны алгоритмы по уничтожению данных тем или иными методами. В данный момент существуют четыре самых популярных стандартов по уничтожению данных:

– стандарт DOD 5220.22-M– department in defence USA 1995;

– стандарт ГОСТ Р50739-95 Россия 1995;

– стандарт VSITR Германия 1999;

– стандарт RCMP TSSIT OPS-II – Канада, национальный стандарт.

Стандарт DOD 22-M был создан в Министерстве обороны США в 1995 году, работает по следующему принципу:

а) первый цикл – в каждом байтном секторе записываются случайные числа (данные);

б) второй цикл – в каждом байтном секторе зачисляются инвертированн ые данные, это – означает в сектор единиц заносятся нули, а в секторы где нули– единицы;

в) третьи цикл – повторяет первый цикл.

Сами Министерства обороны США признают и запрещают использовать данный метод для использования уничтожения информации в сверхсекретные или государственные тайны, они не доверяют программным методам и придерживаться в этом случае физического уничтожение.

Стандарт ГОСТ Р50739-95 Россия так же был выпущен в 1995 году, в стандарте говорится, что очистка жесткого диска должна производится путем записи с маскировки информации одного раза. Только вот проходы и содержание в стандарте вообще не уточняется. Рекомендуется перезапись путем маскировки, но какими методами и почему один раз это нужно делать не обосновываются, поэтому для меня этот стандарт не играет роли. [3]

Немецкий стандарт VSITR, был выпущен в 1999 году, принцип работы следующий:

а) Цикл первый: запись с нулями 0x00 в каждом бите;

б) Цикл второй: запись единицами 0xFF в каждом бите;

в) Цикл третьи: повторяет первый цикл;

г) Цикл четвертый: повторяет второй цикля;

д) Цикл пятый; повторяет третьи цикл;

е) Цикл шестой: повторяет четвертый цикл;

ж) Цикл седьмой: запись 0xAA в каждом бите.

Скорость перезаписи долгая, надежность высокая. Помимо государственных стандартов, существуют несколько отдельные методы от независимых экспертов в области информационной безопасности. Самые популярные из них это два метода – Шнайдера и Гутмана.

Шнайдер предлагает метод состоящий из семь проходов, первые два как он говорит это запись единиц и нулей, и последние пять случайными числами.

Однако из всего этого он не обосновывал предложенные им проходы и маскировки. Но сам он сказал следующее: «Последние исследования Национального института стандартов и технологий, выполненные с помощью электронных туннельных микроскопов, показали, что даже этого может быть недостаточно. Честно говоря, если ваши данные достаточно ценны, можете считать, что их полное удаление с магнитного носителя невозможно. Сожгите носитель или сотрите его в порошок; Дешевле купить новый носитель, чем потерять ваши секреты».

Алгоритм Гутмана – метод был разработан Питером Гутманом и Коллином Пламбом, представлен в 1996 году в конце июля. Метод включает в себя 35 проходов, которые рассчитаны на уничтожение записей закодированные способами MFM и RLL.

MFM – код Миллера в квадрате, один из видов линейного кодирования. Служит для цифровых данных от передатчика к приемнику по одному биту за один такт. Каждый информационный бит кодируется из сочитание двух битов 1 или 0. Для легких дисков использование MFM сделала объем хранение информации в два раза лучше, такие легкие диски назывались парные диски или двойной плотности, но вскоре был выпущен новый более эффективный метод RLL кодирования.

RLL – этот метод кодирования содержит группы из нескольких битов, вместо одного бита в один такт времени. Идея состоит в том, чтобы соединять клоковые очереди полярности и очередь полярности данных, это делается чтобы допустить более плотную запись на поверхность диска. Эти два параметра и есть RLL, если расшифровать, то RUN это относится к продолжительности записываемой информации без смены полярности, параметр run length это самая короткая длина между двумя смены полярности, в свою очередь run limit это сама большая длина без смены полярности. Из этого следует сказать, что длина между двумя сменами полярности никак не может быть слишком длинной, а иначе они потеряют синхронизацию битов. В данный момент есть улучшенные версий PRML и ERML.

Схема кодирования пишется как RLL (x,y), x это run length и y это run limit, самая популярная схема кодирования информации на накопителях это версия RLL 1.7/2.7. Для кодирования нужно иметь определенный словарь, которое совпадает с входными данными и выходными, можно это рассмотреть на словаре в случае версий 2.7 RLL.

Для примера давайте возьмем последовательный бит 10001111(0x8fh), будем представлять последовательно контроллером как 10-0011011 и закодируем это в NRNN-NNNNRNNN-RNNN. Если заметили, то в данной схеме, каждая последовательность кодировки из словаря заканчивается на NN, из этого можно увидеть, что минимальная длина сменами двух полярности приравнивается к 2. Максимальная длина будет приравниваться к 7, достигаться будет в этом кодирования с двух последовательностями 0011-0011.

Если сравнивать эту таблицу с таблицами для FM и MFM, можно заметить интересные стороны. Можно увидеть нарастающую сложность

кодировки, требуется 7 различных последовательностей и рассматриваться одновременно до 4 битов. Среднее количество полярности смен на один бит равно 0,4635 можно округлить до 0,5. Это можно сказать одна треть от FM и две трети от MFM, по сравнению со старой кодировкой FM, теперь мы сможем записать больше рас втрое информации на один и тот же участок поверхности диска. На рисунке 1.1, показано кодированная форма записи байта 10001111 в случае FM, MFM, RLL 2.7 кодировки.

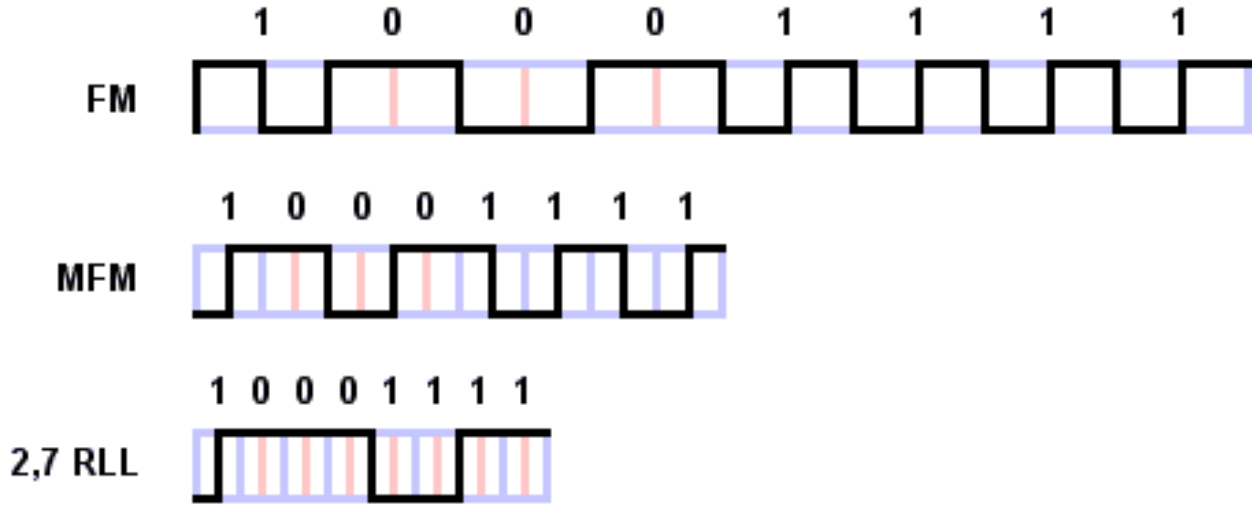


Рисунок 1.1 – Кодирования FM, MFM, 2.7 RLL

PRML – кодирования, чтения схемы работают, используя смены определение полярности и в соответствии представлению их с кодирующей схемой, что используется при записи информации. Сигнал считывается с диска, используя усилитель и головку, после этого на схему подают декодирования и улавливания. Контроллер переводит сигнал в цифровую форму, следя при этом постоянно за сигналом головки синхронно с внутренним клоком и определяя всплески от напряжения, которые приводят к смене полярности. Этот метод хорошо работает если всплески напряжения будут достаточно большими, чтобы отличать их от шума. В это время плотность записи вырастает и сигнал для распознавания становиться все сложнее, амплитуда пиков становится ниже, а также появляется явления интерференции между соседними всплесками. Происходит интересная связь, для того чтобы понизить интерференцию нужно уменьшать амплитуду записываемых данных, в это же время снижая амплитуду уменьшается помехозащищённость, из-за этого удорожается и усложняется чтения головки и схемы распознания и конечно же декодирования.

Чтобы справиться с этими проблемами были предложены сделать новые методы распознавания данных. Технология, называемая PRLM, расшифровывается как partial response maximum likelihood, которая полностью изменяет принцип чтения и декодирования данных с поверхности дисках. Вместо того чтобы отличать каждый всплеск, контроллер PRML применяет

огромную тактовую частоту дискретизации при переносе аналогового сигнала в цифровой восстанавливая структуру чтения в цифровой форме, используя разные методы фильтров для обработки цифрового сигнала. То есть он рассматривает не один всплеск, а целый временной интервал, считанными сигналами. Затем полученные результаты контроллер сравнивает и берет самые похожие наборы данных. Что значит для этого метода не обязательно считывать сигнал целиком, хватит и часть считанного сигнала, после этого контроллер определяет какая это часть больше похожа и только потом декодирует данные. Благодаря этому методы плотность поверхности диском записи увеличилось на 40 процентов по сравнению старыми схемами, использующие детектированием всплесков.

ERML – революция, созданная технология была улучшенным вариантом PRML. Сам принцип метода остался тем же, только были улучшены алгоритмы работоспособности анализаторов схем. Благодаря этому прорыв поверхности плотность записи дисков увеличилось до 70 процентов, по сравнению с методом PRML.

В новых современных жестких дисках используются различные версии именно ERML метода, при считывания данных. Таким образом в современных носителях жесткого диска происходит считывание информации только по частям, а не полностью сам диск, и по части восстанавливается оригинальный битовый набор.

Теперь, когда разобрались с методами MFM, RLL вернемся к методу Гутману. Выбор проходов рассчитан на то, что пользователь не знает механизм кодирования диска, поэтому метод включает в себя проходы, которые разработанные специально для трех типов привода. Но если сам пользователь знает какому типу кодировки относится привод, он может уверенно выбрать только те проходы, которые нужны для его диска. Для дисков с разными механизмами кодирования нужны разные проходы. Многие проходы были созданы для дисков, закодированных схемами MFM и RLL. Для современных дисков старые методы кодирования не используются, что означает многие проходы метода Гутмана только лишние. С 2001 года в конструкциях жестких дисков ATA, IDE, SATA встроена поддержка «Secure Erase», это устраняет необходимость использования метода Гутмана при стирания всего диска. [4]

Метод Гутмана используется в первые 4 прохода записи случайными символами, в каждый байт каждого сектора, но с 5 по 31 проход записывается определенными последовательностями, но опять так и в последние 4 прохода снова запись идет случайными символами. С 5 по 31 проходы были разработаны с учетом схемы конкретного магнитного кодирования, как целевой проход. На блинах жесткого диска запись идет во все дорожки, конечный результат скрывает любые данные на диске, только самые современные технологии физического сканирования диска способны восстановить любые данные, но это лишь в теории, а доказательств еще не было.

RCMP TSSIT OPS-II – Канадский национальный стандарт представляет собой программное обеспечение, на основе данных метода очистки используется в различных программах для уничтожения данных для перезаписи существующей информации на жестком диске или другом устройстве, для хранения информации. Канадский RCMP TSSIT OPS-II осуществляет удаление данных используя 7 шагов – данные переписываются 6 раз, чередующиеся нулями и единицами и последние случайными данными.

Американский национальный стандарт NAVSO (Navy Staff Office Publication) P-5239- 26 разработан в 1993 году, используется ВМС США. Данный метод предусматривает 3 цикла перезаписи для MFM-кодированных устройств:

а) в первом цикле – записывается # 01;

б) во втором – # 7ffffff;

в) в третьем – последовательность случайных чисел.

Вывод

В данной главе мы узнали методы гарантированного удаления данных, рассмотрели каждый метод и как они работают. Из всех методов, я буду использовать «Программный метод», потому что он наиболее безопасен для меня и выйдет менее затратным. Так же обосновал актуальность темы «Метода гарантированного удаления данных», все проделанные работы в данной главе будут упоминаться во второй и третьей главе, поэтому первая глава послужит как фундамент для всей моей дипломной работы.

Таким образом гарантированное уничтожение данных используется для защиты информации от утечек, которые могут возникнуть в связи с неправильной утилизацией запоминающих устройств и их последующим использованием злоумышленником. Может происходить как с уничтожением носителя, так и без.

Гарантированное уничтожение информации без уничтожения носителя актуально в случаях: продажи / дарения носителя, передачи носителя в другое подразделение или организацию, если возможна потеря носителя (вследствие потери или хищения).

2 Выбор программ и методы форензики

2.1 Список программ для метода гарантированного удаления данных

В данной главе будут описаны ряд программ, которые будут использованы в третьей главе практической части, так же рассмотрим, что такое форензика.

Для экспериментальной работы будут использован жесткий диск модели, 500 GB Barracuda SN: WDE1FRV7 WWN 500C5009DF9DE60.

В эксперименте в качестве удаления будут использованы пять файлов разных форматов:

– 1.Doc;
– 1.JPG;
– 1.Mp4;
– 1.Mp3;
– 1.Exe.

Список программ для практической части:

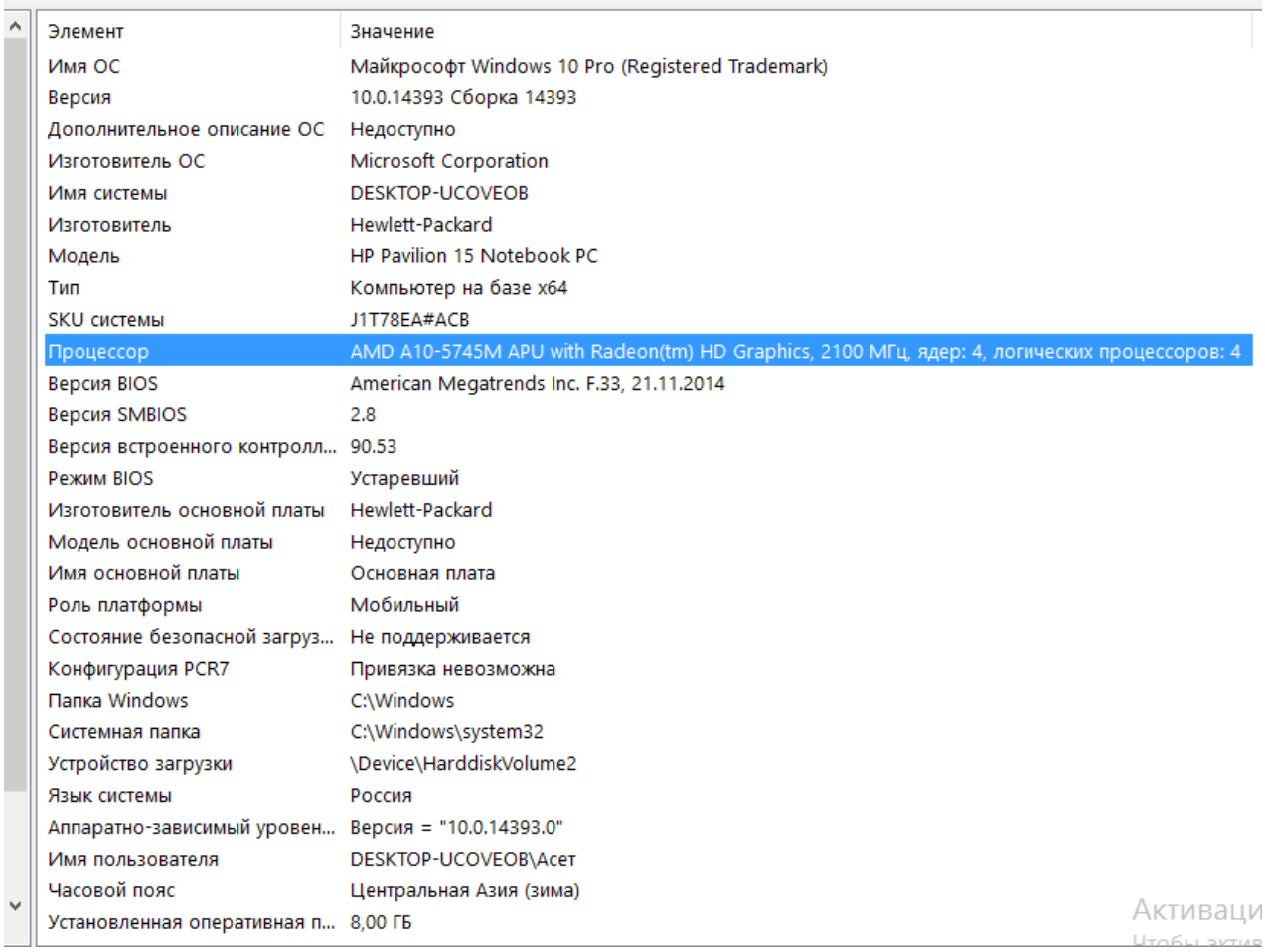
– Ccleaner;
– Eraser;
– DiskWipe;
– O&O safeerase.

Для работы в практике буду использовать ноутбук со средней мощности, сведение о ноутбуке смотрим на рисунок – 2.1.

Причина выбора этих программ, является тем, что они хорошо зарекомендовали себя на рынках и многие рекомендуют их для использования удаление данных.

2.2 Описания программ

Eraser – программа полностью на английском языке, русской вариаций нету. В данный момент он используется только для ОС Windows xp/Server 2003/2008/Windows 7/8/10 Windows Server 2012. Может перезаписывать информацию с множество вариантами, как так в эту программу встроены 14 собственных шаблонов и даже редактор для создания новых. Программа имеет хорошую документацию и центр помощи на официальном сайте. Так же на официальном сайте есть активный форум, где обсуждают те или иные проблемы, которые могли возникнуть у пользователей. Программа работает со всеми дисками, поддерживает так же IDE/SCSI/RAID и FAT16, FAT32, NTFS разделы. На каком языке была написана программа не говорится. Есть планировщик, можно выборочно удалять файлы. [6]



Элемент	Значение
Имя ОС	Майкрософт Windows 10 Pro (Registered Trademark)
Версия	10.0.14393 Сборка 14393
Дополнительное описание ОС	Недоступно
Изготовитель ОС	Microsoft Corporation
Имя системы	DESKTOP-UCOVEOB
Изготовитель	Hewlett-Packard
Модель	HP Pavilion 15 Notebook PC
Тип	Компьютер на базе x64
SKU системы	J1T78EA#ACB
Процессор	AMD A10-5745M APU with Radeon(tm) HD Graphics, 2100 МГц, ядер: 4, логических процессоров: 4
Версия BIOS	American Megatrends Inc. F.33, 21.11.2014
Версия SMBIOS	2.8
Версия встроенного контролл...	90.53
Режим BIOS	Устаревший
Изготовитель основной платы	Hewlett-Packard
Модель основной платы	Недоступно
Имя основной платы	Основная плата
Роль платформы	Мобильный
Состояние безопасной загруз...	Не поддерживается
Конфигурация PCR7	Привязка невозможна
Папка Windows	C:\Windows
Системная папка	C:\Windows\system32
Устройство загрузки	\Device\HarddiskVolume2
Язык системы	Россия
Аппаратно-зависимый уровен...	Версия = "10.0.14393.0"
Имя пользователя	DESKTOP-UCOVEOB\Acer
Часовой пояс	Центральная Азия (зима)
Установленная оперативная п...	8,00 ГБ

Рисунок 2.1 – Сведение о ноутбуке, который будет использован в эксперименте

Ccleaner гигант среди всех списков программ, он является не только самой популярной, но и самой оптимизированной и на порядок удобнее всех других программ. Вице президентами продукта являются Луиза Кинан, Паул Янг и Джемми Кован. [9]

Программа с закрытым исходным кодом, оптимизированный под 32 и 64 разрядных операционной системы Windows. Утилита создана британской частной компаний под названием Piriform Limited, написана утилита на одной самой популярной программы C++. Самое большое отличие и лучшая сторона программы в том, что обновления и оптимизация дистрибутивов выходит каждый месяц. За декабрь 2012 года с официального сайта было совершено более 1 миллиарда скачивания. Программа состоит из 4 версии для пользователей:

– Free – бесплатная версия, отличие от других в том, что к ней не предлагается приоритетная тех. поддержка от разработчиков;

– Home – для пользователей домашнего ПК с поддержкой разработчиков;

– Business – бизнес версия может использоваться различными компаниями на рабочих ПК. Разработчики дают улучшенную версию премиум бизнес поддержки для предпринимателей со всеми в комплекте дистрибутивов.

– Network – сетевая версия утилиты, для оптимизации работы в больших корпоративных сетях любой величины.

Кроссплатформенная программа может работать помимо Windows, на MacOS. А также платформа поддерживает андроид приложение мобильных телефонов, что очень делает программу полезной. Программа может стирать данные как выборочно, так и весь диск. Так же программа легко находит и сортирует все логи из браузеров, дамп файлов, временных и клоновых файлов, которые уже не нужны. Программа оптимизированно великолепно, стиль дизайна и удобство на высоком уровне. Утилита поддерживает четыре вида стирания смотрим на рисунок – 2.2.

Более профисиональная версия стоит 30 долларов на подписку на месяц. Входит в состов туда как и восстановление данных, сохранение, то есть бэкап, оптимизация ЖД. Помимо всего этого утилита поддерживает облачное хранение данных, что делает крайно удобно, если вдруг организации или коммерческие банки решились стирать данные все с жесткого диска, но при этом с платной услугой могли резервно хранить в защищенных облачных сервисов компании Ccleaner.

Если спросите в чем уникальность этой программы, то можно смело ответить разнообразность в удалении и оптимизировании любых файлов, историй, дамп истории, журналирования от системных руководств ОС и.т.д. Есть версия и для переносимых носителей (USB-флеш накопители, Memory Stick. Ipod. Mp3). Можно работать программой используя командную строку, для быстрых или экстренных случаев стирания диска.

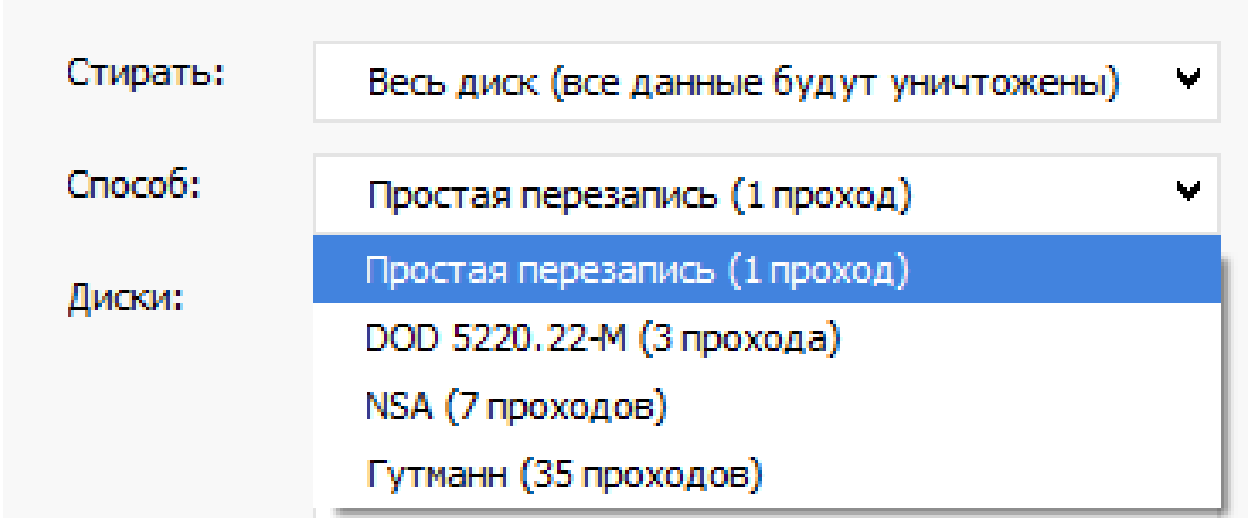


Рисунок 2.2 – Утилита Ccleaner, содержит 4 метода стирания дисков

Disk Wipe выпускается как Freeware под лицензией EULA. Disk Wipe бесплатно для личного или коммерческого использования без каких-либо ограничений. Disk Wipe не содержит рекламное ПО или вредоносное ПО! Программа была создана в февраль 2009 года.

Особенности Disk Wipe:

– постоянно стирает конфиденциальные данные о разделах и томах диска;

– портативный, не требуется установка;

– использует несколько усовершенствованных алгоритмов измельчения (dod 5220-22.m, us army, peter guttman), чтобы безопасно стереть данные;

– поддерживает все популярные файловые системы windows, ntfs, fat, fat32;

– он использует быстрый формат перед очисткой диска для повышения производительности;

– работает с usb-накопителями, sd-картами и другими портативными запоминающими устройствами;

– маленький, легкий, не содержит рекламного по.

Программа работает с любым устройством хранения данных, таким как USB-накопитель, различные SD, мини-и микро SD-карты и все другие устройства, которые можно использовать в качестве хранилища данных и отформатированы с помощью NTFS, Fat или Fat32 (некоторые mp3-плееры и камеры и т.д.). [7]

O&O safeerase – группа O & O состоит из четырех компаний, занимающиеся разработкой и маркетингом программного обеспечения. Старейшим из четырех является O & O Software GmbH, из которого выходят O & O Services GmbH и exono GmbH. В 2006 году O & O Software GmbH приобрела мажоритарный холдинг в acticom GmbH, компании, специализирующейся на разработке программного обеспечения для мобильных телефонов. Все компании имеют свои штаб-квартиры в Берлине, Германия. O & O не просто производит программное обеспечение, но также разрабатывает индивидуальные клиентские решения. Именно поэтому O & O Services GmbH была создана в 2002 году. Эта компания берет на себя требования клиентов для индивидуальных бизнес-приложений и делает их реальностью, предлагая полный комплекс услуг компаниям для разработки своей продукции. Они могут опираться на многолетний опыт, накопленный O & O Group в создании и продаже успешных программных продуктов. Независимо от того, являются ли это веб-приложениями или настольными компьютерами, O & O Services отвечает требованиям ИТ-клиентов наших клиентов эффективно и оперативно. Как сертифицированный партнер Microsoft, O & O Services является специалистом в области разработки с использованием технологии Microsoft .NET.

O & O Software GmbH, основанная в Берлине, с 1997 года разрабатывает и продает стандартное программное обеспечение для Windows. Ее клиентами являются частные клиенты, компании и государственные органы. Продукты успешно продаются в более чем 140 странах, как напрямую, так и через сеть партнеров. Портфель продуктов включает приложения для оптимизации производительности, восстановления данных, безопасного удаления данных и администрирования, все под Windows. Продукция O & O завоевала множество

наград и сравнительных тестов, названных в этом процессе как технологический лидер в своей области.

Особенности продукта по мнению самих производителей:

– мгновенное стирание выбор файлов в контекстном меню вызывает мини-диалог, в котором удаление может быть немедленно выполнено;

– постоянное удаление файлов, папок, карт памяти и usb-накопителей;

– удалить весь компьютер, не требуется загрузочный носитель;

– удаление интернет-трассировок и временных файлов программы;

– шесть способов окончательного удаления конфиденциальных данных;

– подробные отчеты как доказательство удаления;

– инструмент анализа для поиска небезопасных удаленных файлов;

– адаптированный метод удаления для ssd (trim);

– расширенное управление отчетами и мероприятиями .net framework 4.6.1;

– поддерживает windows 10, windows 8.1 и windows 7. [6]

2.3 Компьютерная криминалистика – Форензика

Термин «форéнзика» произошел от латинского «foren», что значит «речь перед форумом», то есть выступление перед судом, судебные дебаты – это был один из любимых жанров в Древнем Риме, известный, в частности, по работам Цицерона. Термин «forensics» является сокращенной формой «forensic science», дословно «судебная наука», то есть наука об исследовании доказательств – именно то, что в русском именуется криминалистикой. Соответственно, раздел криминалистики, изучающий компьютерные доказательства, называется по-английский «computer forensics». При заимствовании слово сузило свое значение. Русское «форензика» означает не всякую криминалистику, а именно компьютерную. [10]

В практической части, будут показаны секреты восстановление данных путем компьютерной криминалистики. Даже если безвозвратно удалить все данные, можно их, не используя оборудования найти эскизы предыдущих файлов в ОС, путем секретных и скрытых ходов. Научить пользователей этому искусству будет очень полезно, потому что, зная эти скрытые ходы можно их же предотвратить и принять меры, чтобы окончательно удалить все данные, которые мы стерли путем перезаписи. Таким образом, по окончании этих процедур даже сами криминалисты не смогут доказать, восстановить или же найти хоть какие-то зацепки об удаленных данных. Методы будут понятны и легко усеваемые для простых или же продвинутых пользователей ПК, думая с этим не должно появиться какие-либо сложности.

При использование каждого метода будем восстанавливать данные для начала собственными методами, используя сторонние программы, но также буду использовать услуги платных дата центров, где работают эксперты по восстанавлению данных. Я взял центр по восстановлению данных - «Местоположение: 050004, Казахстан, г.Алматы, ул. Панфилова 92, 6-этаж, оф. 47 уг.ул. Айтеке-би (б. Октябрьская).

2.4 Среда разработки ПО и алгоритм программы

Разработка ПО осуществляется на среде Delphi 7, причина выбора этого программного языка в его легкости написания кода, улучшеную откладку, наличие самого быстрого компилятора, возможности визуального построение интерфейса. Также хочется отметить, что я раньше работал на этом языке программирования, что представляет для меня еще больше удобства нежели другие языки программирования. Блок схемы программы можно увидеть в «приложение А».

Алгоритм программы:

1) выбирается любой файл;

2) выбираем количество проходов для перезаписи выбранного файла, в моей программе проходов 1,3,5,10,15;

3) выбранный файл находится в буфере, в котором будет подготовка перезаписи;

4) каждый бит выбранного файла перезаписывается данными который состоит с длинной 256 случайными символами;

5) пока все биты выбранного файла не будут перезаписаны столько сколько было выбранно для перезаписи проходов, файл не будет удален;

6) после завершение всех проходов, файл будет гарантированно удален.

Вывод

В данной главе были рассмотрены ряд программ для практической части. Каждую программу кратко описали, что оно из себя представляет. Так же узнали что такое форензика, и что из него можно извлечь для практической части удаления данных. Был выбран и обоснован программный язык, на котором будет разработана программа гарантированного удаления данных, также расмотрен алгоритм программы.

3 Практическая часть

3.1 Программа Eraser

После запуска программы, перед нами появиться окно из трех вкладок, смотрим на рисунки 3.1, 3.2:

1) erase schedule;
2) settings;
3) help.

Сразу же переходим во вкладку «Setting/Настройки». Eraser – это настраиваемая программа, которая позволяет вам изменять настройки, соответствующие вашей модели угроз. Тем не менее, настройки по умолчанию, поставляемые с готовым продуктом Eraser, относительно безопасны для большинства пользователей. Но нас совсем это не устраивает, потому что мы будем брать определённый метод, который мы раньше описывали в первой главе дипломной работы.

Обратите внимание для того, чтобы настройки вступили в силу, вам нужно выбрать кнопку «Сохранить настройки» в верхней правой части страницы настроек. Некоторые настройки также требуют перезагрузки для вступления в силу.

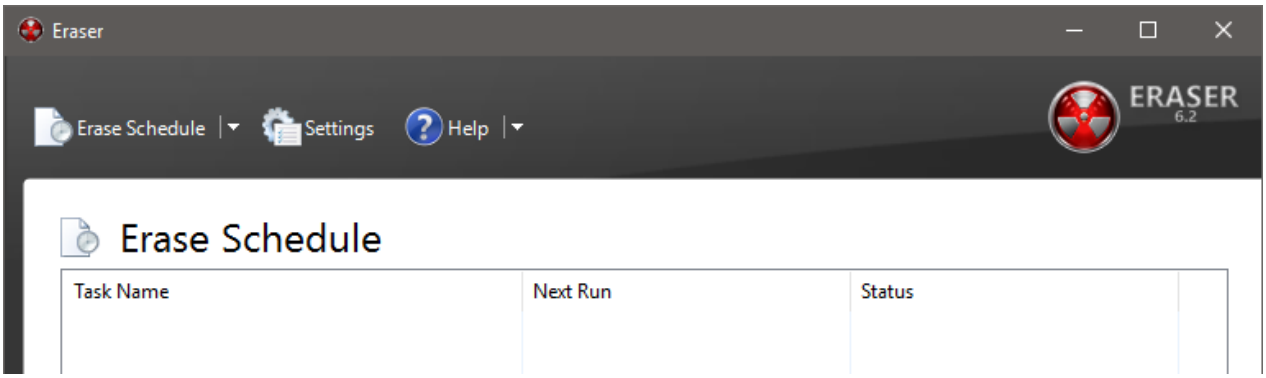


Рисунок 3.1 – Главное окно программы

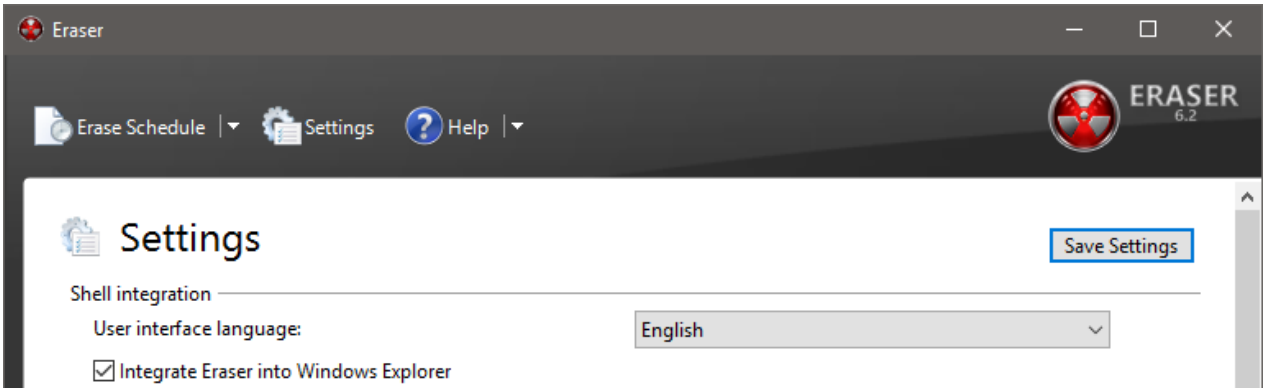


Рисунок 3.2 – Окно настроек

Поставьте сразу же галочку на Integrate Eraser into Windows Explorer, при щелчке правой кнопкой мыши на поддерживаемых элементах в проводнике Windows появится контекстное меню Eraser.

Default file erasure method и Default unused space erasure, первое мы создаем настройки на удаление только Файлов или папок из файлов, второе идет затирания всего диска которую мы укажем, будь это весь диск или часть его логической памяти. Для начало мы попробуем использовать первый метод стирания файлов, методом DOD 5220.22-M– department in defence USA 1995 с 3 проходами, смотрим на рисунок 3.3.

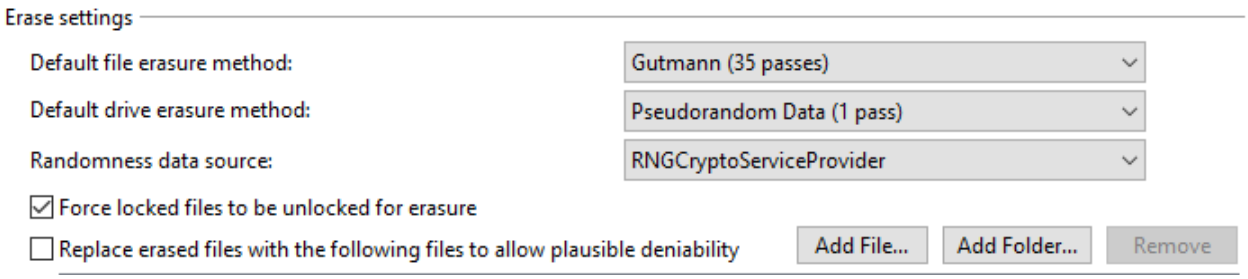


Рисунок 3.3 – Настройки удаление файлов и всего диска

Поставьте так же галочку на Force locked files to be unlocked for erasure, когда Eraser пытается стереть файл, но он заблокирован программой, Eraser попытается принудительно разблокировать файл для стирания; если он не установлен, файл будет проигнорирован Eraser и будет отвечать на это как ошибка.

Для подключение жесткого диска к ноутбуку в качестве как внешнего носителя, мне понадобиться 2.5 Inch Sata USB3.0 Hard Drive Enclosure, 5 max Gbps, 2.5 HDD/SDD, Tool free.

