

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: 4e2f9139ba15a0d4286d92591c33c4baa3db 00e5127cc6d9bac2e059d9e606f7

- 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.

Файл > Загрузки > Allegretto > Important collections		
Имя	Дата изменения	
Folder KeePass	07.10.2024 16:52	
Folder LibreOffice	07.10.2024 16:52	
Folder Others	07.10.2024 16:52	
Folder Proton Mail	07.10.2024 16:52	
Folder Thunderbird	07.10.2024 16:52	
Folder Tor Browser	07.10.2024 16:52	
Folder Tor_History	09.10.2024 18:41	
File shadow.E01	09.10.2024 18:33	
File shadow.E01.txt	09.10.2024 18:33	

Файл > Загрузки > Allegretto > Modules		
Имя	Дата изменения	
Folder FileFolderAccess	07.10.2024 16:53	
Folder KeywordSearches	07.10.2024 16:53	
Folder LiveResponse	07.10.2024 16:53	
Folder ProgramExecution	07.10.2024 16:53	
Folder Registry	07.10.2024 16:53	
Folder VolumeInformation	07.10.2024 16:53	
File 2024-09-23T14_31_40_6032557_ConsoleL...	23.09.2024 17:47	

Компьютер > Загрузки > Allegretto > Target	
Имя	Дата изменения
C	07.10.2024 17:01
2024-09-23T14_10_34_0407475_ConsoleLog.txt	23.09.2024 17:15
2024-09-23T14_10_34_0407475_CopyLog.csv	23.09.2024 17:15
2024-09-23T14_10_34_0407475_SkipLog.csv.csv	23.09.2024 17:15

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

Загрузки > Allegretto > Target > C	
Имя	Дата изменения
\$Extend	07.10.2024 16:53
\$Recycle.Bin	07.10.2024 16:53
ProgramData	07.10.2024 16:53
Users	07.10.2024 16:53
Windows	07.10.2024 17:02
\$Boot	23.09.2024 17:15
\$LogFile	23.09.2024 17:15
\$MFT	05.09.2024 15:09
\$Secure_\$SDS	05.09.2024 15:09

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

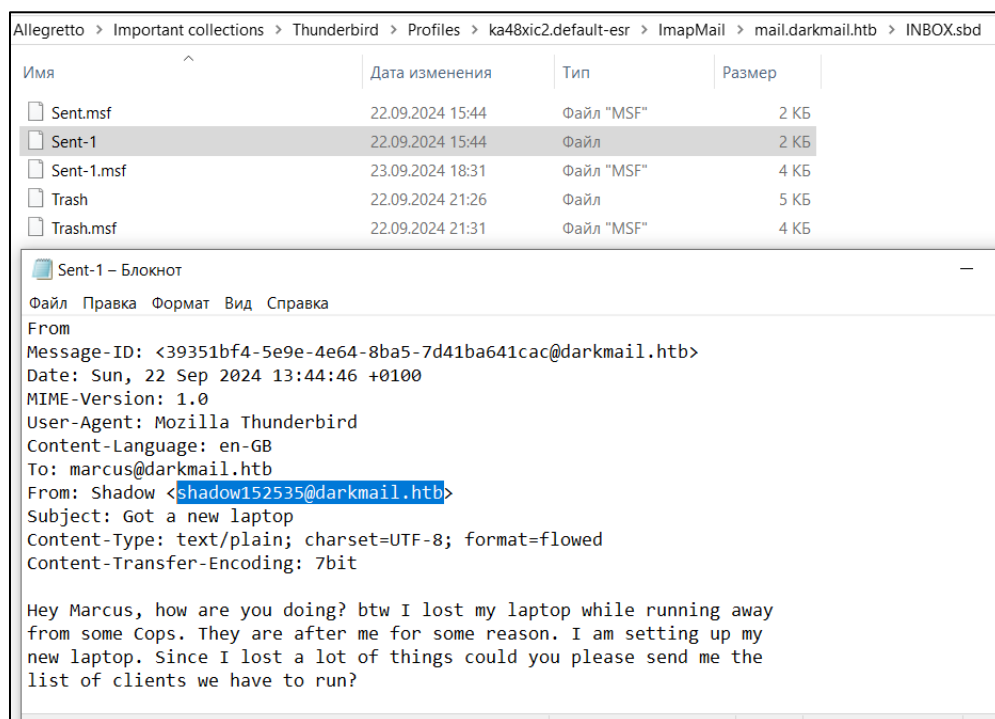
Processed C:\Users\Public\$MFT in 5,7368 seconds

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
```

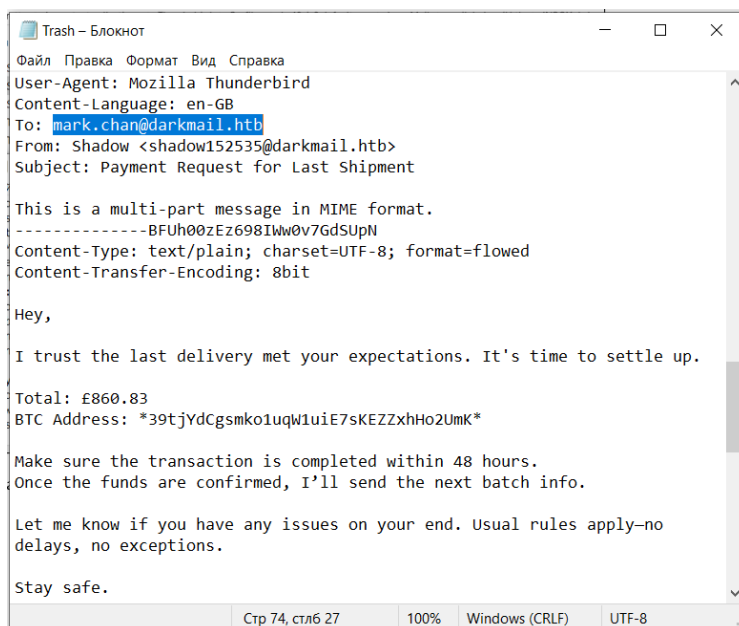
4. Далее открываем его в Timeline Explorer. Ищем «QGIS» и по условиям задания находим его версию (Q1).

Timeline Explorer v2.0.0.1			
File Tools Tabs View Help			
20250916144916_MFTECmd_\$MFT_Output.csv			
Drag a column header here to group by that column			
	In Use	Parent Path	File Name
▼	<input type="checkbox"/>	C:	C:
	<input checked="" type="checkbox"/>	.\Program Files\QGIS 3.34.11\apps\Python312\lib...	configui.py
	<input checked="" type="checkbox"/>	.\Program Files\QGIS 3.34.11\apps\Python312\lib...	dbgcon.py
	<input checked="" type="checkbox"/>	.\Program Files\QGIS 3.34.11\apps\Python312\lib...	dbgpyapp.py
	<input checked="" type="checkbox"/>	.\Program Files	QGIS 3.34.11
	<input checked="" type="checkbox"/>	.\Users\shadow\AppData\Local\QGIS\QGIS3\cache\d...	1od66zpk.d
	<input checked="" type="checkbox"/>	.\Users\shadow\AppData\Local\QGIS\QGIS3\cache\d...	25843epc.d
	<input checked="" type="checkbox"/>	.\Users\shadow\AppData\Local\QGIS\QGIS3\cache\d...	17tkok18.d

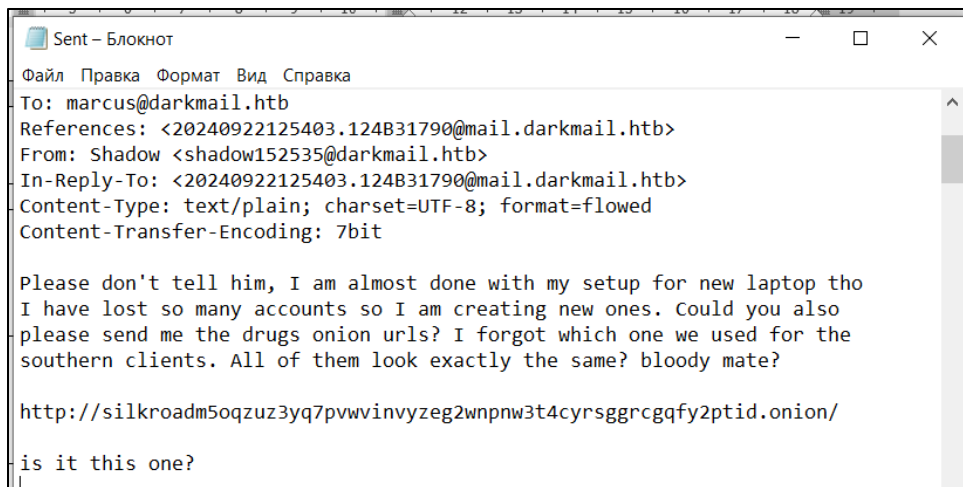
5. В каталоге «Allegretto\Important collections\Thunderbird\Profiles\ka48xic2.default-esr\ImapMail\mail.darkmail.htb\INBOX.sbd\» находим файлы писем пользователя Shadow в Darkmail. В файле **Sent-1** обнаруживаем адреса электронной почты **shadow152535@darkmail.htb** и **marcus@darkmail.htb** (Q2)



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**

Important collections > Tor Browser > Browser > TorBrowser > Data > Browser > profile.default				
Имя	Дата изменения	Тип	Размер	
compatibility.ini	22.09.2024 12:00	Параметры конф...	1 КБ	
containers.json	22.09.2024 12:01	Исходный файл J...	1 КБ	
content-prefs.sqlite	22.09.2024 21:45	Файл "SQLITE"	256 КБ	
cookies.sqlite	22.09.2024 22:57	Файл "SQLITE"	512 КБ	
enumerate_devices.txt	22.09.2024 13:16	Текстовый докум...	1 КБ	

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

cookies.sqlite ▶ moz_cookies							
Search tables...		Reset Filters		Records: 21		Search 21 records...	
Tables (1)	name	value	host	path	expiry	lastAccessed	creationT
moz_cookies							
	1 PHPSESSID	gre619s64hjm3sob...	wbz2lrxhw4dd7h5t...	/	1727024294	1727009932710000	172700
	2 PHPSESSID	2lnhk1p493l1fesqt2...	iwgpyxn6qv3b2tw...	/	1727024312	1727009950330000	172700
	3 PHPSESSID	v45rlagqe9emij9ligf...	kl4gp72mdxp3uelic...	/	1727024317	1727009955699000	172700
	4 PHPSESSID	uqhpqcobcj6vu448j...	sga5n7zx6qity7uuv...	/	1727024336	1727010126981000	172700
	5 PHPSESSID	msmb2teiptg53jl3h...	xf2gry25d3tyxkiu2xl...	/	1727024338	1727009976450000	172700
	6 token	VmtaYVUxUnRWbF...	silkroadm5oqzuz3y...	/	1727096480	1727030020304000	172701
	7 PHPSESSID	5dmio92fp10tnuua...	mp3fpv6xbrwka4sk...	/	1727024514	1727010152497000	172701
	8 PHPSESSID	cfc7jsuj6rm6h4mks...	ovai7wvp4yj6l3wbz...	/	1727024517	1727010155581000	172701

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



EpochConverter

Epoch & Unix Timestamp Conversion Tools

The current Unix epoch time is 1758187884

Convert epoch to human-readable date and vice versa

1727030020304000

Timestamp to Human date

[batch convert]

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

Assuming that this timestamp is in **microseconds (1/1,000,000 second)**:

GMT: Sunday, 22 September 2024 г., 18:33:40.304

Your time zone: воскресенье, 22 сентября 2024 г., 21:33:40.304 GMT+03:00

Relative: A year ago

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)

Архивариус 3000 (4.79/x64) - Поисковая система для дома и офиса

Поиск

Индекс

Сервер

Помощь

Другое

Введите запрос: hotmail

Найти

Назад

Вперед

Атрибуты поиска

Область поиска: Мой компьютер : C:\Users\Ярослава\Downloads\Allegretto\

Имя файла	Вес	Папка	Дата
... aspx?uid=fe9/affe5614/14bfb52d3468a0/cb6 Mark shadow152535@hotmail.com for closure		moc.evil.tnuocca. NWKTK0yh-Pfo	https://login
moz_places	(0%, 169 KB, 22.09.2024 22:57:12)		
Proton	shadow152535@hotmail.com	Microsoft account team	marcus@re-gister.com
contacts	(36%, 1 KB, 22.09.2024 22:58:54)		
... verify.proton.me	email shadow152535@hotmail.com	email account-security-noreply@accountprotection.microsoft.com	email marcus
identities	(36%, 1 KB, 22.09.2024 22:58:54)		

Просмотреть

Открыть файл

Сменить вид списка

Очистить результаты поиска

Найдено 38 документов

Обычный поиск

Время: 0.078

Файл 36 из 38

Вхождение 1 из 1

Файл

Правка

Поиск

Вид

Закладки

Средства

Подсветка

Proton

shadow152535@hotmail.com

Microsoft account team

marcus@re-gister.com

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**

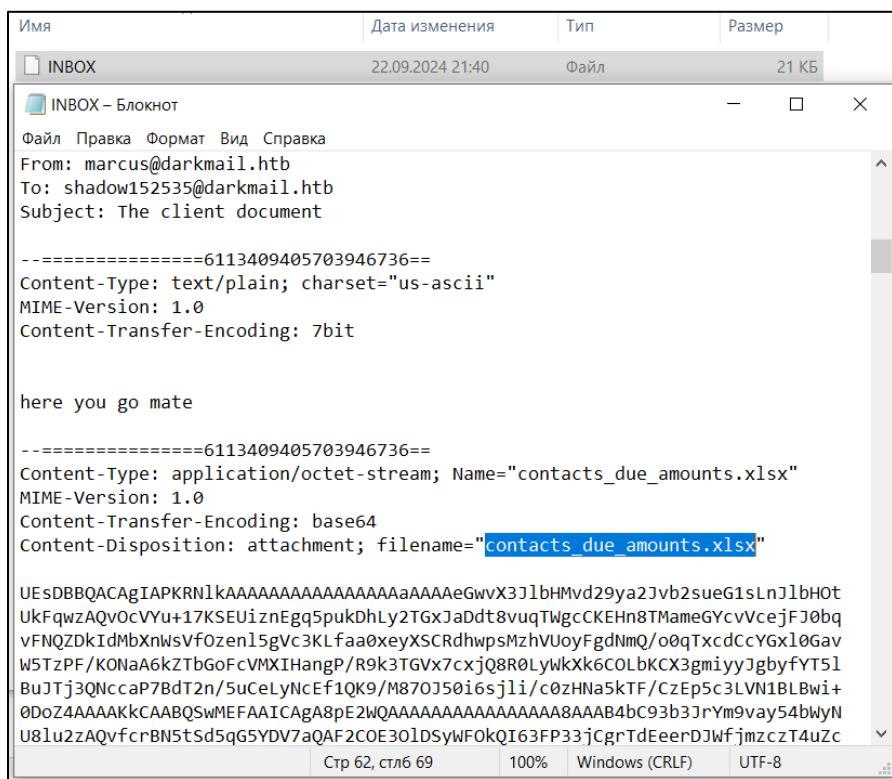
Allegretto > Important collections > Thunderbird > Profiles > ka48xic2.default-esr > calendar-data			
Имя	Дата изменения	Тип	Размер
deleted.sqlite	22.09.2024 21:41	Файл "SQLITE"	96 КБ
local.sqlite	22.09.2024 22:57	Файл "SQLITE"	800 КБ
local.sqlite-shm	23.09.2024 18:29	Файл "SQLITE-SH..."	32 КБ
local.sqlite-wal	22.09.2024 22:57	Файл "SQLITE-WA..."	0 КБ

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

Open File		local.sqlite ▶ cal_events		Search 2 records			
Search tables...		Reset Filters		Records: 2		Search 2 records	
Tables (12)		last_modified	title	privacy	flags	event_start	event_end
<ul style="list-style-type: none"> cal_calendar_schem cal_attendees cal_recurrence cal_properties cal_events cal_todos cal_tz_version cal_metadata cal_alarms cal_relations cal_attachments cal_parameters 		Search column...	Search column...	Search column...	Search column...	Search column...	Search column...
1		1727030487000000	Meet the boss	PRIVATE	260	1734814800000000	1734815700000000
2		1727030539000000	Meet Marcus	NULL	4	1727078400000000	1727125200000000

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).

	A	B	C	D
1	Contact Name	Email	Due Amount (£)	
2	Mark Chan	mark.chan@darkmail.htb	860,83	
3	James Good	james.good@darkmail.htb	553,85	
4	Christopher Berry MD	christopher.berry.md@darkmail.htb	362,95	
5	Sarah Schroeder	sarah.schroeder@darkmail.htb	330,7	
6	Keith Clark	keith.clark@darkmail.htb	319,05	
7	Mark Nixon	mark.nixon@darkmail.htb	600,55	
8	Rebecca Ray	rebecca.ray@darkmail.htb	795,5	
9	Isaiah Huerta	isaiah.huerta@darkmail.htb	109,72	
10	Charles Parker	charles.parker@darkmail.htb	376,22	
11	Kelly Barber	kelly.barber@darkmail.htb	661,09	

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.

Имя	Размер	Сжат	Тип
..			Папка с файлами
xl	46 910	7 168	Папка с файлами
docProps	1 392	764	Папка с файлами
_rels	718	238	Папка с файлами
[Content_Types].xml	1 605	371	Microsoft Edge HTML Do...

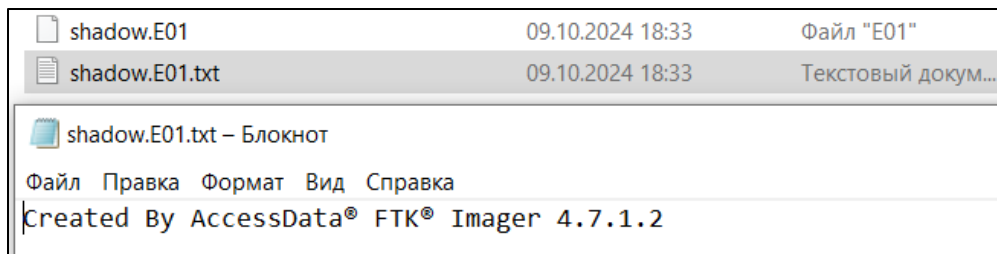
В этой папке проверяем все файлы (3) и в файле **core.xml** находим время создания **2024-09-22 15:44:22**

```

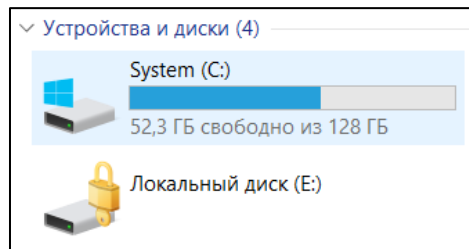
<cp:coreProperties xmlns:cp="http://schemas.openxmlformats.org/package/2006/metadata/cp"
xmlns:dcmime="http://purl.org/dc/dcmitype/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  <dcterms:created xsi:type="dcterms:W3CDTF">2024-09-22T15:44:22Z</dcterms:created>
  <dc:creator>openruhl</dc:creator>
  <dc:description/>
  <dc:language>en-US</dc:language>
  <cp:lastModifiedBy/>
  <dcterms:modified xsi:type="dcterms:W3CDTF">2024-09-22T19:15:37Z</dcterms:modified>
  <cp:revision>2</cp:revision>
  <dc:subject/>
  <dc:title/>
</cp:coreProperties>

```

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

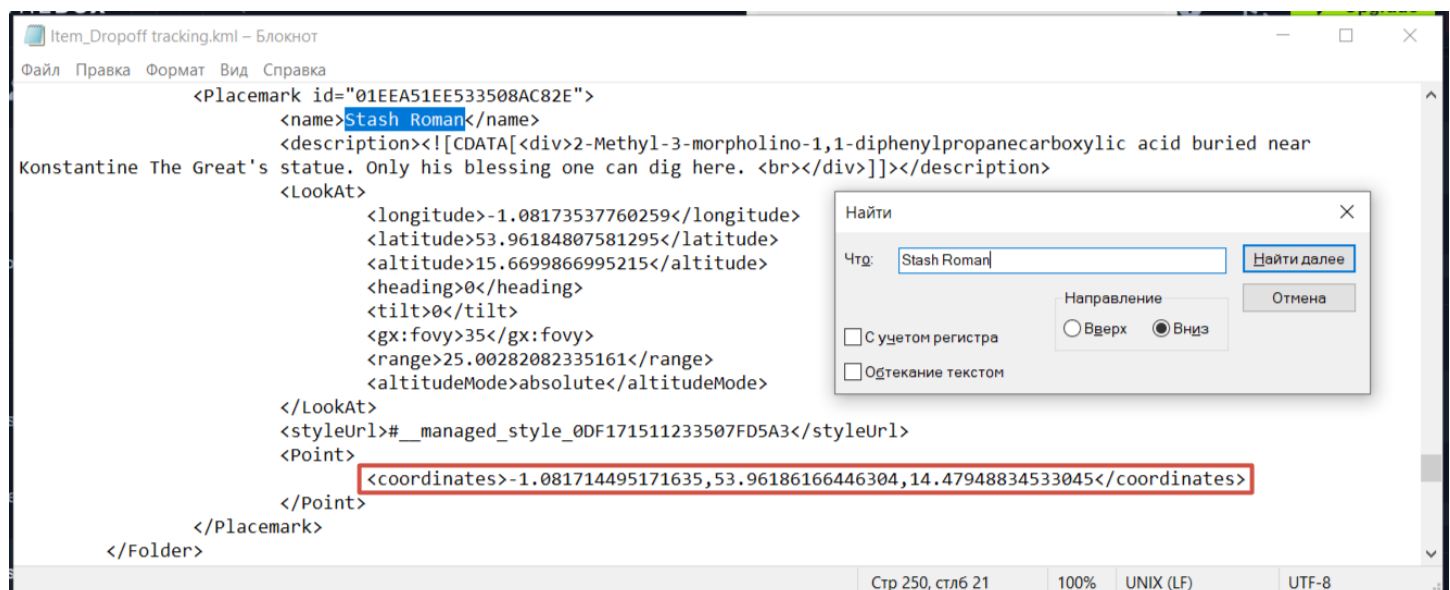


На расшифрованном USB-накопителе находятся файлы:

	Lab_Setup_Notes.pdf	22.09.2024 22:46	Microsoft Edge PD...	2 КБ
	Lawyer_Contact_Information.pdf	22.09.2024 22:46	Microsoft Edge PD...	2 КБ
	Money_Laundering_Plan.pdf	22.09.2024 22:46	Microsoft Edge PD...	2 КБ

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**

Широта (latitude):
 Градусов Минут Секунд

Долгота (longitude):
 Градусов Минут Секунд

Широта (latitude):

Долгота (longitude):

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 восстановлены с зашифрованного носителя сведения, включая удалённый файл с координатами тайников.

9. Приложение:

