



MAGNET
FORENSICS



University of New Haven

CONNECTICUT INSTITUTE OF TECHNOLOGY

2022 Magnet Summit

Android CTF

cyber@cfreg | Jordan Saleh

What I'll Be Covering

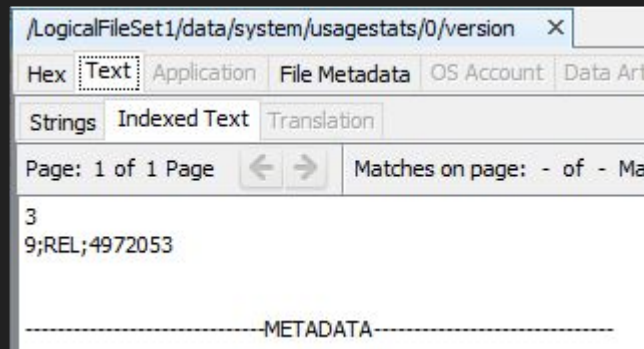
- Tools Used
- Device Information
- Connected Devices
 - Connected Networks
- Web History
- SMS Data
- Geolocation Data
- Snapchat Analysis
- Spotify Analysis

Tools Used

- Autopsy 4.19.3
- Belkasoft Evidence Center X Trial
- DB Browser for SQLite 3.12.2
- CheckArroyo

Device Information

- The Device is a Google Pixel 3 XL
 - This was found from /data/system/usagestats/0/version



9 represents the Android version

4972053 represents the incremental build number

- When you compare the build number to factory images from Google, it matches the Google Pixel 3 XL

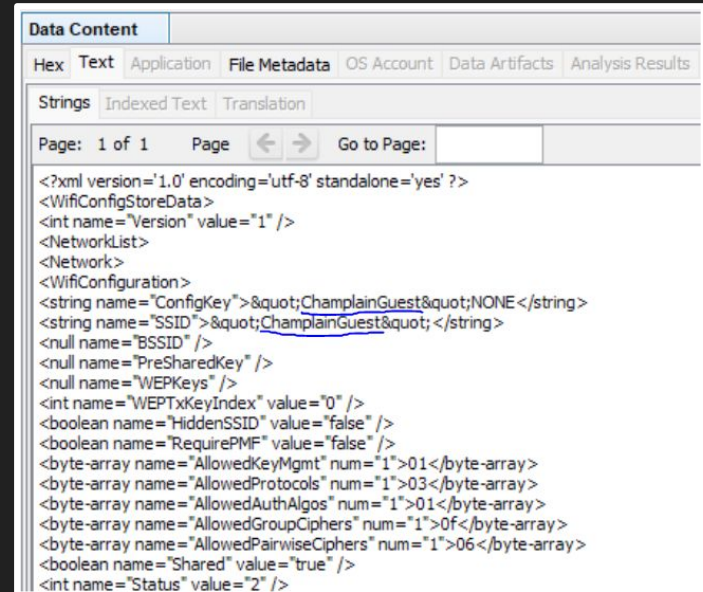
Connected Devices

There were 3 devices that had a history of being paired/connected to the device that Belkasoft was able to identify

Items: 3				
<input type="checkbox"/>		MAC addresses	Device name	First install time (UTC)
<input type="checkbox"/>		d0:5f:b8:33:df:00	Moto 360 DF00	
<input type="checkbox"/>		50:18:09:17:74:22	Mpow Flame	2/13/2022 5:53:52 AM
<input type="checkbox"/>		c9:5c:fd:17:56:c1	Tribit XSound Go	2/13/2022 6:03:22 AM

Connected Networks

Android used to store any wifi credentials within a folder titled **wpa_supplicant**. However, after Android 8.0 released, it moved to a file titled **WifiConfigStore.xml** that can be found within **/data/misc/wifi**



The screenshot shows a software interface for analyzing data content. At the top, there's a tab labeled 'Data Content'. Below it, a row of tabs includes 'Hex', 'Text', 'Application', 'File Metadata', 'OS Account', 'Data Artifacts', and 'Analysis Results'. The 'Text' tab is selected. Underneath, there's a sub-tab bar with 'Strings', 'Indexed Text', and 'Translation', where 'Strings' is active. A pagination bar shows 'Page: 1 of 1' and navigation arrows. The main area displays the XML content of a file, which is a WifiConfigStore.xml. The XML defines a <WifiConfigStoreData> element containing a <NetworkList> with a single <WifiConfiguration> entry. This entry includes fields like <ConfigKey>, <SSID>, <BSSID>, <PreSharedKey>, <WEPKeys>, <WEPKeyIndex>, <HiddenSSID>, <RequirePMF>, <AllowedKeyMgmt>, <AllowedProtocols>, <AllowedAuthAlgos>, <AllowedGroupCiphers>, <AllowedPairwiseCiphers>, <Shared>, and <Status>.

