Отчёт по кейсу: Allegretto

Автор: HTB Sherlocks | Дата: 18.09.2025

1. Введение

> *Мы вели наблюдение за подозреваемым в торговле наркотиками, известным как Shadow. Недавно мы получили информацию о его местонахождении, которая привела нас в квартиру в Лондоне. Во время рейда мы столкнулись с вооружённым сопротивлением, в результате которого пострадали несколько человек. Во время операции Shadow попытался удалить важную информацию со своего компьютера, чтобы избежать ареста. Однако мы успешно задержали его до того, как он успел нанести значительный ущерб. С тех пор мы восстановили важные файлы с его компьютера и хотели бы, чтобы вы проанализировали эти данные, чтобы определить, чем он занимался.*

Вопросы:

Q1. Which version of QGIS is being used by Shadow?
Q2. What is the Shadow's Darkmail email address?
Q3. What is Shadow's Bitcoin address?
Q4. What is the onion URL for the SilkRoad where Shadow sells drugs?
Q5. Based on the cookie's last access, when was the last time Shadow visited the Silk Road website using its onion domain?
Q6. What is Shadow's Hotmail email address?
Q7. When was Shadow supposed to meet his mysterious boss?
Q8. When was the "Contacts Due Amounts" spreadsheet created?
Q9. Which file did Shadow delete from the encrypted USB drive?
Q10. What are Stash Roman's coordinates?

2. Объекты исследования

Имя файла	Источник	Размер	MD5 / SHA256
Allegretto.zip	Получено: HTB Sherlocks / 19.06.2025	618 010 069 байт	MD5: 3566f6577c90a201992e24c36a09a4a2 SHA256: 4e2f9139ba15a0d4286d92591c33c4baa3db00e5127cc6d9bac2e059d9e606f7

- Файл образа .E01 зашифрованного USB-накопителя

- История браузера Tor

- Профили Thunderbird и Proton Mail

- Ключ восстановления BitLocker и .kdbx (keepass)

- Артефакты диска (MFT, USN, prefect и т. д.)

3. Chain of Custody (цепочка хранения доказательств)

Хэш-суммы MD5 и SHA256

```
C:\Users\Ярослава>certutil -hashfile "C:\Users\Ярослава\Downloads\Allegretto.zip" MD5
Хэш MD5 C:\Users\Ярослава\Downloads\Allegretto.zip:
3566f6577c90a201992e24c36a09a4a2
CertUtil: -hashfile — команда успешно выполнена.

C:\Users\Ярослава>
C:\Users\Ярослава>certutil -hashfile "C:\Users\Ярослава\Downloads\Allegretto.zip" SHA256
Хэш SHA256 C:\Users\Ярослава\Downloads\Allegretto.zip:
4e2f9139ba15a0d4286d92591c33c4baa3db00e5127cc6d9bac2e059d9e606f7
CertUtil: -hashfile — команда успешно выполнена.
```

4. Инструменты и окружение

- AccessData FTK Imager 4.7.1.2

- R-STUDIO Network 9.4

- MFTECmd tool ($MFT, $Boot, $J, $SDS, $I30 parser. Handles locked files)

- Timeline Explorer tool (View CSV and Excel files, filter, group, sort, etc. with ease)

- Архивариус 3000 4.79

- SQLite Viewer Web App

5. Методология

- Windows

- Файлы Email

- Зашифрованный USB-накопитель с помощью Bitlocker

- Анализ артефактов диска $MFT

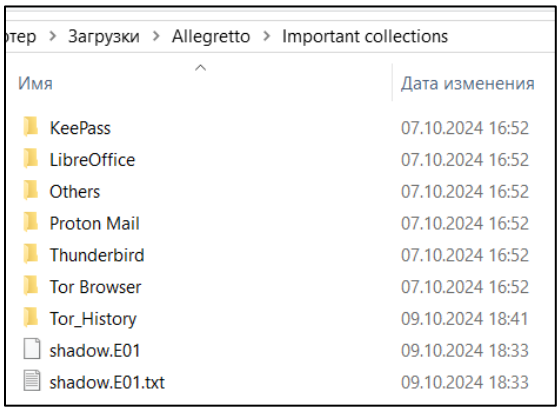
- Анализ USNJournal

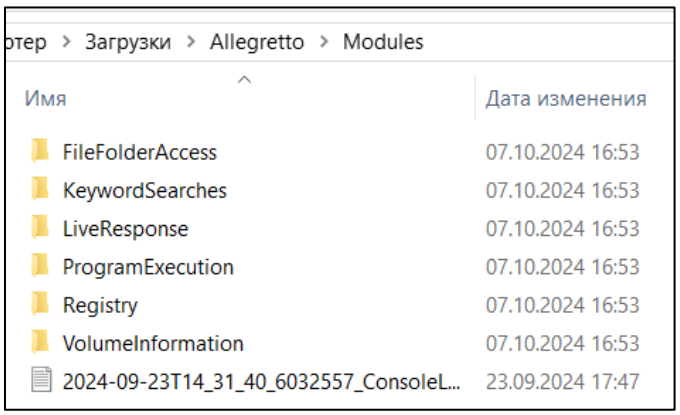
- Анализ истории браузера Tor

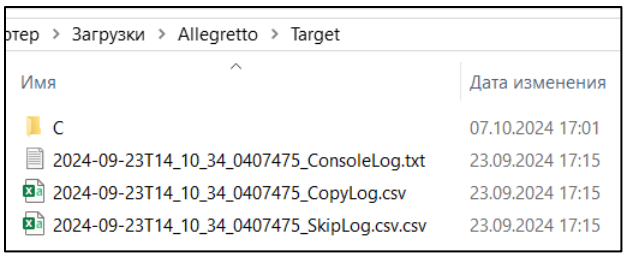
- Просмотр баз данных SQLite

6. Ход исследования (пошагово)

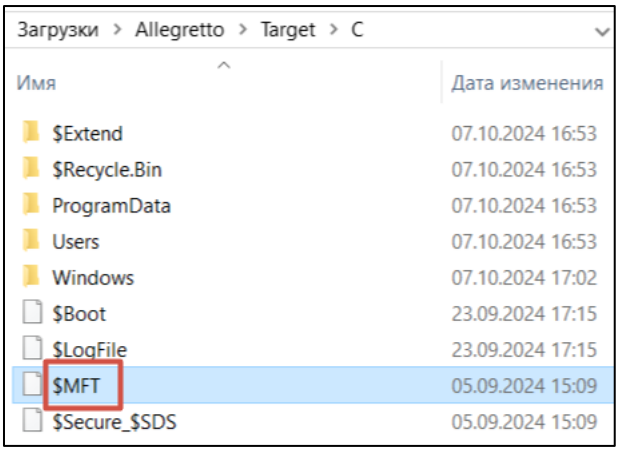
1. У нас имеется архив Allegretto с тремя папками: Important collections, Modules и Target.







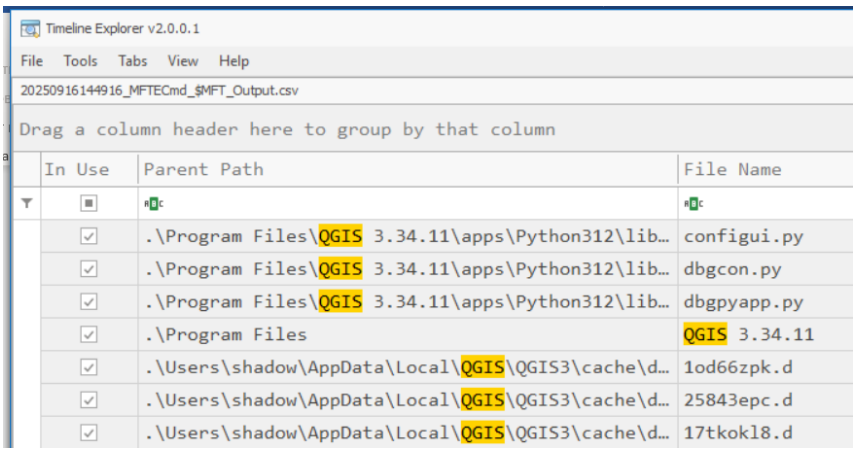
2. В каталоге «Allegretto\Target\C\» обнаруживаем файл $MFT



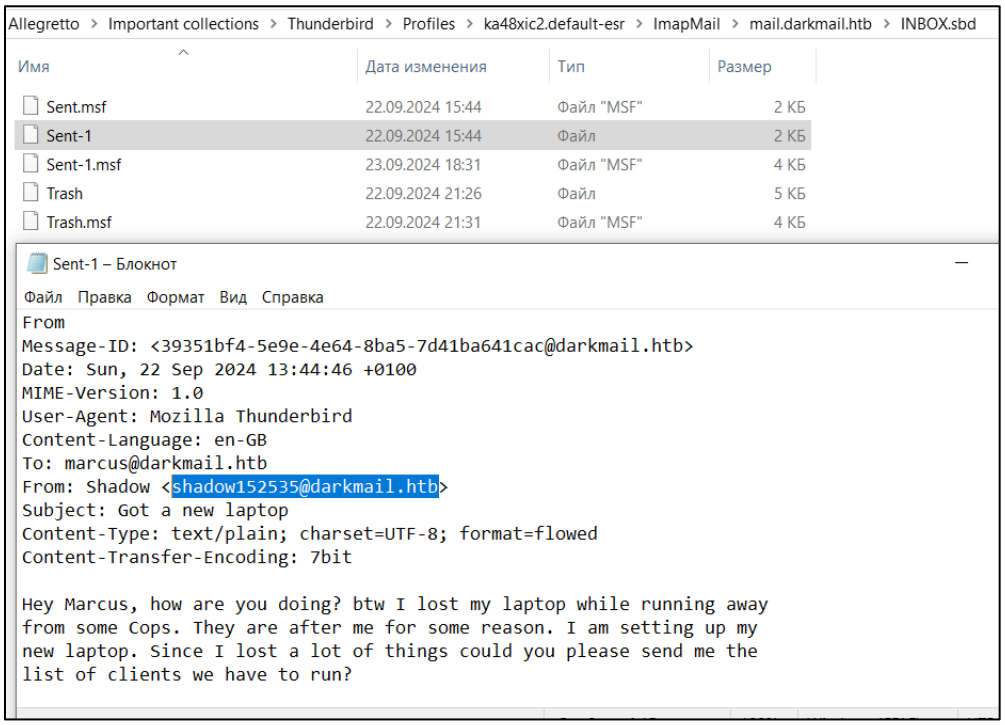
3. Скачиваем MFTECmd и Timeline Explorer для работы с файлом MFT. Запускаем с помощью командной строки MFTECmd и создаем .csv файл с образа $MFT с названием **20250916144916_MFTECmd_$MFT_Output.csv**

```
C:\Users\Public\MFTECmd>.\MFTECmd.exe -f "C:\Users\Public\$MFT" --csv C:\Users\Public\
MFTECmd version 1.3.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/MFTECmd

Command line: -f C:\Users\Public\$MFT --csv C:\Users\Public\

File type: Mft

Processed C:\Users\Public\$MFT in 5,7368 seconds

C:\Users\Public\$MFT: FILE records found: 139 533 (Free records: 0) File size: 136,5MB
        CSV output will be saved to C:\Users\Public\20250915140257_MFTECmd_$MFT_Output.csv
```