На рисунке 3.4, видим I и J, разделы подключенного жесткого диска 500 GB Barracuda SN: WDE1FRV7 WWN 500C5009DF9DE60 подключенный с помощью SATA разъема.

Мы будем удалять логический раздел, содержимое внутри папки «Удаляем», в нем находиться 4 файла разных форматов как:

1) 1.Doc - 6,01 МБ (6 304 670 байт);
2) 1.JPG - 864 КБ (885 224 байт);
3) 1.Mp4 - 29,9 МБ (31 358 556 байт);
4) 1.Mp3 - 3,45 МБ (3 626 212 байт);
5) 1.Exe - 8,67 МБ (9 101 000 байт).

Смотрим на рисунок 3.4.

Рисунок 3.4 – I и J, разделы подключенного жесткого диска 500 GB Barracuda SN: WDE1FRV7 WWN 500C5009DF9DE60 через SATA

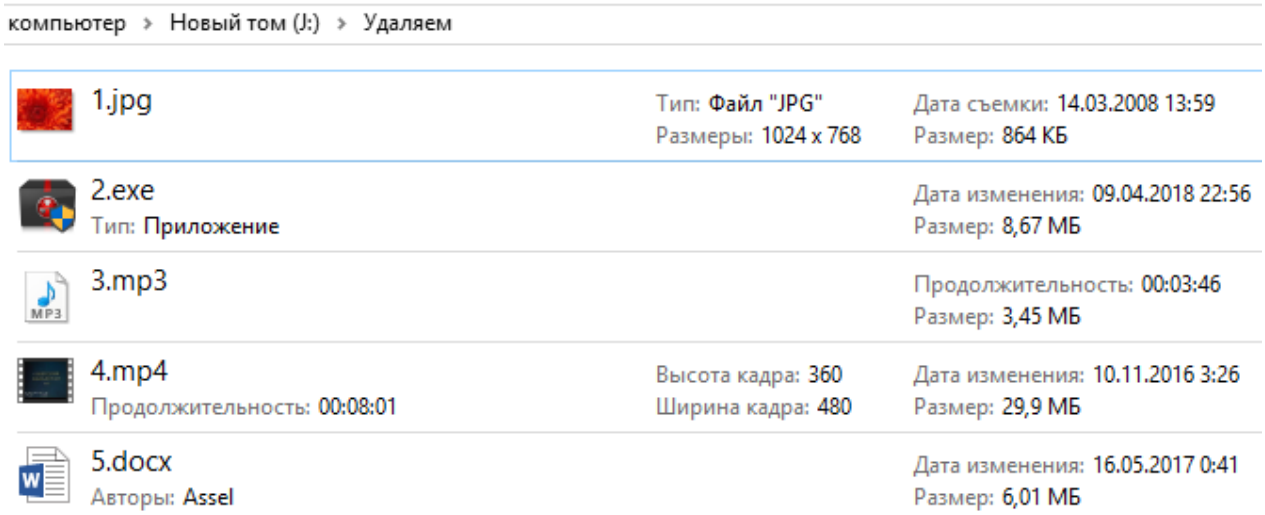


Рисунок 3.5 – Раздел j, папка с данными с пятью разными форматами

Переходим к главному окну программы, и нажимаем на первую вкладку и выбираем новую задачу, мы увидим четыре вида запуска задач это:

1) run manually – Запуск происходит полностью вручную с настройками;

2) run immediately - после того, как диалоговое окно задачи закрыто, задача будет запущена (после выполнения всех запущенных задач). Задачи, установленные для запуска немедленно, будут удалены, если автоматически удалить задачи, которые имеют немедленно и завершена успешно, проверяется на странице настроек eraser, задачи, установленные для немедленного запуска, будут сброшены для запуска вручную по завершении задания, если задача была прервана в процессе выполнения (например, при сбое приложения), задача будет автоматически запускаться снова после перезапуска программы;

3) run at restart - задача будет запущена при следующем перезапуске компьютера. Это полезно для стирания файлов, которые в настоящее время используются. Задачи, установленные для запуска при перезагрузке, будут сброшены для запуска вручную после завершения задачи;

4) recurring – удаление будет происходит по графику, которую вы определите на вкладке Schedule.

Нажимаем на кнопку Add Data, там выбираем тип удаления – «Файлы в Папке» (Files in Folder). Метод мы уже выбрали заранее в настройках, так что там ничего не трогаем, смотрим на рисунок 3.6.

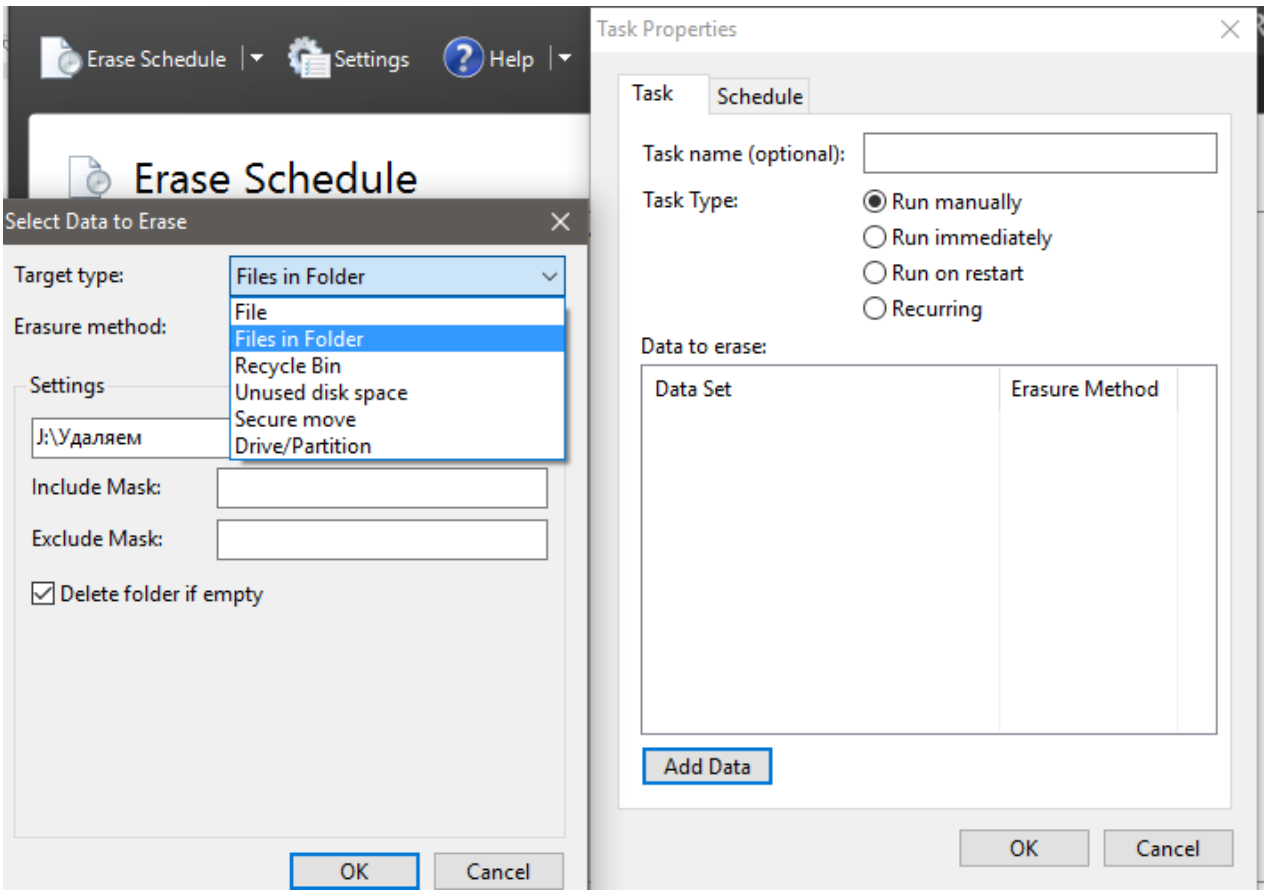


Рисунок 3.6 – Настройка окон задачи для удаления

После нажатие на кнопку ОК, перед главным окном выйдет список задачи, и нажимаем правой кнопкой мышью и запускаем вручную, смотрим на рисунок 3.7. Как видим на рисунках 3.8, 3.9 запуск прошелся успешно и удалилось.

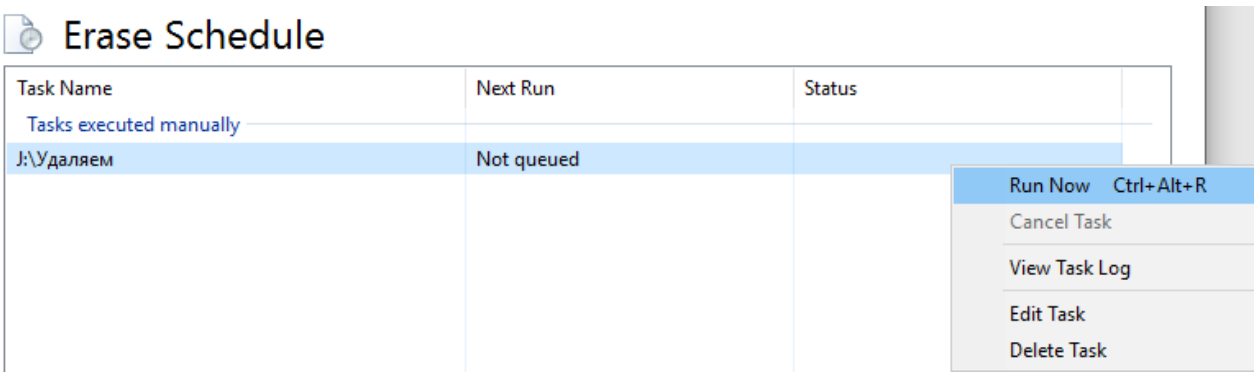


Рисунок 3.7 – Запуск задачи вручную

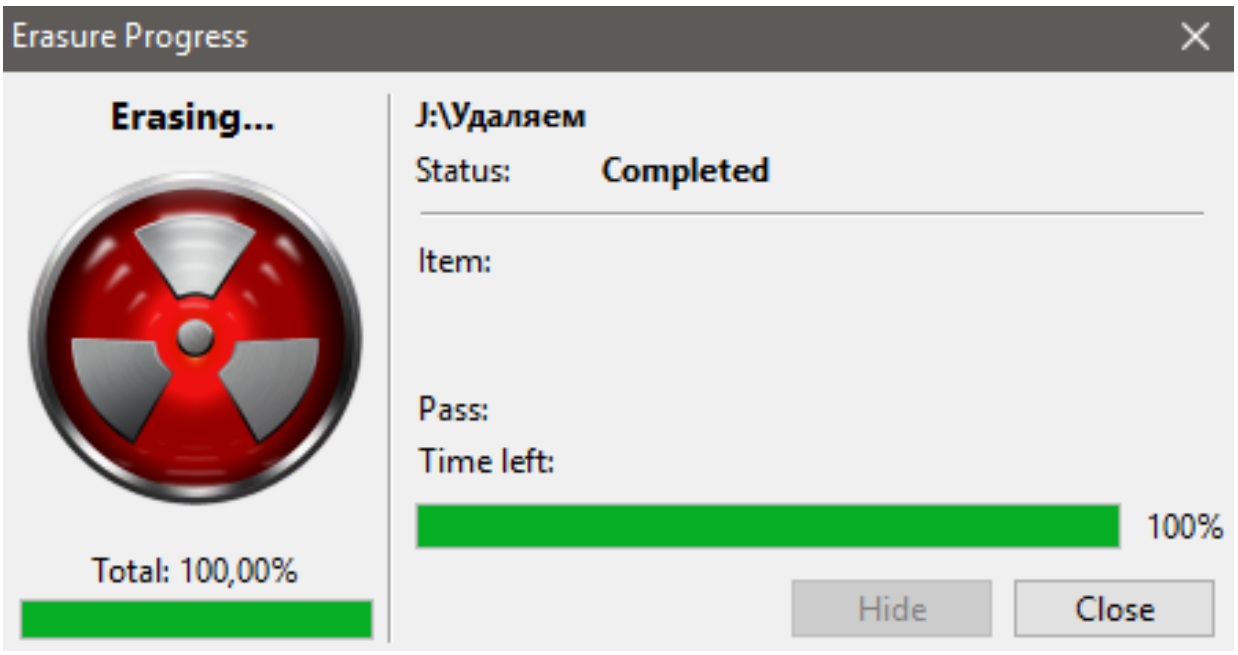


Рисунок 3.8 – Завершение удаления файла

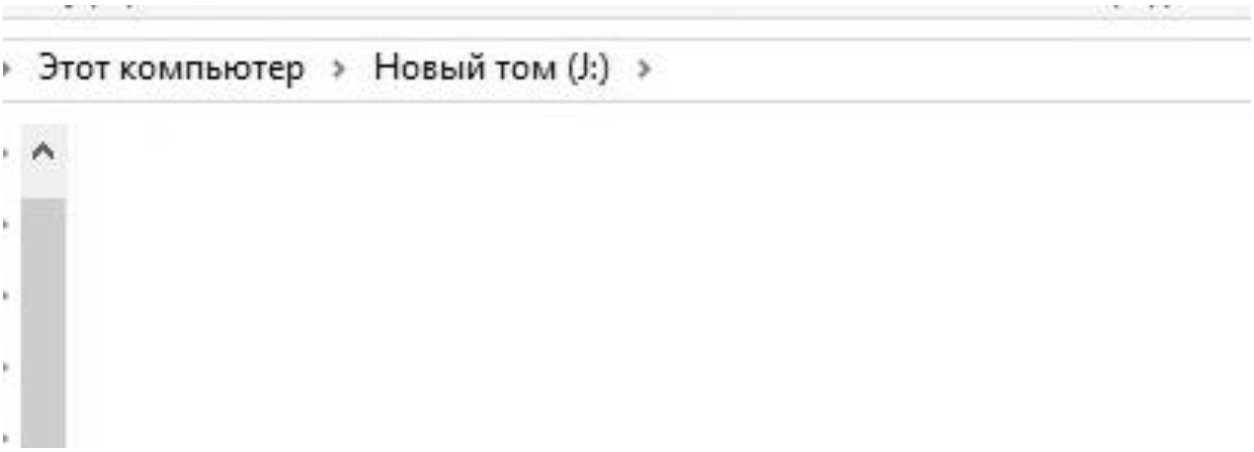


Рисунок 3.9 – Удалилась папка с названием «Удаляем»

Данные удалились за 55 секунд, все 48 МБ. Скорость при перезаписи методом 3 прохода, быстрая.

Теперь обратимся к Форензике, чтобы удостовериться действительно ли удалились файлы с папкой, для этого нам нужно скачать программу AccessData FTK Imager. Это программа независимо от того, идет ли речь о расследовании, судебном разбирательстве или соблюдении требований, AccessData предлагает передовые решения, обеспечивающие мощь судебной экспертизы в ваших руках. В течение 30 лет AccessData работала с более чем 130 000 клиентов в правоохранительных органах, правительственных учреждениях, корпорациях и юридических фирмах по всему миру, чтобы понять и сосредоточиться на своих уникальных потребностях в анализе коллекции. Результат? Продукты, которые дают более быстрый результат, лучшие идеи и больше возможностей подключения. Официальный сайт продукта можно найти ссылку по источнику. [10]

Детально объяснять всю программу не буду, потому что это может занять огромное время, поэтому покажу лишь основы, которые нам хватит для разбирательства с удалением данных, покажу куда надо смотреть и что нужно сделать что бы понять где были изменения или где были удалены файлы или данные. Для начала после открытия программы, нажимаем на кнопку add Evidence item, это мы делаем для того, чтобы создать резервную копию логического диска изначального не тронутого, где все еще есть файлы с папкой «Удаляем», и потом, как только удалим все данные с помощью программы Eraser, сделаем еще одну резервную область логического диска и будем сравнивать между собой изначальную версию с последней (после удаления) смотрим на рисунки 3.10, 3.11.

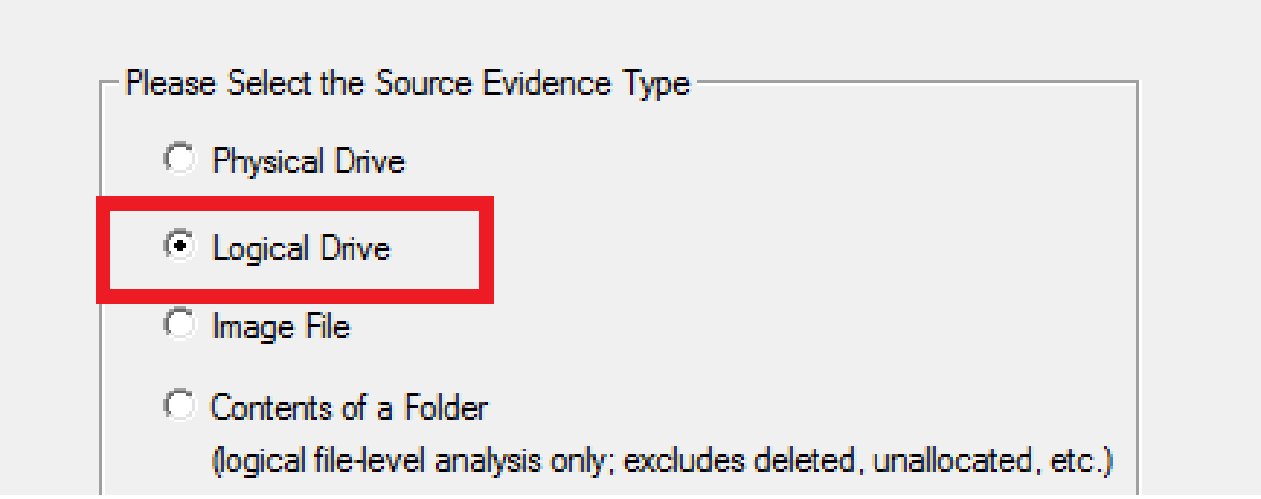


Рисунок 3.10 – Выбор параметра Logical Drive

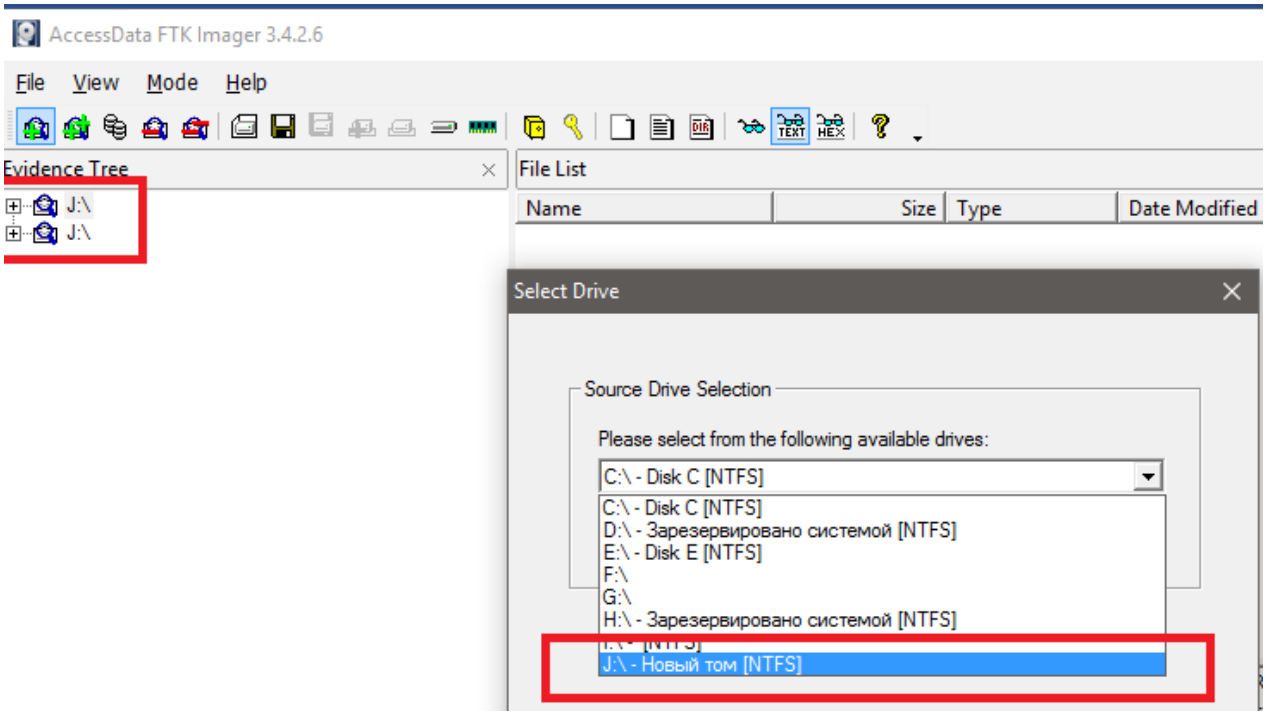


Рисунок 3.11 – Создание копии жесткого диска J

Далее мы заходим в папку логического диска unallocated space, этот раздел содержит все свободные ячейки, так как мы удалили безвозвратно то значит занятое место предыдущее должно освободиться по логике, а значит мы должны искать в свободные ячейки. Ячеек свободных составляет больше 200 000, смотрим на рисунок 3.12.

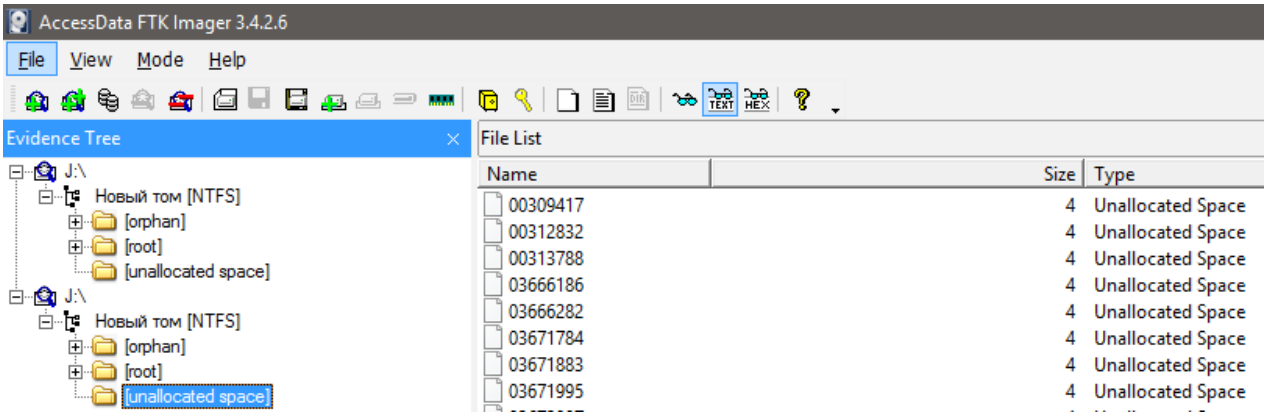


Рисунок 3.12 – Раздел незанятое пространство

На поиски ушло больше 10 минут, но все же я нашел остатки метаданных своих данных которые я удалил, но сперва хочу напомнить, что до этого на логическом разделе ЖД, не было никаких файлов виде Doc, JPG, Mp3, Mp4, exe. Все же я обнаружил остатки памяти в свободных ячейках, благодаря Форензики. На ячейке 11254741 с размером 16 бит, нашлись кусочки формата DOC документа, на рисунке 3.13, мы видим остатки лишь. Но все же как говорилось ранее, гарантия здесь нету полного удаление. Искать полностью все остатки удаленных файлов я не стал, так как доказательство более чем достаточно я предъявил. Но не смотря на найденные файлы, я таки не смог найти формат EXE, смотрим на рисунок 3.14,3.15.

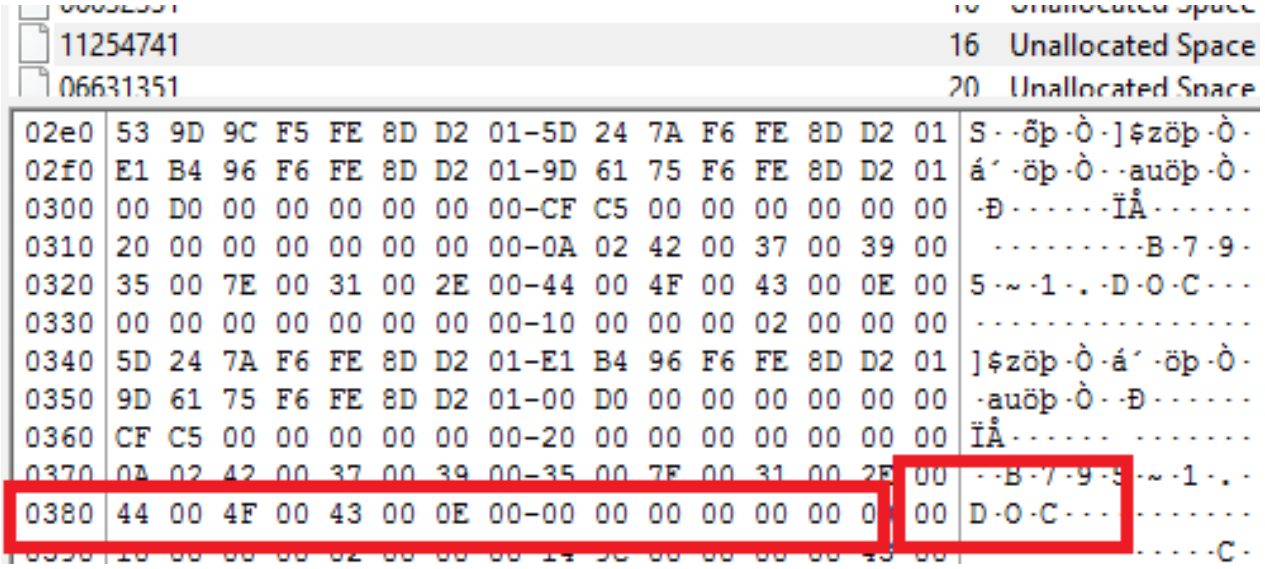


Рисунок 3.13 – Остатки документа формата doc

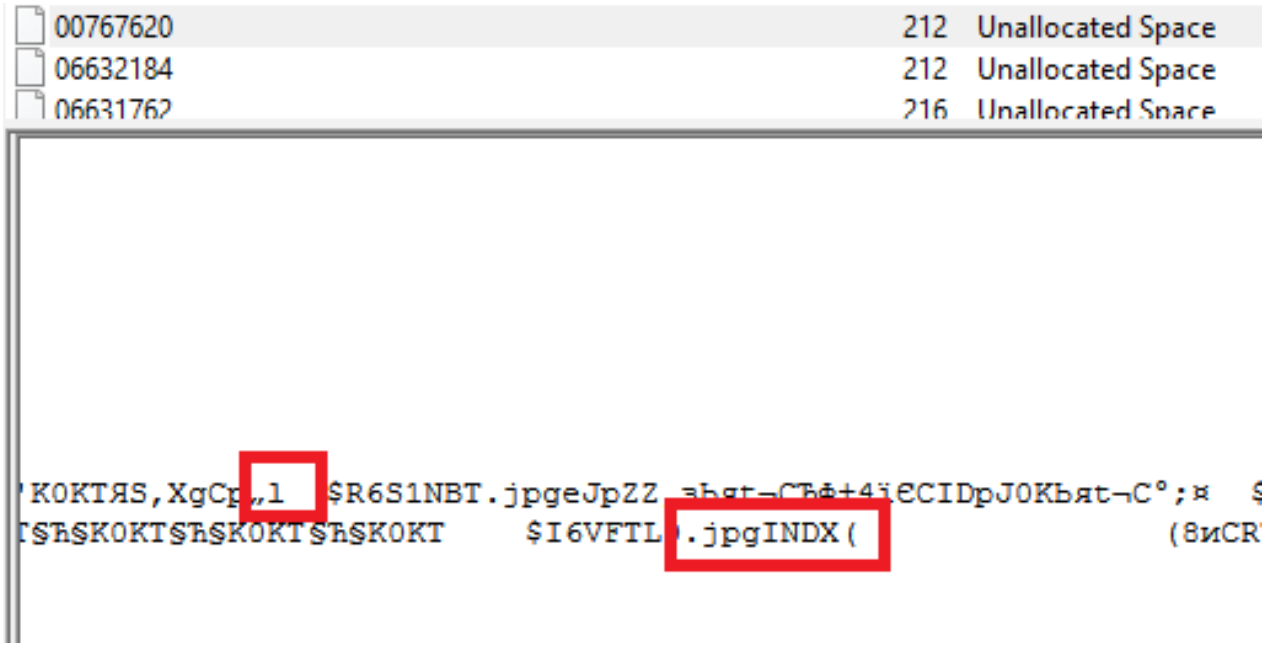


Рисунок 3.14 – Метаданные формата jpg на ячейки 00767620

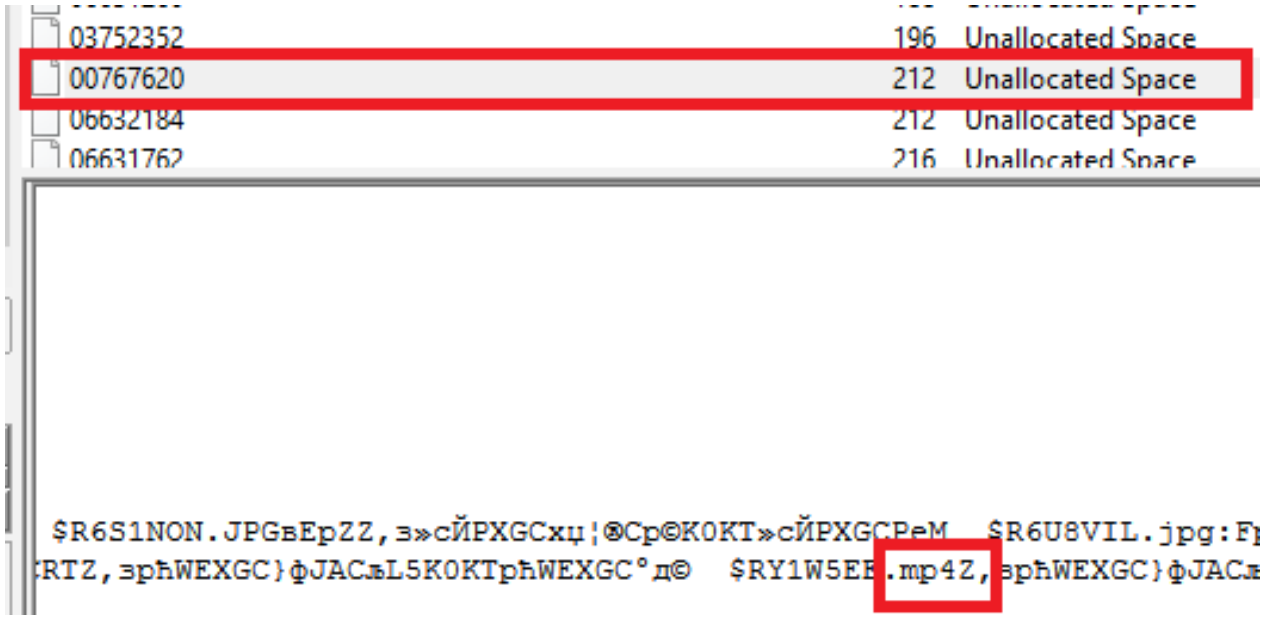


Рисунок 3.15 – Метаданные формата mp4 на ячейки 00767620

Дальнейшее расследования будет идти такими же способами, и далее мы попробуем использовать методы с 3 проходами, смотрим на рисунки 3.16, 3.17:

1) British HMG IS5 (Enhanced) это алгоритм перезаписи с тремя проходами: первый проход - с нулями, второй проход - с одним и последним проходом со случайными данными;

2) US Army AR380-19 представляет собой схему очистки данных, указанную и опубликованную армией США. AR380-19 - это алгоритм перезаписи с тремя проходами. Первый проход со случайными данными, второй со случайным байтом и третий проход с дополнением ко второму проходу США;

3) US Department of Defense DoD 5220.22-M (E) представляет собой алгоритм перезаписи с тремя проходами. Первый проход с нулями, второй проход с одним и последним проходом со случайными данными US.

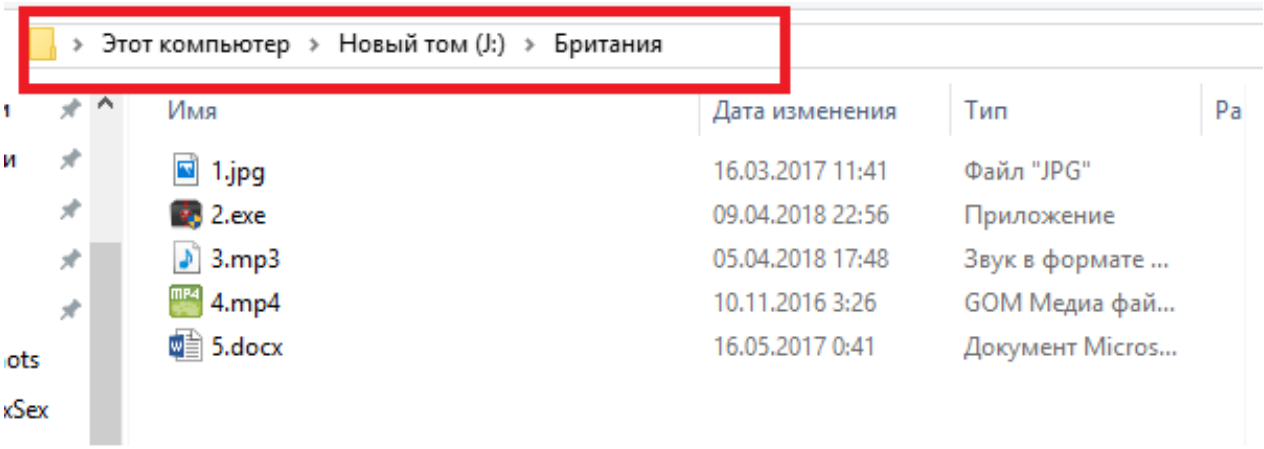


Рисунок 3.16 – Папка с названием «Британия»

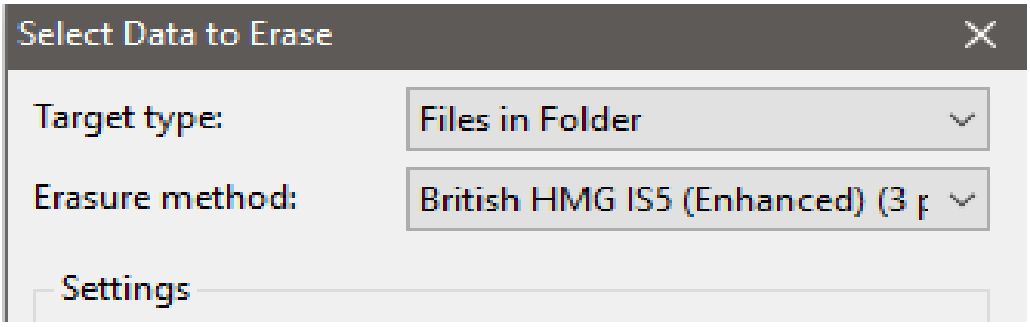


Рисунок 3.17 – Удаление данные методом British HMG IS5

После завершения процедуры благодаря Форензики я смог найти только остатки следы формата Doc, EXE, но оставшиеся форматы mp4, mp3, Jpg мне не удалось найти, так как остальные все ячейки были абсолютно пустыми и забиты нулями. Смотрим на рисунки 3.18, 3.19, 3.20.