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<WifiConfigStoreData>
  <int name="Version" value="1" />
  <NetworkList>
    <WifiConfiguration>
      <string name="ConfigKey">"ChamplainGuest"</string>
      <string name="SSID">"ChamplainGuest"</string>
      <null name="BSSID" />
      <null name="PreSharedKey" />
      <null name="WEPKeys" />
      <int name="WEPKeyIndex" value="0" />
      <boolean name="HiddenSSID" value="false" />
      <boolean name="RequirePMF" value="false" />
      <byte-array name="AllowedKeyMgmt" num="1">01</byte-array>
      <byte-array name="AllowedProtocols" num="1">03</byte-array>
      <byte-array name="AllowedAuthAlgos" num="1">01</byte-array>
      <byte-array name="AllowedGroupCiphers" num="1">0f</byte-array>
      <byte-array name="AllowedPairwiseCiphers" num="1">06</byte-array>
      <boolean name="Shared" value="true" />
      <int name="Status" value="2" />
    </WifiConfiguration>
  </NetworkList>
</WifiConfigStoreData>
```

Web History

The user had some odd web history. The only notable searches involved searches for the Log4Shell vuln found within Log4J (which was also bookmarked), hacking tutorials, and card tricks. It seemed like buddy wanted to be a magician lol

Date Accessed	URL	Title	Comment
2022-01-29 03:12:25 EST	https://www.google.com/search?q=minecraft+icon&oq=mi...	minecraft icon - Google Search	Chrome History
2022-02-13 08:35:19 EST	https://www.google.com/search?q=minecraft+icon&oq=mi...	minecraft icon - Google Search	Chrome History
2022-02-13 06:30:11 EST	https://www.hackingtutorials.org/	Hacking Tutorials - The best Step-by-Step Hacking Tutorials	Chrome History
2022-02-13 06:30:57 EST	https://www.hackingtutorials.org/exploit-tutorials/log4shell...	Log4Shell VMware vCenter Server (CVE-2021-44228) - Hac...	Chrome History

2022-02-13 08:58:45 EST	https://www.google.com/search?q=best+magic+tricks+int...	best magic tricks intermediate - Google Search	Chrome History
2022-02-13 09:00:20 EST	https://www.vanishingincmagic.com/learn-card-tricks/5-ad...	5 Intermediate and Advanced Card Tricks Every Magician S...	Chrome History
2022-02-13 09:02:03 EST	https://www.google.com/search?q=larp&oq=larp&aqs=ch...	larp - Google Search	Chrome History
2022-02-13 09:03:32 EST	https://www.google.com/search?q=larp&client=ms-androi...	larp - Google Search	Chrome History
2022-02-13 09:03:39 EST	https://www.google.com/search?q=larp&client=ms-androi...	larp - Google Search	Chrome History