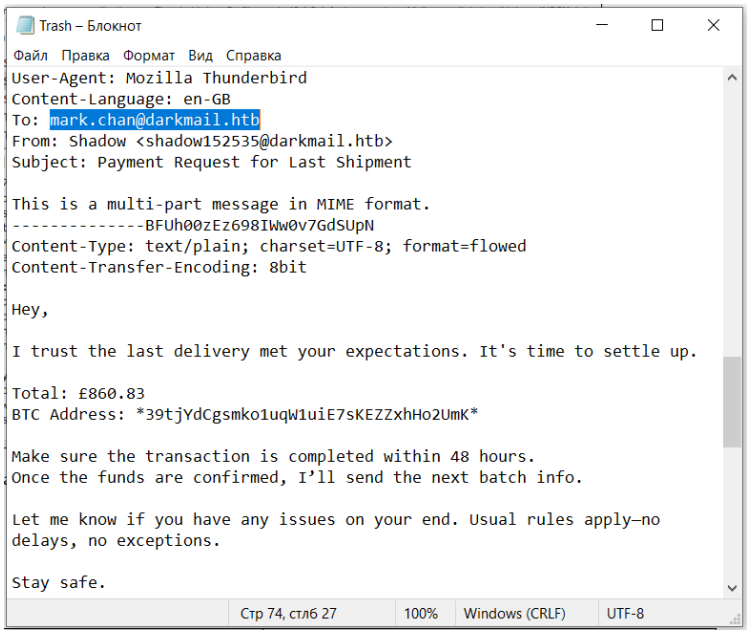
4. Далее открываем его в Timeline Explorer. Ищем «QGIS» и по условиям задания находим его версию (Q1).



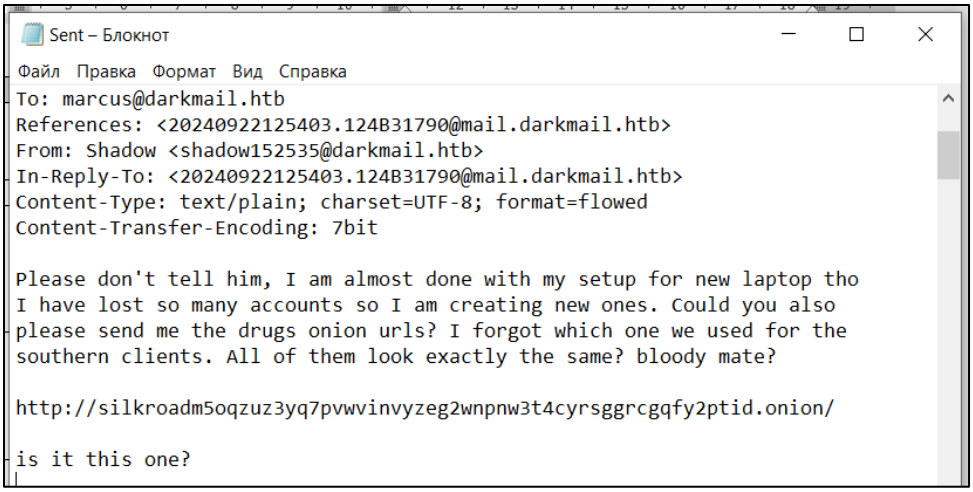
5. В каталоге «Allegretto\Important collections\Thunderbird\Profiles\ka48xic2.default-esr\ImapMail\mail.darkmail.htb\INBOX.sbd\» находим файлы писем пользователя Shadow в Darkmail. В файле **Sent-1** обнаруживаем адреса электронной почты **shadow152535@darkmail.htb** и **marcus@darkmail.htb** (Q2)



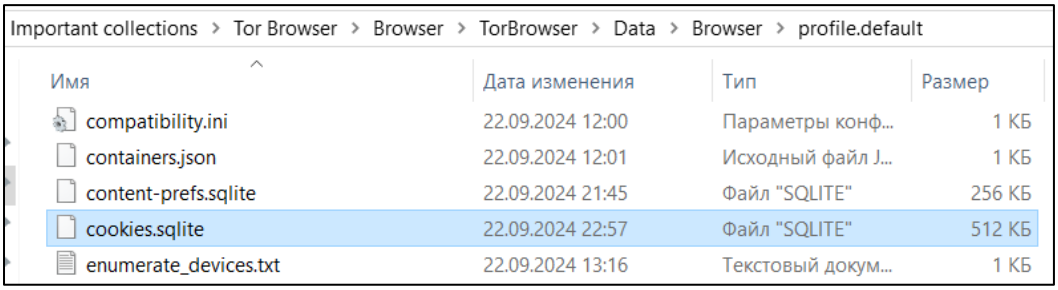
В файле **Trash** находим адрес получателя **mark.chan@darkmail.htb** и BTC адрес ***39tjYdCgsmko1uqW1uiE7sKEZZxhHo2UmK*** (Bitcoin) (Q3).



