Countdown

Contents

Scenario

NYC Police received information that a gang of attackers has entered the city and are planning to detonate an explosive device. Law enforcement have begun investigating all leads to determine whether this is true or a hoax.

Persons of interest were taken into custody, and one additional suspect named 'Zerry' was detained while officers raided his house. During the search they found one laptop, collected the digital evidence, and sent it to NYC digital forensics division.

Police believe Zerry is directly associated with the gang and are analysing his device to uncover any information about the potential attack.

Disclaimer: The story, all names, characters, and incidents portrayed in this challenge are fictitious and any relevance to real-world events is completely coincidental.

Pre-requisites

- Investigations have to be run through the BTLO virtual lab. No need for Kali VM.

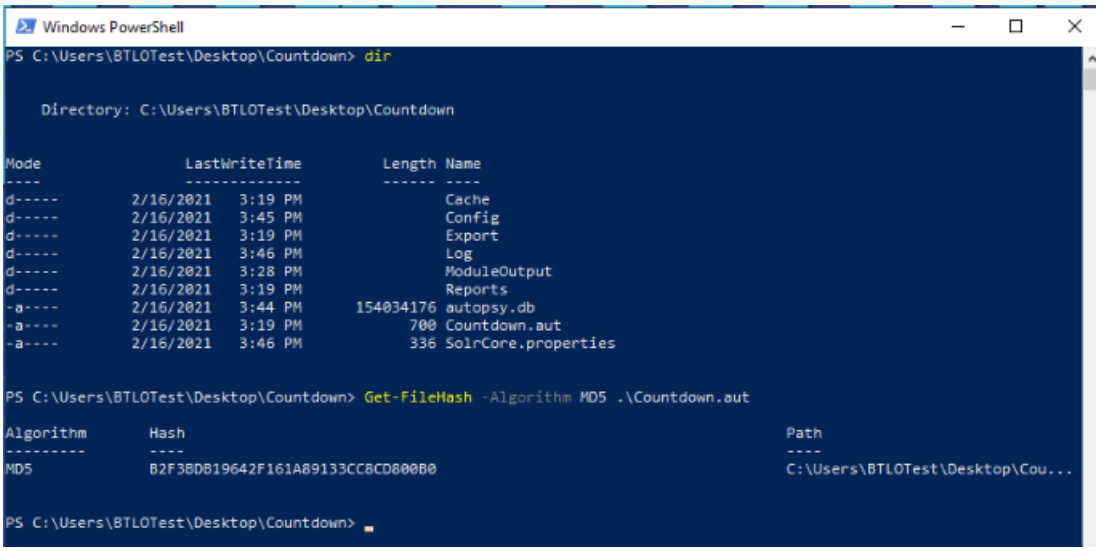
Initial thoughts from scenario

- Police have imaged the laptop, so most likely going to be using Autopsy to analyse the forensic evidence.
- Even though this is a lab, and there's no "real" chain of custody, I'll attempt to follow Ken Zatyko's digital forensics methodology for best practice.
- Could also have to investigate event logs or analyse files with Windows File Analyser, if the evidence collected is on Windows OS.

Challenge Questions

Verify the Disk Image. Submit SectorCount and MD5

- Answer: 25,165,824, 5c4e94315039f890e839d6992aeb6c58



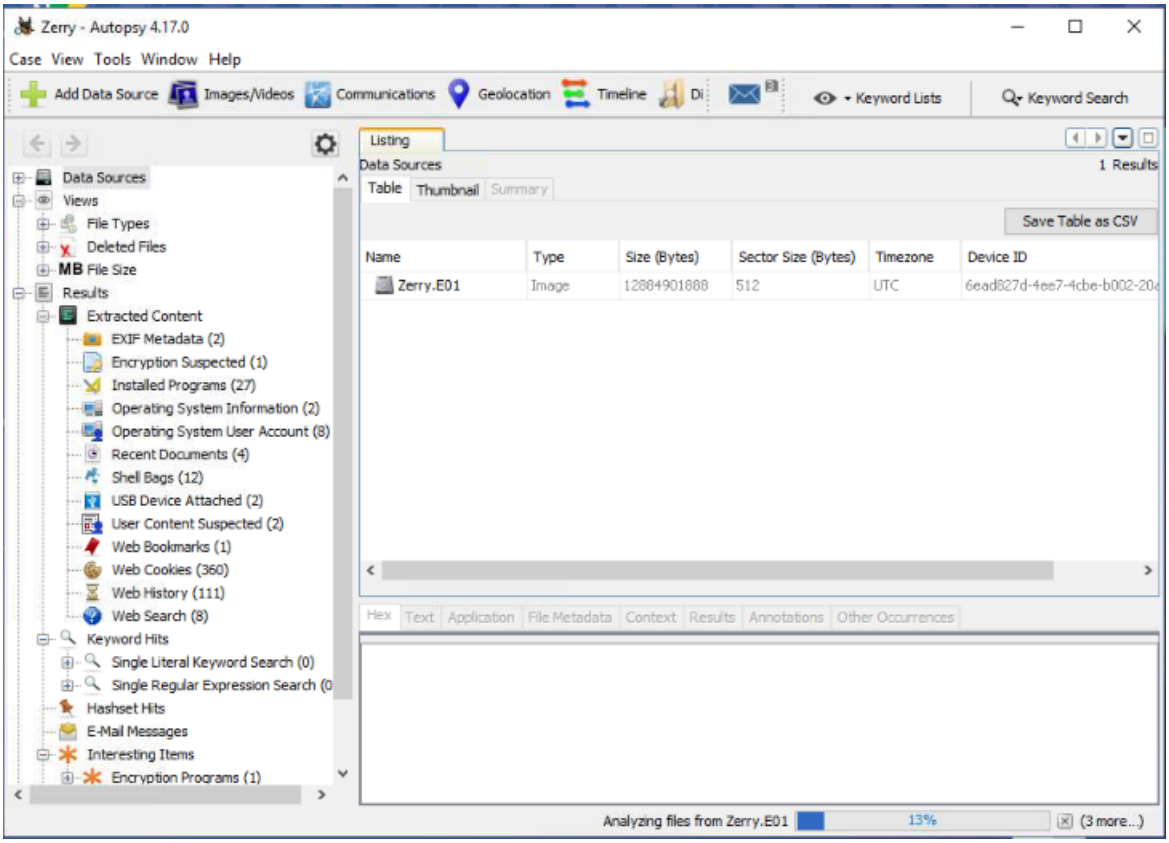
- Located the Zerry.EO1 file saved on the Investigation VM, opened Powershell terminal in that location and ran Get-FileHash to confirm the MD5 hash.
    - This was confirmed against the text file in the challenge (below).

```
Zerry.E01 - Notepad
File  Edit  Format  View  Help
Case Number:
Evidence Number:
Unique Description:
Examiner:
Notes:

--------------------------------------------------------------

Information for E:\Zerry:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1,566
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 25,165,824
[Physical Drive Information]
 Drive Model: VBOX HARDDISK
 Drive Serial Number: VBc9000e54-a9c2d001
 Drive Interface Type: IDE
 Removable drive: False
 Source data size: 12288 MB
 Sector count:    25165824
[Computed Hashes]
 MD5 checksum:    5c4e94315039f890e839d6992aeb6c58
 SHA1 checksum:   ce71f6d999a1de15eccd867ae01fab3d4b20e830

Image Information:
 Acquisition started:   Sat Jan 16 22:34:40 2021
 Acquisition finished:  Sat Jan 16 22:53:56 2021
 Segment list:
  E:\Zerry.E01
```

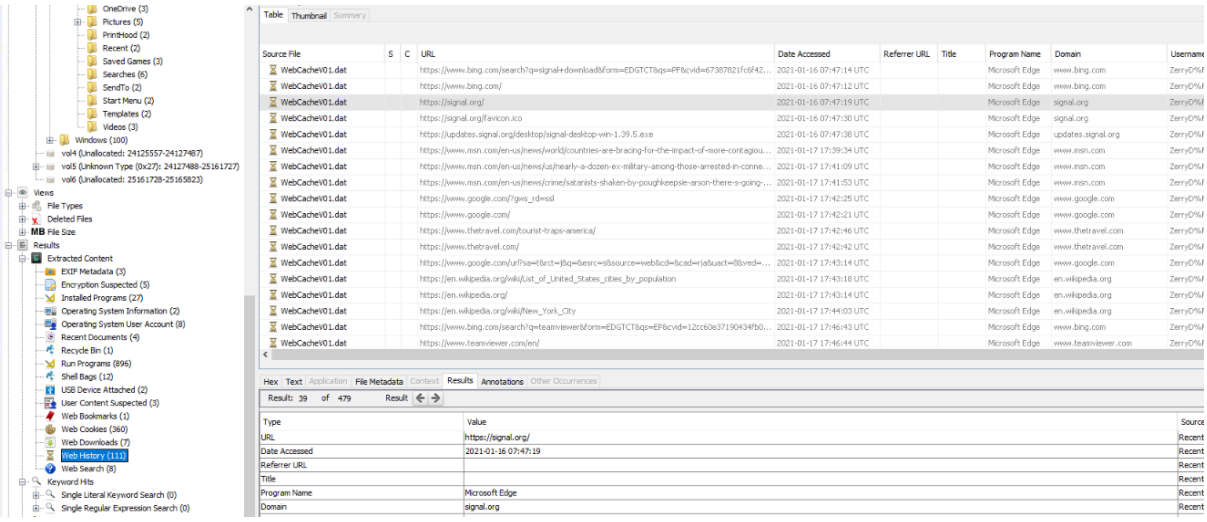
- I tried running various commands to verify the SectorCount of the Zerry image, but none seemed to work on the BTLO VM, so I consulted the walkthrough to learn the command BTLO used but to my surprise they just copied it from the above text file.
    - In my opinion, this doesn't "verify" the MD5, as it could have changed since the file was created, but there are no walkthroughs showing another way that I can find.

What is the decryption key of the online messenger app used by Zerry?

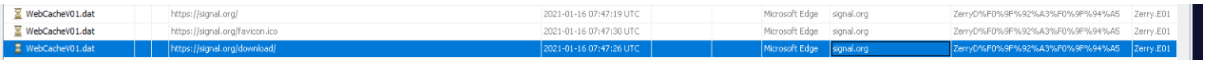
- Answer: c2a0e8d6f0853449cfcf4b75176c277535b3677de1bb59186b32f0dc6ed69998



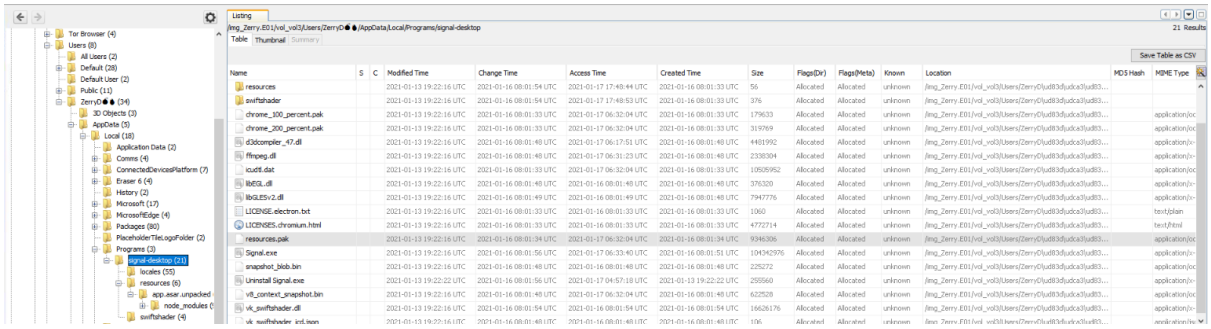
- Made a new case in Autopsy, and loaded the Zerry.EO1 image into it. Selected all the default options for extraction + one related to decryption after reading the challenge questions.



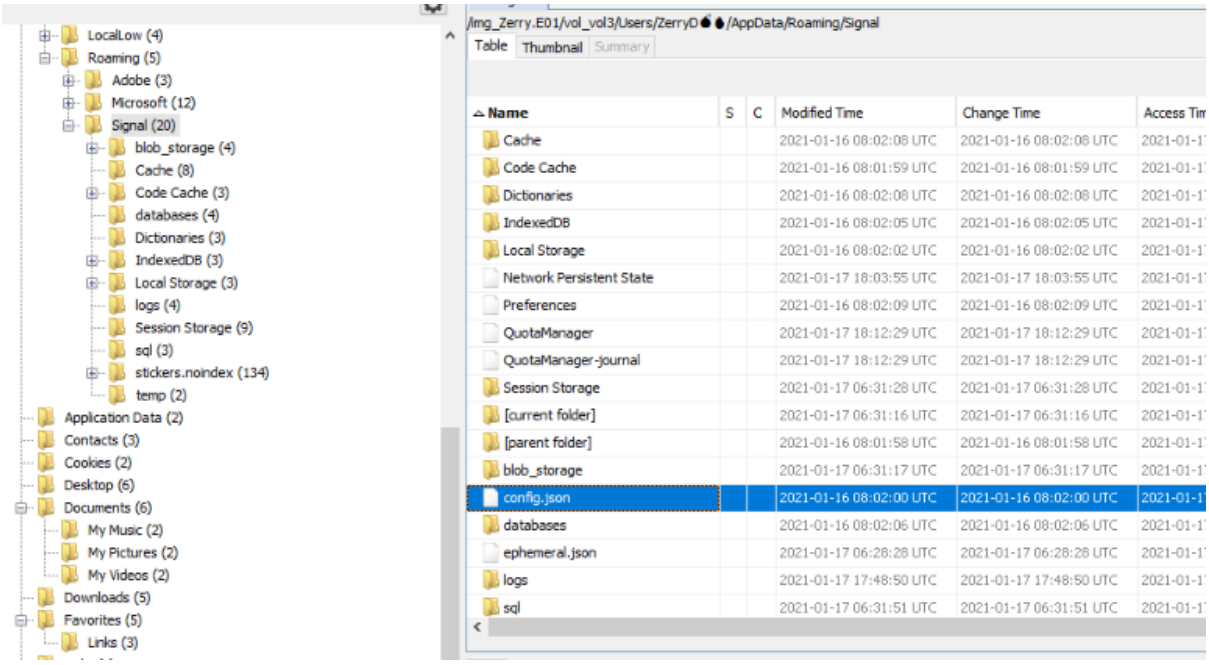
- Scrolling through online/web history shows requests for Signal, which is an encrypted messaging app.



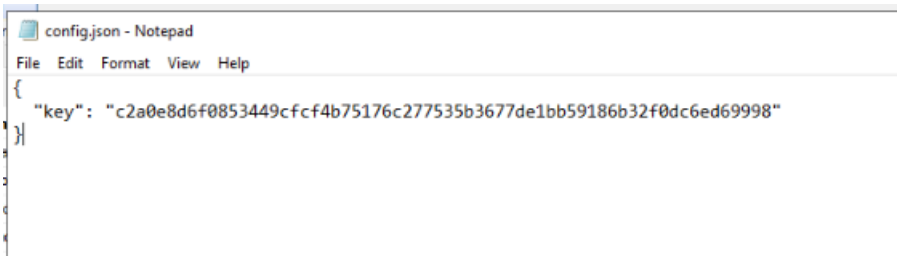
- Ordering Domain a-z shows that Zerry has downloaded Signal.



- Browsing around Zerry's documents/directory structure reveals Signal install/run location.
    - No sign of decryption key in this directory however.
- The AppData\Signal directory is where all important files etc. for Signal are kept.
    - After researching, I learned that all interactions conducted on Signal are stored in a database.

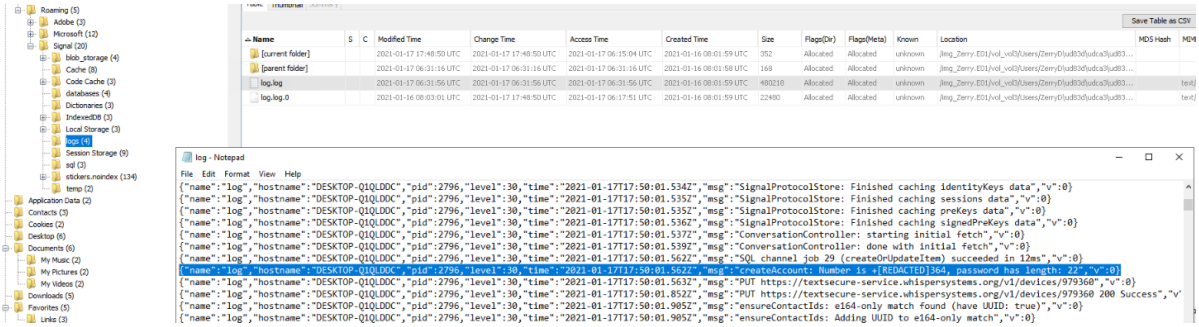


- Reviewing the contents directory showed a config.json file, which seemed like a logical place to start to gain an insight into anything required to configure Signal.
    - Right click > extract file > save > open with Notepad.
    - This file contained the decryption key:

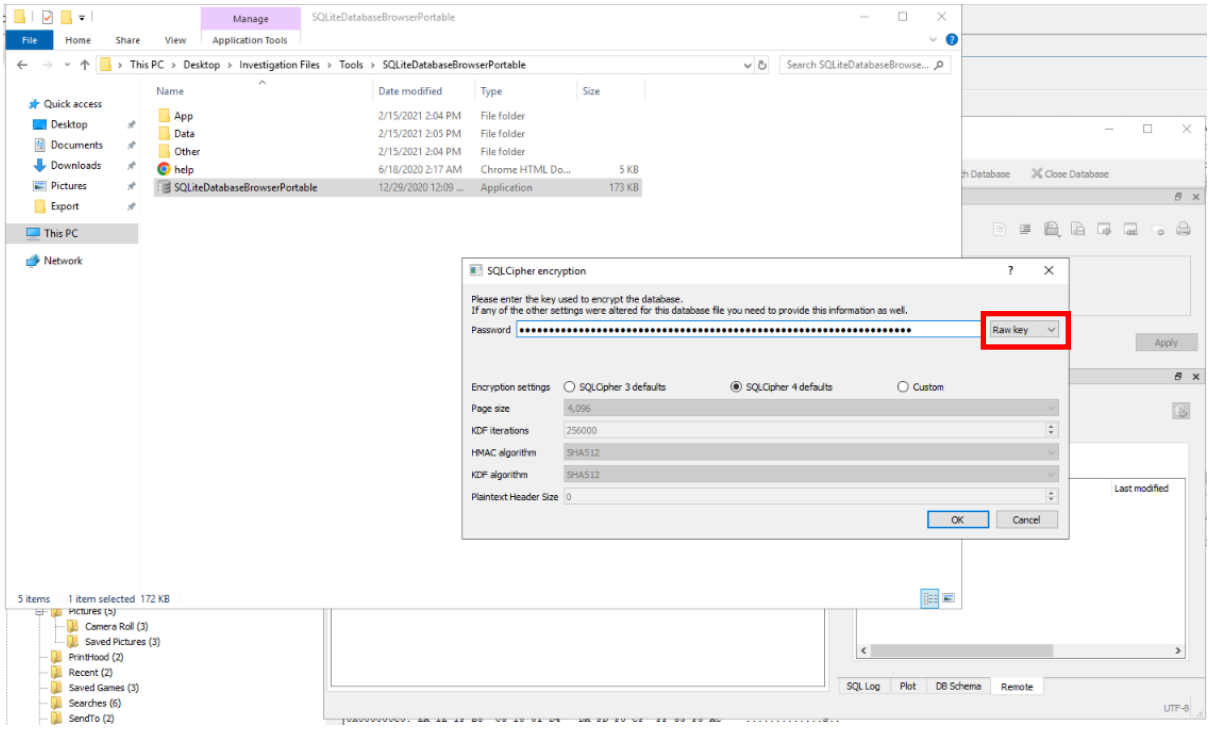


What is the registered phone number and profile name of Zerry in the messenger application used?

- Answer: 13026482364, ZerryThe



- Reviewing the /logs directory within the Signal directory, shows a log.log file. After extracting and opening in notepad, it seems this is the log of Zerry's interactions over Signal
    - Confirms an account is made (number redacted) with a passwords of length 22 characters.
- Also, based on knowledge gained in the previous question all interactions are logged in a database. This can be found under ~/Signal/sql/db.sqlite
    - Then, navigating to the "tools" directory in the desktop folder for the investigation shows SQLite Browser available to run.
    - Extract db.sqlite from the image in Autopsy and open it in SQLite Browser using the encryption key already found.



- Browsing the decrypted database shows a Messages table, showing a conversation between Zerry and someone called Tom

DB Browser for SQLite - C:\Users\BTLOTest\Desktop\Investigation Files\ZerryAutopsyCase\Zerry\Export\db.sqlite

File Edit View Tools Help

New Database | Open Database | Write Changes | Revert Changes | Open Project | Save Project | Attac

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: messages | Filter in any column

	er	expirationStartTimestamp	type	body	messageT
		Filter	Filter	Filter	Filter
1	NULL	NULL	message-history-unsynced	NULL	
2	NULL	1610905925397	outgoing	Hi Tom	
3	NULL	1610857387726	outgoing	Hi Zerry, single account with linked devices is a ...	
4	NULL	1610906042104	outgoing	tq. our higher authority suggested this for the ne...	
5	NULL	1610857506179	outgoing	i 2 researched about it. heard gud reviews on ...	
6	NULL	1610906142092	outgoing	whatzz d assignment???	
7	NULL	1610857589817	outgoing	yeah, before going to that did u remember our ...	
8	NULL	1610906235916	outgoing	yes...golden days 😁	
9	NULL	1610857671645	outgoing	we've 2 use them. download and install them	
10	NULL	1610906294755	outgoing	sure...will do and update	
11	NULL	1610907159324	outgoing	tom, i'm done with the installation	
12	NULL	1610858660886	outgoing	nice. assign: comb 💣 the city. target: as discuss...	
13	NULL	1610907346733	outgoing	understood. i'll stick to the target. what about ...	
14	NULL	1610858926345	outgoing	gud. till now i've this info only. b active here, will ...	
15	NULL	1610907552225	outgoing	ok	
16	NULL	1610858997325	outgoing	hasta la vista 🕺	
17	NULL	1610907631644	outgoing	hasta la vista 👍😁	
18	NULL	1610864063069	outgoing	got the ⏳ send me an expiring email... use tor	
19	NULL	1610864130793	outgoing	there?	
20	NULL	1610864206375	outgoing	yes ...send me	
21	NULL	1610864406509	outgoing	eekurk@baybabes.com	
22	NULL	1610864716477	outgoing	yup received	
23	NULL	1610864744280	outgoing	good. erase the attachment	
24	NULL	1610864820983	outgoing	Erased	
25	NULL	1610864840238	outgoing	gud. focus on work. all d best	
26	NULL	1610864873197	outgoing	sure. hasta la vista 💣🔥	
27	NULL	1610864899748	outgoing	ha ha...let's rock... hasta la vista 🕺	

- There are no tables named anything related to user details, so the next interesting one is "items". Opening it shows us details for Zerry, with a phone number above it:
    - Also, when submitting into the BTLO area to complete the challenge it foregoes the "+" at the start of the number for the area code which is just odd. But only a minor inconvenience I guess…

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: items | Filter in any colum

	id	json
	Filter	Filter
1	deviceNameEncrypted	{"id":"deviceNameEncrypted","value":true}
2	number_id	{"id":"number_id","value":"+13026482364.3"}
3	device_name	{"id":"device_name","value":"Zerry 💣🔥"}

- Then, reviewing the conversations table gives us the profile name.
    - This was horrendous to copy to the BTLO submit area to complete due to the emoji being copied as question marks. Took me multiple attempts to submit it in the correct format the platform wanted which was "ZerryThe" and not what is shown in

the screenshot below including the emoji – which you could argue is the correct profile name…

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: conversations

	id	json	active_at	type	members	name	profileName	profileFamilyName	profileFullName	e164
1	-562f-41cd-a802-e91fae2831b3	{"unreadCount":0,"verified":1,"messageCount":...	1610864901562	private	NULL	NULL	ZerryThe🔥	NULL	ZerryThe🔥	+13026482364

What is the email id found in the chat?

- Answer: eekurk@baybabes.com

Table: messages

	er	expirationStartTimestamp	type	body
1	NULL	NULL	message-history-unsynced	NULL
2	NULL	1610905925397	outgoing	Hi Tom
3	NULL	1610857387726	outgoing	Hi Zerry, single account with linked devices is a gud idea
4	NULL	1610906042104	outgoing	tq. our higher authority suggested this for the new assignment
5	NULL	1610857506179	outgoing	i 2 researched about it. heard gud reviews on privacy and encryption
6	NULL	1610906142092	outgoing	whatzz d assignment???
7	NULL	1610857589817	outgoing	yeah, before going to that did u remember our training days and the use of eraser and tor
8	NULL	1610906235916	outgoing	yes...golden days 😁
9	NULL	1610857671645	outgoing	we've 2 use them. download and install them
10	NULL	1610906294755	outgoing	sure...will do and update
11	NULL	1610907159324	outgoing	tom, i'm done with the installation
12	NULL	1610858660886	outgoing	nice. assign: comb 💣 the city. target: as discussed in our 2020 annual meeting. i hope u r aware of temperature, minutes and seconds
13	NULL	1610907346733	outgoing	understood. i'll stick to the target. what about execution ⏳??
14	NULL	1610858926345	outgoing	gud. till now i've this info only. b active here, will share once i receive. meanwhile make necessary arrangements to comb the city
15	NULL	1610907552225	outgoing	ok
16	NULL	1610858997325	outgoing	hasta la vista 🕶
17	NULL	1610907631644	outgoing	hasta la vista 👍😊
18	NULL	1610864063069	outgoing	got the ⏳ send me an expiring email... use tor
19	NULL	1610864130793	outgoing	there?
20	NULL	1610864206375	outgoing	yes ...send me
21	NULL	1610864406509	outgoing	eekurk@baybabes.com

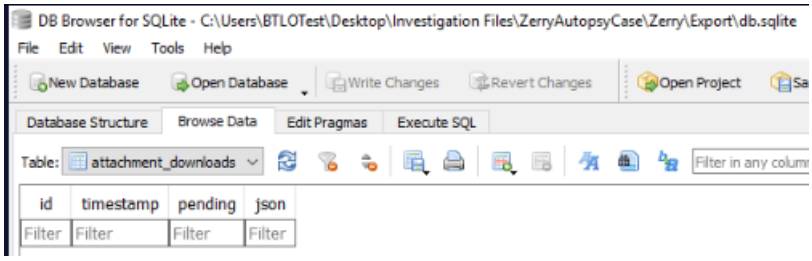
- As we've already reviewed/found the message table, this is pretty straightforward. Simply open it back up, read the conversation between Zerry & Tom, and find the email address.

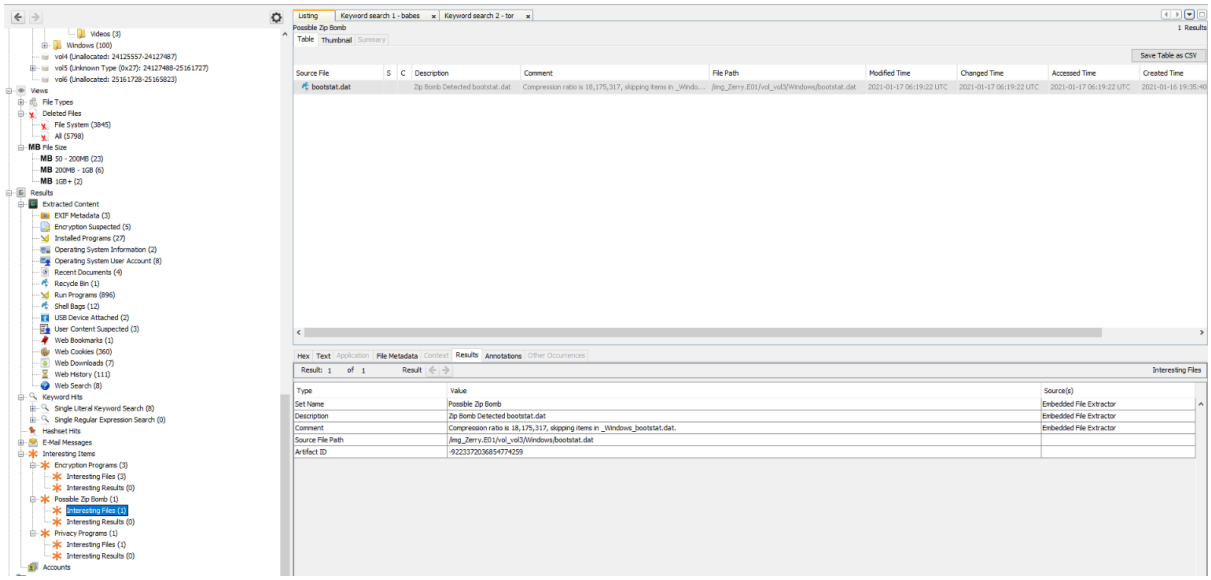
What is the filename(including extension) that is received as an attachment via email?

- Answer: ⏳ 📅.PNG

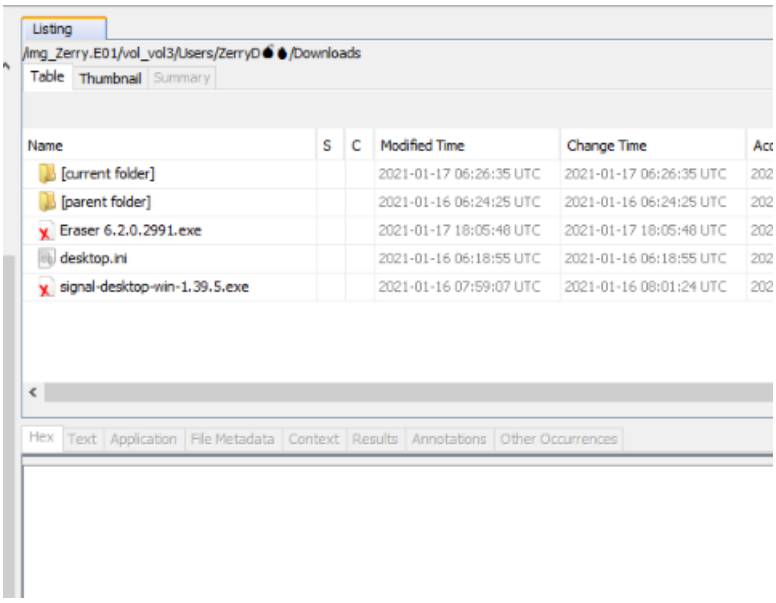
18	610864063069	outgoing	got the ⏳ send me an expiring email... use tor
19	610864130793	outgoing	there?
20	610864206375	outgoing	yes ...send me
21	610864406509	outgoing	eekurk@baybabes.com
22	610864716477	outgoing	yup received
23	610864744280	outgoing	good. erase the attachment
24	610864820983	outgoing	Erased
25	610864840238	outgoing	gud. focus on work. all d best
26	610864873197	outgoing	sure. hasta la vista 💣🔥
27	610864899748	outgoing	ha ha...let's rock... hasta la vista 🕶

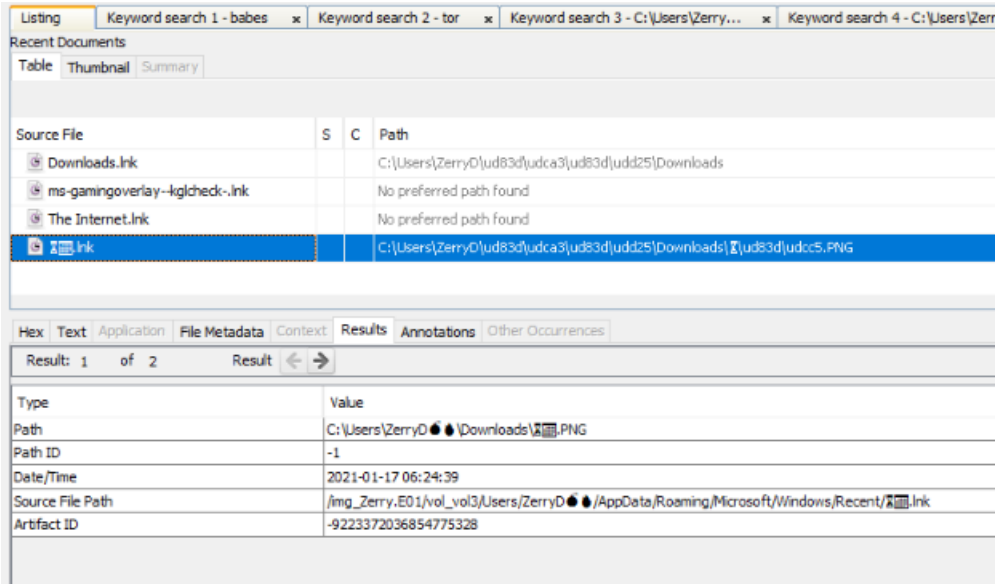
- Starting with the conversations table, we see that the email attachment is erased by Zerry.
  - This is further confirmed by viewing the attachment downloads table and it being empty:





- Reviewing Autopsy's output shows a "Possible Zip Bomb" under the "Interesting Files" section on the left-hand side.
- Reviewing Zerry's downloads in Autopsy reveals only the Signal and Eraser downloads.
- We can also infer, from the conversation, that Zerry has recently accessed the email attachment in some way. Reviewing "Recent Documents" in Autopsy shows a file with a name containing a timer emoji similar to that used in the conversation. However navigating to the saved location shows it as been deleted.

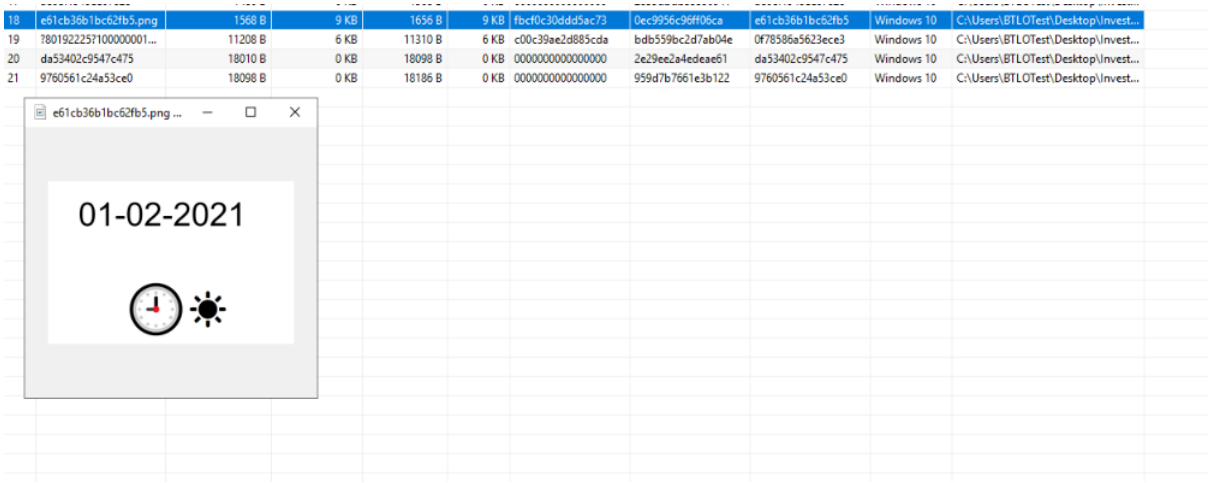




- NOTE: At this stage I consulted the walkthrough, as I was convinced I had the filename in the Path above, but no amount of copying would let me paste it into the challenge submit field. The walkthrough then said to go to Emojipedia, search the emojis and submit them + ".PNG" – I felt this was very obscure but, it was a learning experience discovering that filenames can contain emojis.

What is the Date and Time of the planned attack?

- Answer: 01-02-2021 09:00 AM



- Export thumbcache_256.db from /Users/Zerry/AppData/Local/Microsoft/Windows/Explorer via Autopsy. Open in Thumbcache Viewer.
- There was only one entry ending in .PNG, and selecting/clicking it opened a pop-up with the data & time.

What is the GPS location of the blast? The format is the same as found in the evidence.

- Answer: 40 degrees 45 minutes 28.6776 seconds N, 73 degrees 59 minutes 7.994 seconds W
- GPS location text was stored in a sticky note on the desktop.

- Sticky note data is stored in /img_Zerry.E01/vol_vol3/ZerryD💣🔥/AppData/Local/Packages/Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe/LocalState/plum.sqlite.
- The file does not require exporting, as the encoded text can be read directly in Autopsy's details view.
- The text is encoded in ROT13, and can be placed into CyberChef to get the hidden message.