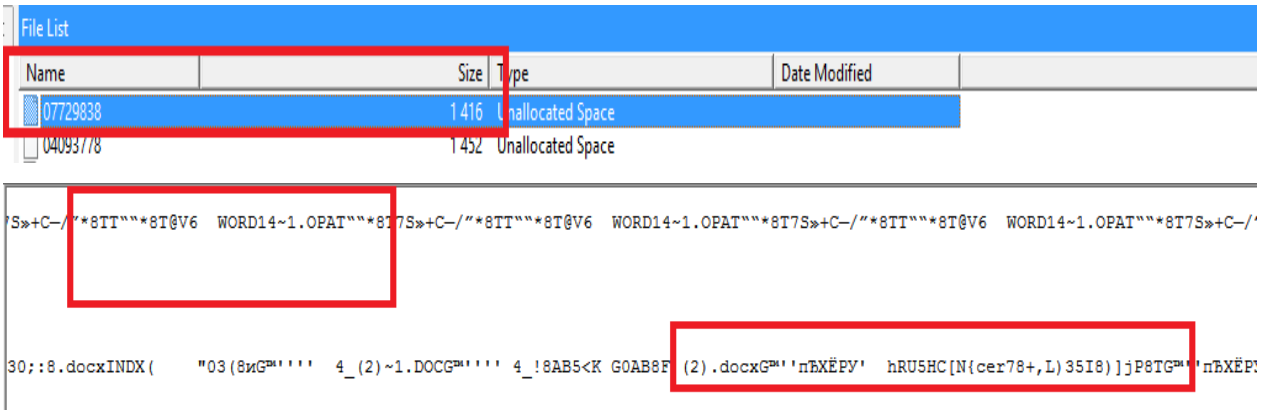


Рисунок 3.18 – Остатки документа на ячейки 07729838

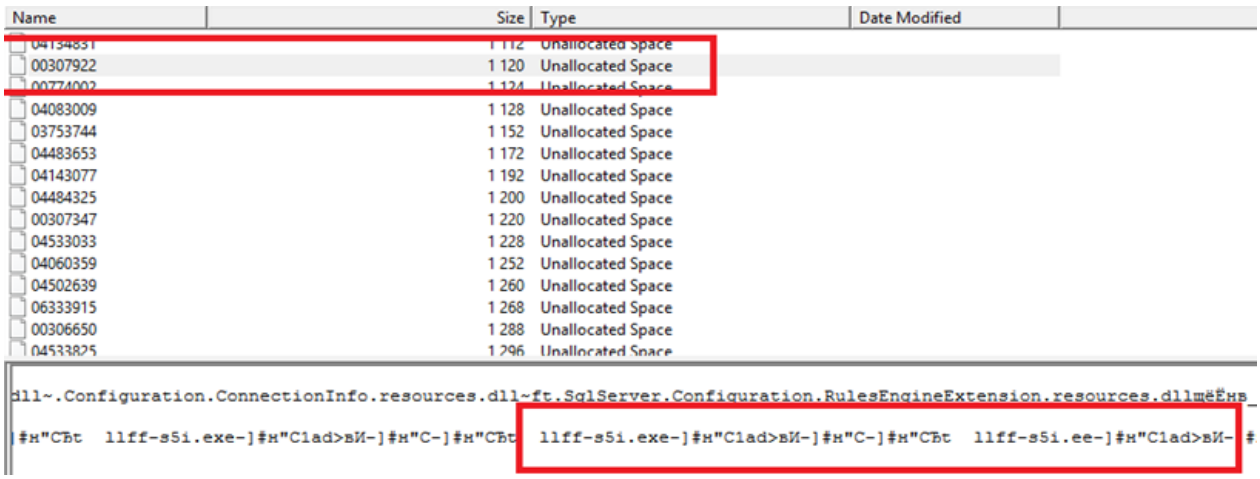


Рисунок 3.19 – Остатки EXE формата на ячейке 00307922

Все ячейки с размером 102 МБ были абсолютно пустыми и нетронутыми, из этого следует сделать вывод, что как только одна ячейка памяти воздвигается к изменению заполнением каких-либо данными, оно забирает часть нужную ему место из пустых ячеек 102 400. Тем самым забирает он автоматический столько сколько ему нужно для вместимости.

После удаления данным методом, я смог найти только корни Документа с форматом DOC, но самое большое что меня шокировала, это то что я смог найти без изменённое название самого документа, этот метод попросту проигнорировал переименование псевдослучайными данными сам документ и благодаря этому я смог найти название документа – «5.doc». Смотрим на рисунки 3.20,3.21,3.22,3.23.

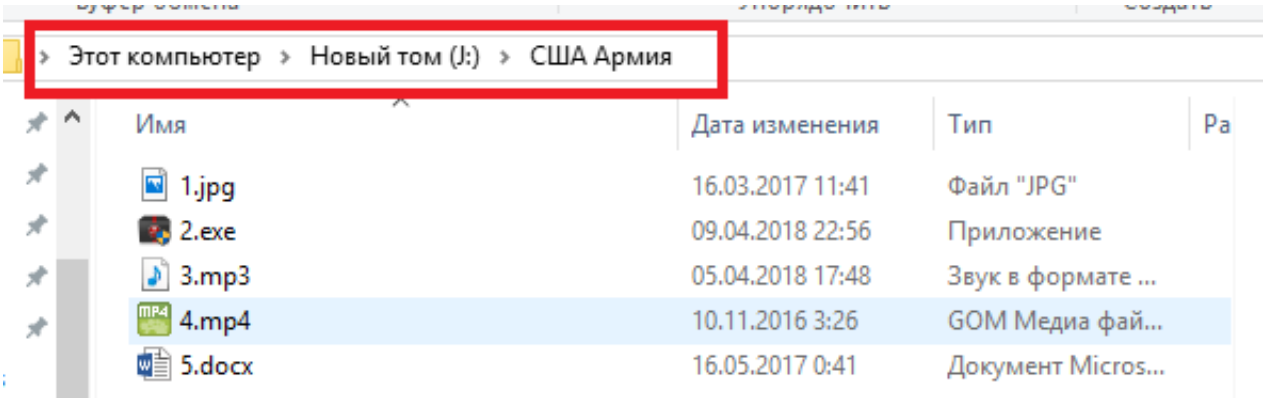


Рисунок 3.20 – Папка «США Армия»

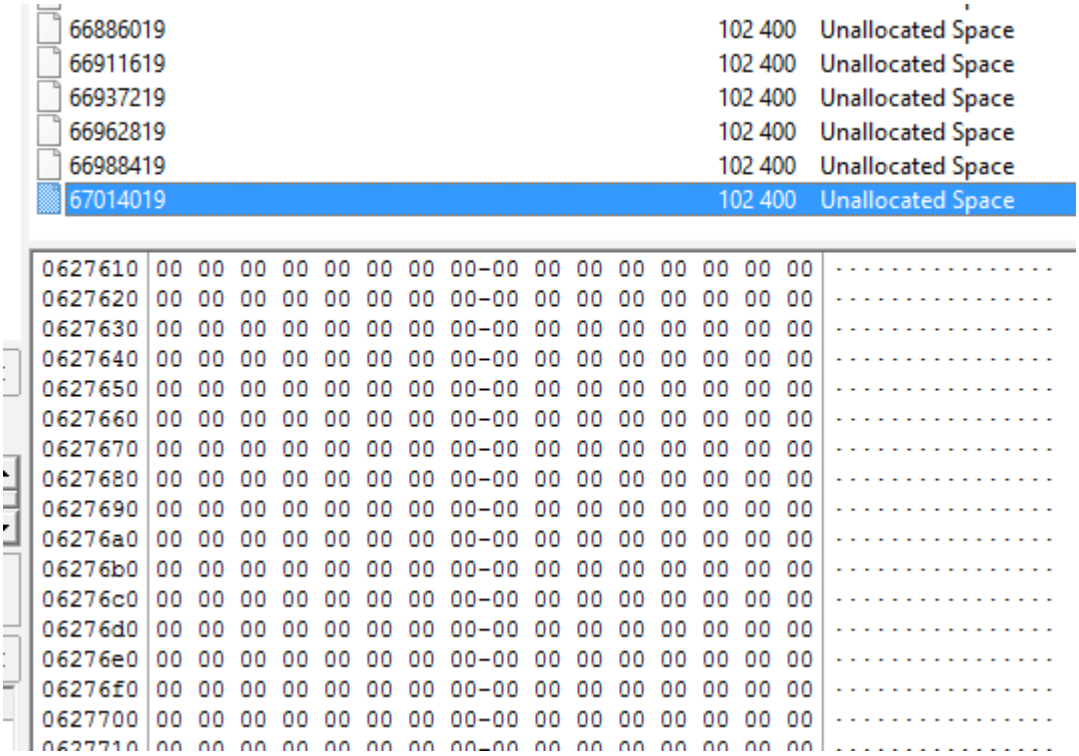


Рисунок 3.21 – Все пустые ячейки с размером 102 400

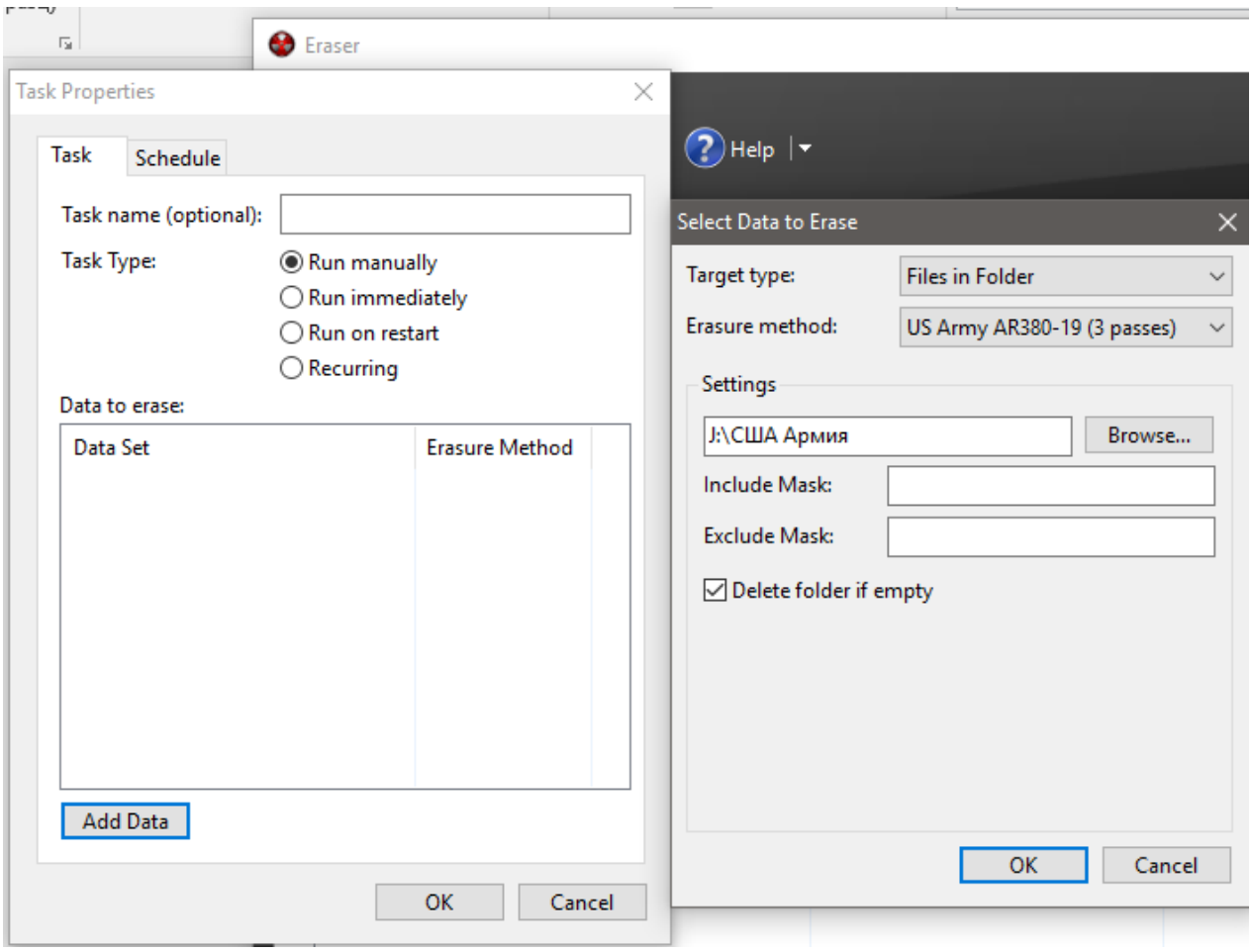


Рисунок 3.22 – Удаление методом US Army AR380-19

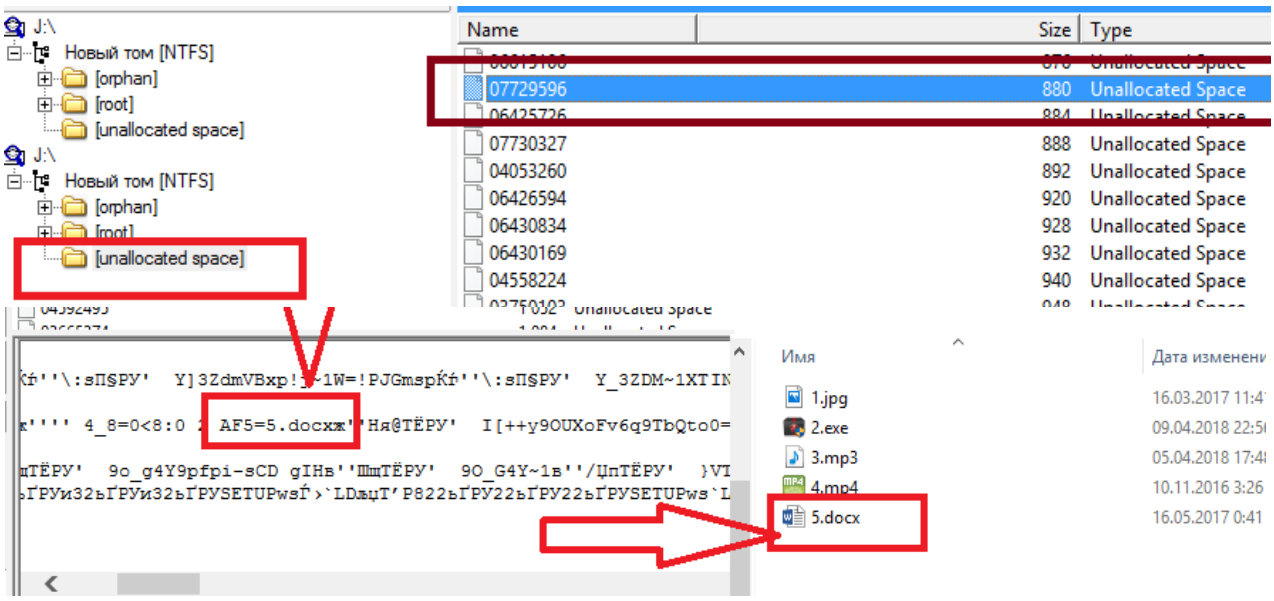


Рисунок 3.23 – Найдена ссылка на удаленный документ без измененным названием на ячейке 07729596

Теперь как мы завершили с экспериментом удаление файлов и папок, попробуем удалить весь физический ЖД с размером 500 гб, методом German VSITR с 7 проходами, смотрим на рисунок 3.23.

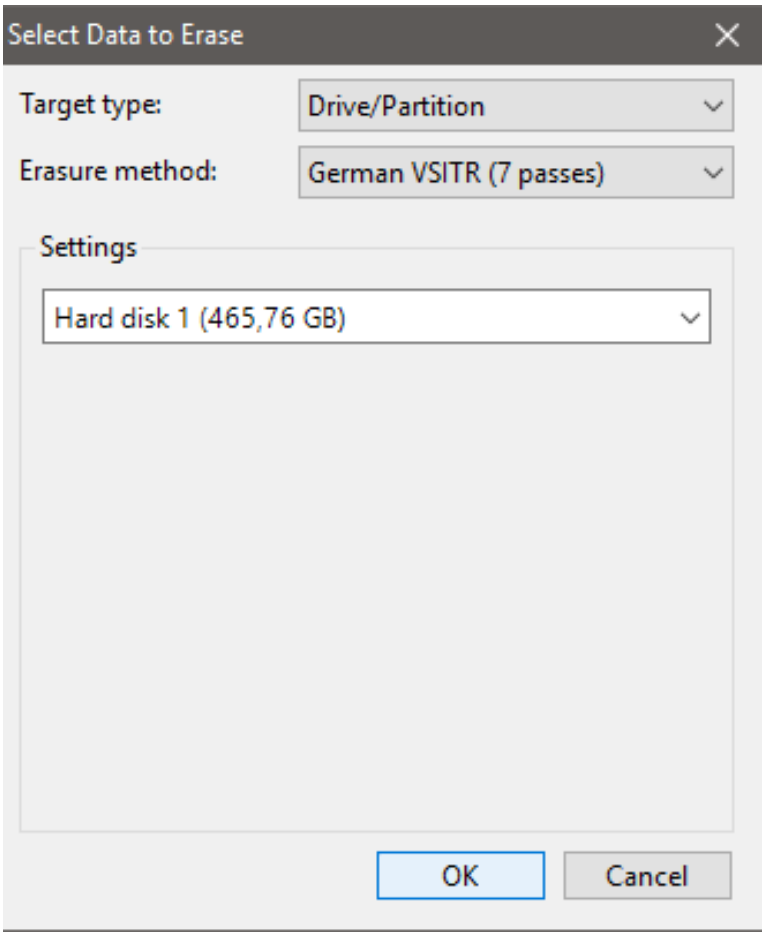


Рисунок 3.24 – Удаление методом German VSITR с 7 проходами

Процедура удаления заняло 35 часов 30 минут. И результат оправдал себя, сразу же проверил методом Форензики, но бессчетно все данные аннулированы и были чистыми, смотрим на рисунок 3.25.

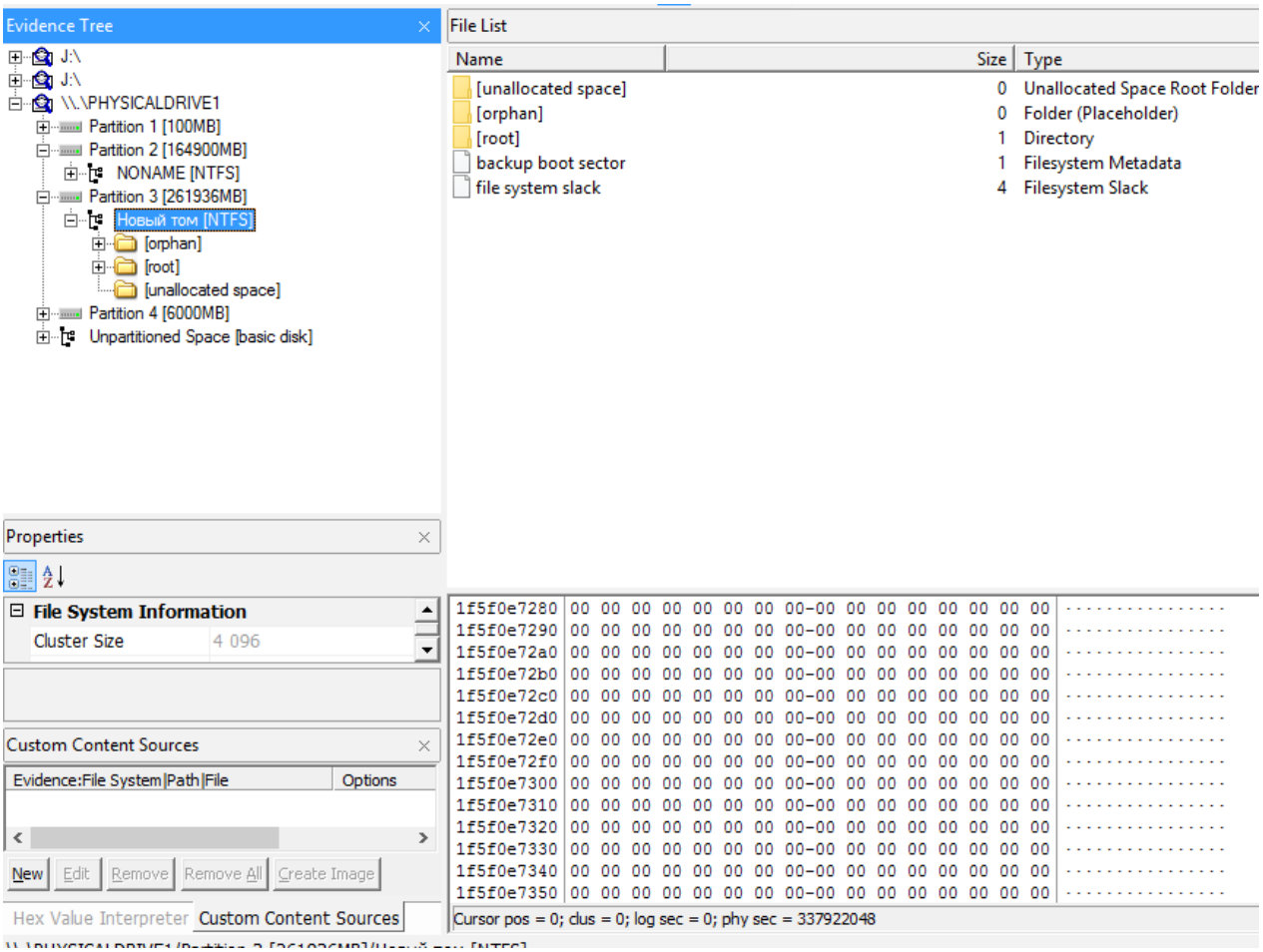


Рисунок 3.25 – Чистый ЖД после процедуры стирания 7 – проходами

Попробовал восстановить с помощью знаменитой программой R-Studio, но результат был тем же, что и на Форензики. Все данные были удалены, кроме системных файлов для поддержки работы ЖД, но гарантированно ли удалены мои данные с папками и прочими файлами разных форматов, чтобы ответить на этот вопрос, я отправил жесткий диск в дата центр специалистом платным услугам, смотрим на рисунки 3.26, 3.27.

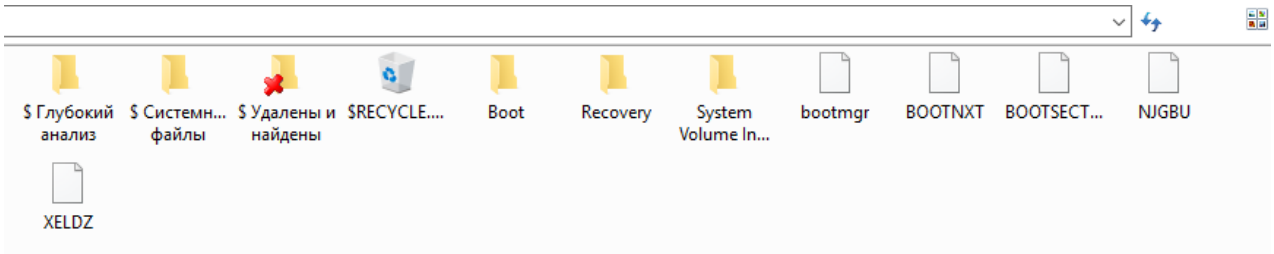
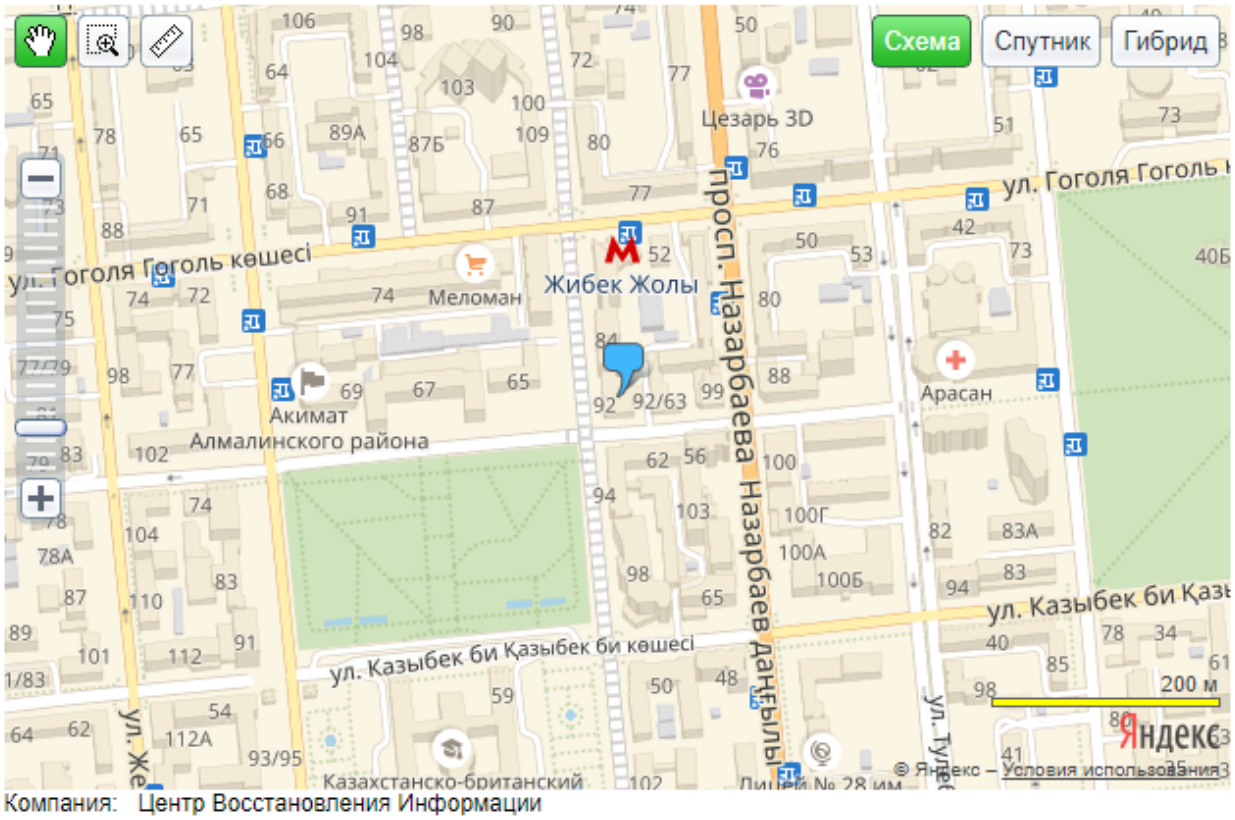


Рисунок 3.26 – Восстановление с помощью программы R-Studio

Время на восстановление ушло 3 дня. Восстановить ничего не удалось. Какие методы используют для восстановления информации «Центр Восстановления Информации», мне не сказали, для них это конфиденциально.



Компания: Центр Восстановления Информации

Телефон: +7 (727) 317-63-06 +7(701) 799-35-12

Местоположение: 050004, Казахстан, г.Алматы, ул. Панфилова 92, 6-этаж, оф. 47 уг.ул. Айтеке-би (б. Октябрьская)

Наш сайт: www.ctvi.kz

Рисунок 3.27 – Центр Восстановления Информации

3.2 Программа O&O SafeErase

Главное окно программы, мы будем использовать два режима удаления, а именно «удаление папок и файлов», «удаление жесткого диска». Смотрим на рисунок 3.28.

Программа содержит шесть разных методов удаления:

1) Overwrite data with zeros;
2) Lowest Security (1 run);
3) Low Security (3 Cycles) US DoD 5220.22-M;
4) Medium security (6 runs) German BSI;
5) High Security (7 runs) DoD 5220.22-M (E);
6) Highest Security (35 runs) Peter Gutmann.

Мы будем использовать методы Medium security (6 runs) German BSI, High Security (7 runs) DoD 5220.22-M (E).

Будем использовать локальный диск j, жесткого диска модели ST500LT012-9WS142. Диск полностью пустой, чистый. Смотрим на рисунки 3.29, 3.30, 3.31.

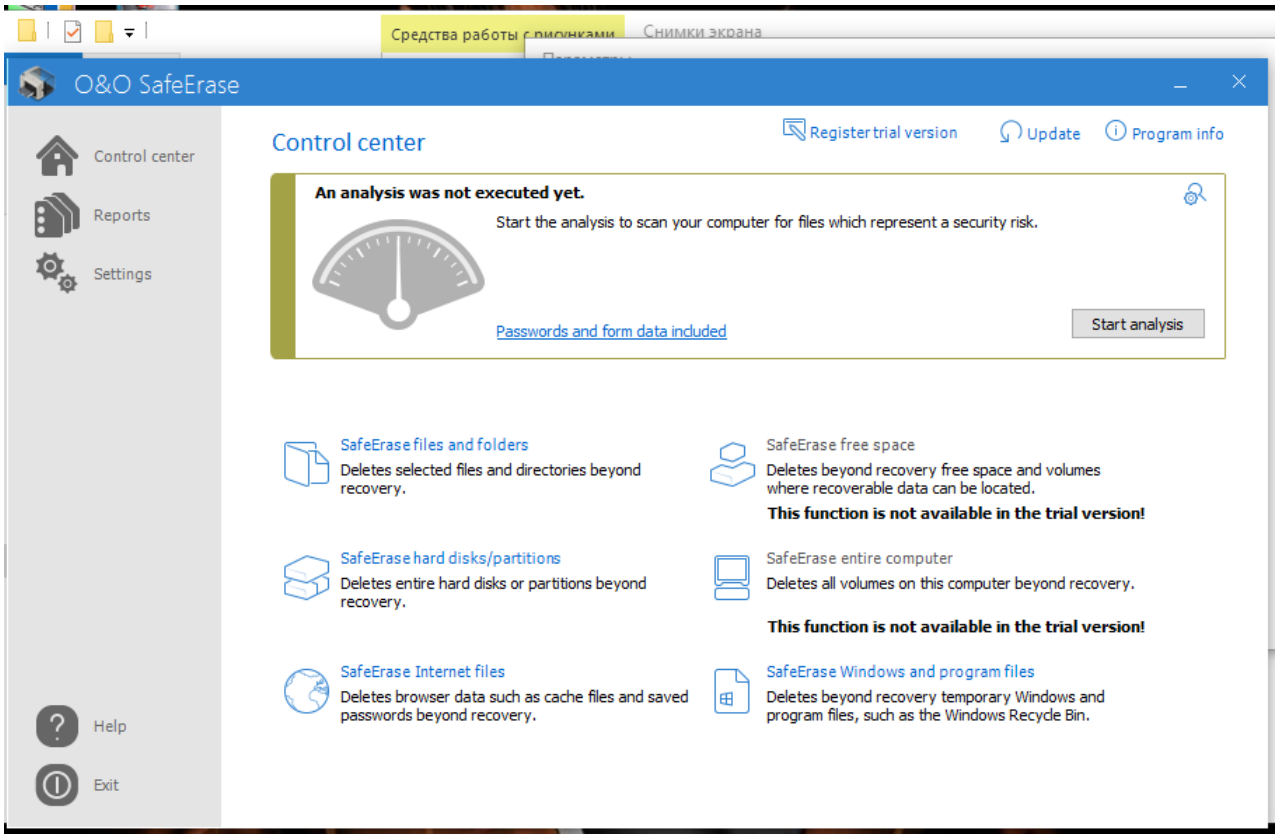


Рисунок 3.28 – Главное окно программы

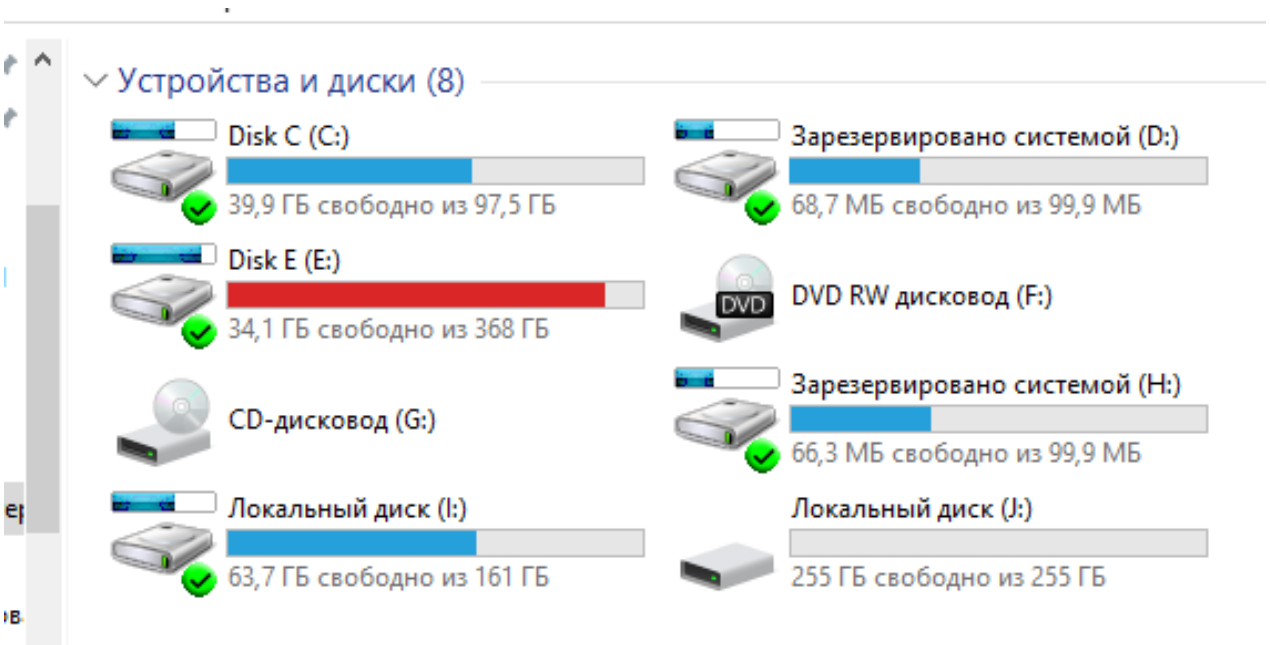


Рисунок 3.29 – Пустой локальный диск J

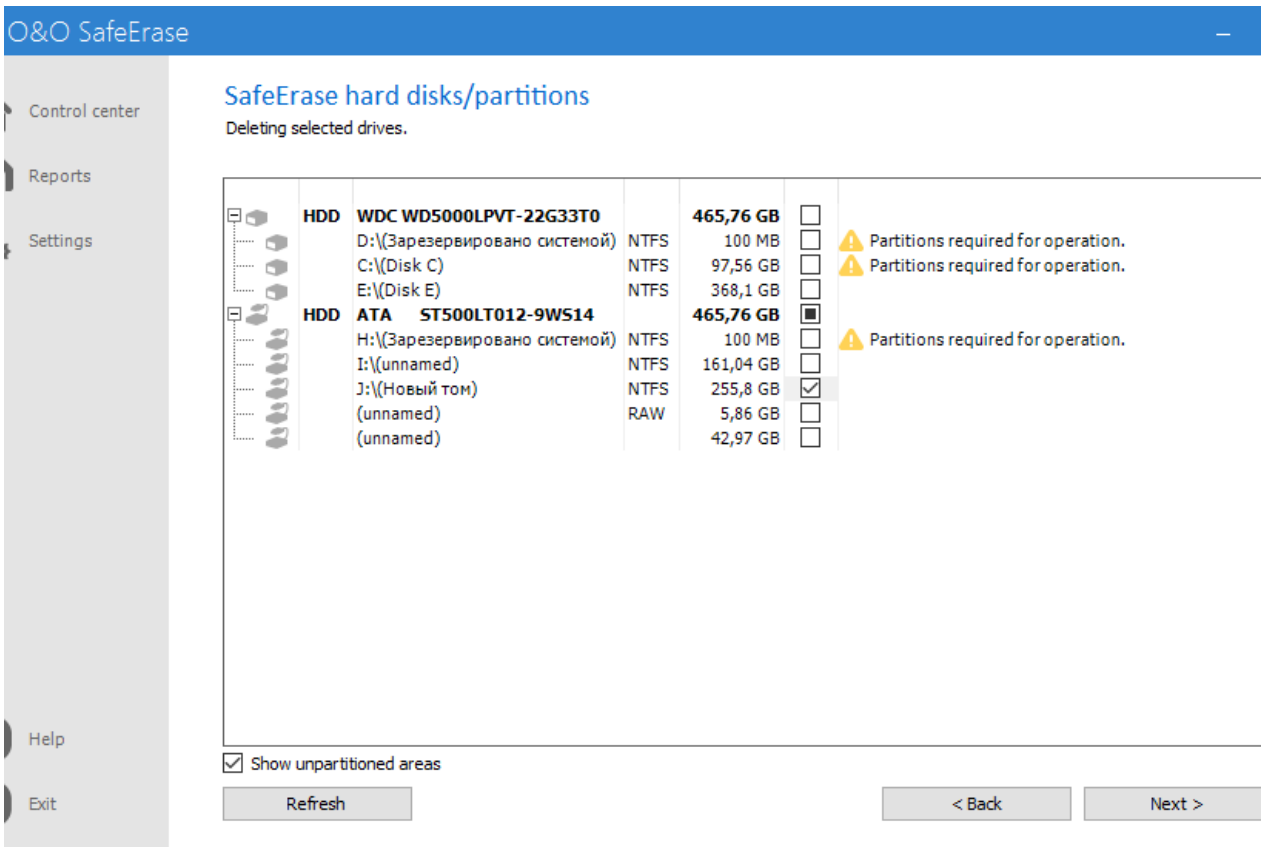


Рисунок 3.30 – Выбор логического раздела J

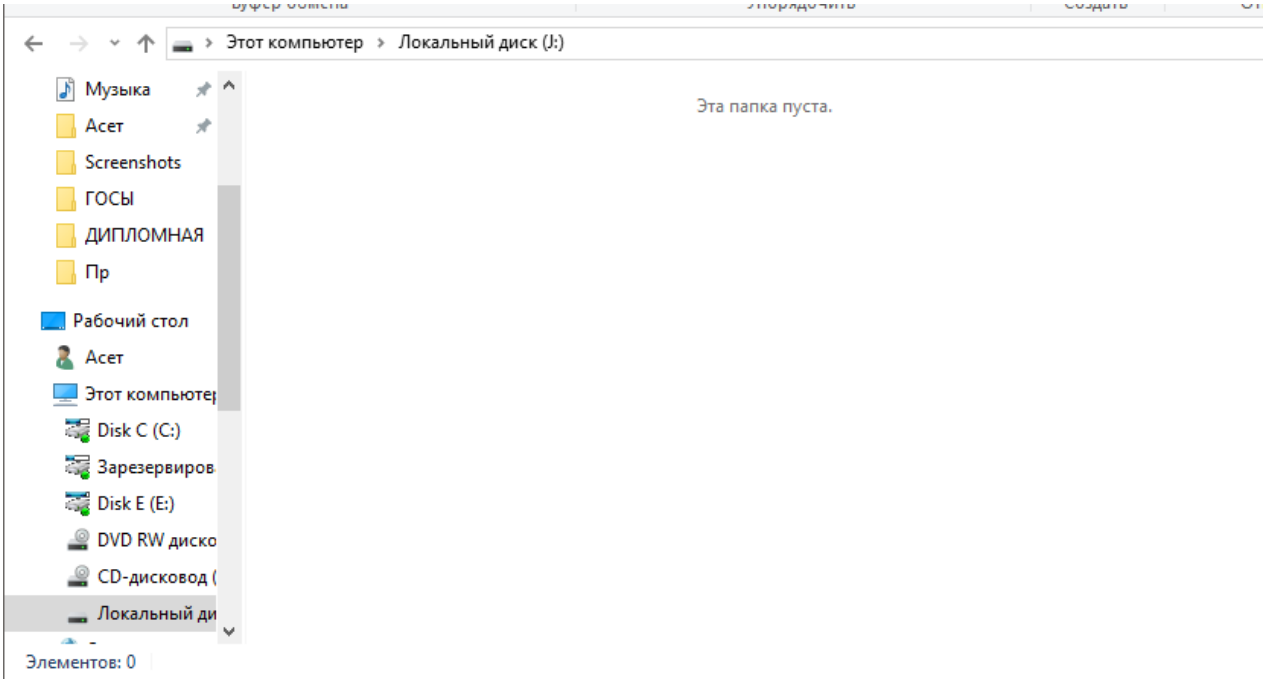


Рисунок 3.31 – Пустой раздел J

Обратимся к Форензики программы FTK imager, смотрим на раздел, и видим, что все ячейки аннулированы и пустые, что значит раздел чист. Смотрим на рисунки 3.32, 3.33.