2022-02-13 09:03:31 EST	https://www.google.com/search?q=larp&client=ms-androi...	larp - Google Search	Chrome History
2022-02-13 09:04:10 EST	https://www.google.com/search?q=larp+shield+diy&tbm=...	larp shield diy - Google Search	Chrome History
2022-02-13 09:04:11 EST	https://www.google.com/search?q=larp+shield+diy&sourc...	larp shield diy - Google Search	Chrome History
2022-02-13 09:05:16 EST	https://www.google.com/amp/s/www.instructables.com/DI...	DIY Small LARP Shield in Under an Hour!	Chrome History
2022-02-13 06:31:22 EST	https://www.hackingtutorials.org/exploit-tutorials/log4shell...	Log4Shell VMware vCenter Server (CVE-2021-44228) - Hac...	Chrome Offline Pages
2022-02-13 09:06:18 EST	https://www.google.com/amp/s/www.instructables.com/DI...	DIY Small LARP Shield in Under an Hour!	Chrome Offline Pages
2022-02-13 09:01:11 EST	https://www.vanishingincmagic.com/learn-card-tricks/5-ad...	5 Intermediate and Advanced Card Tricks Every Magician S...	Chrome Offline Pages

SMS Data

Both Belkasoft & Autopsy didn't report anything notable with SMS data. The user had only received verification codes for platforms like Signal, Discord, Snapchat, and Google. These messages can provide a gauge of what apps the user was frequently using and logging into but aside from that there was nothing of evidentiary value.

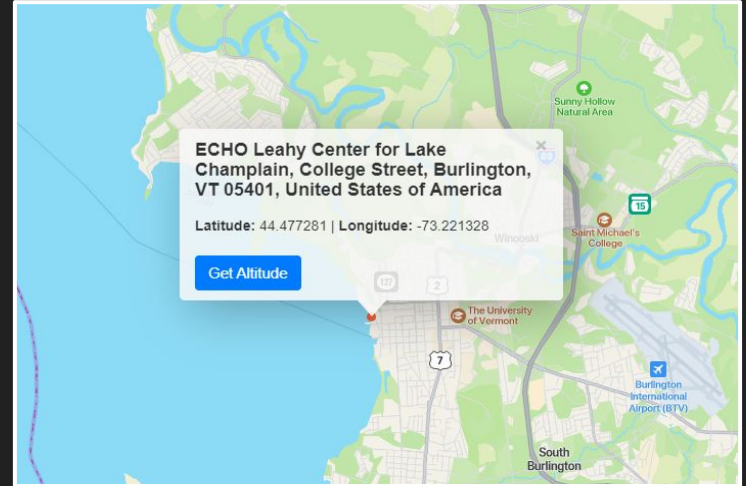
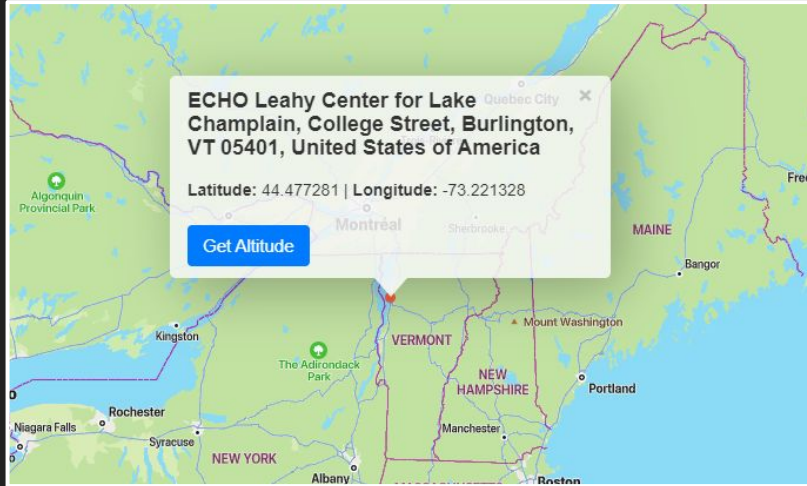
Geolocation Data

The user seemed to enjoy hiking as they had an app called “AllTrails” downloaded which provided a load of geolocation data. They seem to have been planning a trip to go hiking in Vermont and successfully completed both hikes/trips.

Two sets of coordinates were found by Belkasoft that seemed to repeat frequently.

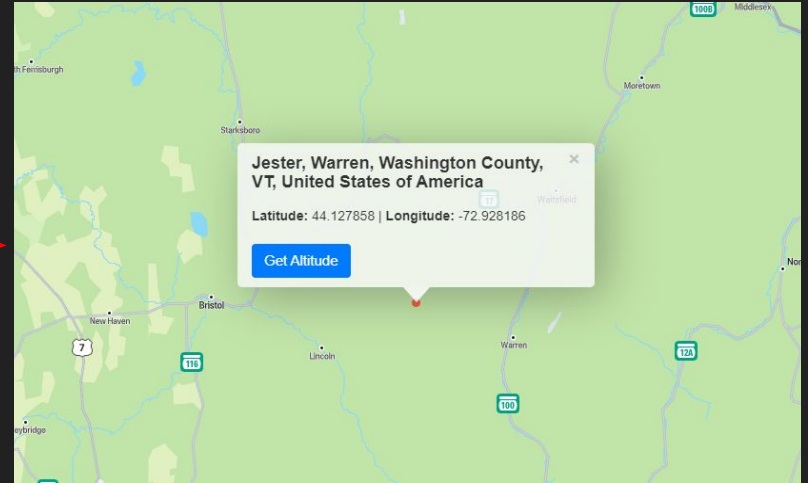
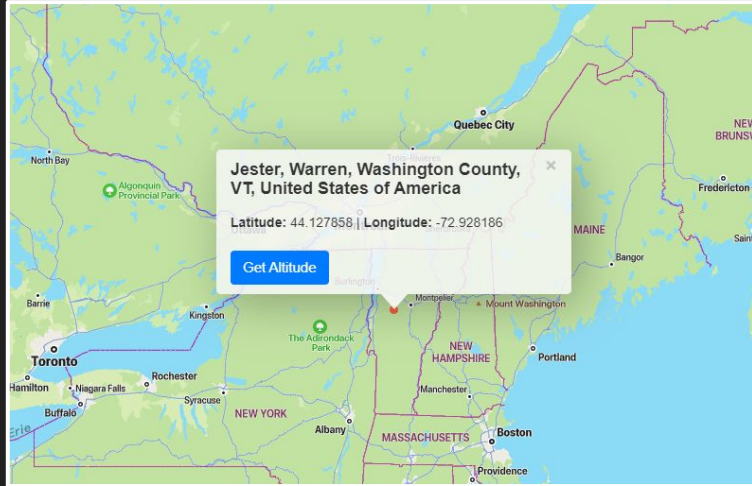
Geolocation Data Cont...

- 44.47728055555556, -73.22132777777777 (Waterfront Park in Burlington, VT)



Geolocation Data Cont...

- 44.127858333333336, -72.92818611111112 (Mt. Abraham Trail in Warren, VT)









Snapchat Analysis

This is where things got quite fun. When analyzing Snapchat data, Snapchat stores everything within databases that can be found within

/data/data/com.snapchat.android/databases

There are two main databases to focus on: **main.db** and **arroyo.db**

- **main.db**: Contains data pertaining to the user such as friends added, snap score, etc.
- **arroyo.db**: Contains data pertaining to messages and conversations

main.db

DB Browser for SQLite - C:\Users\Jordan\Downloads\main.db

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Open Project Save Project Attach Database Close Database

Database Structure Browse Data Edit Pragmas Execute SQL

Table: Friend Filter in any column

	_id	_lastModifiedTimestamp	username	combinedUsernameRowId	userId	displayName	bitmojiAvatarId	bitmojiSelfieId
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	NULL	teamsnapchat	1	84ee8839-3911-492d-8b94-72dd80f3713a	Team Snapchat	NULL	NULL
2	2	NULL	shell_game715	2	6b64d126-d8bf-4e93-b4a5-cabb2321c1de	Rafael Shell	NULL	NULL
3	3	NULL	angie_frank07	4	11e27a14-71cf-4dad-babe-2dbd5799b1be	Angie Frank	408100748_1-s5	10220069

arroyo.db

This database holds a table named **conversation_message** that has any relevant data of the user receiving/sending messages

A column named **creation_timestamp** contains the times of when each message was sent in UNIX Epoch time. Another column named **message_content** contains the actual contents of the message

To parse this database, I like to use a script called “CheckArroyo” by a user named Ogg3 that can be found on Github. It creates a visual representation of what any conversations looked like. In this case, the user only received messages from TeamSnapchat and none of their friends :(

DB Browser for SQLite - C:\Users\Jordan\Downloads\arrayo.db

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Open Project Save Project Attach Database Close Database

Database Structure Browse Data Edit Pragma Execute SQL

Table: conversation_message

	client_conversation_id	client_message_id	server_message_id	client_resolution_id	local_message_content_id	message_content	message_state_type	creation_timestamp
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	141c481a-69fe-587c-97d6-6c0802132d43	0	1	-3080557985965213527	NULL	BLOB	COMMITTED	1644388635325
2	141c481a-69fe-587c-97d6-6c0802132d43	64	3	6648106881768850224	NULL	BLOB	COMMITTED	1644529039561
3	141c481a-69fe-587c-97d6-6c0802132d43	65	4	4979363392278504010	NULL	BLOB	COMMITTED	1644529039629
4	141c481a-69fe-587c-97d6-6c0802132d43	66	5	5284856638529001925	NULL	BLOB	COMMITTED	1644529039691
5	141c481a-69fe-587c-97d6-6c0802132d43	67	6	-6719579305969720207	NULL	BLOB	COMMITTED	1644529039763
6	141c481a-69fe-587c-97d6-6c0802132d43	68	7	1090463642173491787	NULL	BLOB	COMMITTED	1644529039823
7	141c481a-69fe-587c-97d6-6c0802132d43	1	2	-7311923573031970620	NULL	BLOB	COMMITTED	1644388635429

Filter in any column

Edit Database Cell

Mode: Binary

```
0000 08 01 12 12 0a 10 84 ee 88 39 39 11 49 2d 8b 94 .....99.I-...
0010 72 dd 80 f3 71 3a 1a 1d 0a 16 0a 12 0a 10 14 1c r...q:.....
0020 48 1a 69 fe 58 7c 97 d6 6c 08 02 13 2d 43 10 05 H.i.X|.l....C..
0030 9a 06 02 0a 00 22 9f 02 10 01 1a 02 0a 00 22 92 .....".
0040 02 12 8f 02 0a 8c 02 57 65 6c 63 6f 6d 65 20 74 .....Welcome t
0050 6f 20 43 68 61 74 21 20 f0 9f 91 bb 0a 59 6f 75 o Chat! .....You
0060 20 63 61 6e 20 73 65 6e 64 20 6d 65 73 73 61 67 can send messag
0070 65 73 2c 20 73 74 69 63 6b 65 72 73 2c 20 61 6e es, stickers, an
0080 64 20 6d 6f 72 65 20 f0 9f 92 ac 0a 54 61 70 20 d more .....Tap
0090 f0 9f 93 9e 20 6f 72 20 f0 9f 9e a5 20 74 6f 20 .... or .... to
00a0 6d 61 6b 65 20 61 20 63 61 6c 6c 2c 20 6f 72 20 make a call, or
00b0 70 72 65 73 73 20 26 20 68 6f 6c 64 20 f0 9f 9e press & hold ...
00c0 99 20 74 6f 20 6c 65 61 76 65 20 61 20 6e 6f 74 . to leave a not
00d0 65 21 0a 4d 65 73 73 61 67 65 73 20 61 72 65 20 e!.Messages are
00e0 64 65 6c 65 74 65 64 20 62 79 20 64 65 66 61 75 deleted by defau
00f0 6c 74 20 f0 9f 99 8a 0a 54 61 70 20 74 6f 20 73 lt .....Tap to s
0100 61 76 65 20 61 20 6d 65 73 73 61 67 65 20 f0 9f ave a message ..
0110 91 86 0a 59 6f 75 20 63 61 6e 20 61 6c 73 6f 20 ...You can also
0120 73 63 72 65 65 6e 73 68 6f 74 20 43 68 61 74 73 screenshot Chats
0130 20 61 6e 64 20 53 6e 61 70 73 20 f0 9f 93 b2 0a and Snaps .....
0140 48 61 70 79 20 43 68 61 74 74 69 6e 67 20 f0 Happy Chatting .
0150 9f 99 8c 32 00 38 02 32 09 08 bd a5 cd e9 ed 2f ...2.8.2...../
0160 58 02 38 a9 f1 b3 84 d5 9a ea 9f d5 01 4a 16 0a X.8.....J..
0170 12 0a 10 ab 85 aa 04 ca d6 4b 71 98 f0 8e 01 21 .....Kq....!
0180 c2 84 a9 20 01 .....
```

Username: 84ee8839-3911-492d-8b94-72dd80f3713a Snapchat ID: 84ee8839-3911-492d-8b94-72dd80f3713a

Welcome to Chat! 🗨️ You can send messages, stickers, and more 💬 Tap 📞 or 📺 to make a call, or press & hold 📷 to leave a note! Messages are deleted by default 🗑️ Tap to save a message 📌 You can also screenshot Chats and Snaps 📱 Happy Chatting 🥰

Username: 84ee8839-3911-492d-8b94-72dd80f3713a Type: Text message Sent: 2022-02-09 01:37:15.325

Username: 84ee8839-3911-492d-8b94-72dd80f3713a Type: Snap Sent: 2022-02-09 01:37:15.429

Username: 84ee8839-3911-492d-8b94-72dd80f3713a Type: Media Sent: 2022-02-10 16:37:19.561

Personalize your own Bitmoji avatar 🧑🏻

Username: 84ee8839-3911-492d-8b94-72dd80f3713a Type: Text message Sent: 2022-02-10 16:37:19.629

And add excitement to conversations! 🎉

Username: 84ee8839-3911-492d-8b94-72dd80f3713a Type: Text message Sent: 2022-02-10 16:37:19.691

Go to your Profile in Snapchat and tap 'Create Bitmoji'

Username: 84ee8839-3911-492d-8b94-72dd80f3713a Type: Text message Sent: 2022-02-10 16:37:19.763

https://link.snapchat.com/bitmoji/avatar_builder/edit

Username: 84ee8839-3911-492d-8b94-72dd80f3713a Type: Text message Sent: 2022-02-10 16:37:19.823



Spotify Analysis

Any data involving Spotify is found within **/data/data/com.spotify.music/files** in which the local cache folder was holding 2 files named **find** and **recently_played**.

The **recently_played** file held all data of listening history. This means the playlist and the user who uploaded that playlist

"name": "The Lord of the Rings Soundtrack",

"ownerName": "Impakt Records",

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Indexed Text Translation

Page: 1 of 1 Page Go to Page: 256 Script: Latin - Basic

```
{\"length\":2,\"loaded\":true,\"items\":[{\"link\":\"spotify:user:2apxpnfv7299tnutgbn50z3qm:playlist:0uwoqeN6C1NuXwjNVTY5F\",\"collectionLink\":\"null\",\"name\":\"The Lord of the Rings Soundtrack\",\"imageUri\":\"spotify:image:ab67706c000da840ff4b35b853d105f3f8839a\",\"type\":\"playlist\",\"ownerName\":\"Impakt Records\",\"publisher\":\"null\",\"artistName\":\"null\",\"subtitle\":\"null\",\"mediaType\":\"null\",\"available\":true,\"isCollaborative\":false,\"isLoading\":false,\"isOwnedBySelf\":false,\"isFollowing\":true,\"inCollection\":false,\"numTracks\":64,\"tracksInCollectionCount\":0,\"syncProgress\":0,\"formatListType\":\"\",\"formatListAttributes\":{},\"madeForName\":\"null\",\"madeForUsername\":\"null\",\"isOnDemand\":false,\"isBook\":false,\"isOffline\":\"no\",\"targetUri\":\"spotify:user:2apxpnfv7299tnutgbn50z3qm:playlist:0uwoqeN6C1NuXwjNVTY5F\",\"uri\":\"spotify:user:2apxpnfv7299tnutgbn50z3qm:playlist:0uwoqeN6C1NuXwjNVTY5F\",\"loading\":false},{\"link\":\"spotify:playlist:1JPJKSQYEbegvHlgpkF0\",\"collectionLink\":\"null\",\"name\":\"Matrix 4 Resurrections Soundtrack Playlist 12.22.21 The Matrix Resurrections Movie 2021\",\"imageUri\":\"spotify:image:ab67706c000da840ff4b35b853d105f3f8839a\",\"type\":\"playlist\",\"ownerName\":\"Bonbonniere\",\"publisher\":\"null\",\"artistName\":\"null\",\"subtitle\":\"null\",\"mediaType\":\"null\",\"available\":true,\"isCollaborative\":false,\"isLoading\":false,\"isOwnedBySelf\":false,\"isFollowing\":true,\"inCollection\":false,\"numTracks\":79,\"tracksInCollectionCount\":0,\"syncProgress\":0,\"formatListType\":\"\",\"formatListAttributes\":{},\"madeForName\":\"null\",\"madeForUsername\":\"null\",\"isOnDemand\":false,\"isBook\":false,\"isOffline\":\"no\",\"targetUri\":\"spotify:playlist:1JPJKSQYEbegvHlgpkF0\",\"uri\":\"spotify:playlist:1JPJKSQYEbegvHlgpkF0\",\"loading\":false}],\"unfiltered.length\":2,\"unranged.length\":2,\"loading\":false}
```

"ownerName": "Bonbonniere",

"Matrix 4 Resurrections Soundtrack Playlist 12.22.21 The Matrix Resurrections Movie 2021"



MAGNET
FORENSICS®

Magnet Targeted Location Guides

<https://www.magnetforensics.com/targeted-location-guides/>



H E X O R D I A

Hexordia Forensic Courses

<https://www.hexordia.com/>

<https://cyber5w.com/>

- Where can you find this CTF?

You can find the files for the CTF here:

<https://cfreds.nist.gov/all/MagnetForensics/2022AndroidMagnetCTF>

- My official write up for this CTF:

My official write up for this CTF can be found on my Github @sudo-jordan along with some other CTF writeups