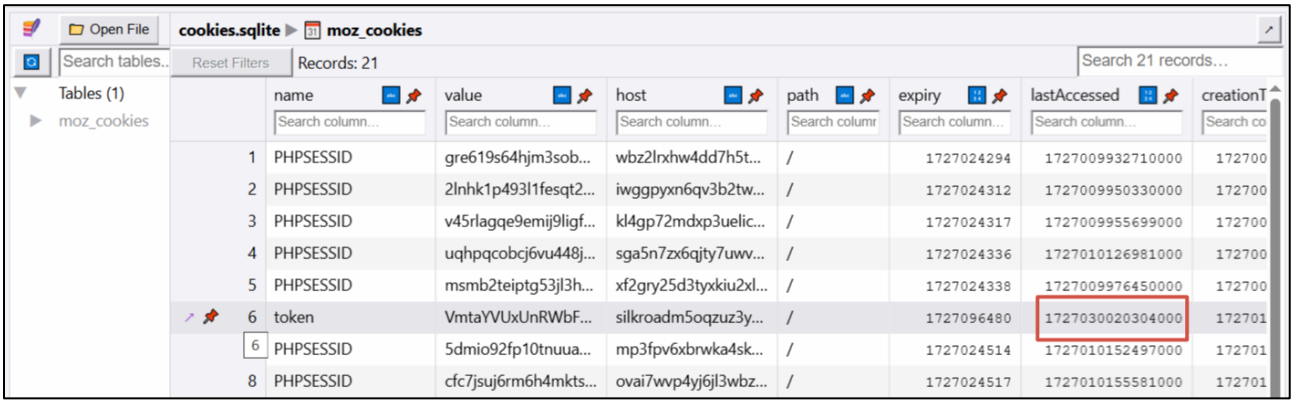
6. В каталоге «Allegretto\Important collections\Thunderbird\Profiles\ka48xic2.default-esr\Mail\Local Folders» находим файл **Sent,** в котором находится onion URL для SilkRoad где Shadow продает наркотики: **http://silkroadm5oqzuz3yq7pvwvinvyzeg2wnpnw3t4cyrsggrcgqfy2ptid.onion** (Q4).



7. Для ответа на вопрос Q5 «Основываясь на последнем доступе к файлу cookie, когда Shadow в последний раз посещал веб-сайт Silk Road?», открываем каталог «Allegretto\Important collections\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\», в котором находится файл **cookies.sqlite**

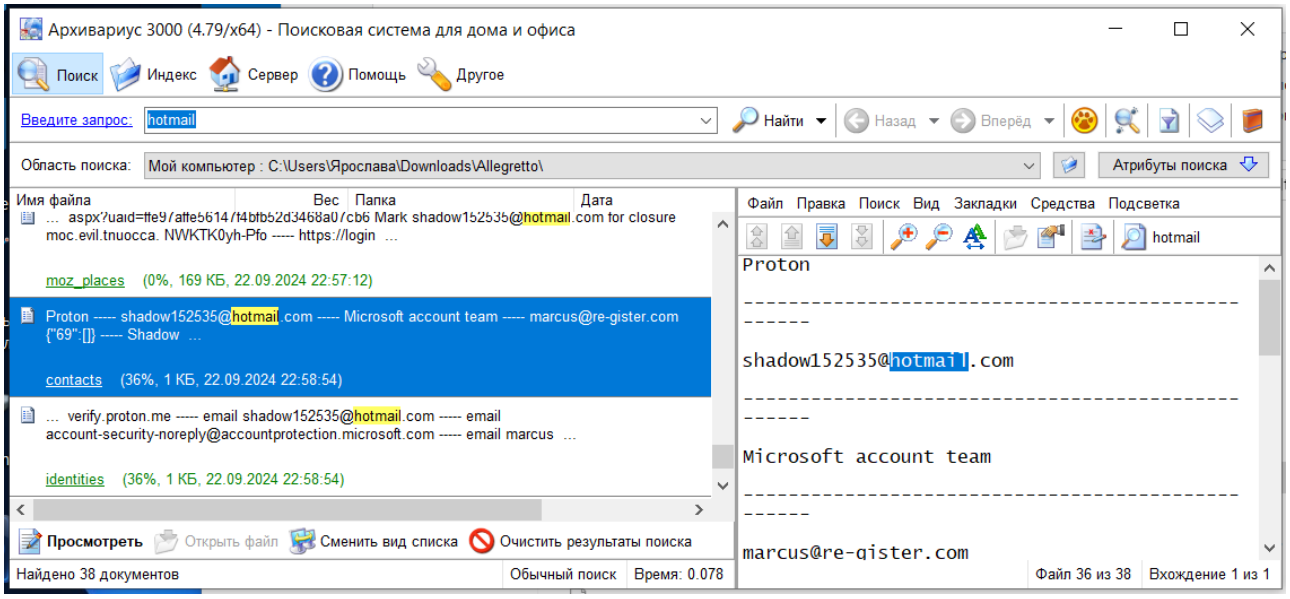


С помощью веб-приложение для просмотра SQLite открываем файл и находим время последнего доступа.

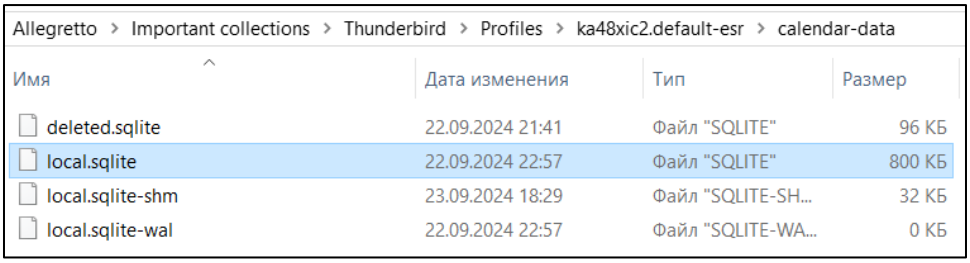


Время странное, но оно в Unix формате, поэтому его надо преобразовать в понятное **2024-09-22 18:33:40**

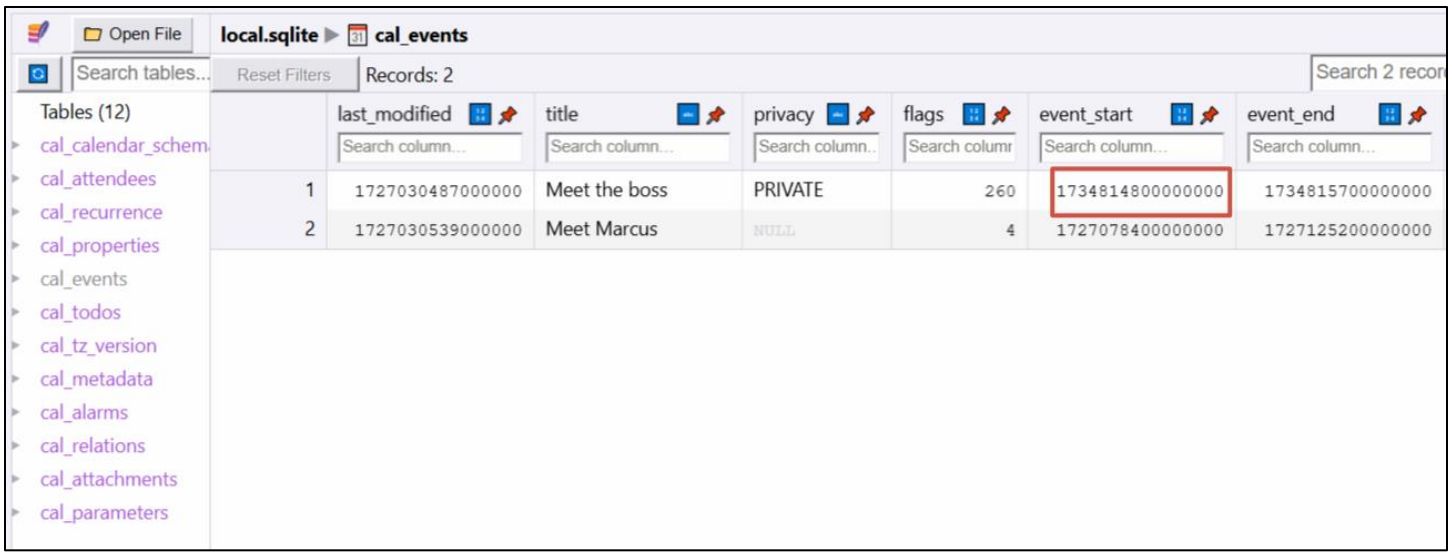
8. Для поиска Hotmail воспользуемся Архивариус 3000 поиск по ключевому слову, в результате чего находим почту: **shadow152535@hotmail.com** (Q6). (но вероятнее всего почта находится в какой-то sqlite базе)



9. Чтобы определить, когда Shadow должен встретиться со своим таинственным боссом (Q7), ищем календарь. В каталоге «Allegretto\Important collections\Thunderbird\Profiles\ka48xic2.default-esr\calendar-data\» находим файл **local.sqlite**

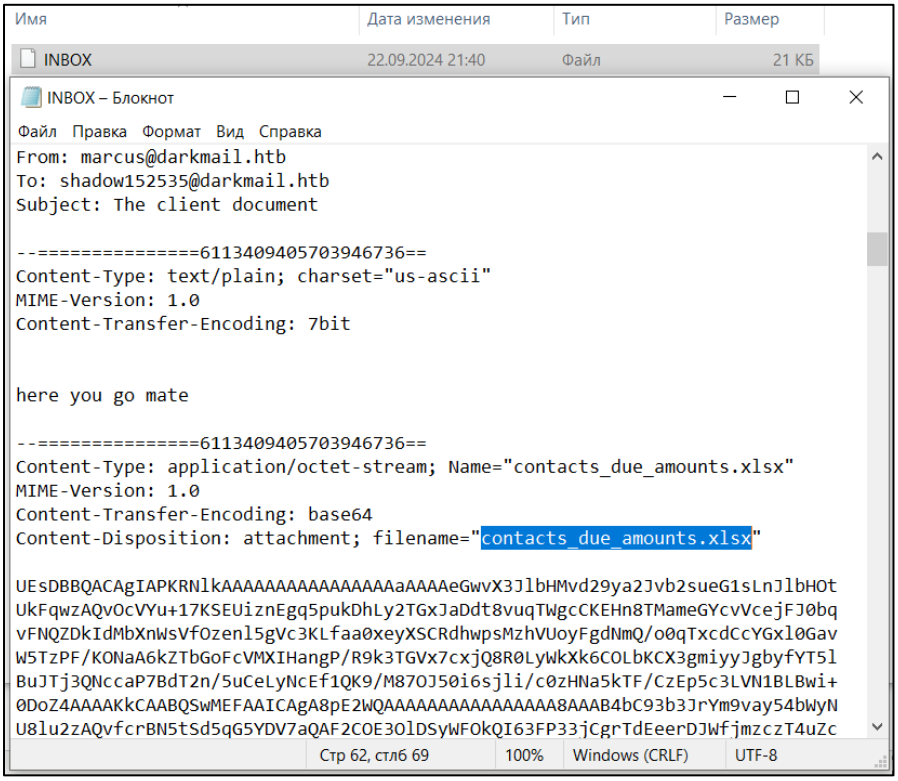


С помощью веб-приложение для просмотра SQLite открываем файл и находим встречу с боссом.

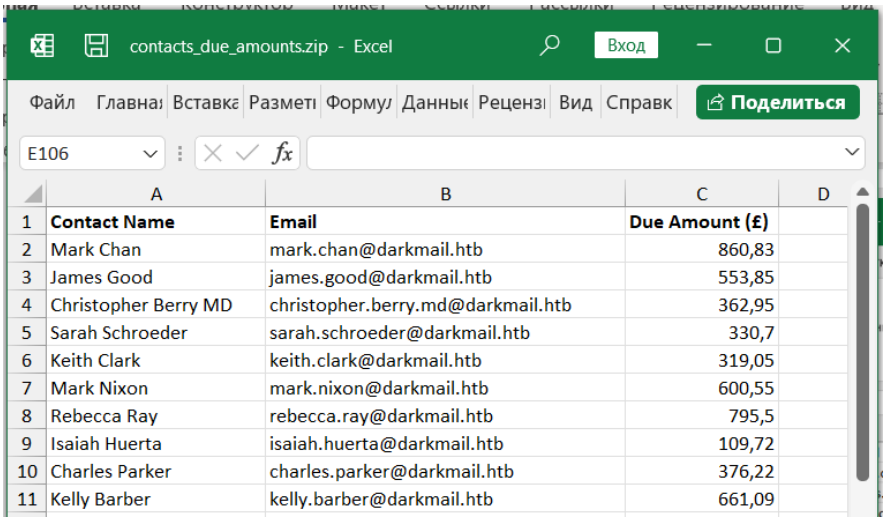


Преобразовываем время в понятное: **2024-12-21 21:00:00**

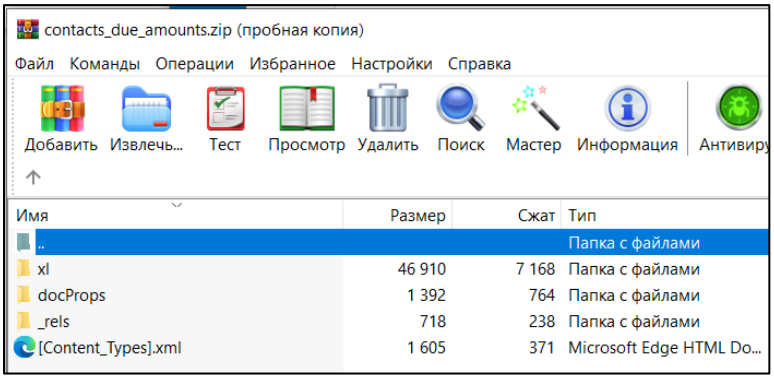
10. В каталоге «Allegretto\Target\C\Users\shadow\AppData\Roaming\Thunderbird\Profiles\ka48xic2.default-esr\ImapMail\mail.darkmail.htb\» находим файл **INBOX** со списком клиентов.



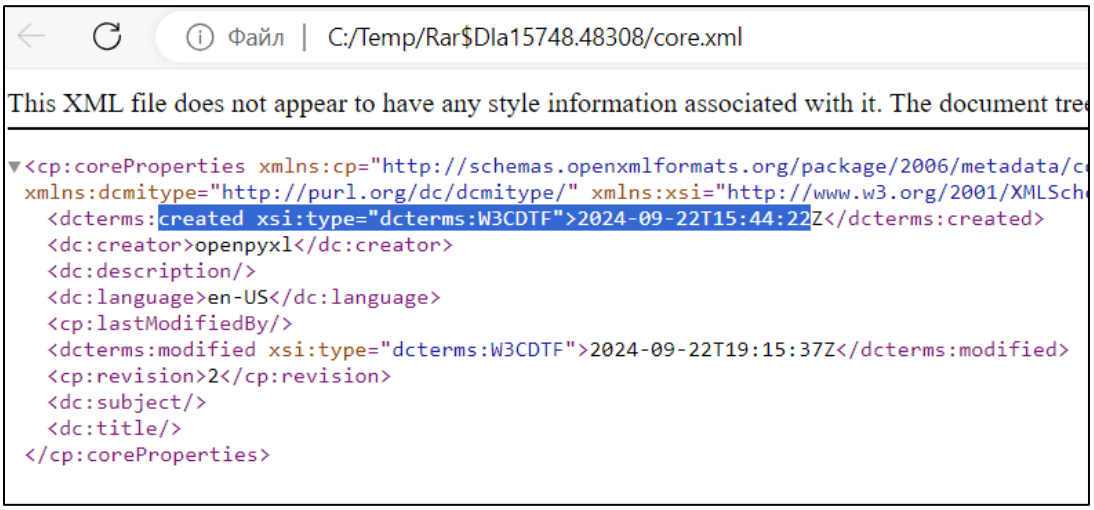
Код начинается с последовательности UEsDB…, что указывает на то, что это zip-архив в BASE64-кодировке. Расшифровываем и получаем архив **contacts_due_amounts.zip**. Как известно, файл Excel — это просто набор XML-файлов, определяемых форматом Office Open XML и упакованных в zip-архив. Открываем его в формате Excel и получаем данные о покупателях (100 строк).