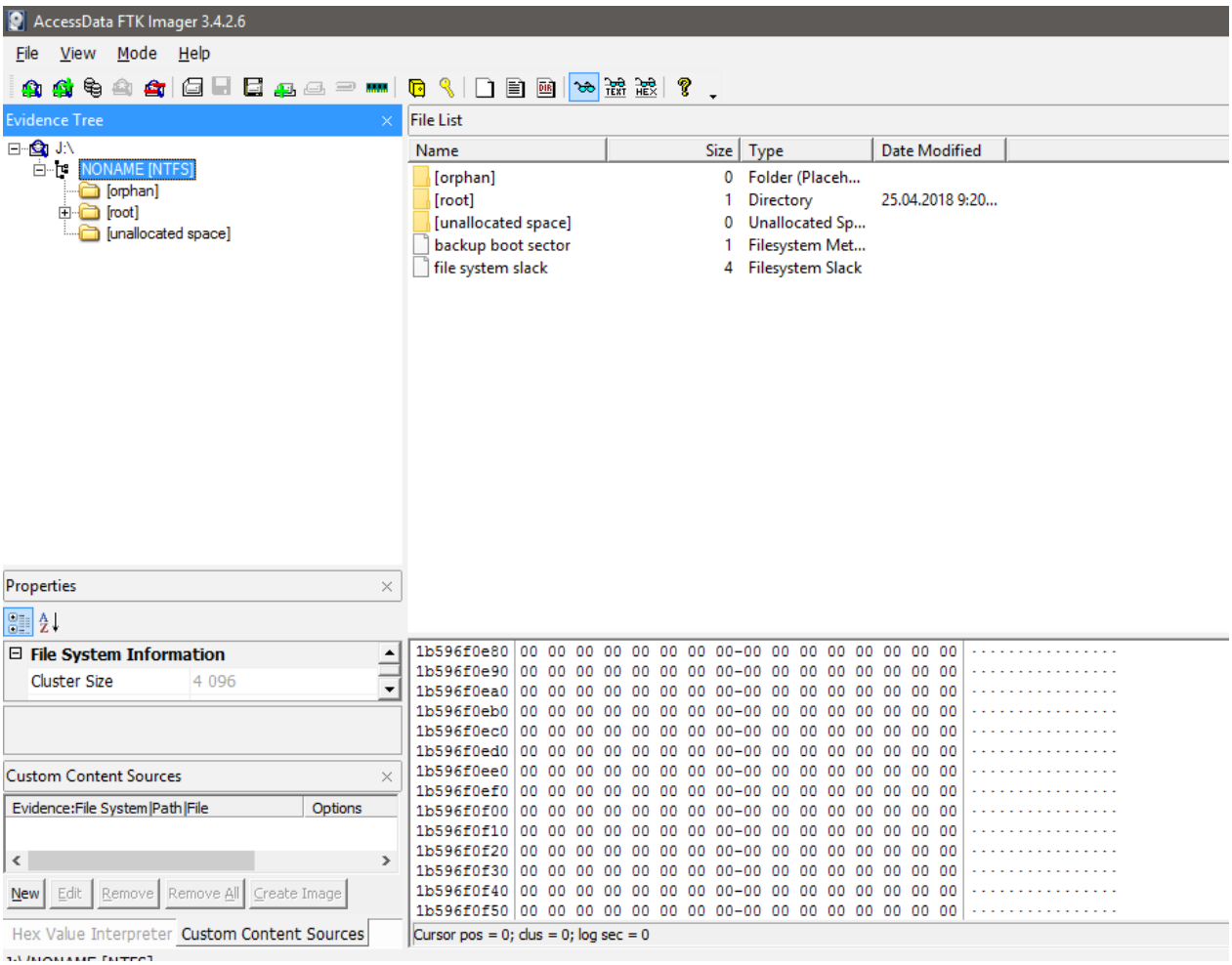


Рисунок 3.32 – Сканирования логического раздела программой AccessData FTK Imager

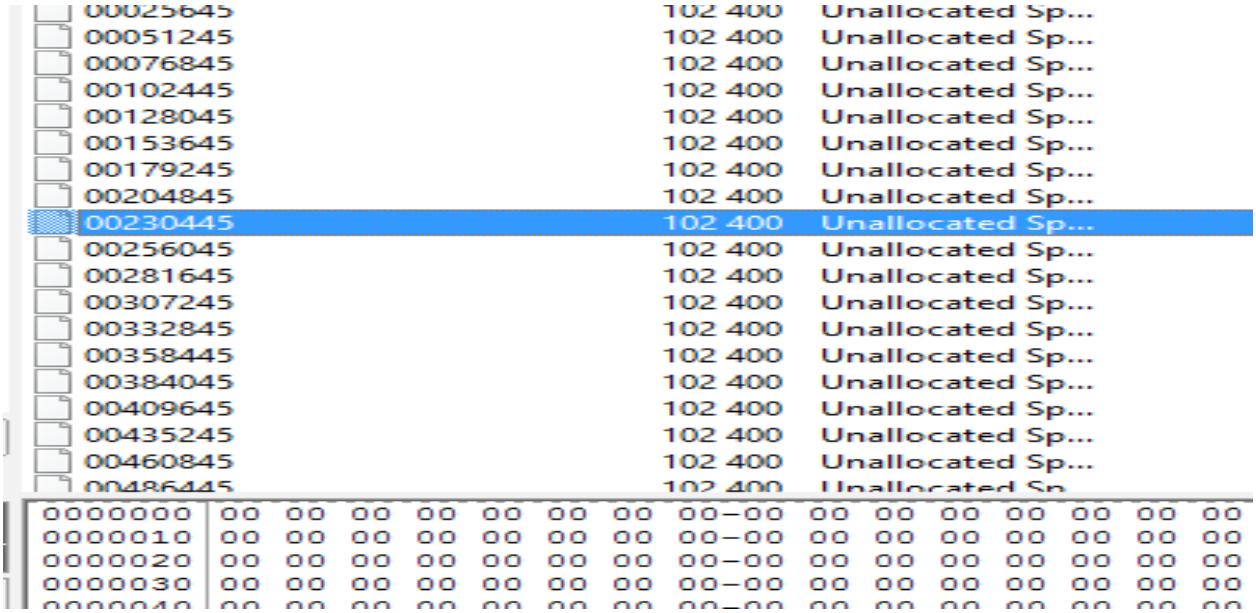


Рисунок 3.33 – Папка незанятое пространство полностью свободная

Папку «Файлы», копируем на пустой логический раздел J. Папка содержит форматы exe, jpg, doc, mp3, mp4. На рисунке 53 можно увидеть, что в логическом разделе появилась папка «Файлы» с данными. Теперь удалим их с помощью метода шесть проходов Medium security (6 runs) German BSI. Смотрим на рисунки 3.34, 3.35, 3.36, 3.37,3.38,3.39,3.40.

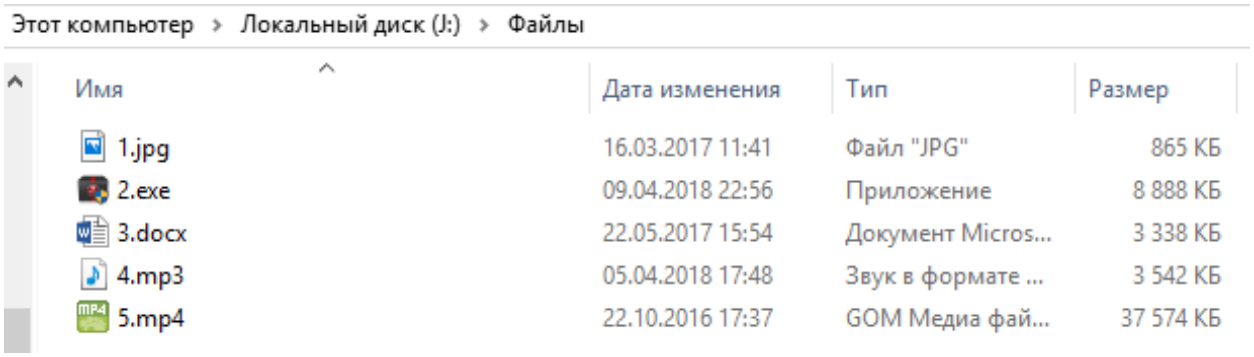


Рисунок 3.34 – Папка «файлы»

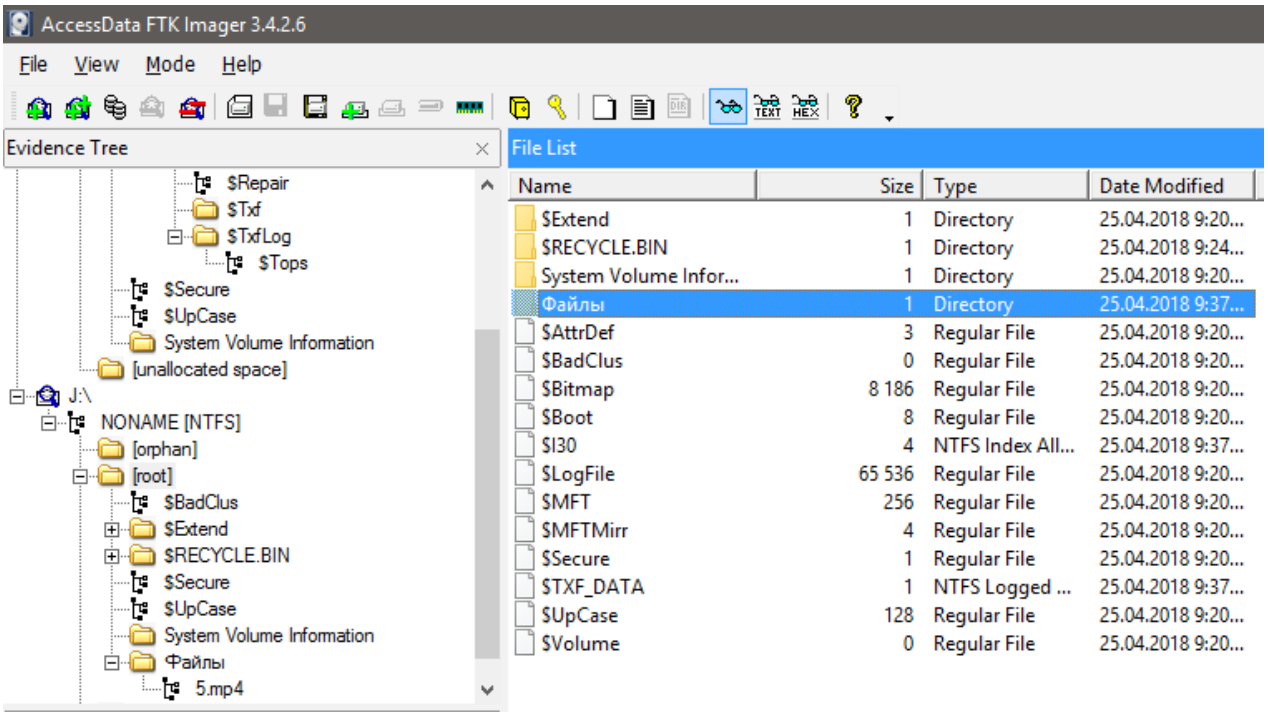


Рисунок 3.35 – FTK Imager, папка «Файлы»

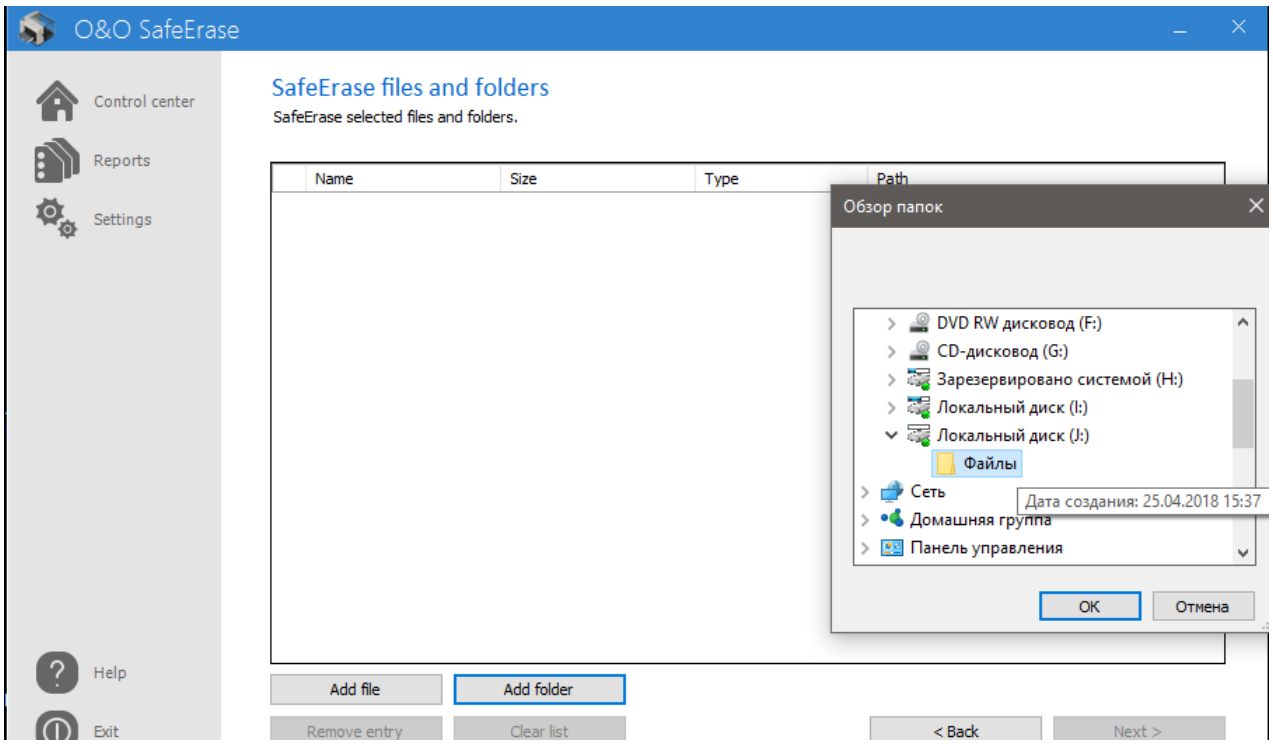


Рисунок 3.36 – Удаляем в режиме files and folders

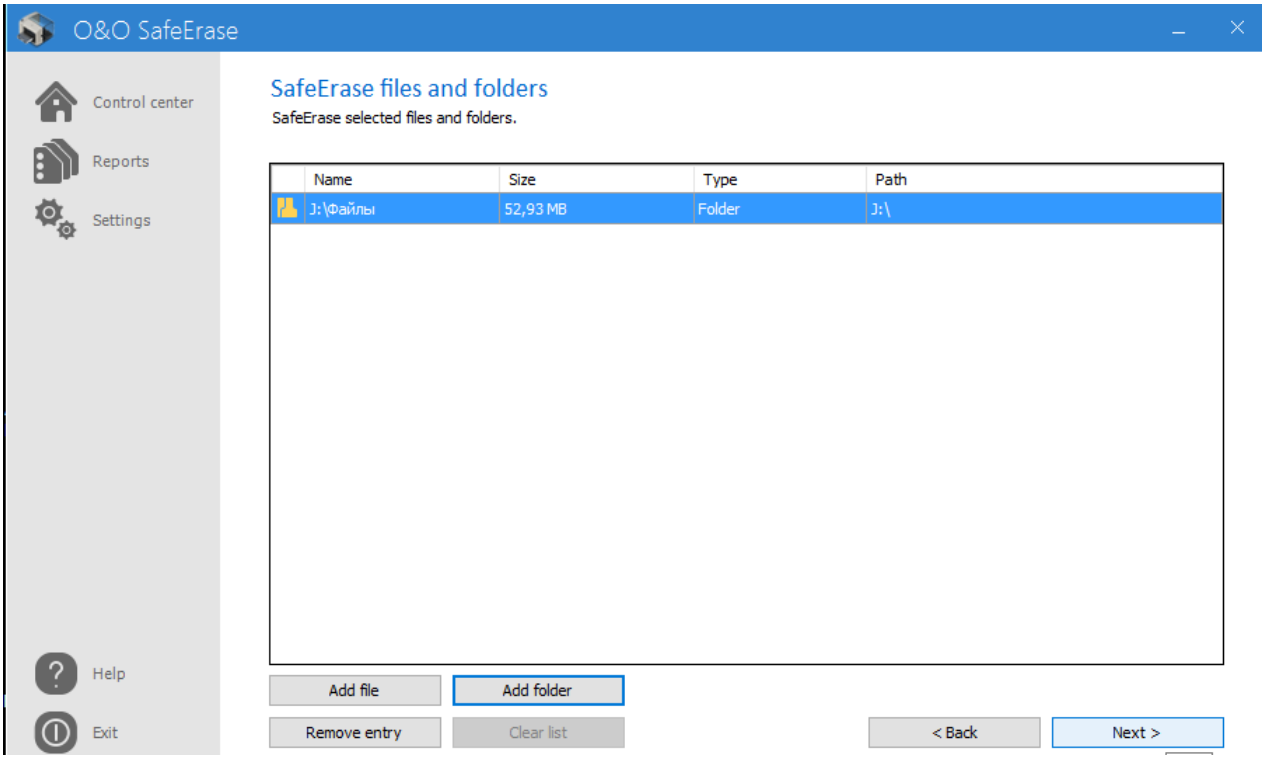


Рисунок 3.37 – Выбор папки «Файлы»

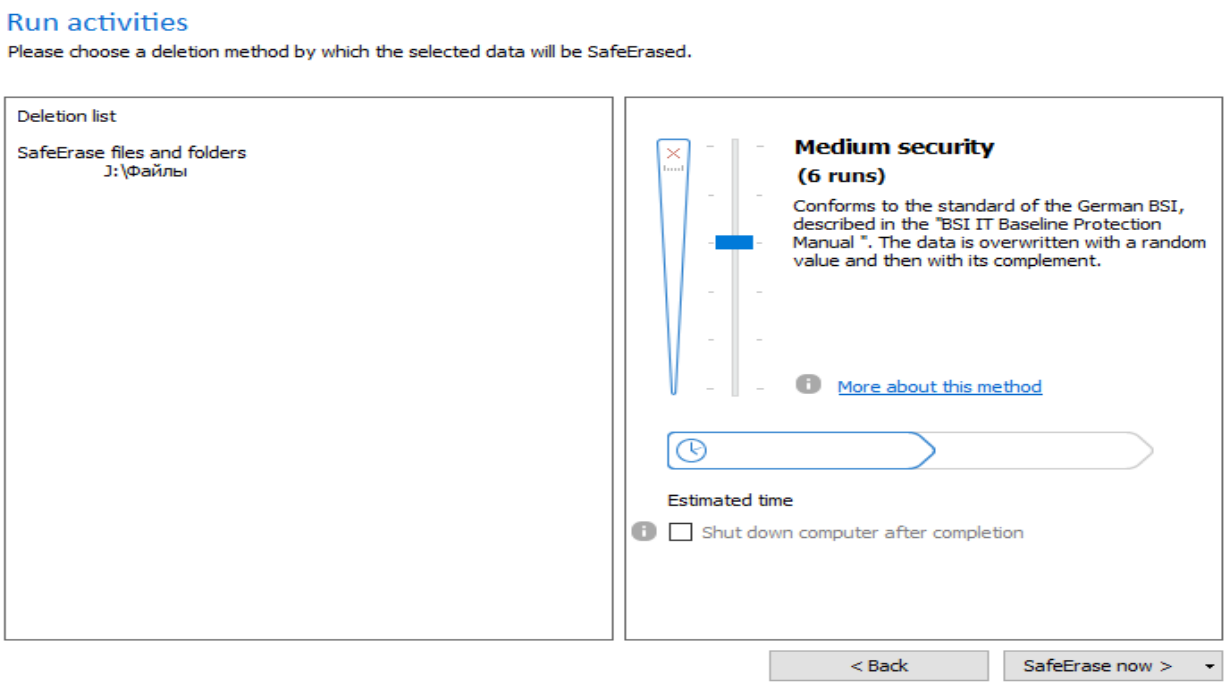


Рисунок 3.38 – Выбор метод с шестью проходами

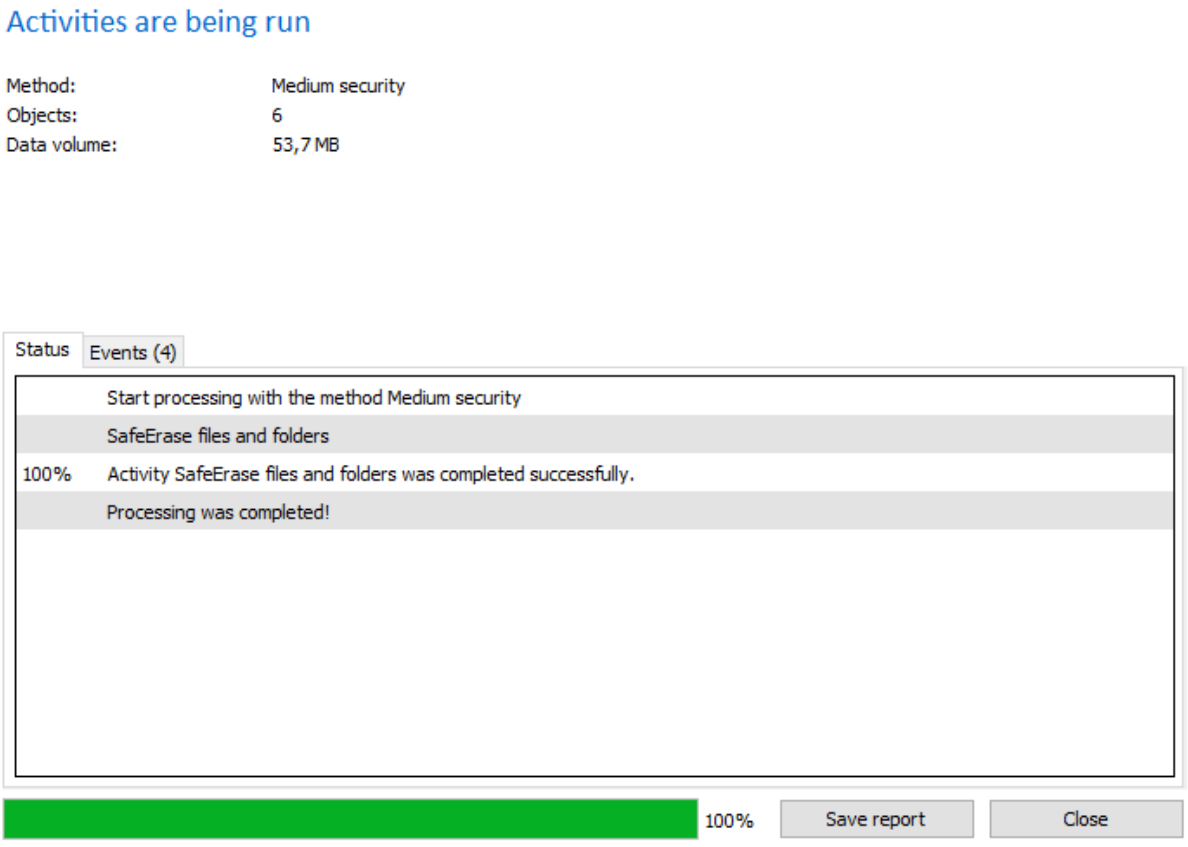


Рисунок 3.39 – Процесс удаления завершено

Смотрим снова на раздел j, и видим, что данные удалились. Проведем теперь компьютерную криминалистику, будем искать удаленные данные, если это возможно.

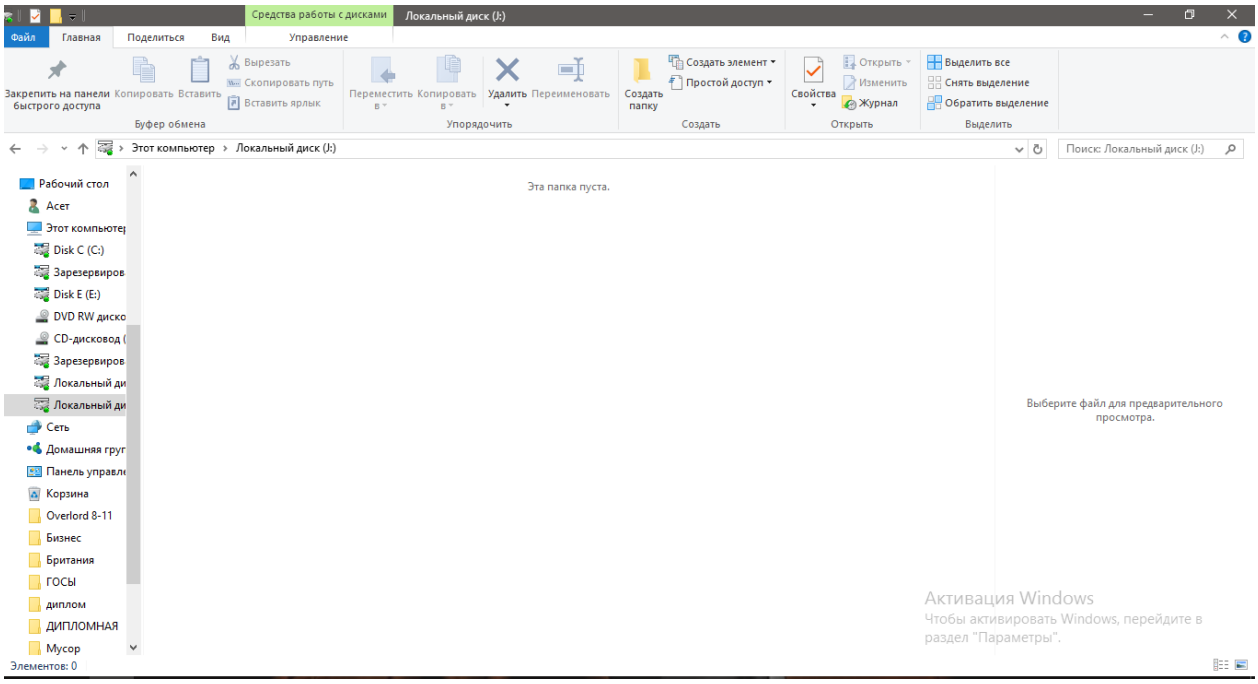


Рисунок 3.40 – Раздел пуст

Смотрим на рисунок 3.41, 3.42 видим, что появилась новая папка с названием ZZZZZ, оно лежит в разделе Root, папка содержит только что удаленную информацию все они переименованы. Все удаленные данные не были перемещены в раздел «Unallocated space», содержимое внутри файлов заполнились маской, но размер исходных файлов не были изменённые, это можно увидеть на рисунке 3.43.

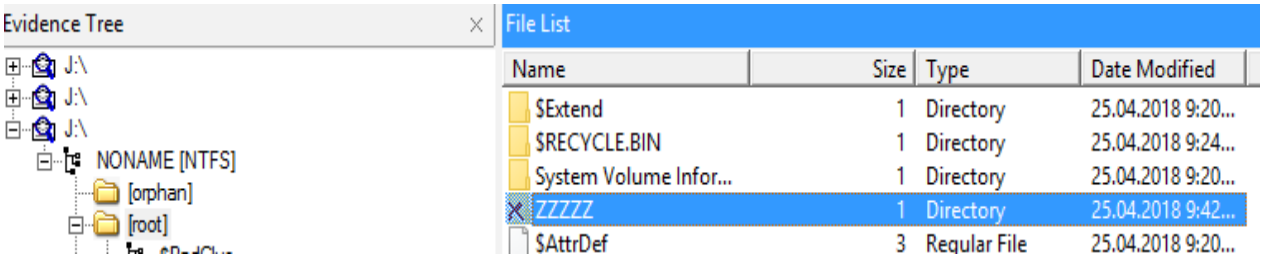


Рисунок 3.41 – Переименованная и удаленная папка «Файлы»

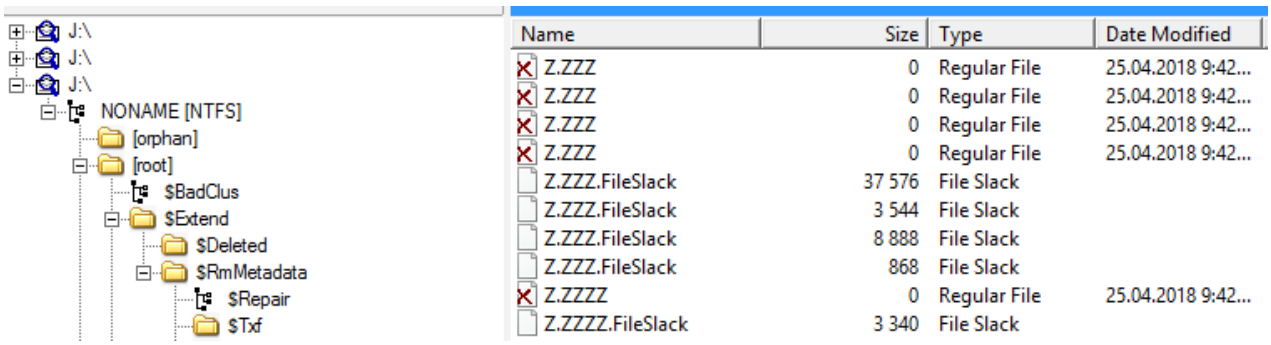


Рисунок 3.42 – Все удаленные файлы

Данный метод очень слабый, потому что при удалении мы не должны даже видеть эскизы прошлых файлов, а в нашем случае все наоборот, мы даже можем зарегистрировать время, дату, когда были удалены эти все файлы. Смотрим на рисунок 3.43.

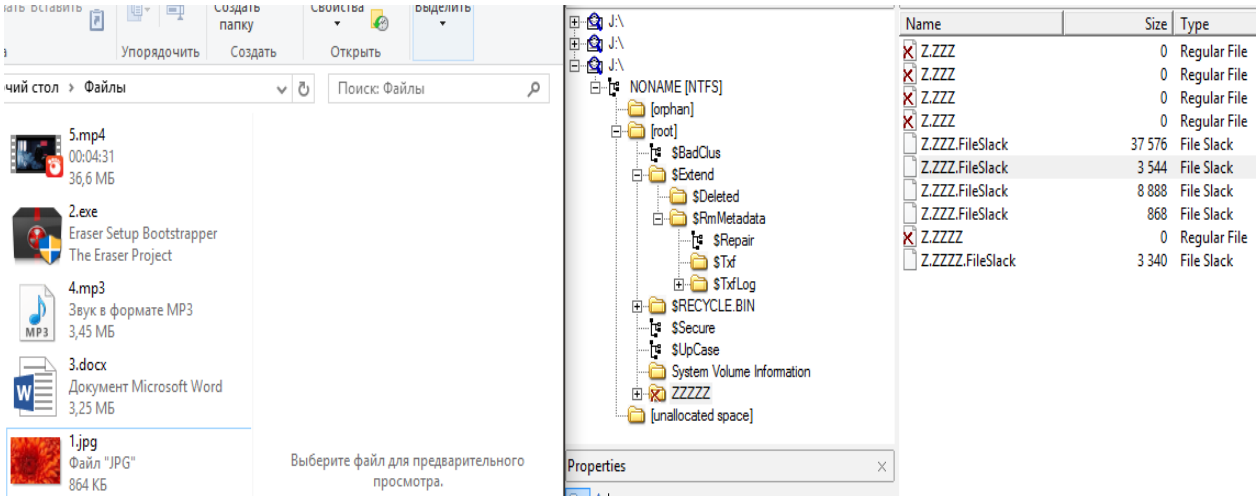
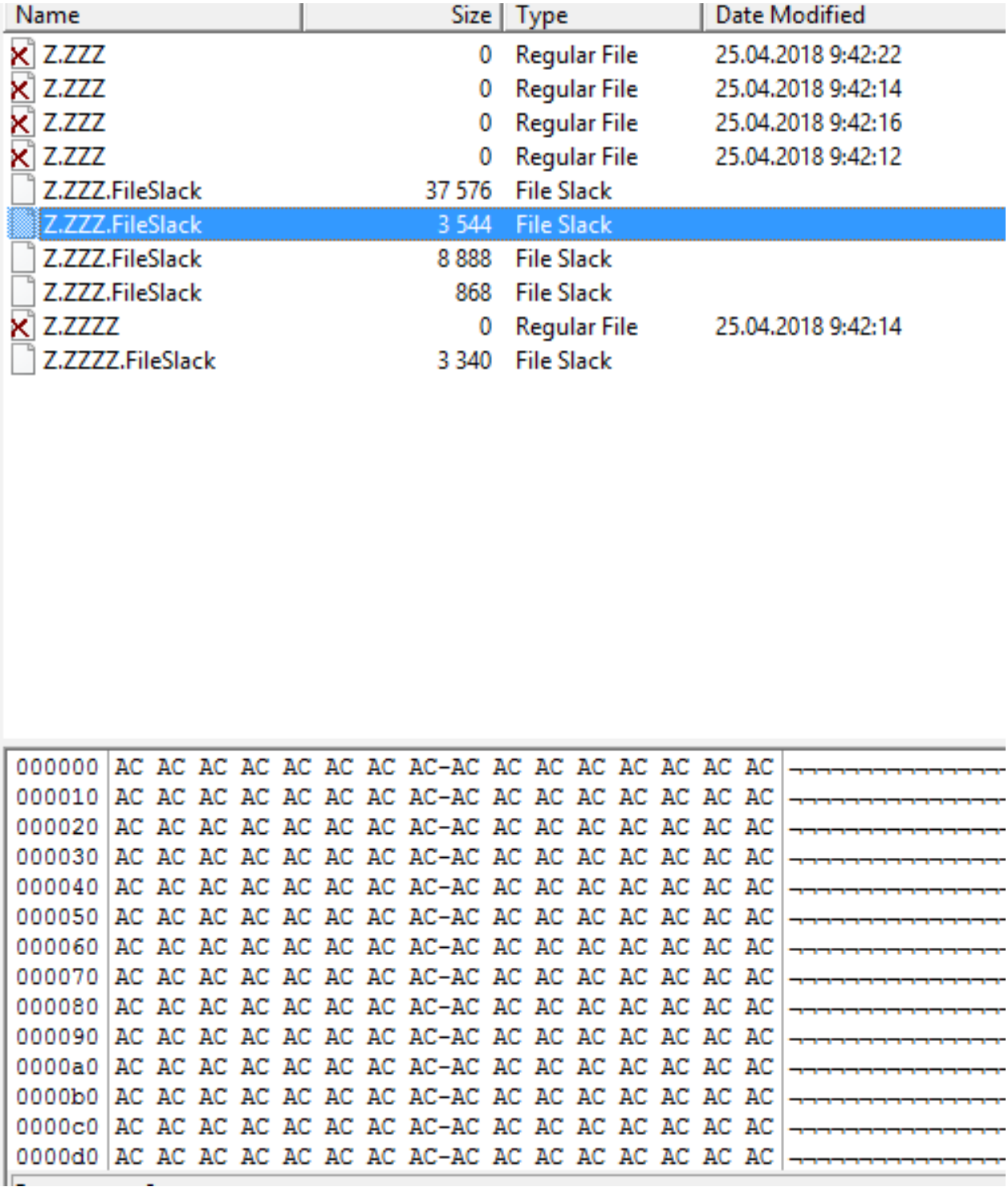


Рисунок 3.43 – Размеры файлов исходных и удаленных совпадает, время и дата удаления так же зафиксированы

Внутри файлов при виде HEX формате, можно заметить, что все пункты заполнились одними и теми же данными «AC», смотрим на рисунок 3.44.



Name	Size	Type	Date Modified
Z.ZZZ	0	Regular File	25.04.2018 9:42:22
Z.ZZZ	0	Regular File	25.04.2018 9:42:14
Z.ZZZ	0	Regular File	25.04.2018 9:42:16
Z.ZZZ	0	Regular File	25.04.2018 9:42:12
Z.ZZZ.FileSlack	37 576	File Slack	
Z.ZZZ.FileSlack	3 544	File Slack	
Z.ZZZ.FileSlack	8 888	File Slack	
Z.ZZZ.FileSlack	868	File Slack	
Z.ZZZZ	0	Regular File	25.04.2018 9:42:14
Z.ZZZZ.FileSlack	3 340	File Slack	

Рисунок 3.44 – Содержимое удаленных файлов при виде HEX формате

Благодаря обычной программе R-studio, я смог восстановить все удаленные данные и даже саму папку. Вывод только один, метод удаления в режиме files and folders неэффективны. Смотрим на рисунки 3.45, 3.46, 3.47,3.48.

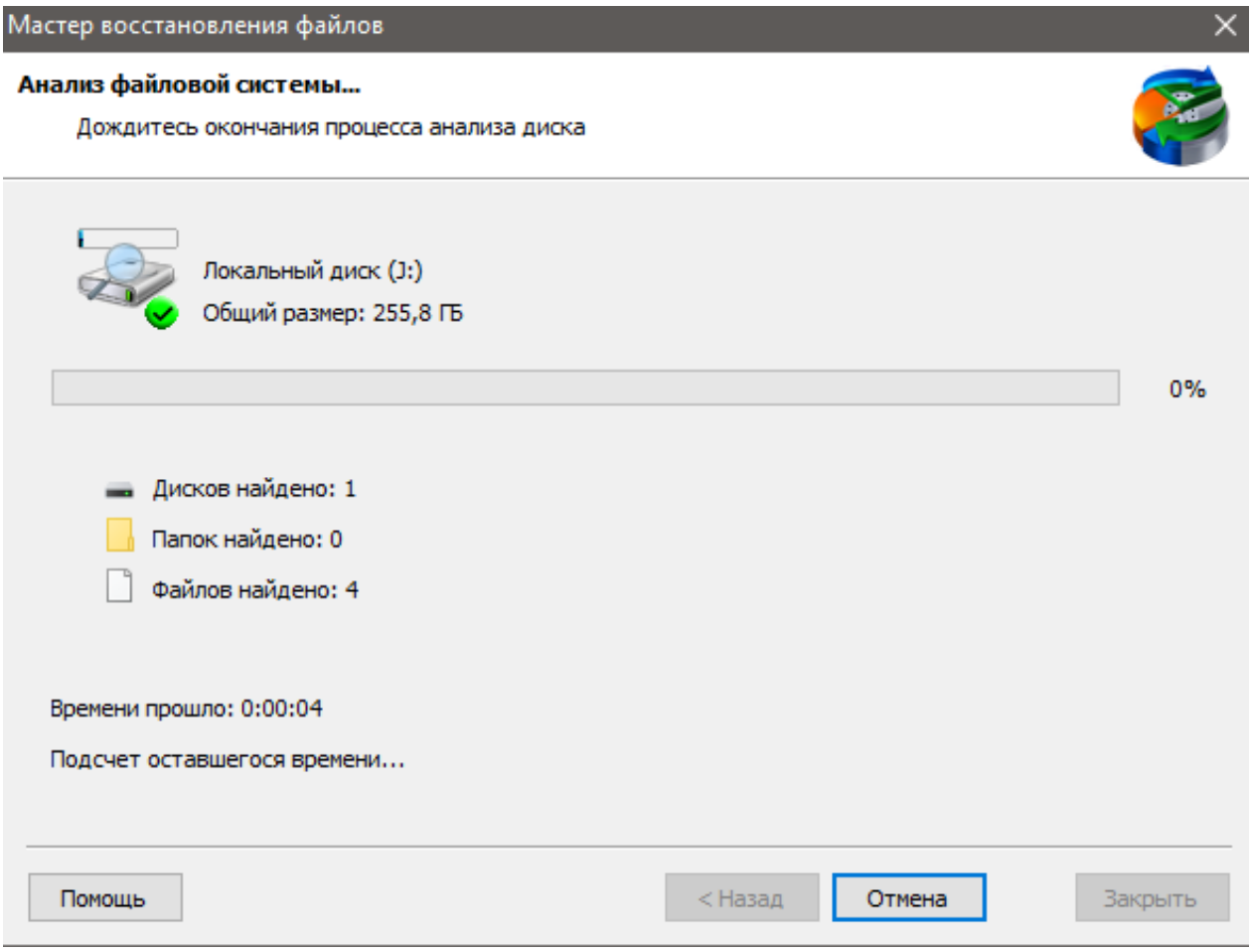


Рисунок 3.45 – Процесс глубокого анализа раздела диска J

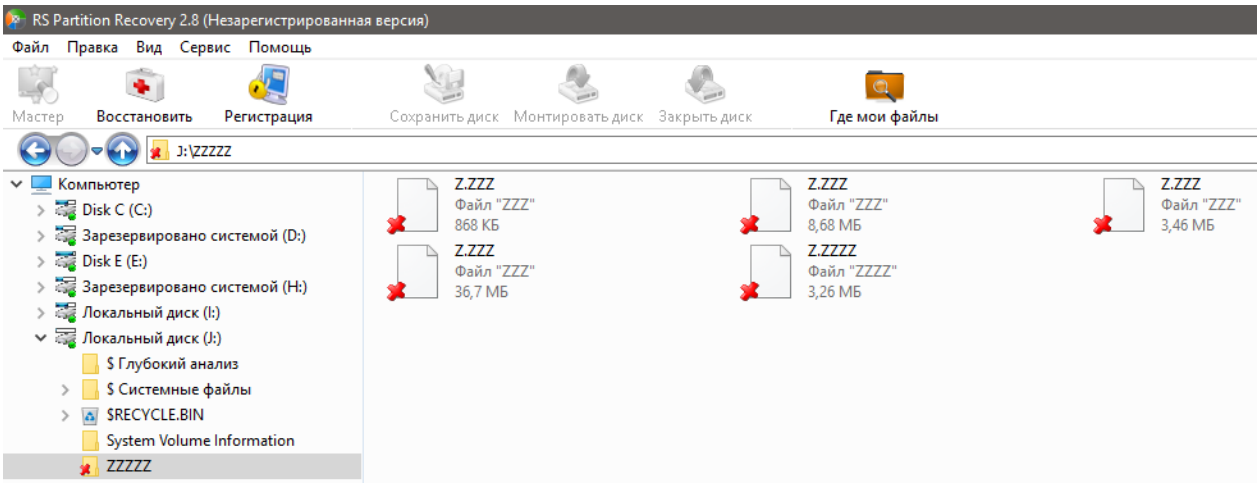


Рисунок 3.46 – Восстановления удаленных файлов

Теперь удалим весь раздел J, в режиме удаления Hard disk/partitions, с размером 250 гб, методом 7 проходов NSA. Процесс удаление займет огромное время.

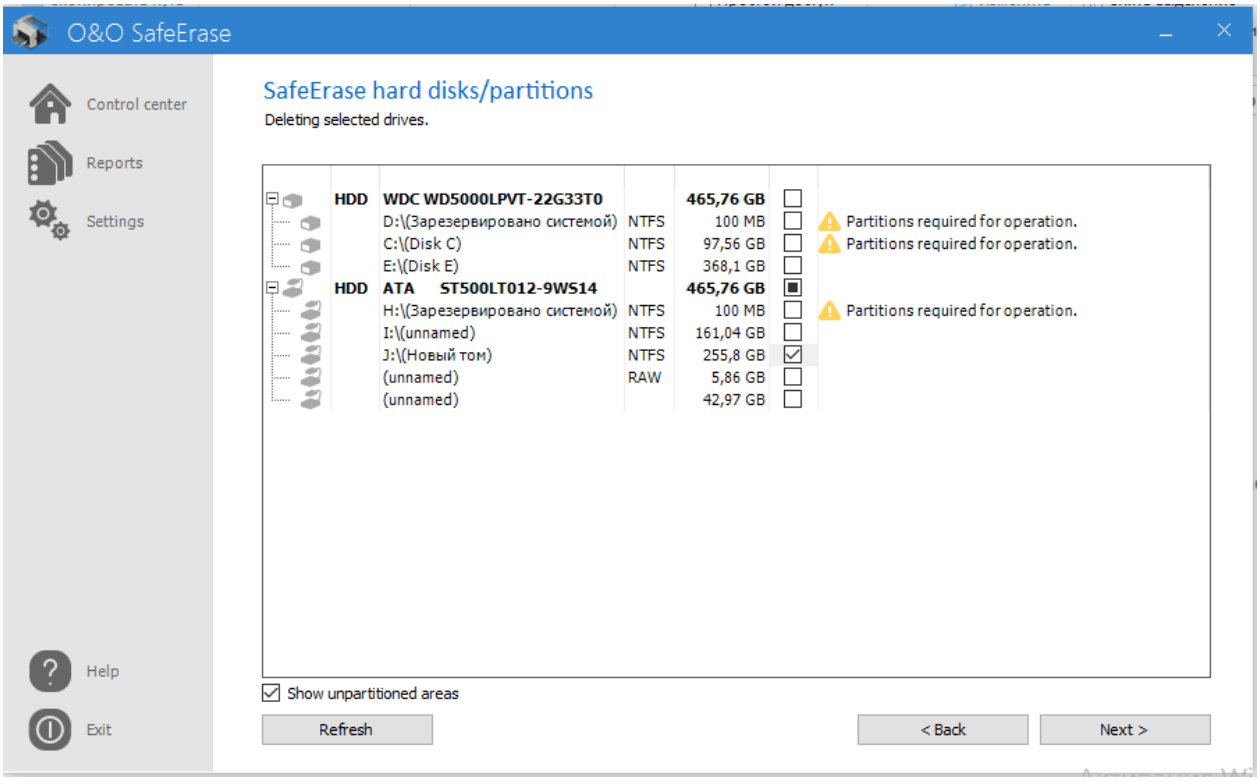


Рисунок 3.47 – Выбираем раздел J, в режиме удаления Hard disk/partitions

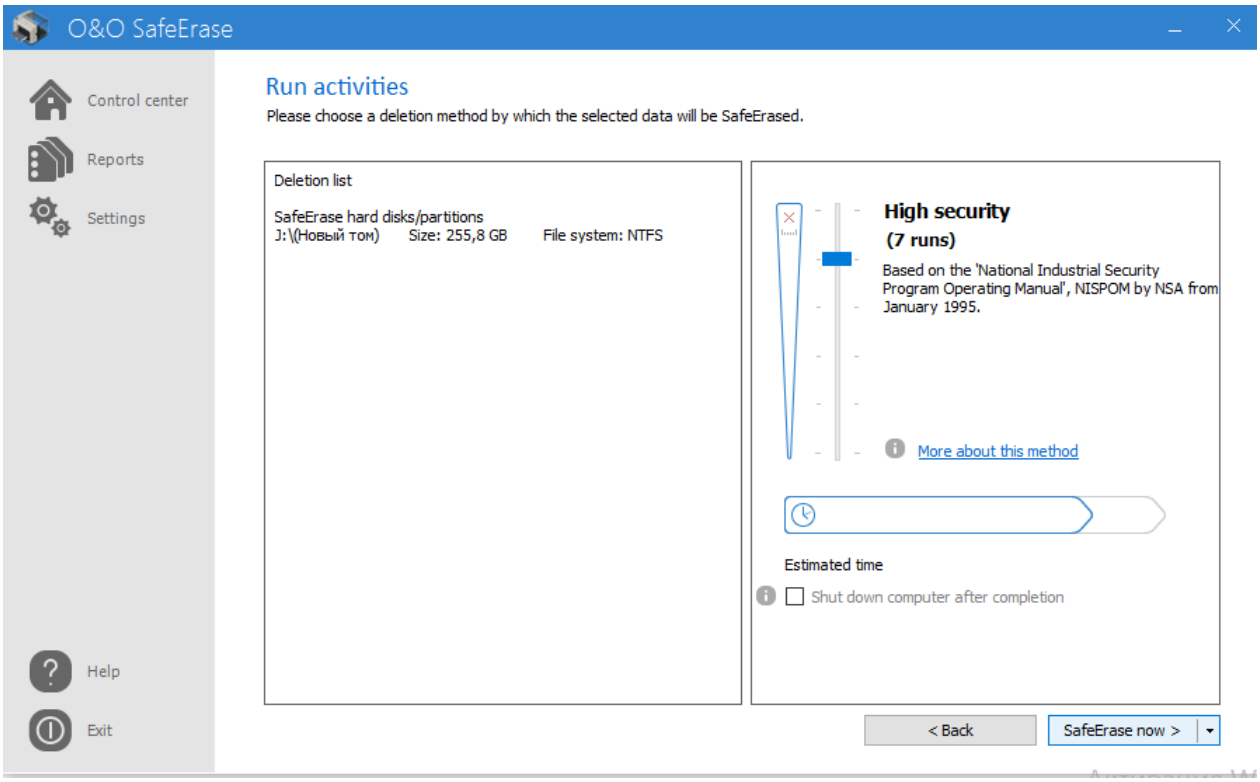


Рисунок 3.48 – Выбираем метод 7 проходами NSA

Процесс удаления заняло 10 часов 20 минут. Был очищен раздел диска j, смотрим на рисунок 3.49.

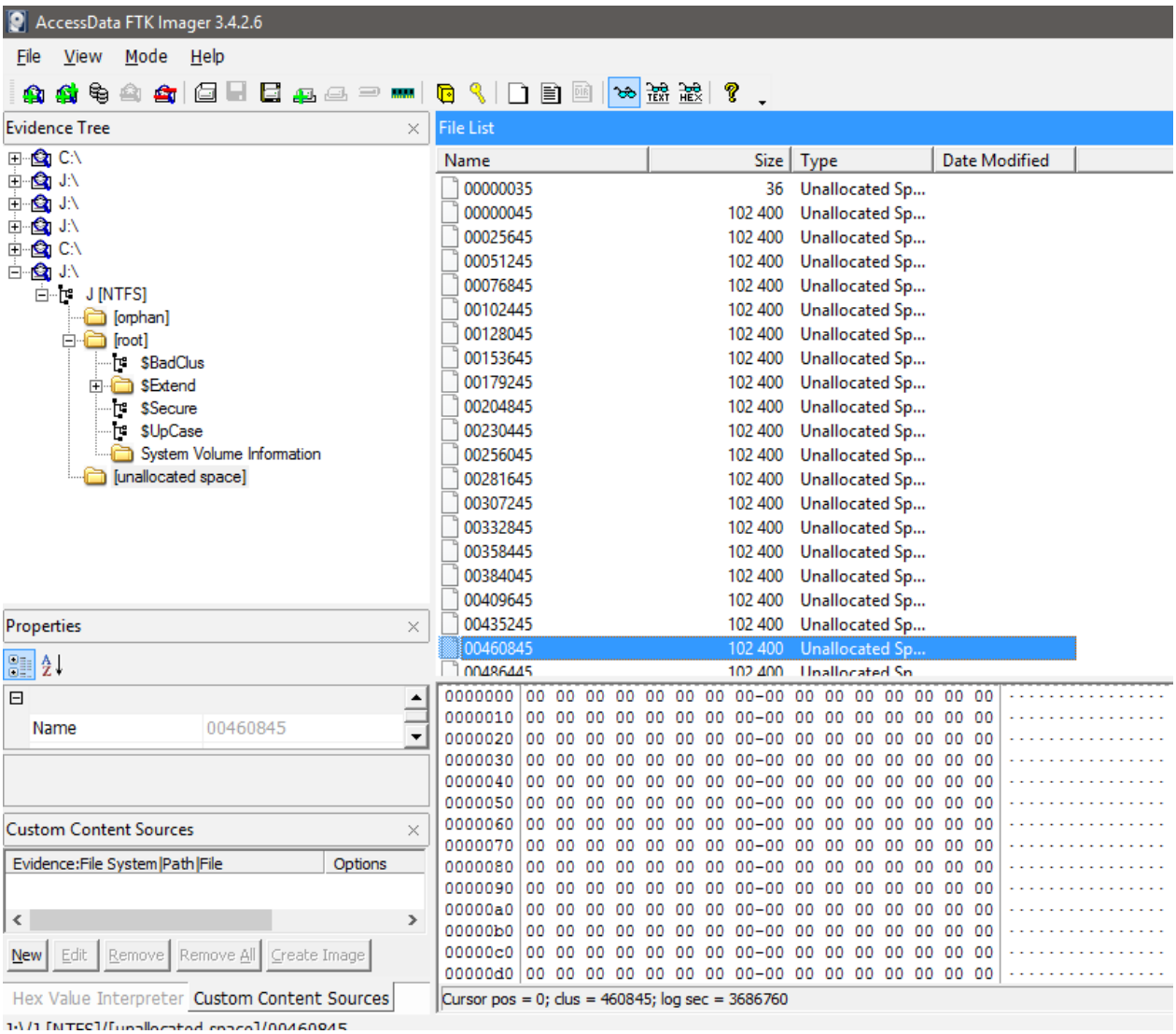


Рисунок 3.49 – Чистый раздел j

Восстановления невозможно, программа R-studio ничего не нашел, метод удаления с помощью NSA, 7 проходами удачно показал себя. Эффективный метод в режиме удаления hard disk/partition. Смотрим на рисунок 3.50. Восстановление в дата центре заняло 3 дня, результатов восстановления не было.

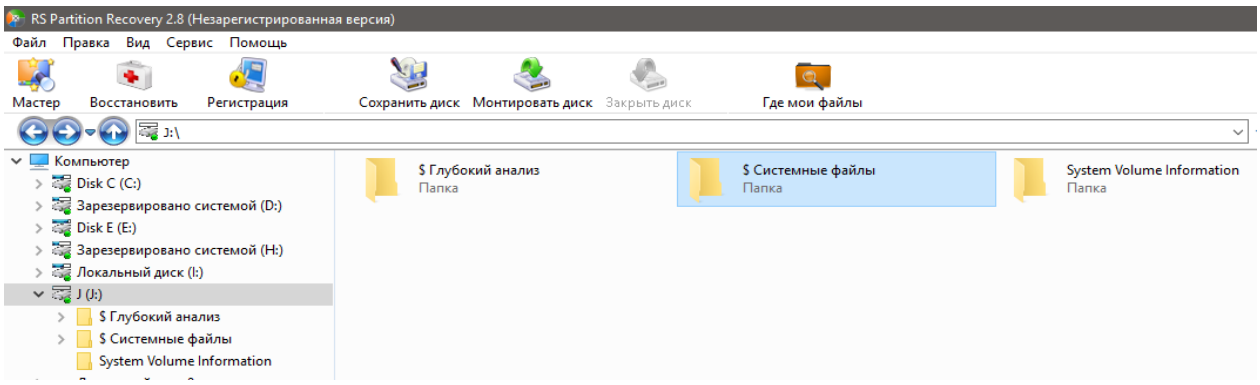


Рисунок 3.50 – Глубокий анализ раздела J, программой R-studio

3.3 Программа Disk Wipe

В отличие от других программ, Disk Wipe не требует установки, он запускается от имени администратора. После того как запуститься программа, он сразу обнаружит все ЖД диска и так же внешние устройства. К сожалению, в отличие от других программ, эта программа не может удалять отдельные файлы или папки, он берет сразу весь раздел ЖД. Выбираем нужный для стирания раздел диска смотрим на рисунок 3.51. После этого жмем на кнопку Wipe Disk, нам он позволит выбрать файловую систему, смотрим на рисунок 3.52. Далее нас ждет выбор метода стирания, так как до этого мы испробовали стирания с 7 проходами, попробуем на этот раз знаменитый Российский ГОСТ метод с 2 проходами, с высокой скоростью. Будем стирать логический раздел J с размером памяти в 255 гб. При выборе раздела, на главном окне будет показана вся информация о разделе. После выбора метода, нам выдаст окно с стандартным предупреждением о том, что вы можете потерять все данные при стирании диска, для того чтобы продолжить стирания, нам нужно в поле надписи написать «erase all», смотрим на рисунок 3.53. Далее нам нужно снова подтвердить, что мы действительно хотим продолжить операцию стирания диска, смотрим на рисунок 3.54,3.55.

Источник ссылки на программу. [7]

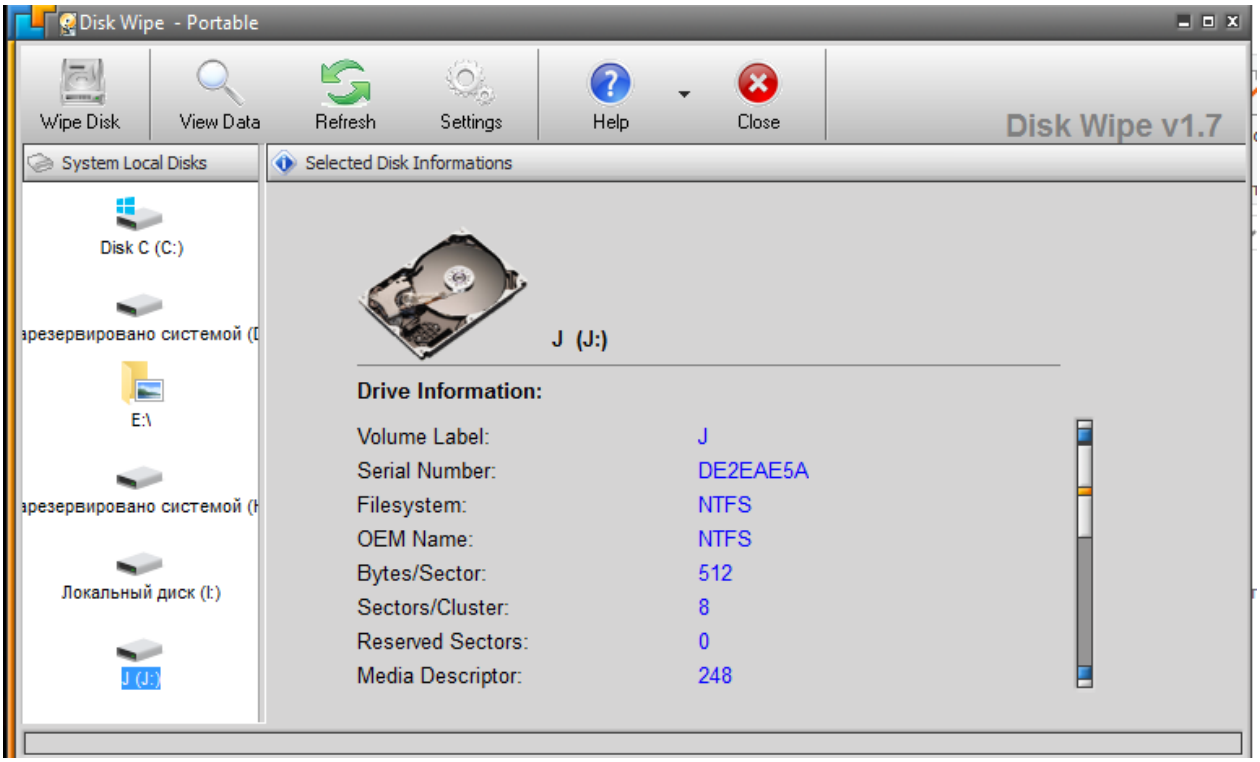


Рисунок 3.51 – Главное окно программы, выбираем раздел J

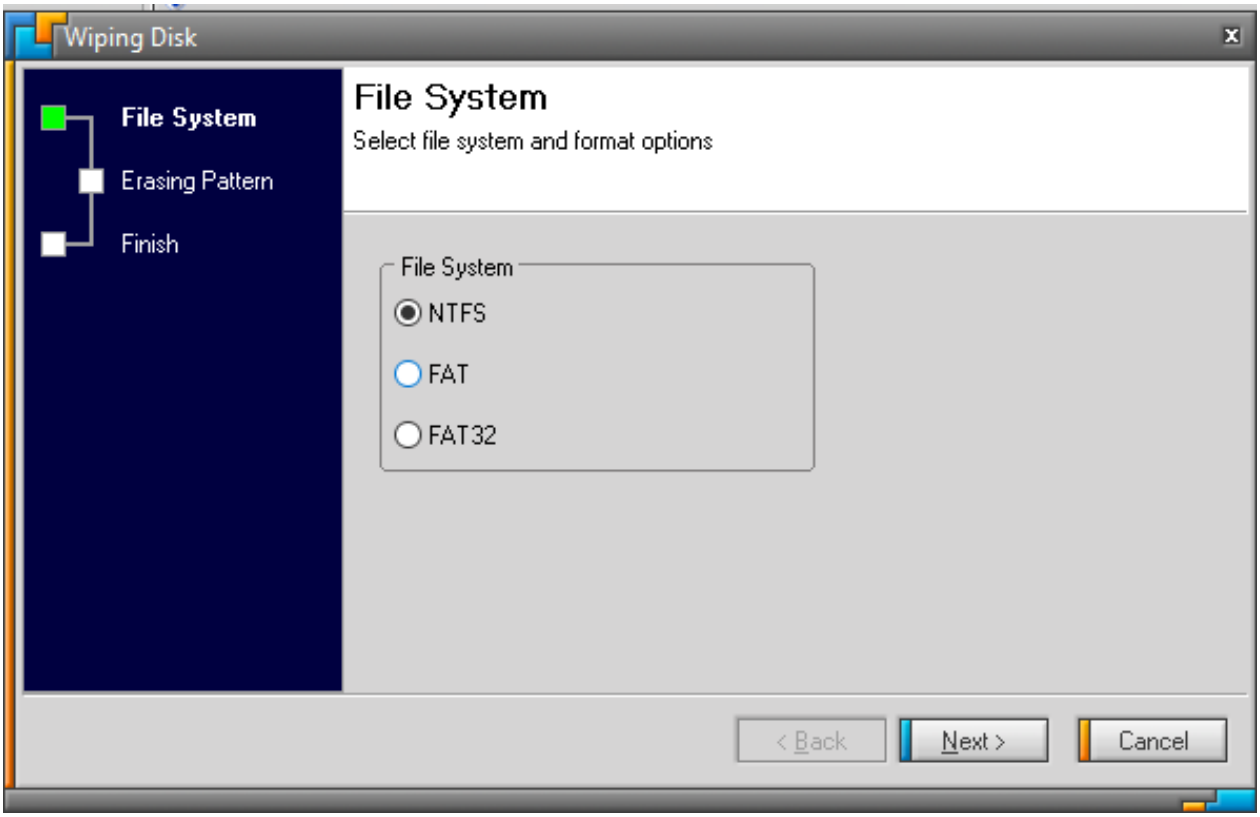


Рисунок 3.52 – Выбираем формат NTFS

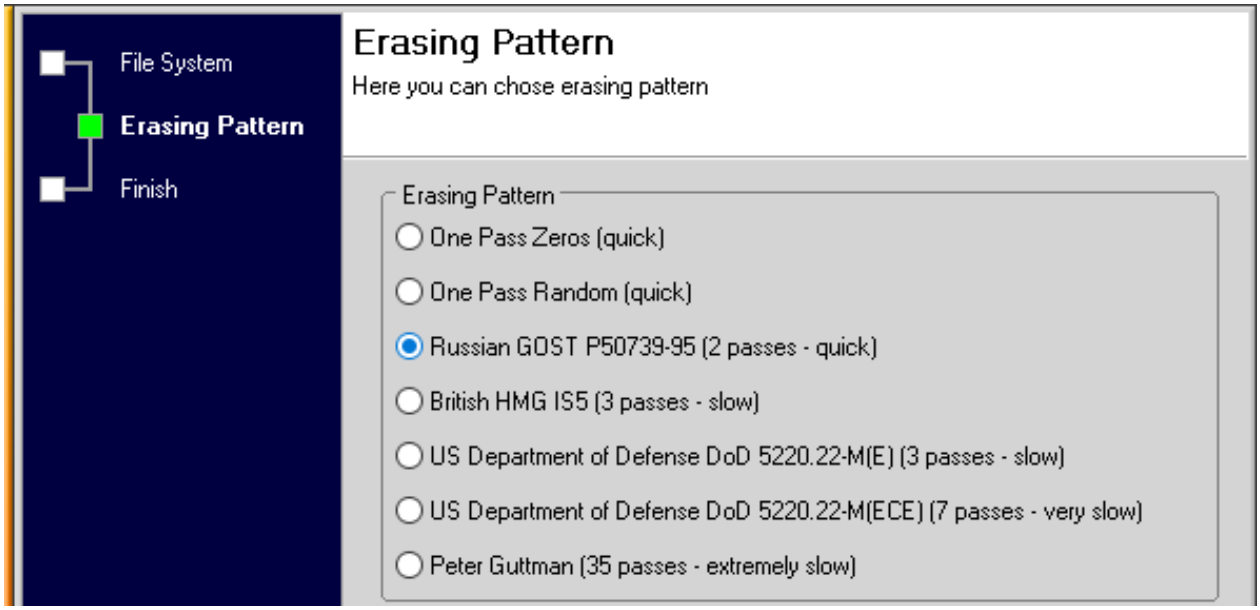


Рисунок 3.53 – Выборка методов стирания, выбираем метод ГОСТ Россия ,2 – прохода

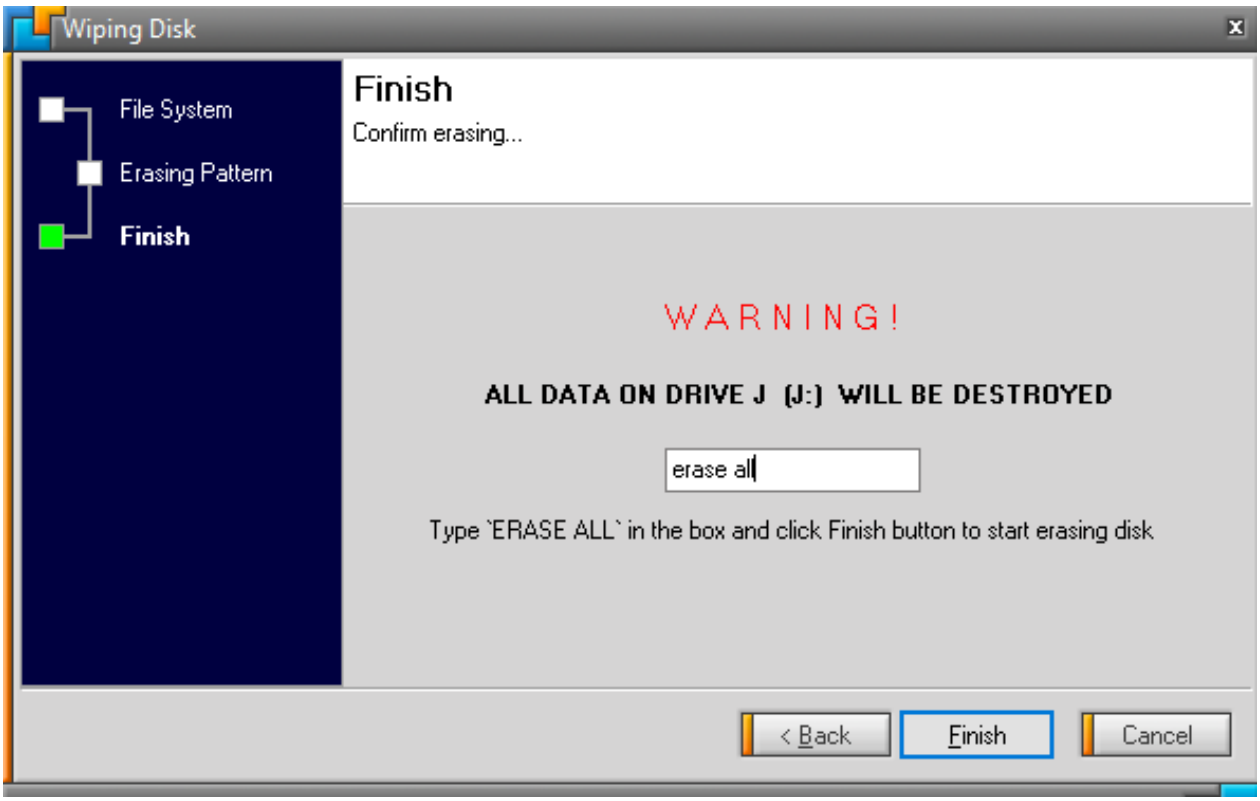


Рисунок 3.54 – Окно с предупреждением, пишем в поле надписи Erase all

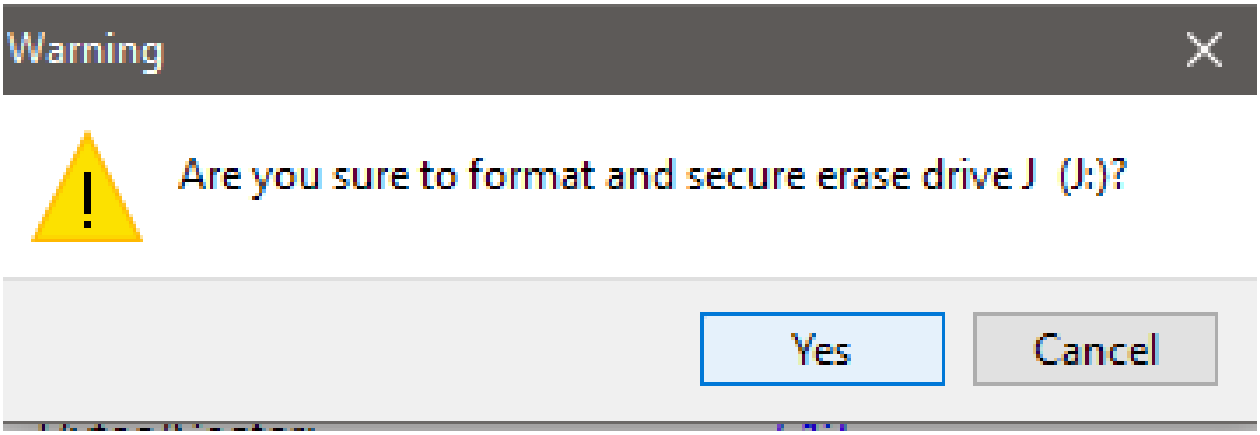


Рисунок 3.55 – Окно с предупреждением, соглашаемся на стирания

Стирания методом ГОСТ Россия 2 – прохода, заняло 4 часа 51 минута. При просмотре на раздел виде двоичного кода, мы видим, что все кластеры заполнились масками «D5», смотрим на рисунок 3.56. Полный анализ по восстановлению GetDataBack, показал все разделы, которые были удалены. Смотрим на рисунок 3.57.

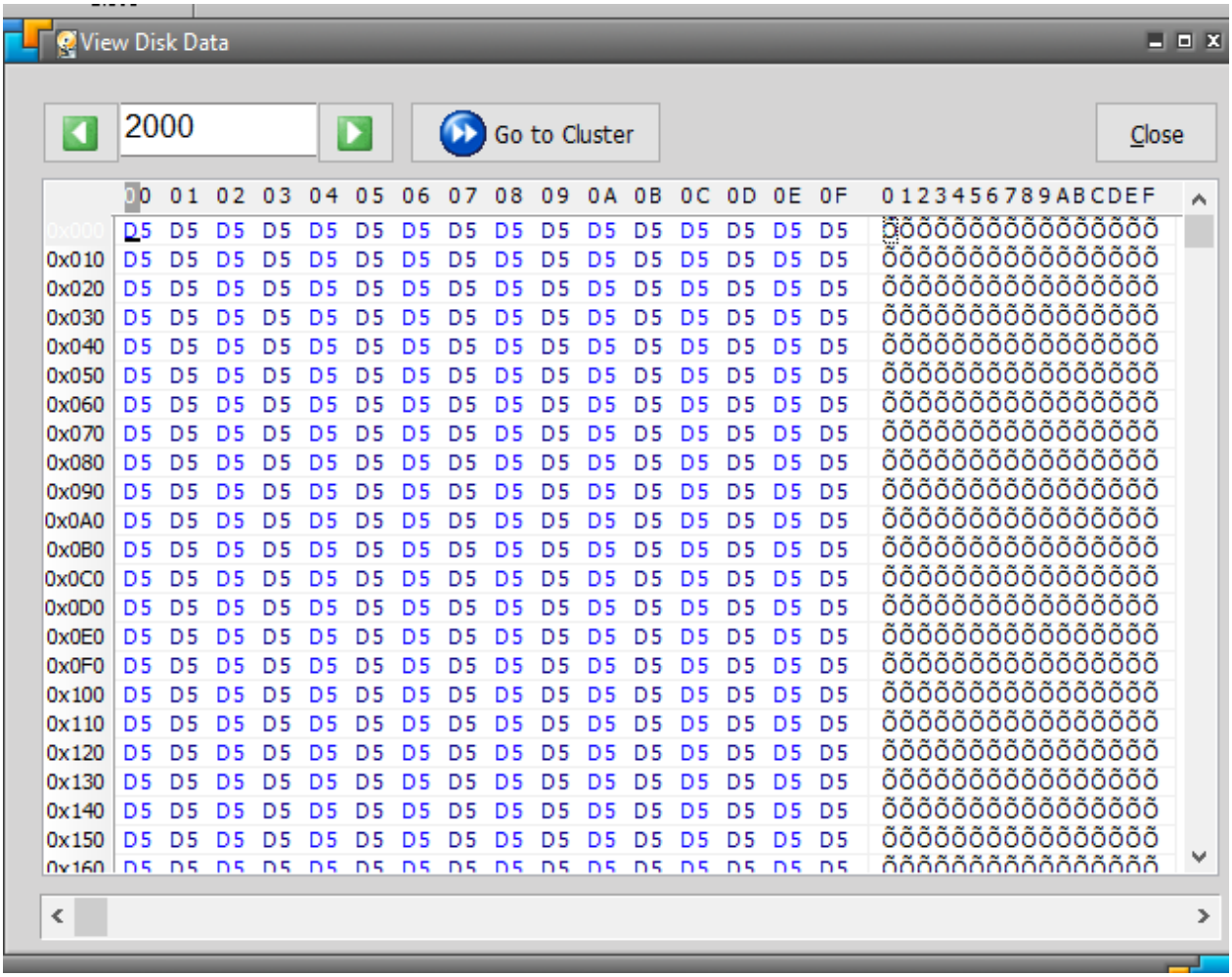


Рисунок 3.56 – Просмотр раздела диска J в двоичном коде

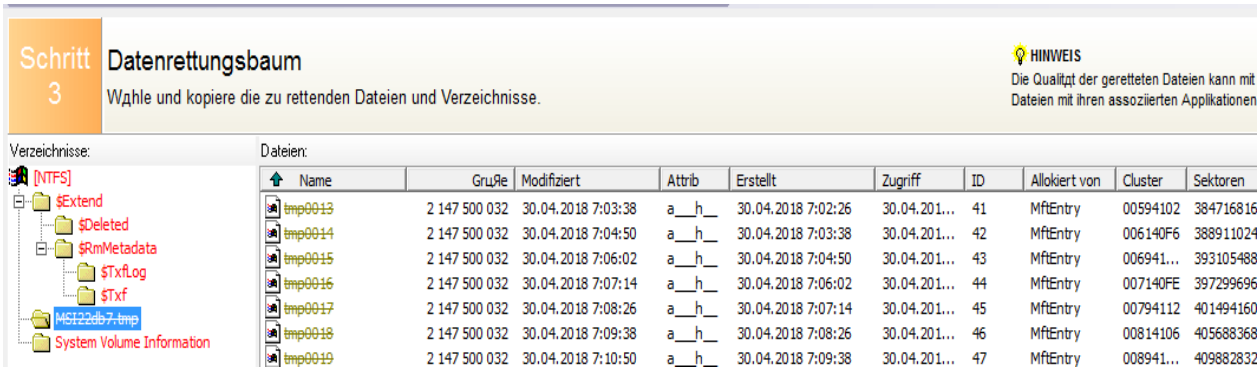


Рисунок 3.57 – Найденые удаленые файлы, в формате tmp, временного файла.

Все процедуры при стирании диска, DiskWipe записал отдельно в папку, которую он создал автоматический, папка включается как история удаления кластеров.

Все найденные файлы были зафиксированы как временные в формате tmp, если присмотреться, то можно увидеть, что все файлы имеют 2гб размер. Из этого можно сделать вывод, что найти данные которые были удалены,

восстановить очень трудно. Атрибуты всех файлов архивированы с чтением. Эффект удаления даже с двумя проходами ГОСТ Россия, показал себя удачно. Так как все удаленные файлы были архивированы и временными, следующая запись на ЖД заменит удаленные временные файлы путем записи поверхностно, что приведет еще более затруднению восстановлению информации. Из этого можно сделать вывод, что при удалении всего ЖД даже с двумя проходами дает очень высокую надежность по удалению данных.

3.4 Программа Ccleaner

Установка программы персональная, как и в предыдущих программах. Когда запускаем программу от имени администратора, в первую очередь нужно зайти в вкладку программы «сервис», и выбираем кнопку «стирания дисков», перед нами появится все списки носителей, выбираем нужный нам раздел для стирания, в нашем случае это логический диск «J», так как в предыдущих экспериментов мы испробовали 2,3,6,7 проходов, в этом случае попробуем в 1 проход стирания дисков. Смотрим на рисунок 3.58, источник ссылки. [8]

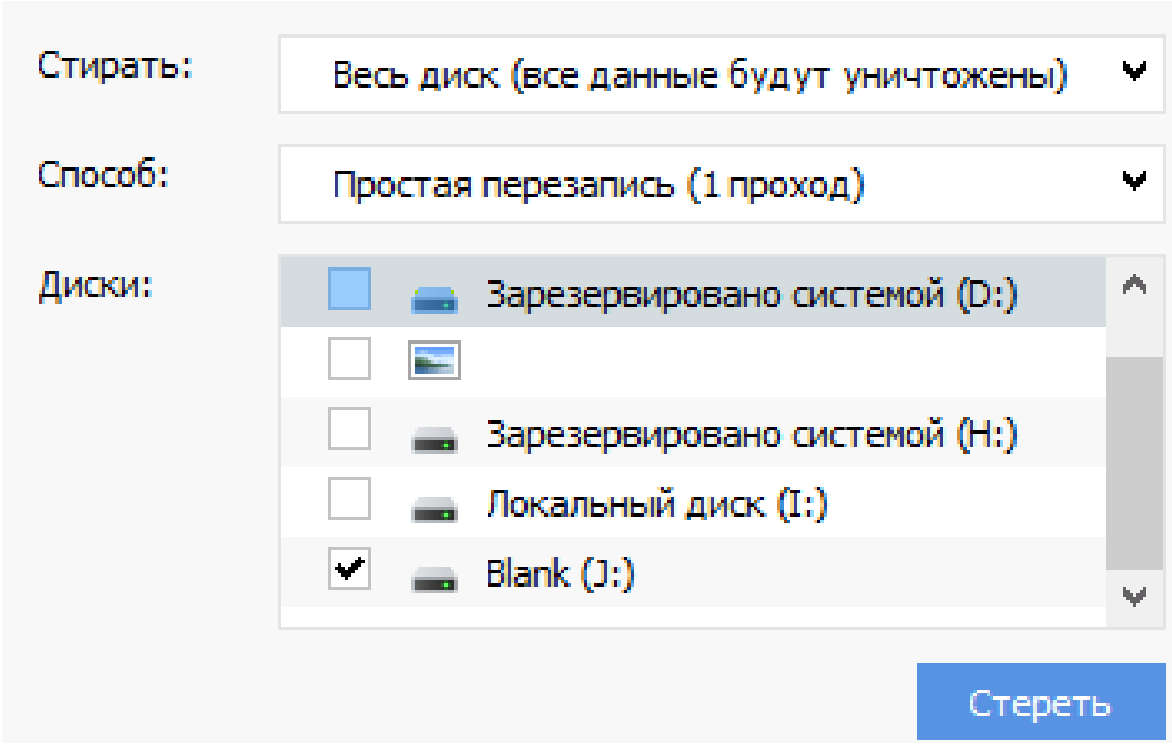


Рисунок 3.58 – Программа Ccleaner, вкладка сервис, стирание диска в 1 проход

Далее нажимаем кнопку «стереть», перед нами выйдет окно с предупреждением и нужно ввести в поле надписи код «erase», жмем кнопку ок. Смотрим на рисунок 3.59. Стирания диска раздела J, заняло 2 часа в один проход. Довольно долго, учитывая, что удаления проходили всего лишь в 1 проход. Этим и отличается программа Ccleaner от других, он намного дольше

стирает чем другие программы. Смотрим на рисунок 3.60. В самом логическом разделе диска находилась та же папка «файлы», смотрим на рисунок 3.61.

Все данные были стерты, смотрим на программу FTK, разбираемся в компьютерной криминалистике. Смотрим на рисунок 3.62. Все кластеры пустые.

Восстанавливаем данные с помощью программы R-studio, смотрим на рисунок 3.63. Глубокий анализ по восстановлению данных заняло 3 часа, программа смогла найти лишь контейнер транзакций о ЖД с размером 10 МБ.

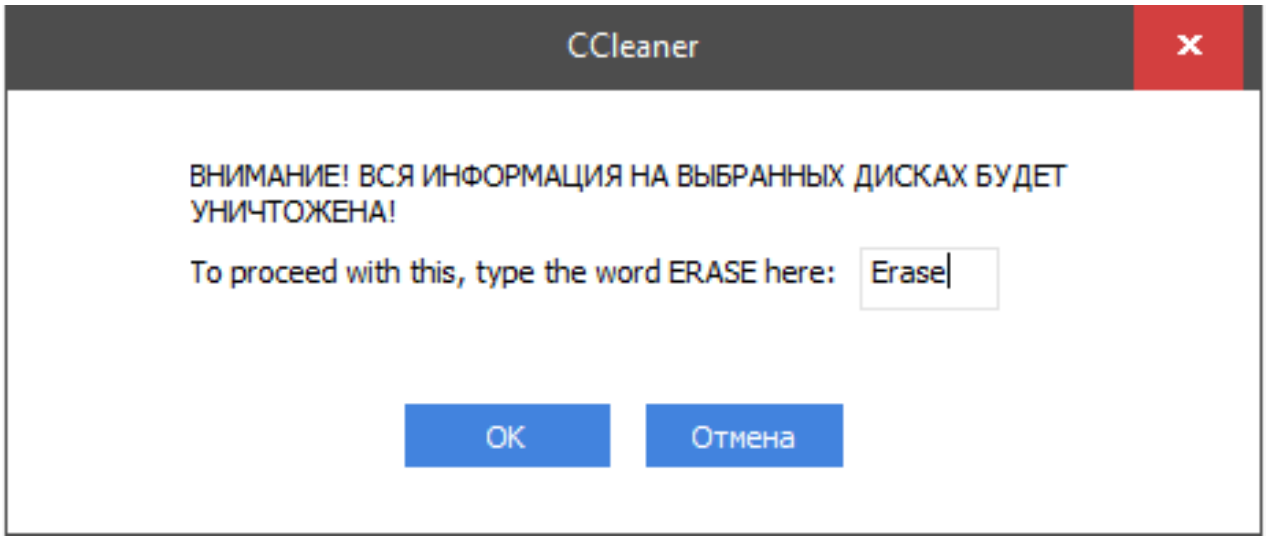


Рисунок 3.59 – Окно с предупреждением, вводим код erase

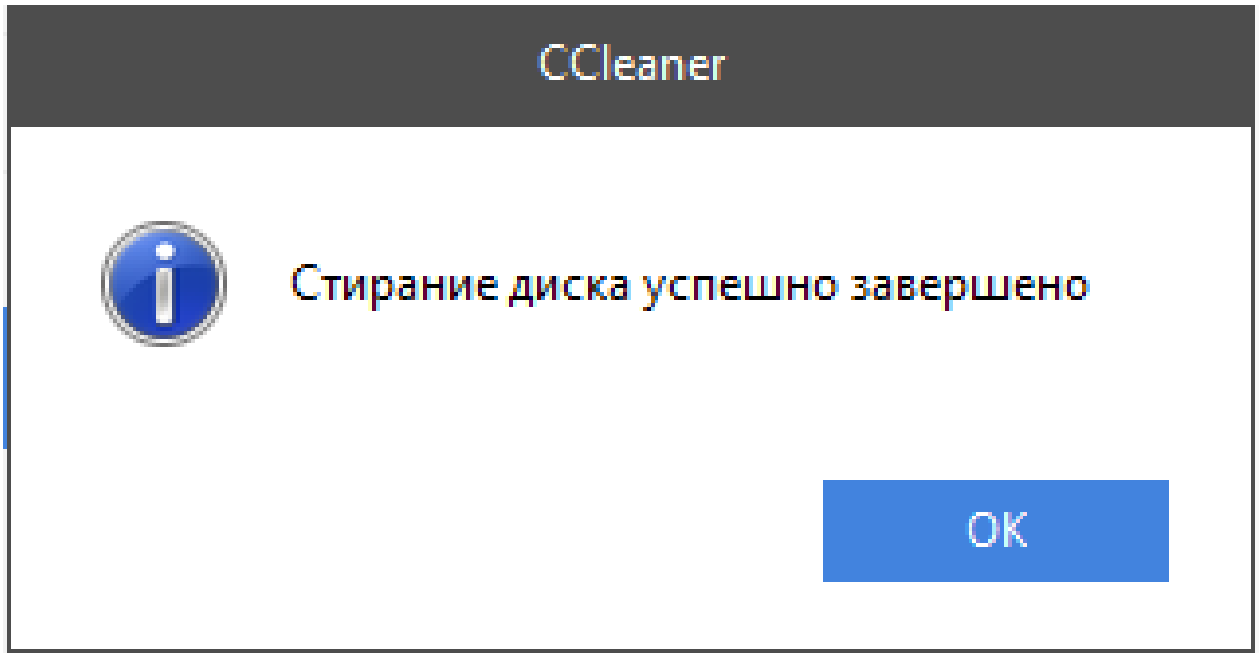


Рисунок 3.60 – Завершение стирания диска J в 1 проход

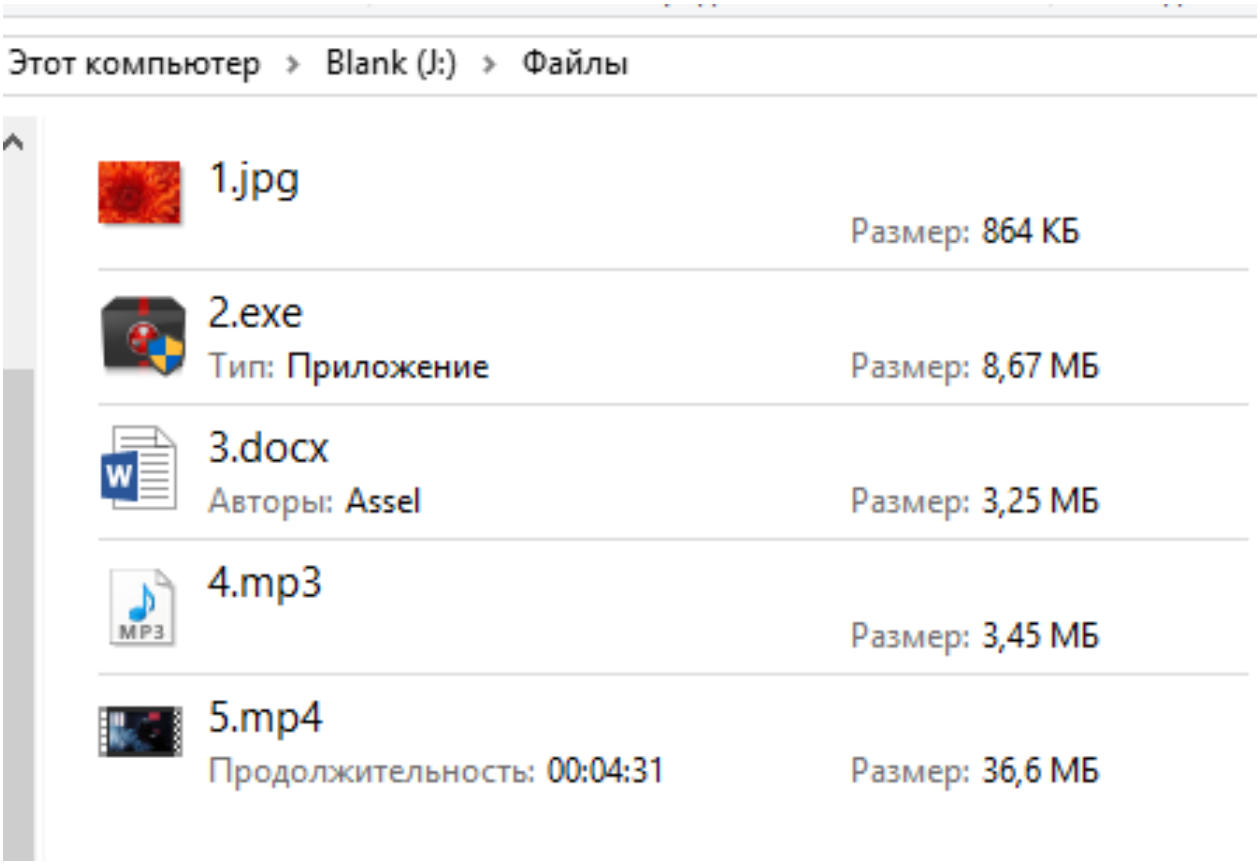


Рисунок 3.61 – Содержимое папки «файлы»

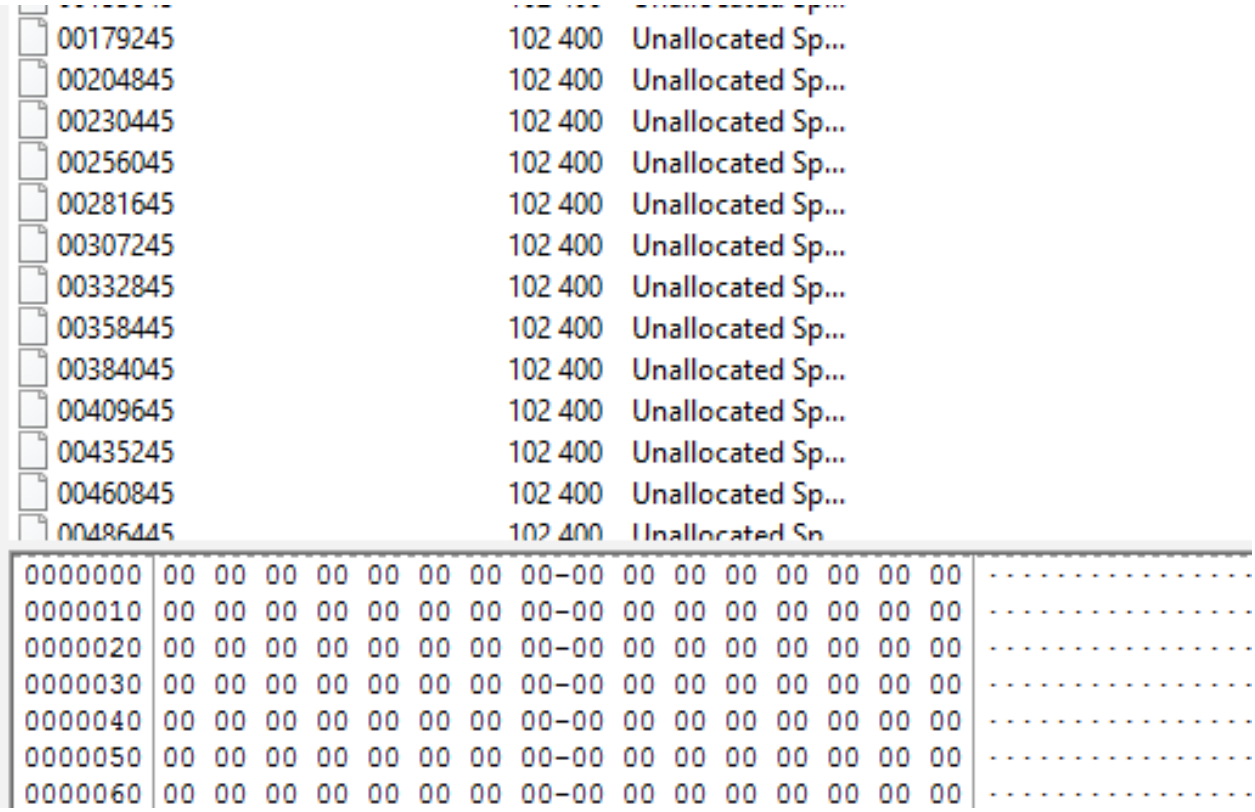


Рисунок 3.62 – Смотрим содержимое диска после стирания в 1 проход

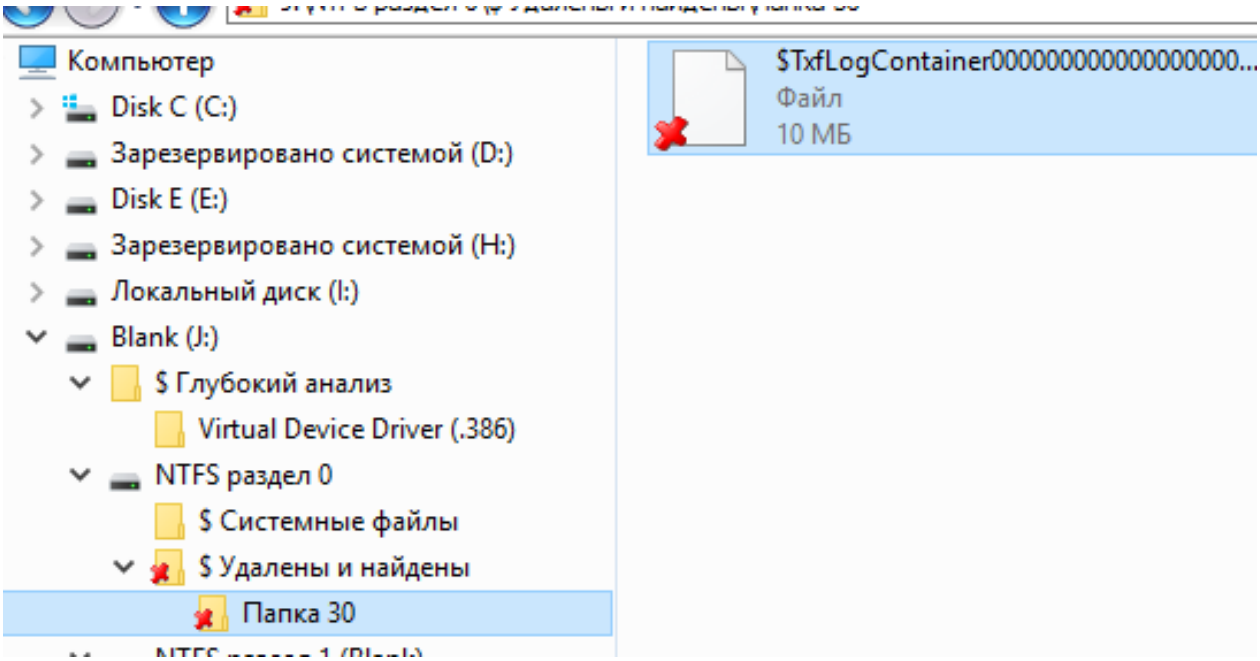


Рисунок 3.63 – Восстановление файла транзакций TxtLogConteiner

Программа Ccleaner работает дольше всех предыдущих, но эффект впечатляет. Даже с 1 проходам удаления данных, показал хороший результат. Вскрыв контейнер транзакций в шестнадцатеричном коде, я не обнаружил ничего, все секторы были аннулированы. Смотрим на рисунок 3.64.

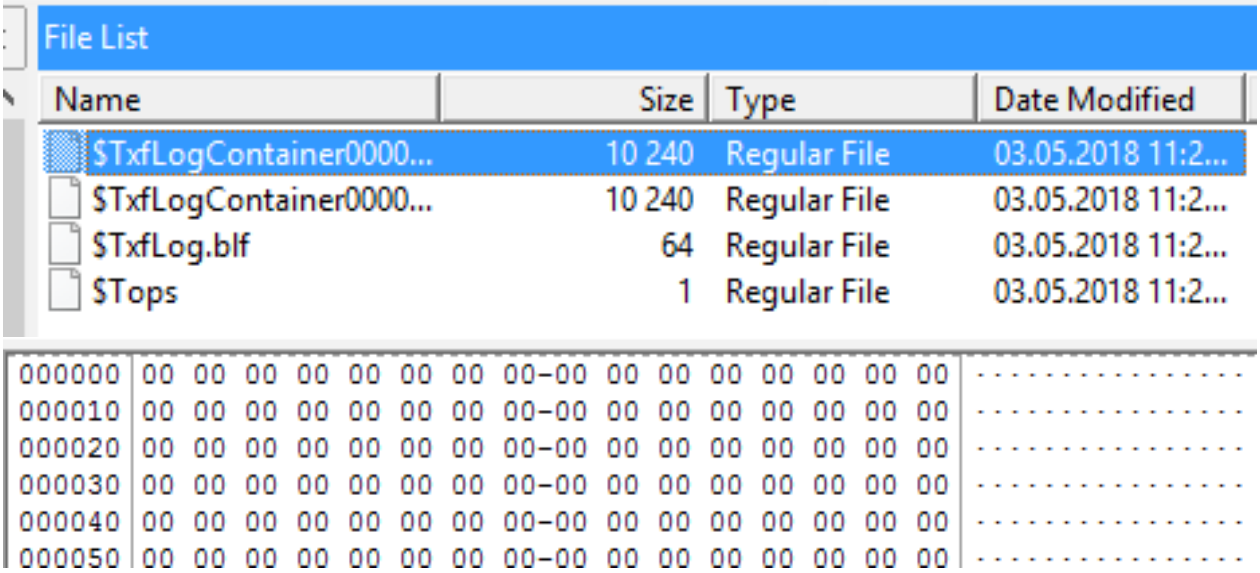


Рисунок 3.64 – Информация о файле TxtLogConteiner

Попробовал восстановить данные с помощью программы Disk Digger, результат тот же что у программы R-studio, программа нашла файл TxtLogConteiner. Сканирования заняло 7 часов, смотрим на рисунок 3.65.

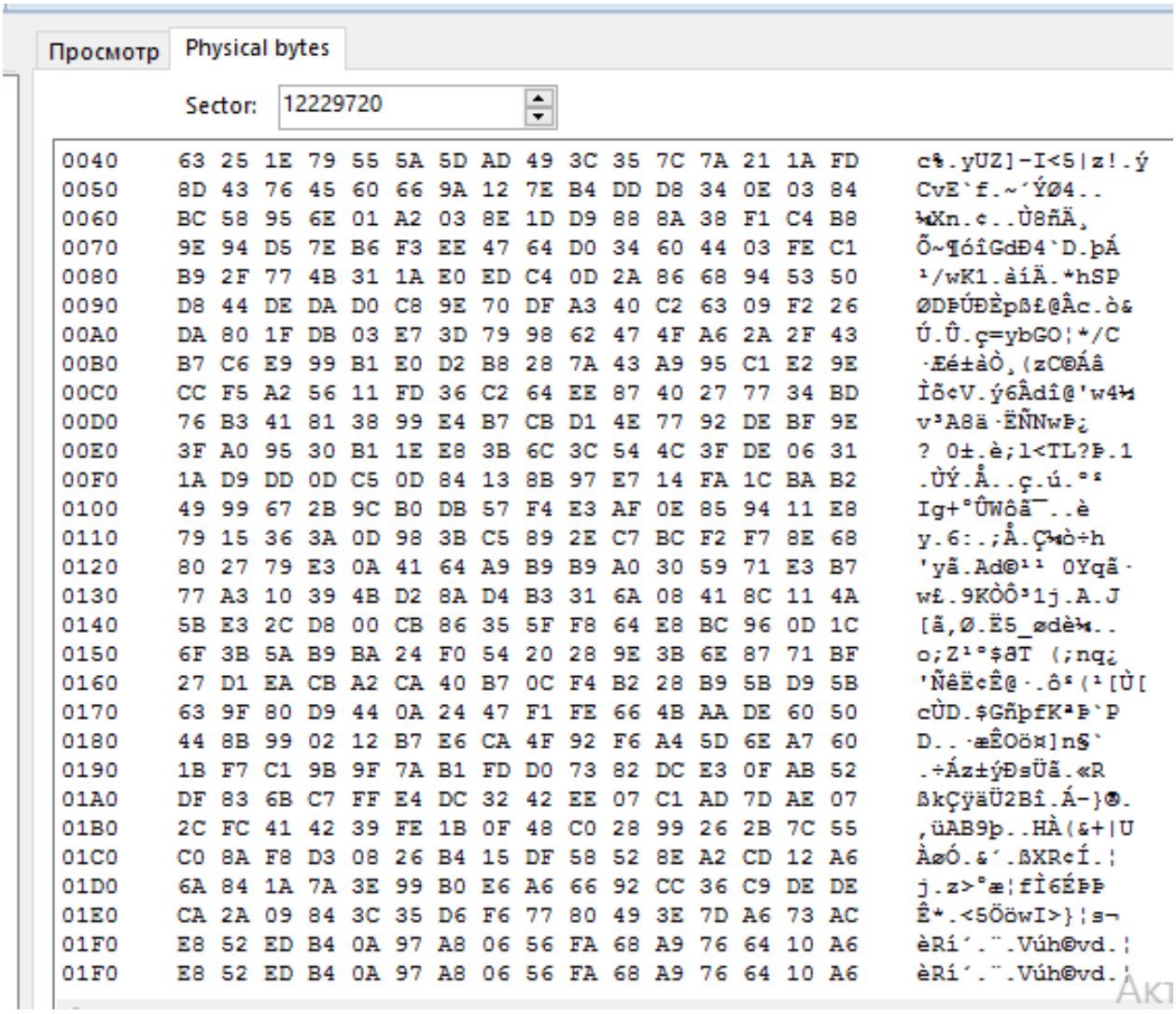


Рисунок 3.65 – Восстановление раздела диска j, с помощью Disk Digger

3.5 Призраки изображения

Представим, что у нас в папке есть фотография, мы решили удалить ее с помощью перезаписи в 3 прохода, думая, что теперь эту фотографию никто не сможет восстановить. Но тут есть одна большая ошибка, которую многие совершают даже профессионалы. Дело в том, когда мы создаем внутри папки или же перемещаем какое-либо изображения, даже после безвозвратного удаления файла, остается его призрачные эскизы внутри сомой папки. Этот призрачный файл называется Thumbs.db. Этот файл создается операционной системой, то есть специальное хранилище, в котором сохраняются эскизы изображений из папки, в которой они была. Для эксперимента, создадим папку с любым названием, и переместим туда любое изображения. Так же нужно в настройке «Проводники» поставить галочку, отобразить все скрытые файлы. Смотрим на рисунок 3.66, 3.67.

Посмотреть содержимое системного файла Thumbs можно с помощью специальной утилиты Thumbnail Database Viewer. В папке с названием «Призрак», есть одна фотография с форматов jpg, удалим ее с помощью eraser,

а теперь после удаления, мы можем заметить, что в папке «Призрак», остался по-прежнему не тронутый его эскизы. Смотрим утилитой Thumbnail Database Viewer содержимое системного файла, и видим, что остались его старые эскизы фотографии, смотрим на рисунок 3.68, 3.69.

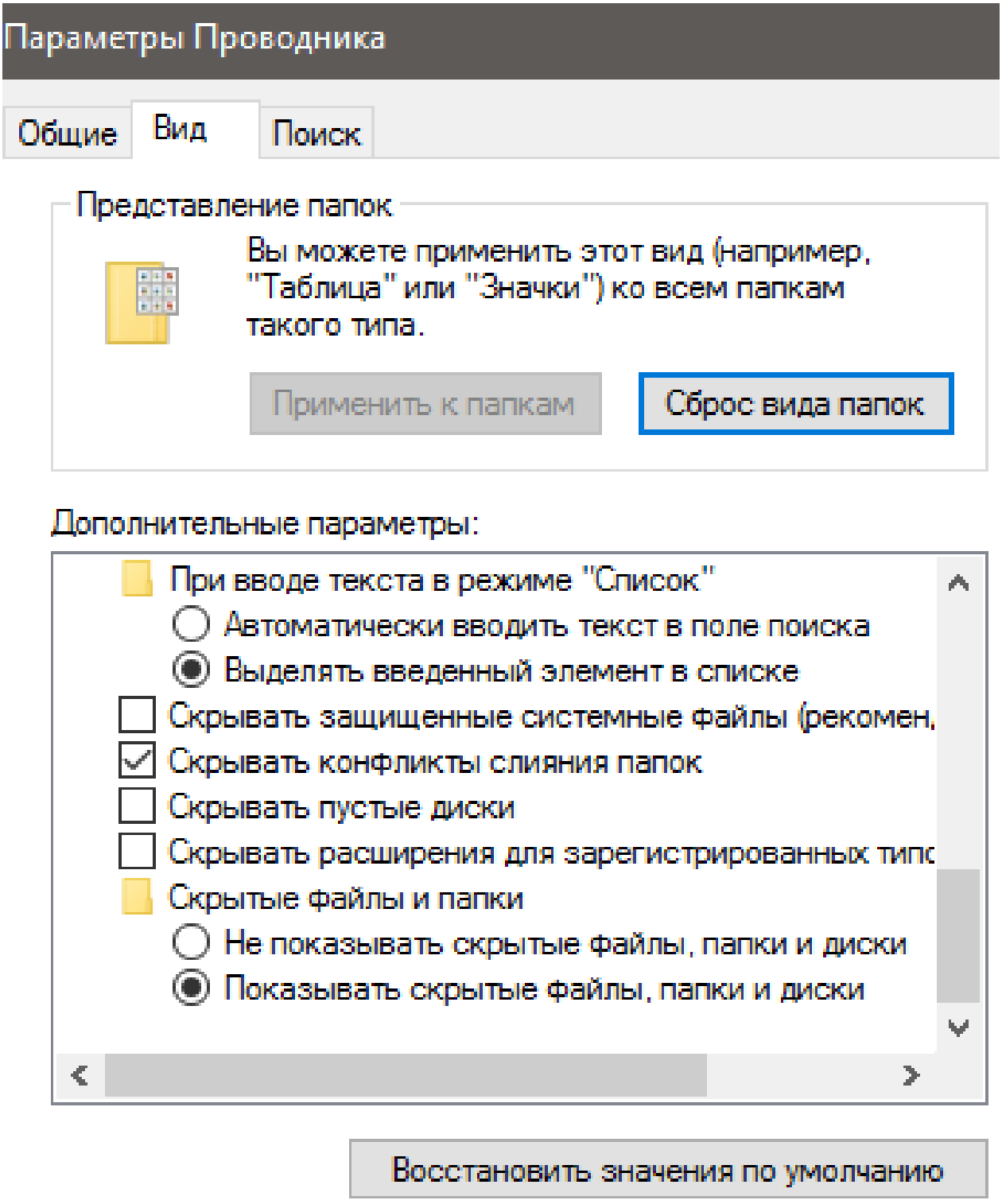


Рисунок 3.66 – Отображение скрытые файлы, папки и диски

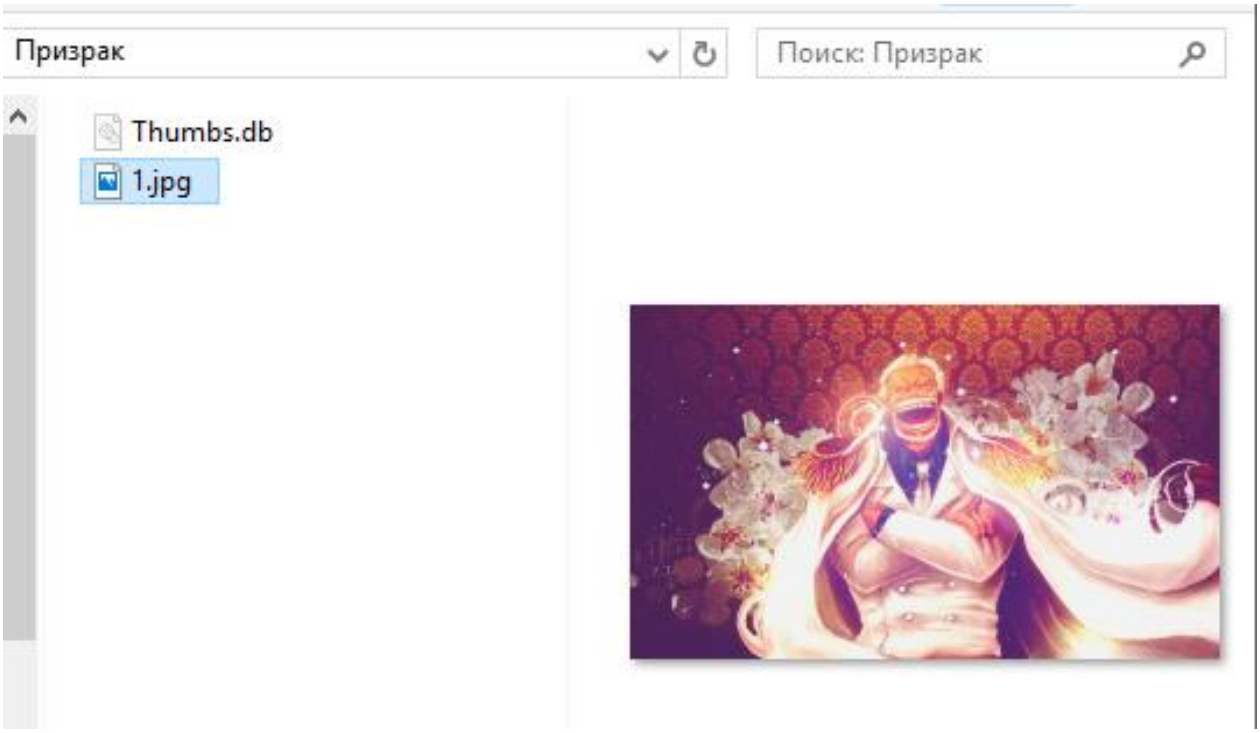


Рисунок 3.67 – Папка «Призрак», картинка 1.jpg и его эскизы Thumbs.db

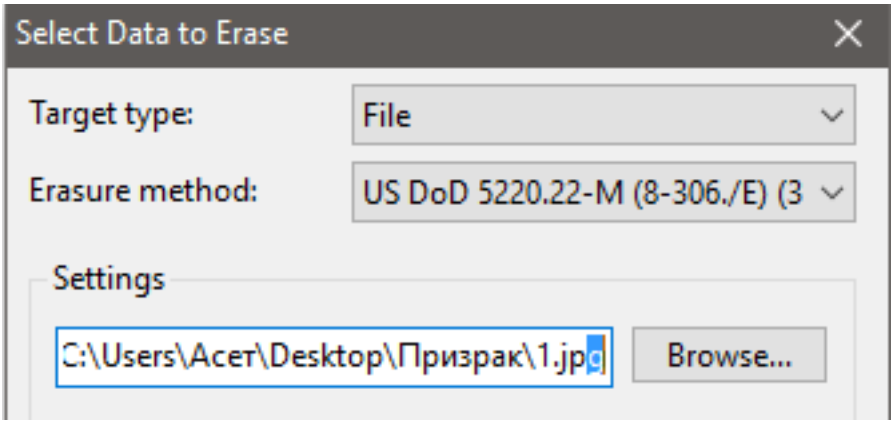


Рисунок 3.68 – Удаление картинки безвозвратно путем стирания в 3 – прохода

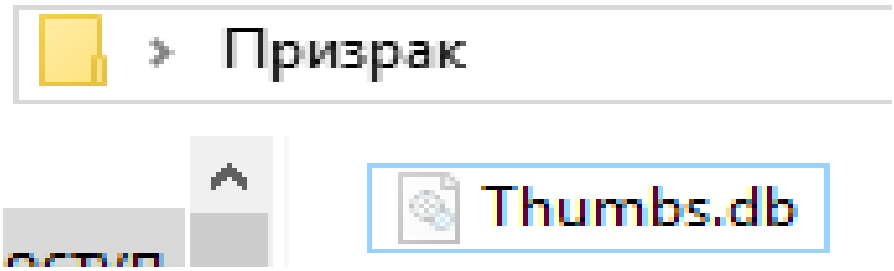


Рисунок 3.69 – Успешно удалилась картинка, но остался его эскиз

Запуск программы Thumbnail Database Viewer, и попробуем открыть Thumbs.db, и что мы видим, как раз-таки саму фотографию, которую удалили до этого безвозвратно как мы думали. Смотрим на рисунок 3.70.

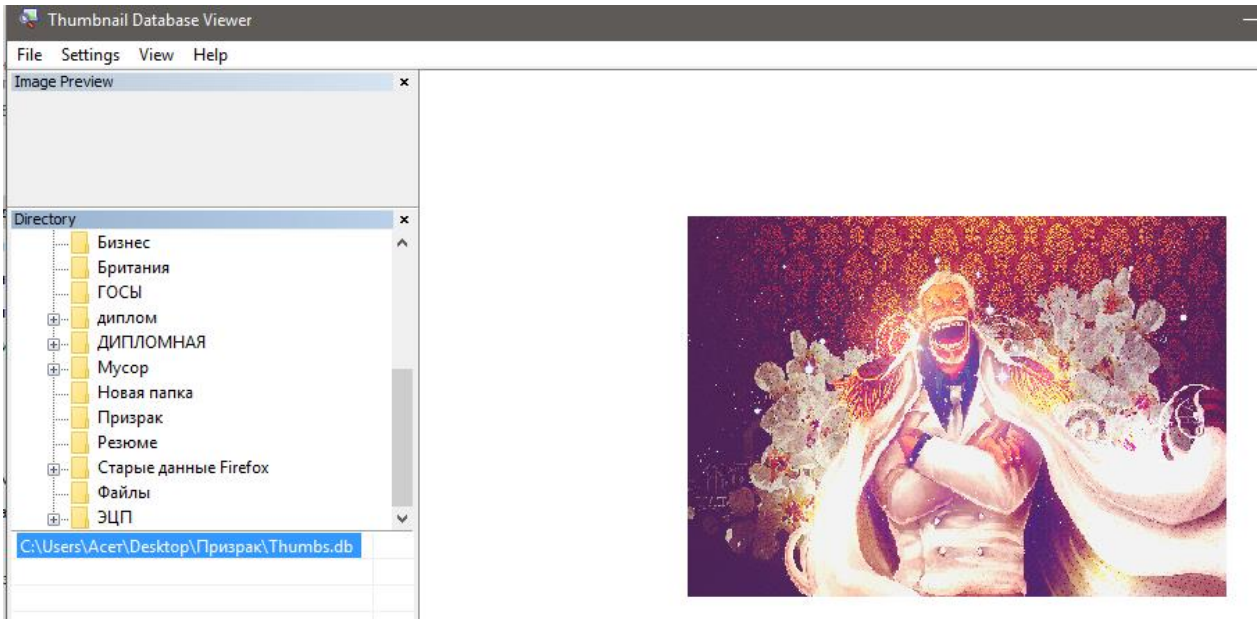


Рисунок 3.70 – Открытие системного файла Thumbs.db

Для того чтобы такого не было, нужно отключить кэширования эскизов в файлах Thumbs.db. Для этого нужно зайти в групповые политики, во вкладку поиск напишите команду gpedit.msc, и надо выбрать «конфигурация пользователя», далее нужно следовать по адресу административные шаблоны, компоненты Windows, проводник. После этого найдите файл «Отключить кэширование экскизов в скрытых файлах thumbs.db» и задайте параметр отключить. Смотрим на рисунок 3.71.

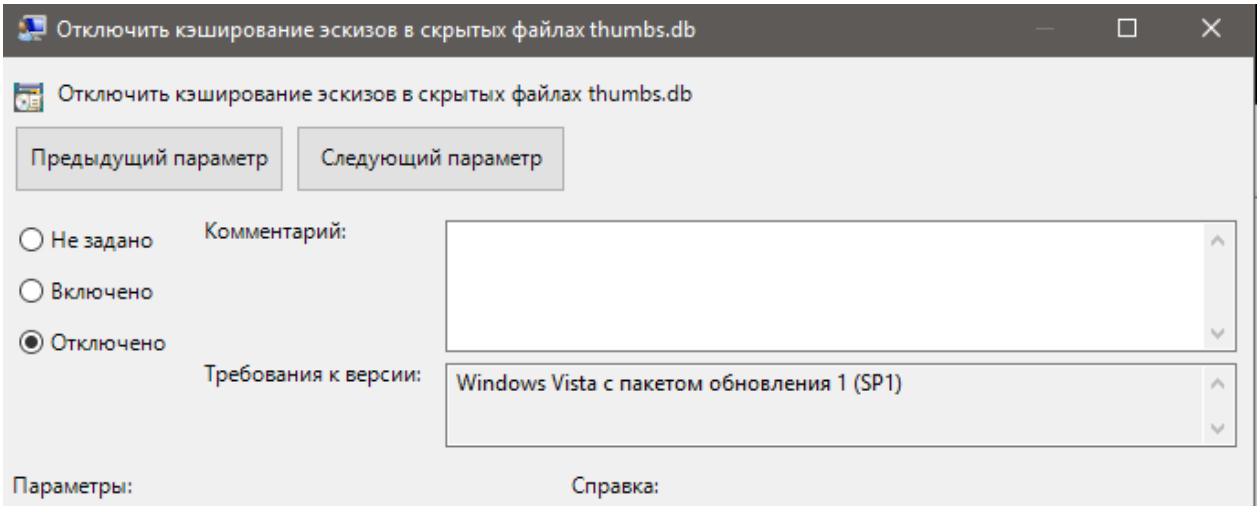


Рисунок 3.71 – Групповая политика, отключение скрытых эскизов

Добавил в папку «Призраки» еще пару разных картинок, и как видим, что эскизы теперь не создаются, смотрим на рисунок 3.72. Но оставшиеся до отключения эскизов системные файлы thumbs.db нужно удалить все вручную безвозвратно.

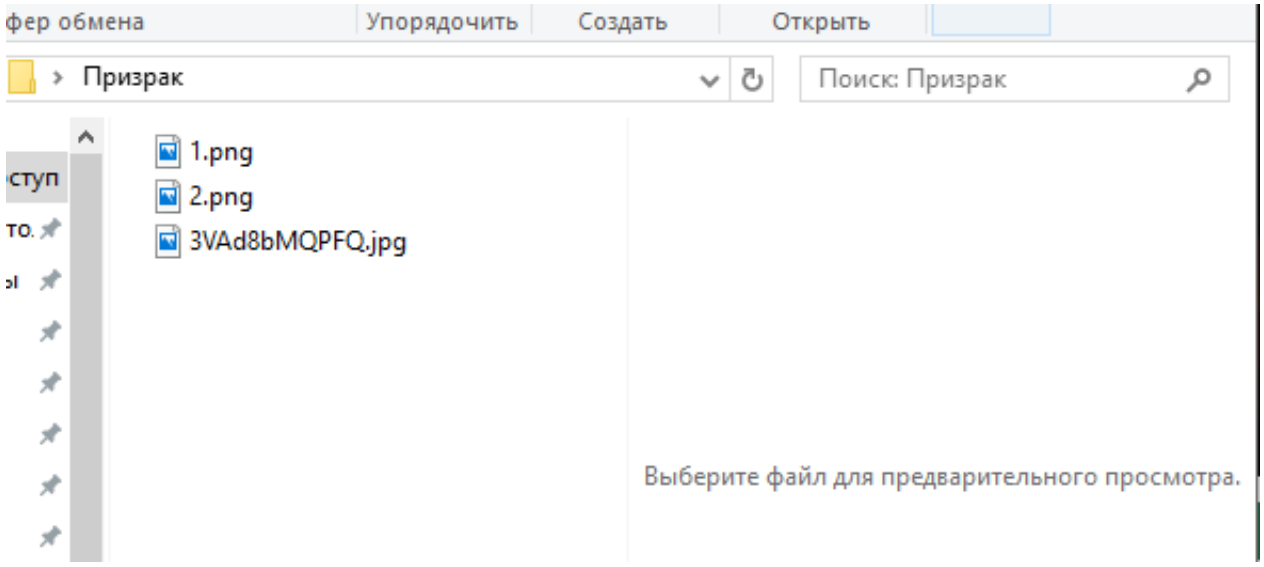


Рисунок 3.72 – Папка «Призрак», без эскизов системного файла thumbs.db

3.6 Реализация авторской программы

Программа разрабатывается на Delphi 7, все данные находятся в одной форме с несколькими кнопками, в каждой кнопке привязана определенная функция. Смотрим на рисунок 3.73 в левую часть, как видим на рисунке, у нас есть 8 разных публикаций:

1) OpenDialog1: TOpenDialog – диалоговая окно;
2) Open: TButton – функция для открытия действие кнопки;
3) Path: TStaticText – выборка пути файла;
4) Delete: TButton – кнопка удаление;
5) StaticText1: TStaticText – оформления текста;
6) Splitter1: TSplitter – оформления кнопок;
7) Num: TTrackBar – ползунок выбора;
8) Level: TStaticText – уровень.

Полный листинг программы и блок-схемы можно увидеть в приложение А.

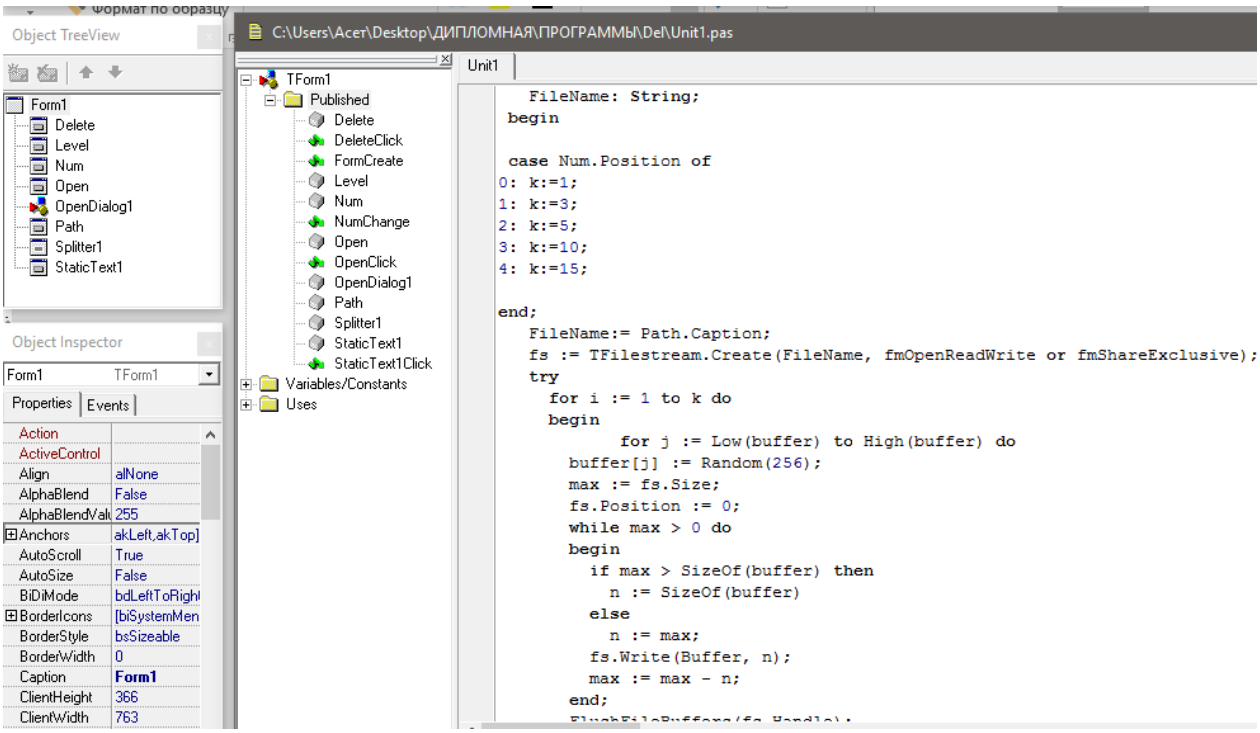


Рисунок 3.73 – Окно программы Delphi 7, программная часть

3.6.1 Тестирования ПО

Смотрим на рисунок 3.74, как видно мы выбрали для удаления файл в формате docx, проходов 15, уровень «Очень надежный». Файл находится на пустом жестком диске J. Для убеждения что файла нету, смотрим на рисунок 3.75, как видно на рисунке, документ удален, размер файла составляет 0 бита, также название документа полностью перезаписана случайными символами. Смотрим незанятое пространство на рисунке 3.76, как видим метаданные формата docx остался, но сам документ восстановить невозможно в прежнее состояние никаким образом.

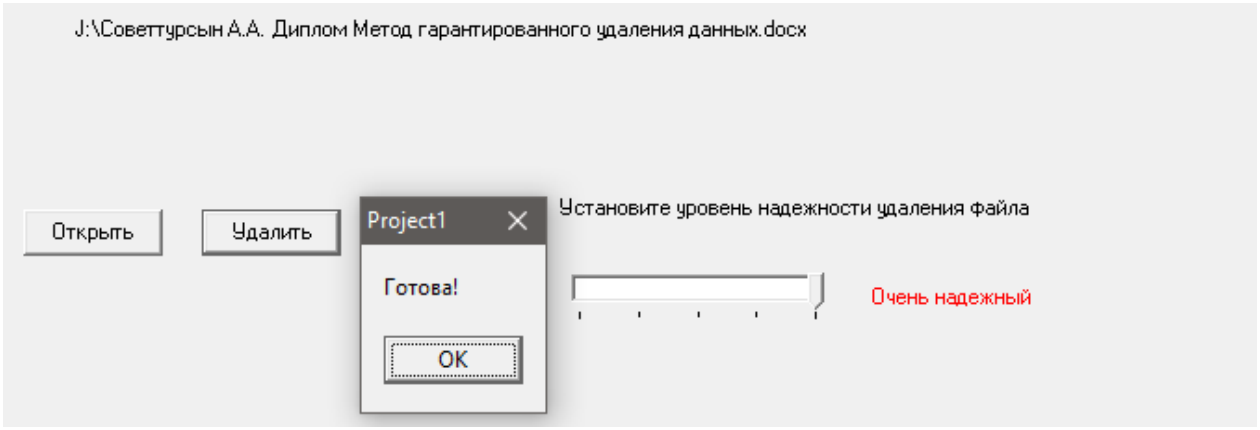


Рисунок 3.74 – Реализация программы

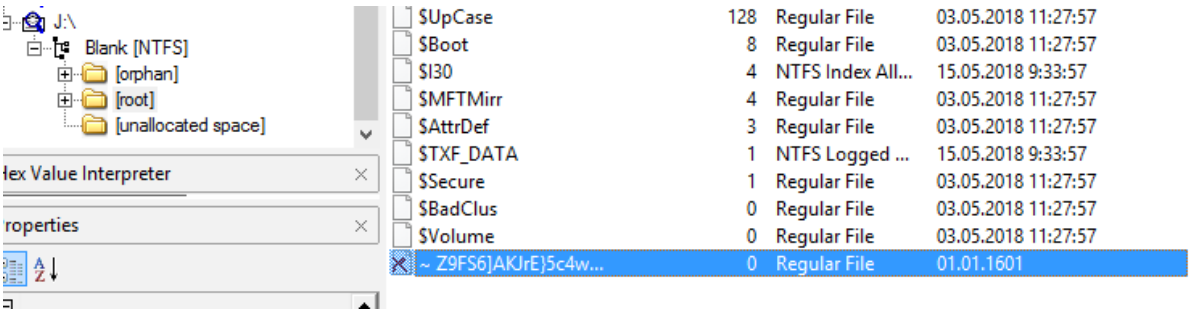


Рисунок 3.75 – Документ удален

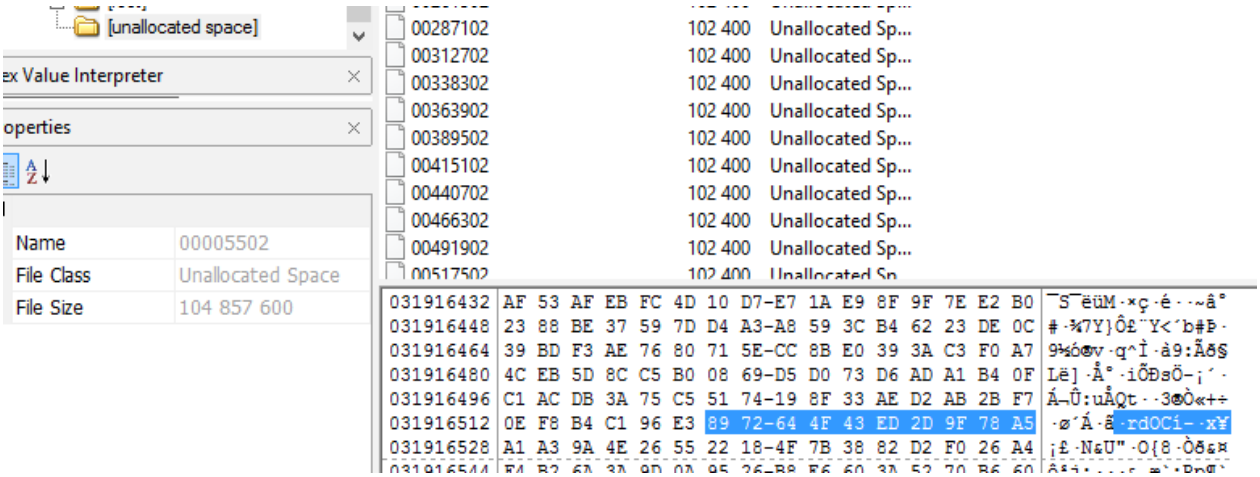


Рисунок 3.76 – Метаданные документа

Удалим теперь другие форматы, jpg, Mp4, Mp3, Exe, смотрим на рисунки 3.77,3.78,3.79,3.80.

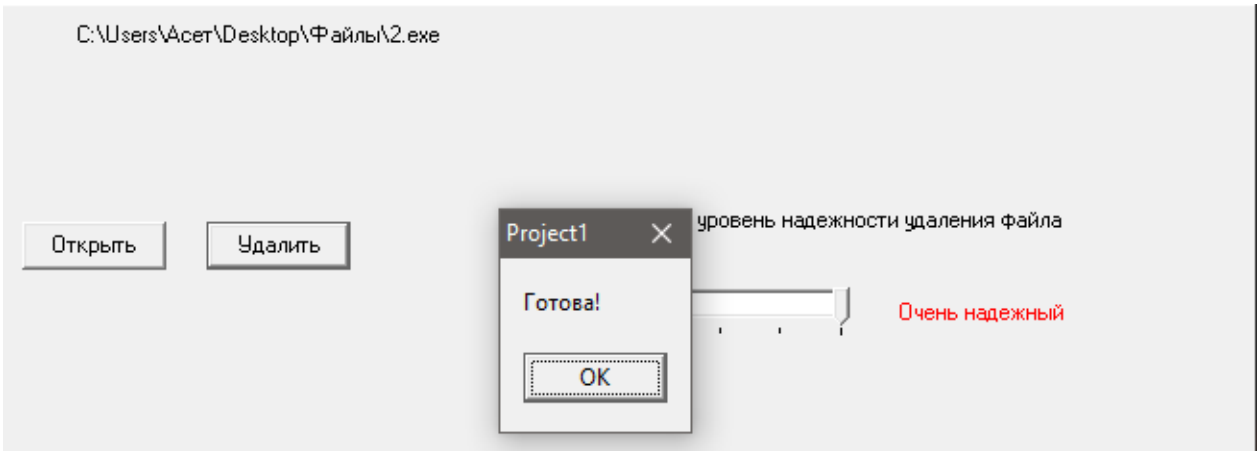


Рисунок 3.77 – Удален формат Exe

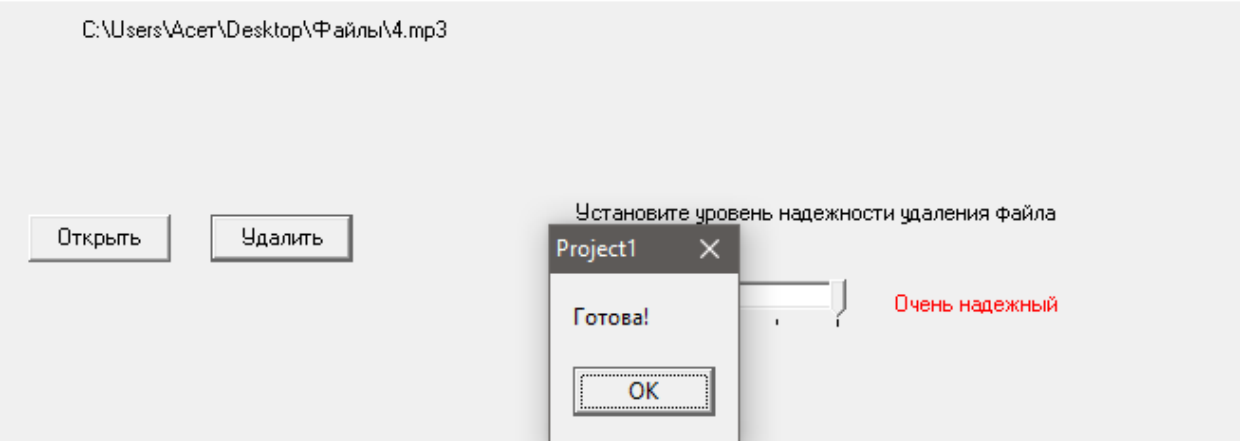


Рисунок 3.78 – Удален формат Mp3

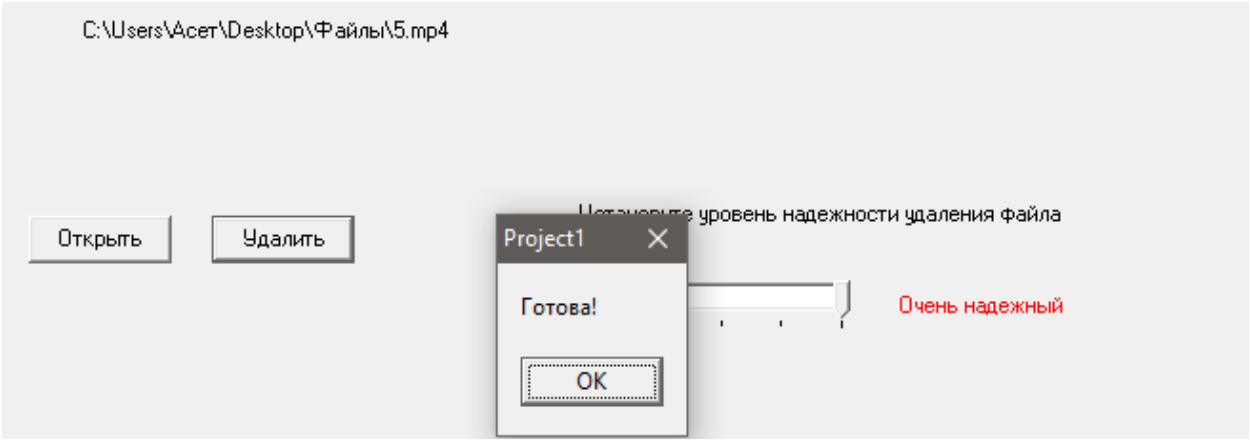


Рисунок 3.79 – Удален формат Mp4

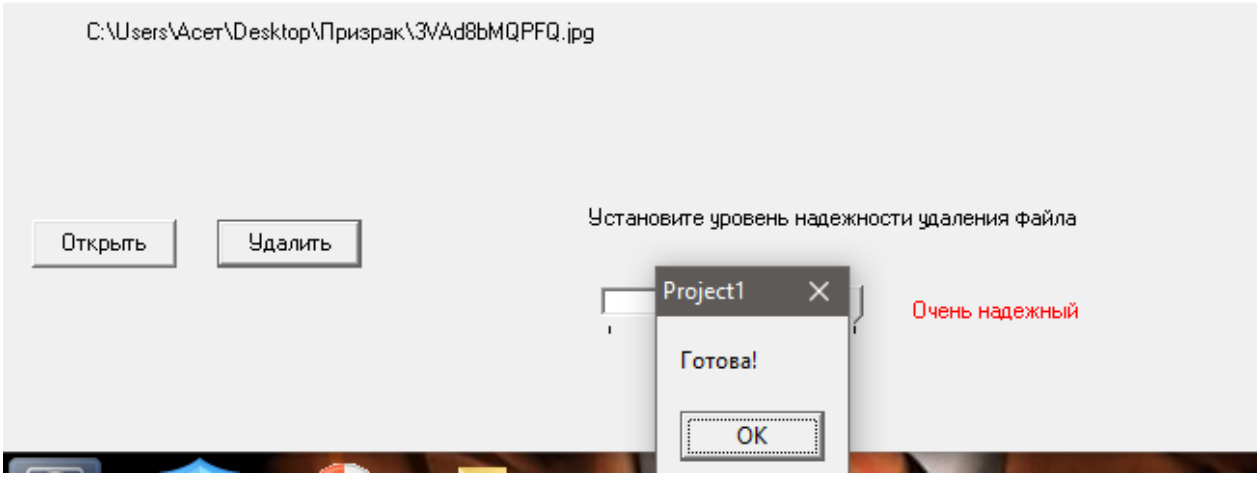


Рисунок 3.80 – Удален формат jpg

После удаления всех файлов, делаем копию диска j, с помощью программы FTK, заходим в незанятое пространство и ищем метадные всех удаленных файлов, смотрим на рисунки 3.81,3.82,3.83,3.84,3.85.

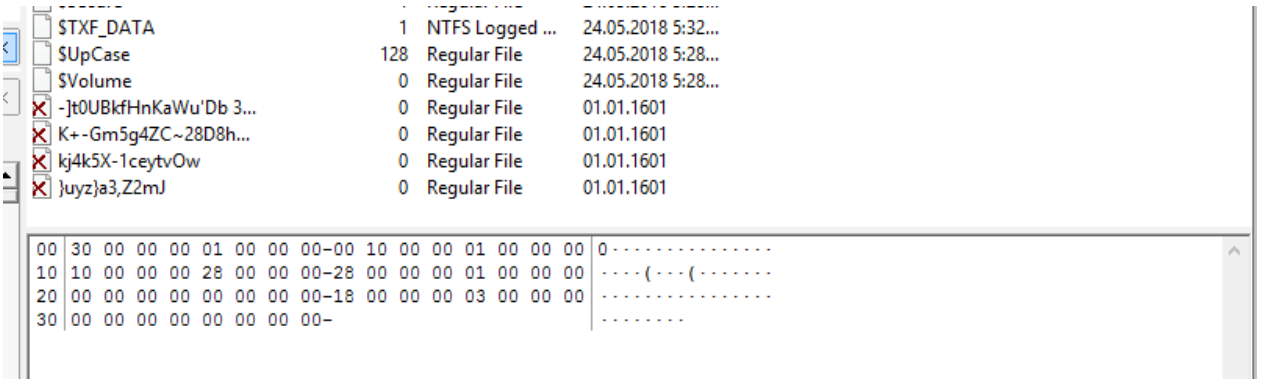


Рисунок 3.81 – Все файлы удалены и переименованы, размеры файлов стерты

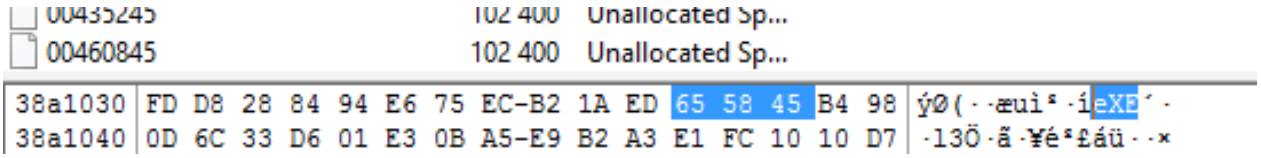


Рисунок 3.82 – Метаданные Exe формата, найдены в секторе 00000045

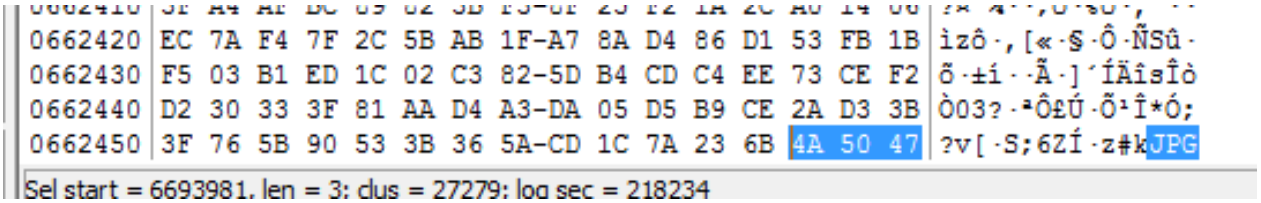


Рисунок 3.83 – Метаданные Jpg формата, найдены в секторе 00025645

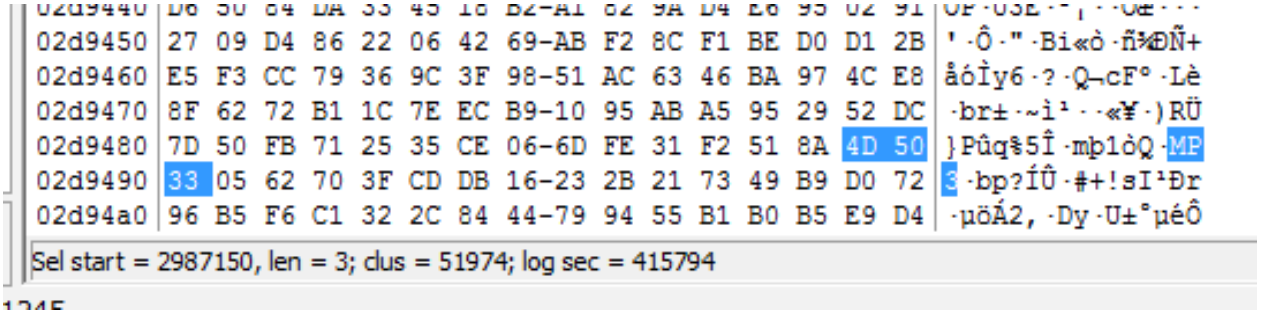


Рисунок 3.84 – Метаданные Mp3 формата, найдены в секторе 00051245

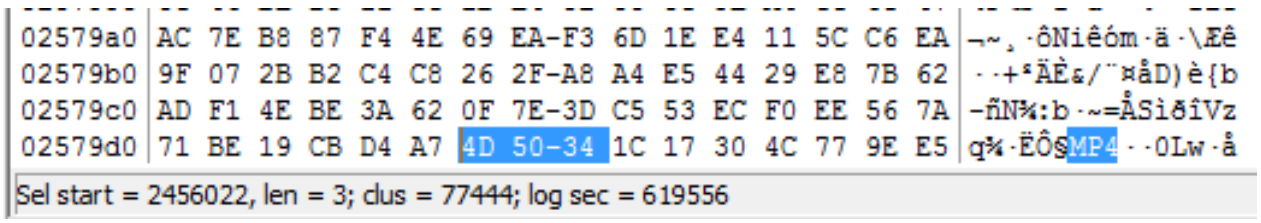


Рисунок 3.85 – Метаданные Mp4 формата, найдены в секторе 00076845

Вывод

Выводы по удалению данных отдельно как файлы или папки, то в этом случае найти метаданные резко повышается и качество гарантии удалении резко понижается. Хоть мы из предыдущих экспериментов путем удаления файлов и папок нашли какое-какие метаданные, но восстановить их полностью на 100% невозможно, это объясняется тем, что на одном кластера, где хранится информация была перезаписано многократно случайными битами. Хоть мы благодаря «Форензики» и узнаем, что действительно была удалена некая информация того или иного формата и даже дату удаления, мы никогда не узнаем его содержимое, потому что восстановить информацию в исходное состояние невозможно. Но если речь идет о стирания всего жесткого диска или других носителей информации, то даже метаданные никогда не будут восстановлены. Итоговые данные проделанных работ приведены в «приложение Б».

4 Технико-экономическое обоснование

4.1 Расчет затрат на исследования

Необходимые затраты на исследования дипломного проекта производится на известные сметы, которая включает следующие:

– Материальные затраты;
– Расчет затрат на оплату труда;
– Расчет затрат по социальному налогу;
– Расчет электроэнергию;
– Прочие затраты.

Материальные затраты состоит из основных вспомогательных материалов, энергии, необходимых для расследования проекта, смотрим на таблицу 4.1.

При покупке нового ноутбука HP pavilion 15 notebook PC в нем есть встроенная операционная система и дополнительные ПО, поэтому затраты на новую операционную систему Windows 10 и лицензионную MS Office считаться не будут.

Таблица 4.1 – Затраты на необходимые ресурсы

Наименования материала	Марка	Количество	Ценза за ед. в тенге	Сумма в тенге
Ноутбук	HP pavilion 15 notebook PC	1	110 000	110 00
Жесткий диск	500 GB Barracuda SN: WDE1FRV7 WWN 500C5009DF9DE60	1	15 000	15 000
SATA USB	2.5 Inch Sata USB3.0 Hard Drive Enclosure, 5 max Gbps, 2.5 HDD/SDD, Tool free	1	4000	4000
Мышка	USB Logitech G102 Prodigy	1	13 000	13 000
Модем	TP-Link TLWR740N	1	8000	8000
Итого	150 000			

Общая сумма затрат на материальные ресурсы (Зм) определяется по формуле:

$$Зм = \sum Pi \times Цi, \quad (4.1)$$

где Pi - расход i-го вида материального ресурса, натуральные единицы;

Цi - цена за единицу i-го вида материального ресурса, тг;

i - вид материального ресурса;

n - количество видов материальных ресурсов.

ЗМ = 110 000 + 15 000 + 4000 + 13 000 + 8000 = 150 000 тенге

Материальные затраты на дипломный проект составят 150 000 тенге. Все материальные затраты лягут на основные средства.

4.2 Расчет трудоемкости

Для точного определения трудоемкости исследования дипломного проекта приведен перечень всех основных этапов и видов работ, которые необходимо выполнить. Трудоемкость работы определялась согласно нормам времени на проведение расчетов, анализа и исследований. Форма разделения работ по этапам с указанием трудоемкости их выполнения приведена в таблице 4.2.

Таблица 4.2 – Поэтапно распределения работ по трудоемкости

Этапы исследования метода гарантированного удаления данных	Виды работ	Трудоемкость исследователя чел х ч.
1 этап	Поиски литератур по удалению данных	50
2 этап	Ознакомления с литературами по удалению данных	30
3 этап	Составления плана по методу гарантированного удаления данных	10
4 этап	Покупка нужных средств для исследования метода гарантированного удаления данных	10

Продолжения таблицы 4.2

Этапы исследования метода гарантированного удаления данных	Виды работ	Трудоемкость исследователя чел х ч.
5 этап	Составления аналитического обзора существующих ПО для гарантированного удаления данных	40
6 этап	Реализация проекта и экспериментирования разных вариантов методов по удалению данных	360
7 этап	Составления отчета по всем методам гарантированного удаления данных	15
8 этап	Выборка и тестирования наилучших методов гарантированного удаления данных	10
9 этап	Оформления 1 главы темы дипломного проекта	40
10 этап	Оформления 2 главы темы дипломного проекта	15
11 этап	Оформления 3 главы темы дипломного проекта	40
12 этап	Оформления 4 главы темы дипломного проекта	4
13 этап	Оформления 5 главы темы дипломного проекта	5
14 этап	Итог исследования	10
ИТОГО трудоемкость выполнения дипломного проекта		549

Количество часов в одном рабочем дне равно 8 часам. То есть количество дней, затраченных на осуществление цели дипломного проекта – 68 рабочих дней.

4.3 Расчет затрат на электроэнергию

Поскольку в процессе производства используется электрооборудование, необходимо рассчитать затраты на электроэнергию. Затраты на электроэнергию для производственных нужд включают в себя расходы электроэнергии на оборудование и дополнительные нужды.

Время работы оборудования для исследования берется равным 549 часов для ноутбуков и модема, данное количество часов было рассчитано в таблице 4.2.

$$Э = Зэл.эн.обор + Здоп.нуж, \quad (4.2)$$

где Зэл.эн.обор – затраты на электроэнергию оборудования;
Здоп.нуж. – затраты электроэнергии на дополнительные нужды.

Расходы электроэнергии на оборудование рассчитывается по формуле:

$$Зэл.эн.обор = \sum W \times Кисп \times S \times T, \quad (4.3)$$

где W – потребляемая мощность, Вт;
Кисп – коэффициент использования (Кисп = 0,7..0,9);
T – время работы;
S – тариф (1кВт/ч = 16,65тг).

Результаты расчета затрат на электроэнергию представлены в таблице 4.3.

Таблица 4.3 – Результаты затрат электроэнергии

Наименования приборов	Паспортная мощность кВт	Коэффициент мощности	Время работы оборудования, ч	Цента ЭЭ тг/кВт ч	Сумма тенге
Ноутбук	0.6	0.7	549	16,65тг	3746.9
Модем	0.08	0.9	300	16,65тг	359.64
SATA USB	0.012	0.9	549	16,65тг	96.345
Жесткий диск	0.005	0.9	549	16,65тг	41.13
Освещение	0.3	0.7	549	16,65тг	1919,5
Итого	6163,515 тенге				

Зэл.эн.обор =3746.9+359.64+96.345+41.13+1919.5=6163.515

Затраты на дополнительные потребности берутся по укрупненному показателю в размере 5% от затрат на оборудование:

$$Здоп.нуж = 5\% \times Зэл.эн.обор, \quad (4.4)$$

Затраты на дополнительные потребности рассчитаны по формуле (4.4):

Здоп.нуж = 0.05 × 6163.515= 308.17 (тенге)

Таким образом суммарные затраты на электроэнергию составляют:

Э = 6163.515 + 308.17 = 6471,685 (тенге)

4.4 Расчет затрат на оплату труда

Над разработкой проекта работают два сотрудника:

– руководитель проекта – изучение предметной области, анализ требований к системе, проверка и поддержка;

– студент – исследования, составления плана, изучения ПО, экспериментирования и тестирования, составления отчета и оформления работ.

Общая сумма затрат на оплату труда (Зтр) определяется по формуле:

$$Зтр=\sum ЧСi \times Ti\ , \qquad (4.5)$$

где ЧСi - часовая ставка i-го работника, тг;

Ti - трудоемкость разработки модели, чел.×ч;

i - категория работника;

n - количество работников, занятых разработкой ПП.

На этапах исследования, участники задействованы неравноценно, для этого необходимо рассчитать часовую ставку работника, а затем общий размер заработной платы. Часовая ставка работника может быть рассчитана по формуле:

$$ЧСi = ЗПi/\ ФРВi, \qquad (4.6)$$

где ЗПi - месячная заработная плата i-го работника, тг;

ФРВi- месячный фонд рабочего времени i-го работника, час.

Месячная заработная плата сотрудников:
Профессор – 150 000 тг;
Студент – 80 000 тг.

ЧСi = 150 000 / 22 × 8 = 852.27 тг/ч
ЧСi = 80 000 / 22 × 8 = 454.54 тг/ч

Часовая ставка научного руководителя составляет 852.27 (тг/ч), трудоемкость руководителя – 90 ч. Часовая ставка студента составляет 454.54 (тг/ч), трудоемкость исследования – 549 ч. Рассчитаем общую сумму затрат на оплату труда по формуле (4.5):

Зтр = 852.27 × 90 + 454.54 × 549 = 76 704.3 + 249 542.46 = 326 246.76 (тенге)

Результаты расчета затрат на оплату труда показаны в таблице 4.4.

Таблица 4.4 – Расчет затрат на оплату труда

Категория работника	Трудоемкость исследования дипломного проекта	Часовая ставка, тг/ч	Сумма, тг
Научный руководитель	90	852.27	76 704.3
Студент	549	454.54	249 542.46
Итого	326 246.76 тенге		

4.5 Расчет затрат по социальному налогу

Социальный налог – согласно Налоговому кодексу Республики Казахстан составляет 9,5% от ФОТ (фонда оплаты труда). Следует отметить, что пенсионные отчисления не облагаются социальным налогом.

$$Сн = (ФОТ- ПО) \times 0.095, \quad (4.7)$$

где ПО - отчисления в пенсионный фонд, 10% от ФОТ.

Социальный налог рассчитываем по формуле (4.7):

ПО = 326 246.76 × 0.1 = 32 624.676 тенге;
Сн = (326 246.76 – 32 624.676) × 0.095 = 27 894.097 тенге

Результаты расчета затрат представлены в таблице 4.5.

Таблица 4.5 – Затраты по социальному налогу

Категория работника	Количество человек	Заработная плата, тг	Пенсионные отчисления	Социальный налог, тг
Научный руководитель	1	76 704.3	7670.43	6558.217
Студент	1	249 542.46	24 954.246	21 335.8803
Итого	27 894. 097 тенге			

4.6 Амортизация основных фондов, прямолинейный метод

Годовые нормы амортизации ОФ принимаются по налоговому кодексу РК или определяются, исходя из возможного срока полезного использования ОФ. Амортизация основных фондов определяется по формуле (4.8):

$$Аг = (Соб \times НА) / 100, \quad (4.8)$$

где Соб – стоимость оборудования;
НА – норма амортизации (норма амортизация = 25).

По формуле 4.8 рассчитаем сумму амортизационных отчислений за год для ноутбука:

Аг = (110 000 х 25)/100 = 27 500 тг

Рассчитаем сумму амортизации за время работы:

Ар = (27 500 х 68)/365 = 5123 тг

Аналогичным способом рассчитаем сумму амортизации для остального оборудования. Результаты расчетов приведены в таблице 4.6

Таблица 4.6 – Амортизация основных фондов

Наименования оборудования	Стоимость, тг	Годовая норма амортизации,%	Сумма амортизации за год, тг	Сумма амортизации за время работы дипломного проекта,тг
Ноутбук	110 000	25	27 500	5123
Модем	8 000	15	1200	223
SATA USB	4000	15	600	111,5
Жесткий диск	15 000	15	3750	700
Мышка	13 000	15	3250	605
ИТОГО амортизация ОС			36 300	6762,5

4.7 Смета затрат

Смета затрат на исследования и составления метода гарантированного удаления данных на основании полученных данных по отдельным статьям составляется смета затрат по форме, приведенной в таблице 4.7.

Таблица 4.7 – Смета затрат на исследования и составления метода гарантированного удаления данных

Статьи затрат	Сумма, тг
Затраты на оборудования	150 000
Затраты на электроэнергию	6471.685
Оплата труда	326 246.76
Затраты по социальному налогу	32 298.42
Амортизация основных фондов	6762,5
ИТОГО	521 779.365

Вывод

В данной главе были произведены расчеты экономических затрат на приобретение необходимого оборудования и программного обеспечения для исследования и составления метода гарантированного удаления данных, включая расчет на оплату труда. Полностью рассчитал затраты, направленные на покупку оборудования; расчет трудоемкости; расчет эксплуатационных расходов: социальный налог и пенсионные отчисления, расходы на электроэнергию и амортизация основных фондов. Для потребителей экономический эффект будет исходить из: снижения затрат на использование оборудования, повышения экономической эффективности использования основных средств на исследования. Качественный эффект для потребителя состоит в том, что выбранный метод по гарантированному удалению данных позволит улучшить качество безопасного ликвидации, эксплуатации носителей информации, без потери конфиденциальных данных, для обеспечения информационной безопасности и производительности труда на рабочем месте. Используя мои методы исследования по гарантированного удаления данных, средние предприятия может сэкономить большие деньги на носители информации, то есть жесткие диски и USB флешки и прочее носители информации. Используя программные методы гарантированного удаления данных средние предприятия может повторно использовать свои носители информации и не выкидывать или сжигать до полного уничтожения как написано в уставе и подписаным Бакытжан Сагинтаевым 2016 году. Но если взять крупные предприятия как коммерческие банки, то для них физически уничтожить носитель информации не составит больших затрат так как предприятие может себе это позволить не жалей среднее предприятие или организация, например, школы, институты, средние компании и так далее.

5 Безопасность жизнедеятельности

5.1 Характеристика условий труда программиста

Данной дипломный проект посвящен исследованию подобрать эффективный метод по гарантированному удалению данных. Исследование будет проходится в большом кабинете в 200 м^2, поэтому нужно определить и рассчитать сколько нужно для этого кабинета искусственное освещение, рассчитать количество светильников для хорошего обзора видение, чтобы глаза программиста не утомлялись быстро. Исследование по методу гарантированному удалению данных будет осуществляться с использованием компьютерной техники и электронного оборудования.

Трудовая деятельность относится к группе В (отладка программ, перевод и редактирования и др.). Продолжительность работ превышает 6 ч и выполняемые работы относятся к III категории работ, выполняемые в оптимальных условиях труда при благоприятных нагрузках. Установлены перерывы по 20 мин каждый через 2 ч после начала работ, через 1,5 ч и 2, 5 ч после обеденного перерыва или же по 5-15 мин через каждый час работы. Общее время перерывов не превышает 60 мин.

В трудовом участке обязаны быть учтены меры защиты от вероятного влияния опасных и вредоносных факторов производства. Степени этих факторов не должны быть выше предельных значений, оговоренных правовыми, техническими и санитарно-промышленными общепризнанными мерками. Данные нормативные документы обязывают к созданию в рабочем месте условий работы, при которых влияние опасных и вредоносных факторов на работающих ликвидировано совсем, или находится в допустимых пределах.

Данная глава дипломного проекта посвящена рассмотрению следующих вопросов:

– установление подходящих обстоятельств работы инженера или программиста;

– расчет освещенности.

Научно-техническое развитие привнес значительные перемены в требование производственной работы сотрудников интеллектуальной работы. Их деятельность стало наиболее активным, интенсивным, вызывающим значительных затрат умственной, психологической и физиологической энергии. Данное вызвало единого постановления трудностей эргономики, гигиены и организации работы, регламентации систем работы и отдыха.

Работа с ПК характеризуется существенным интеллектуальным усилием и раздражительно-психологической загрузкой операторов, большой напряженностью визуальной деятельность и довольно огромный загрузкой в мышцы рук присутствие работе с клавиатурой ЭВМ. Огромное роль обладает разумная конструкция и размещение компонентов трудового зоны, то что немаловажно с целью укрепления подходящей рабочей позы человека-оператора.

В ходе деятельность с компьютером следует придерживаться верный порядок работы и отдыха. В ином случае у персонала помечаются существенное напряжённость визуального аппарата с возникновением претензий в неудовлетворение работой, ведущие боли, нервозность, несоблюдение сна, утомление и нездоровые чувства в глазах, в пояснице, в области шеи и руках. [16]

5.2 Параметры микроклимата в помещениях

Характеристики микроклимата имеют все шансы меняться в широких пределах, в то время как важным обстоятельством жизнедеятельности человека считается поддержание постоянства температуры тела вследствие терморегуляции, т.е. возможности организма корректировать ответную реакцию тепла в окружающую среду. Принцип нормирования микроклимата – создание оптимальных обстоятельств с целью теплообмена тела человека с окружающей средой.

Вычислительная оборудование считается основой значительных тепловыделений, что способен послужить причиной к увеличению температуры и уменьшению относительной влаги в помещении. В комнатах, где определены ПК, обязаны соблюдаться конкретные характеристики микроклимата. В санитарных нормах СН-245-71 определены величины характеристик микроклимата, формирующие удобные условия. Эти нормы устанавливаются в связи с периода года, характера трудового процесса и характера производственного помещения (см. табл. 5.1).

Объем комнат, в каковых расположены сотрудники вычислительных центров, не должен быть меньше 19,5м3/человека с учетом максимального числа одновременно работающих в смену. Общепризнанных мерок подачи свежего воздуха в помещения, где находятся ПК, приведены в табл. 5.2. [16]

Таблица 5.1 Параметры микроклимата для помещений, где установлены компьютеры

Период	Параметр микроклимата	Велечина
Холодный	Температура воздуха в помещении Относительная влажность Скорость движения воздуха	22…24 °С 40…60 % до 0,1 м/с
Теплый	Температура воздуха в помещении Относительная влажность Скорость движения воздуха	23…25 °С 40…60 % 0,1…0,2 м/с

Таблица 5.2 Нормы подачи свежего воздуха в помещения, где расположены компьютеры

Характеристика помещения	Объемный расход подаваемого в помещение свежего воздуха, $м^3$ /на одного человека в час
Объем до 20 $м^3$ на человека 20…40 $м^3$ на человека	Не менее 30 Не менее 20 Естественная вентиляция

С целью предоставления удобных условий применяются как организационные методы (здравая предприятие выполнения работ в зависимости от времени и дней, смена работы и отдыха), таким образом и технические средства (вентиляция, кондиционирование воздуха, отопительная система).

5.3 Режим труда

При работе с компьютером очень важную роль играет соблюдение здравого режима труда, перерывов и отдыха. В случае не соблюдение норм, у персонала отмечаются напряжение зрения, появление жалоб на усталость в работе, боли в голове, спины, глаз, нарушение сна и.т.п, что в последствие снижает уровень и качество работы.

В табл. 5.3 представлены сведения о перерывах, которые необходимо делать при работе на компьютере, в зависимости от продолжительности рабочей смены, видов и категорий трудовой деятельности с ВДТ (видео дисплейный терминал) и ПЭВМ (в соответствии с СанПиНом 2.2.2 542-96 «Гигиенические требования к видео дисплейным терминалам, персональным электронно-вычислительным машинам и организации работ»).

Таблица 5.3 Время регламентированных перерывов при работе на компьютере

Категория работы с ВДТ или ПЭВМ	Уровень нагрузки за рабочую смену при видах работы с ВДТ			Суммарное время регламентированных	
	Группа А, количество знаков	Группа Б, количество знаков	Группа В, часов	При 8-часовой смене	При 12-часовой смене
I	до 20 000	до 15 000	до 2,0	30	70
II	до 40 000	до 30 000	до 4,0	50	90
III	до 60 000	до 40 000	до 6,0	70	120

Примечание. Время перерывов дано при соблюдении указанных Санитарных правил и норм. При несоответствии фактических условий труда требованиям Санитарных правил и норм время регламентированных перерывов следует увеличить на 30%.

В соответствии со СанПиН 2.2.2 546-96 все виды трудовой деятельности, связанные с использованием компьютера, разделяются на три группы:

– группа А: работа по считыванию информации с экрана ВДТ или ПЭВМ с предварительным запросом;

– группа Б: работа по вводу информации;

– группа В: творческая работа в режиме диалога с ЭВМ.

Эффект лучше будет во время перерывов, если сотрудник будет делать гимнастику, или в комнате где рассчитана для отдыха персонала с удобной мебелью, зеленой зоной, прохладной обстановкой.

5.4 Расчет естественной освещенности

Тип помещения: Компьютерная аудитория

Параметры помещения (L x B x H), м:20x10x4

Высота окна h_{0K}, м: 2,5

Разряд зрительной работы: IV, а

Коэффициенты отражения: $Р_{пот}$=70%, $Р_{ст}$=50%, $Р_{пол}$=30%

Высота начала окна $h_{Н.0К}$, м: 1 Световой пояс: г. Акмолинкская $Н_{зд}$, м: 26

Расстояние до рядом стоящего здания, Р, м: 12 уровень условной рабочей поверхности $h_{пов}$- 0,8 м

Расчет естественного освещения заключается в определении площади световых проемов.

Общую площадь окон определяем по формуле (5.1) [12] для бокового освещения:

$$S0 = (Sn \times ен \times n0 \times Кзд \times Кз) / (100 \times \tau0 \times r1), \quad (5.1)$$

где Sn – площадь пола помещения, м2;

ен – нормированное значение КЕО;

екео – значение КЕО по таблице 3.12 [1] для IV пояса: екео = 0,9;

m – коэффициент светового климата, определяется по таблице 3.1 [12] для ориентации световых проемов ЮВ m=0,8;

Кз – коэффициент запаса по таблице 3.11 [1]: Кз = 1,5;

kЗД – коэффициент, учитывающий затенение окон противостоящими зданиями (kЗД = 1);

τ0 – общий коэффициент светопропускания $\tau_0 = \tau_1 \cdot \tau_2 \cdot \tau_3 \cdot \tau_4$;

τ1 – коэффициент светопропускания материала по таблице 6 [16]: для двойного стекла τ1 = 0,8;

τ2 – коэффициент, учитывающий потери света в переплетах светопроёма по таблице 7 [12]: τ2 = 0,7;

τ3 – коэффициент, учитывающий потери светав несущих конструкциях, при боковом освещении равен 1;

τ4 – коэффициент, учитывающий потери света в солнцезащитных устройствах, см. таблицу 3.6 [16]: τ4 =1.

$$Sn = B \times L, \quad (5.2)$$

где Sn – площадь помещения;
L – длина помещения;
B – ширина помещения.

$$en = ekeo \times m, \quad (5.3)$$

$Sn = 10 \times 20 = 200м^2$
$en = 0.9 \times 0.8 = 0.72$
$\tau 0 = 0.8 \times 0.7 \times 1 \times 1 = 0.56$
$L / (B / 2) = 20 / (10 / 2) = 4$

$\eta 0$ – световая характеристика окон по таблице 3.2. [16]

$$h1 = hок + hн.ок – hпов, \quad (5.4)$$

где h1 – высота от уровня условной рабочей поверхности до верха окна;
hc - расстояние от светильника до перекрытия;
hp - высота рабочей поверхности над полом;
h - высота помещения.
r1 – коэффициент, учитывающий повышение КЕО при боковом освещение благодаря свету, отраженному от поверхностей помещения и подстилающего слоя, прилегающего к зданию, см. таблицу 3.9. [17]

$h1 = 2.5 + 1 – 0.8 = 2.7$ м
$B / h_1 = 10 / 2.7 = 3.704$ значит $n_0 = 8$
$r_1 = 1.8$
$H / B = 4 / 10 = 0.4$
$L / B = 20 / 10 = 2$
$(Рпот + Рст + рпол) / 3 = (50 + 30 + 70) / 3 = 50\%$

Кзд – коэффициент, учитывающий затенение окон противостоящими зданиями по таблице 3.8. [17]

$$Р / Нзд = 12 / 26 = 0.462, \quad (5.5)$$

$К_{зд} = 1,7$

Подставим все значения в расчетную формулу:

$S0 = (200 \times 0.72 \times 8 \times 1.7 \times 1.5) / (100 \times 0.56 \times 1.8) = 29.143м^2$

Так как предусматривали двустороннее боковое освещение, то площадь световых проемов на одной стороне будет 29:2=14,5 м^2

Так как высота оконных проемов 2,5 м, то, следовательно, длина их составит 14,5:2,5=5,8 м.

Таким образом, площадь световых проемов составит с обеих сторон по 14,5 м^2 (5,8 х3 м) (см. Рисунок 5.1).

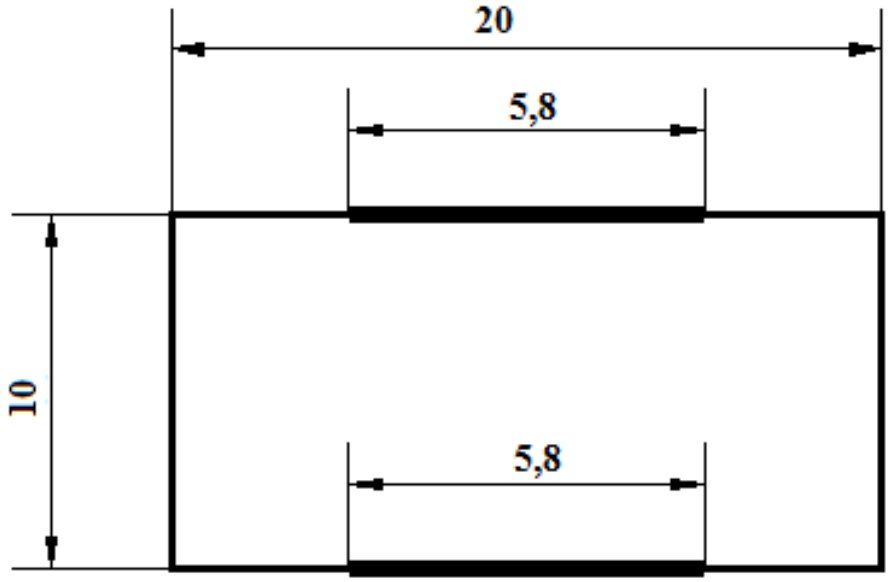


Рисунок 5.1 – схема освещения при естественном освещении

5.5 Расчет искусственного освещения

Определение расчетной высоты подвеса:

$h = H – (h + h) = 4 – (0.8 + 0.2) = 3м$

Из таблицы 3 [12] выбираем ртутные лампы HPL-N, мощностью 125Вт и световым потоком F=6200 лм.

Определим индекс помещения:

$i = (20 \times 10) / (3 \times (20 + 10)) = 2.222$

По таблице 5.11 [17] определим коэффициент светового использования светового потока $\eta = 55\%$:

Количество ламп при необходимой освещенности Е=200лк:

$$N = (E \times S \times Z \times Кз)/(F \times \eta), \quad (5.6)$$

где Z – коэффициент неравномерности освещения, равный $1{,}1 \div 1{,}2 \approx 1{,}15$

Кз – коэффициент запаса, принимаемый равным 1,5 для заданного типа помещения;

S – площадь помещения, м2.

$N = 200 \times (20 \times 10) \times 1.15 \times 1.5) / 6200 \times 0.55 = 20$

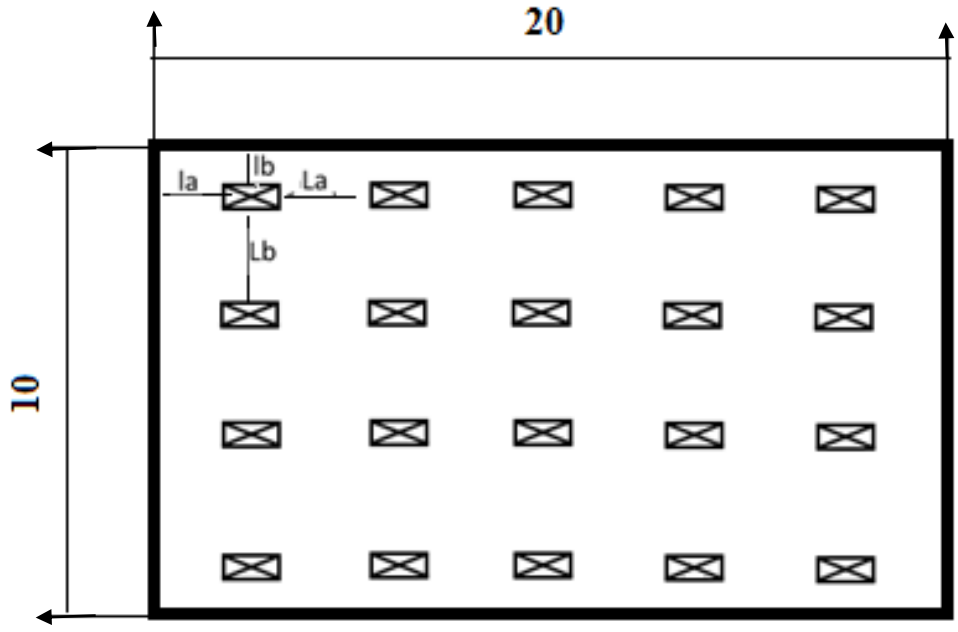


Рисунок 2.2 – Схема расположения светильников

Расчет расстояния между светильниками.

В длину:

$LA = 1.3 \times 3 = 3.9$ м

В ширину:

$LB = 0.8 \times 3 = 2.4$ м

Расстояние от стены до ближайшего светильника:

$$l(A,B) = L(A,B)/2, \quad (5.7)$$

В длину:

$lA = 3.9 / 2 = 1.95$ м

В ширину:

$lB = 2.4 / 2 = 1.2$ м

Намечаем контрольную точку А. Для нее определяем суммарную условную освещенность всех светильников следующим образом:

Находим проекцию расстояния на потолок от точки А до светильника – di;

Далее определяем угол между потолком и прямой di. По этому углу находим условную освещенность.

Проверим, выполняется ли условие: Er > Енорм

Коэффициент запаса Кз = 1,5;

Коэффициент учитывающий действие равноудаленных светильников μ=1,15;

Световой поток F=6200 лм.

Таблица 5.4 – Светораспределение светильника

Сила света I_a кд в направлении угла α										
0	5	15	25	35	45	55	65	75	85	90
242	241	230	215	190	158	119	76	40	10	0

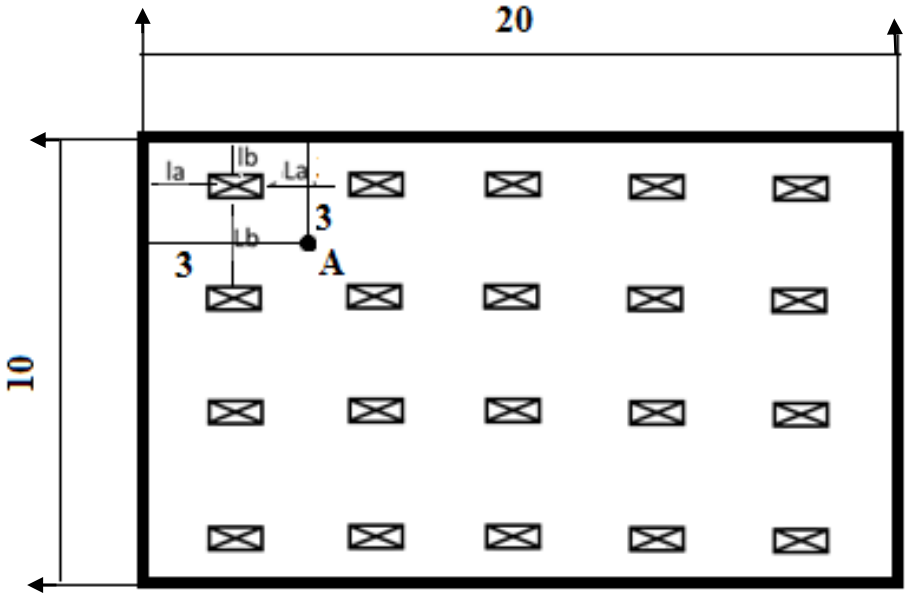


Рисунок 5.3 – Произвольно помещенная точка А на расстоянии 3-х метров от обоих стен, относительно левого верхнего угла

Суммарная условная освещенность равна:

er = 54.647 лк

Суммарная освещенность:

Er = 6200 ×1.15 × (54.647/(1000 × 1.5)) = 259.755 лк

Так как Er > Енорм (259,755 > 200), то осветительные приборы и их расположение подобраны верно. [16][17][18][19]

Вывод

В данной главе был проведен анализ оптимальных условий труда для исследования метода гарантированного удаления данных и рассчитаны необходимые меры безопасности труда. Помимо этого, был проведен расчет и сделан анализ освещенности помещения, где будут проводится исследование метода гарантированного удаления данных, по результатам которого можно сделать вывод, что расчет площади световых проемов соответствует нормам естественного освещения рабочей зоны, количество и тип светильником используемые в данной рабочей зоне достаточно для обеспечения искусственного освещения. Далее, был сделан анализ рабочих перерывов, что не приведёт к снижению качество работы, а наоборот повысит уровень работы, был представлен эргономические требования к рабочему месту.

Заключение

Во время выполнения дипломного проекта были исследованы методы гарантированного удаления и написана программа для гарантированного удаления данных.

Проделав большую работу в области удаления данных, я пришел к выводу, что достаточно одного прохода стирания всего диска для гарантированного удаления данных, стирать нужно именно весь жесткий диск или другие виды носители информаций, а не отдельно файлы или папки. В качестве доказательства можно посмотреть на главу 3.4, где был произведен метод удаления путём одного стирания благодаря программе ccleaner. Для наглядности давайте представим, что у нас есть некая информация точнее данные, которые содержат, например, картинку в формате jpg мы поместили эту картинку на свой жёсткий диск, благодаря программе компьютерной криминалистики FTK мы сможем увидеть расположение этой картинки на секторе 276400, или же, например, взять обычный шестнадцатеричный преобразователь, с которого можно посмотреть весь жесткий диск и его сектора, а теперь удалим этот жесткий диск путем безвозвратного удаления одним проходом. После этой процедуры мы можем видеть, что на секторе 276400 вместо предыдущих данных теперь остались только нули, то есть даже следы картинки были перезаписаны. Конечно вы можете сказать, что в правоохранительных органах есть более дорогие и современные оборудования для восстановления данных, чем программные, я говорю о магнитной микроскопии суть метода кроется в том, чтобы определить состояние каждого бита до перезаписи, то есть был ли он равен единице или нулю. Представим, что у нас есть текст в кодировке ASCII, это значит, что каждый символ кодируется восемью битами, а значит если хоть один бит будет восстановлен неправильно, тогда получится совсем другой символ. Можно в качестве примера взять слово «Anti», в бинарном коде он выглядит так 1000001 1101110 1110100 1101001, представим теперь, что магнитная микроскопия восстановила все биты кроме последнего, то есть в конце вместо «1», он восстановил «0», тогда мы получим слово «Anth». Как видим получилось совсем другое слово, и я говорю о простом текстовом файле. А если пойдет речь о восстановления гигабайтных информации БД, изображения, архивы, видео форматы и.т.д. Самое главный минус в этом это то, что метод очень долгий и дорогой, титанический труд, за который не возьмется ни один человек.

Программные методы стирания диска всегда были и останутся по времени удаления долгими, но что же делать если будет рейдерский захват какого-либо предприятия или же проникновения от злоумышленника в серверский центр для похищение жесткого диска, в этом случае нам помогут дорогостоящие оборудования, которые уничтожают любые носители информации за считанные секунды методом размагничивание поверхности носителя, эти методы мы классифицировали в первой главе. В качестве примера такого оборудования можно взять импульс-9В (до 9 дисков hdd/ssd).

Применяется в чрезвычайных ситуациях, для уничтожения информации на HHD/SSD. Оборудование помещает в себя более 9 дисков при том, что легко можно встроить его в серверную часть. При взломе сервера или же попытки украсть носителей информации, мгновенно автоматический сработает оборудование и путем размагничивания уничтожит все данные на жестком диске. [13] Активация работает как вручную, так и удаленно. Итоговые данные проделанных работ расписано в «приложение Б».

В коммерческих банках, все свои данные на носителях они хранят и архивируют. Но в случае неисправности жесткого диска, они копируют все данные на новый рабочий жесткий диск, а старые жесткие диски сжигают до полного уничтожения. Но взять, например, среднее предприятия, где организация не может себе позволить сжечь или же уничтожить физический жесткие диски, они вынуждены использовать программные методы для стирания дисков и дальше повторно использовать носители информации. В этих случаях мои методы актуальны, так как ранее говорилось, что достаточно и одного прохода стирания ЖД, что дает быстроту и эффективный метод гарантированного удаления данных.

Список литературы

1 Беседин Д.И., Боборыкин С.Н., Рыжиков С.С. Анализ возможностей предотвращения утечки информации, хранящейся в накопителях на жестких магнитных дисках. // «Специальная техника», №1, 2009.

2 Боборыкин С.Н., Рыжиков С.С. Оценка эффективности средств уничтожения информации, хранящейся в накопителях на жестких магнитных дисках. // «Специальная техника», №3, 2010.

3 Болдырев А.И., Сталенков С.Е. Надежное стирание информации — миф или реальность?. // «Защита информации. Конфидент», № 1, 2011.

4 Мирин А.Ю. Модель канала утечки информации с жесткого магнитного диска ПЭВМ. Труды всеармейской науч.практ. конф. «Инновацио нная деятельность в Вооруженных силах Российской Федерации». – СПб.: ВУ С, 2012.

5 Кэрри Б. Криминалистический анализ файловых систем. / Кэрри Б. — СПб.: Питер, 2013.

6 Eraser vEraser 6.2.0.2982 // eraser.heidi.ie: Официальный сайт программы Eraser. URL: https://eraser.heidi.ie/ (Дата обращение 04.02.18)

7 DiskWipe v1.7 // diskwipe.org: Официальный сайт программы DiskWipe. URL: http://www.diskwipe.org/ (Дата обращение 10.02.18)

8 O&O SafeErase Professional 7.0 // oo-software.com: Официальный сайт программы O&O SafeErase. URL: https://www.oo-software.com/en/safeerase-hard-drive-data-secure-deletion (Дата обращение 10.02.18)

9 Ccleaner v.5.31 // ccleaner.com: Официальный сайт программы Ccleaner. URL:https://www.ccleaner.com/ccleaner (Дата обращение 15.02.18)

10 Компьютерная криминалистика (Форензика) статья и ряд программ // www.spy-soft.net: Официальный сайт программы. URL: http://www.spy-soft.net/cmputer-forensics/#___RAM (Дата обращение 10.03.18)

11 Файлы – призраки. Компьютерная криминалистика // xakep.ru: Официальный сайт новостей кибер атак. URL: https://xakep.ru/2011/03/29/55194/ (Дата обращение 14.03.18)

12 Гультяев А. К. Восстановление данных / А. К. Гультяев. – СПб.: питер 2014.

13 Рохманюк В. М. Аппаратура экстренного уничтожения записей на магнитных носителях / В. М. Рохманюк, Е. М. Фокин. - М: БДИ.

14 Центр ресурсов компьютерной безопасности // csrc.nist : Центр безопасностей форензики. URL:https://csrc.nist.gov/ (Дата обращение 20.03.18)

15 Аманжолова К. Б., Алибаева С. А. Экономика предприятии телекоммуникации: Учебное пособие. - Алматы: АИЭС, 2003.

16 Абдимуратов Ж. С., Мананбаева С. Е. Безопасность жизнедеятельности. Методические указания к выполнению раздела «Расчет производственного освещения» в выпускных работах для всех специальностей. Бакалавриат - Алматы: АИЭС, 2009.

17 Корольченко А.В. Естественное и искусственное освещение. - М.: Изво Москва, 2004.

18 Справочная книга по светотехнике / М. Б. Айзенберга. - М.: Энергоатомиздат 1983.

19 Никитин В. Д. Расчет освещения точечным методом. — Томск: ТПИ им. С. М. Кирова, 1985.

20 Справочная книга для проектирования электрического освещения / Г. М. Кнорринга. - П.: Энергия, 1976.