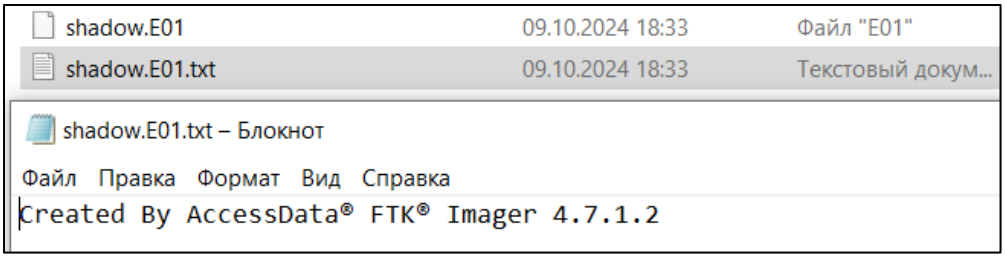
11. Для ответа на вопрос Q8 «Когда была создана электронная таблица contacts_due_amounts.xlsx», распаковываем zip-архив и обнаруживаем папку docProps (Document Properties) — *папка в структуре файла, которая включает метаданные документа, такие как автор, название, дата создания и другие свойства*.



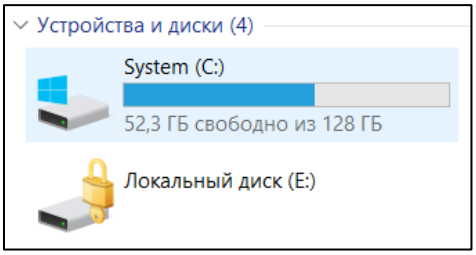
В этой папке проверяем все файлы (3) и в файле **core.xml** находим время создания **2024-09-22 15:44:22**



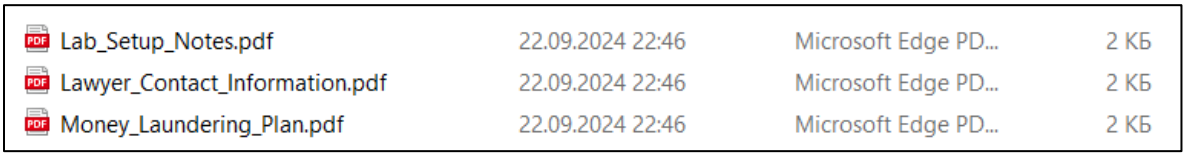
12. Далее, обращаем внимание на файл **shadow.E01** в каталоге «Allegretto\Important collections\», созданный с помощью AccessData FTK Imager.



Диск монтируем с помощью AccessData FTK Imager. Он оказывается защищенным программой Bitlocker. Открываем паролем восстановления, найденным в одном из текстовых файлов: 356400-709885-041448-681967-471328-040931-346357-184591

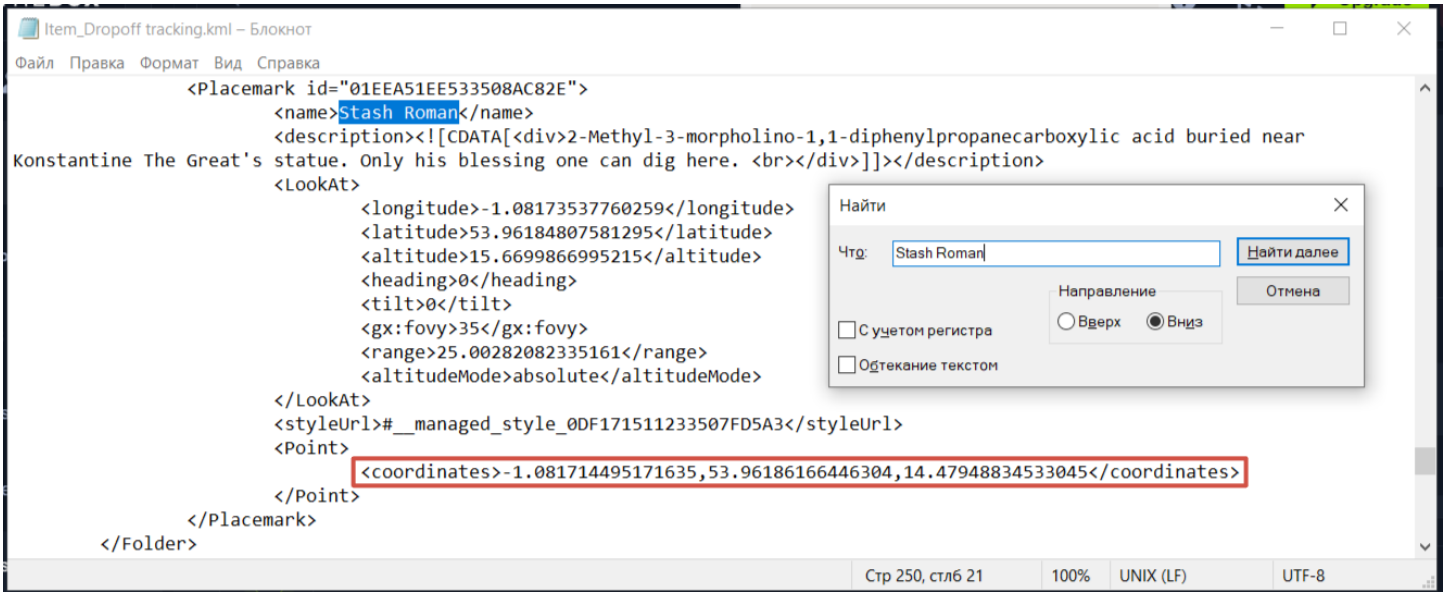


На расшифрованном USB-накопителе находятся файлы:

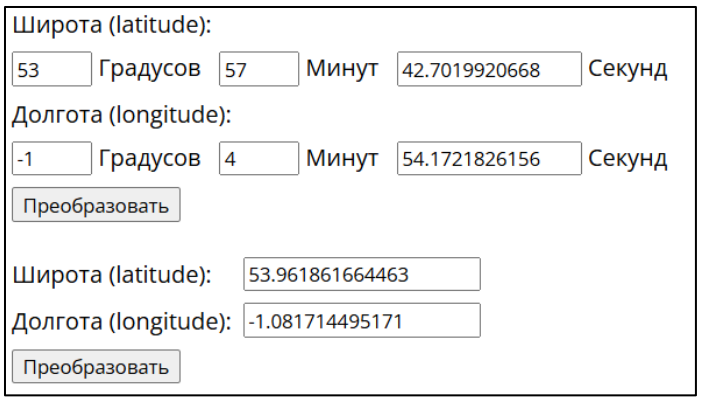


13. Для ответа на Q9 необходимо найти удаленный файл. С помощью R-Studio сканируем смонтированный диск и находим удаленные файлы. Восстанавливаем из каталога «\Locations\» файл **Item_Dropoff tracking.kml.** Однако для ответа нужно знать диск и каталог: **E:\Locations\Item_Dropoff tracking.kml**

14. KML – это формат файла для отображения географических данных. Поэтому используем восстановленный файл для ответа на Q10 «What are Stash Roman's coordinates?», открывая его в блокноте и используя поиск.



Переводим координаты **53°57'42"N 1°04'54"W**



7. Находки

	Имя	Путь	Описание
1.	$MFT	Allegretto\Target\C\	База данных, в которой хранится информация о содержимом тома с файловой системой NTFS.
2.	NTUSER.DAT	Allegretto\Target\C\Users\shadow\	Файл реестра user
3.	Sent-1	Allegretto\Important collections\Thunderbird\Profiles\ka48xic2.default-esr\ImapMail\mail.darkmail.htb\INBOX.sbd\	Текстовый файл, содержащий переписку. Обнаружена инфа о адресе электронной почты Shadow
4.	Trash	Allegretto\Important collections\Thunderbird\Profiles\ka48xic2.default-esr\ImapMail\mail.darkmail.htb\INBOX.sbd\	Текстовый файл, содержащий переписку. Обнаружена инфа о биткоин адресе
	Sent	Allegretto\Important collections\Thunderbird\Profiles\ka48xic2.default-esr\Mail\Local Folders\	Текстовый файл, содержащий переписку. Обнаружена инфа о Onion URL для SilkRoad
	cookies.sqlite	Allegretto\Important collections\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\	База данных с временем посещения веб-сайта Silk Road
	local.sqlite	Allegretto\Important collections\Thunderbird\Profiles\ka48xic2.default-esr\calendar-data	База данных с событиями из календаря
	INBOX	Allegretto\Target\C\Users\shadow\AppData\Roaming\Thunderbird\Profiles\ka48xic2.default-esr\ImapMail\mail.darkmail.htb\	Текстовый файл, содержащий переписку. Обнаружен зашифрованные текст, который представляет собой список клиентов
	contacts_due_amounts.zip	Созданный файл	Содержит Excel таблицу
	core.xml	contacts_due_amounts.zip\docProps\	Файл с метаданными документа: дата создания .xlsx
	shadow.E01	Allegretto\Important collections\	Образ диска VMware Virtual disk SCSI Disk Device
	Item_Dropoff tracking.kml	E:\Locations\	Восстановленный файл, который был удален с зашифрованного USB (хранит в себе координаты)

8. Выводы и рекомендации

В ходе проведённого исследования по кейсу Allegretto удалось установить ключевые артефакты цифровой активности Shadow. Были выявлены используемые им сервисы для анонимной коммуникации и торговли (Darkmail, SilkRoad), зафиксированы криптовалютные реквизиты для расчётов, а также данные о клиентах и финансовых операциях. Установлены точные временные метки, связанные с последними действиями в браузере Tor, созданием файлов и планированием встреч, что позволило восстановить хронологию событий. Были восстановленны с зашифрованного носителя сведения, включая удалённый файл с координатами тайников.

9. Приложение: