

Magnet Forensics CTF



Magnet Forensics User Summit 2023 (ONLINE) CTF After Action Writeup

By Matthew Plascencia

CIPHER (Unanswered: 2)

salad are for THE chumps

Q: Pa'z H-Tl, Thypv

A: After reading the question once and then once again, pick out the word "SALAD" and notice that the Caesar Cipher could be assumed from that word, since it's a salad. When you brute-force the Caesar cipher, you get the following correct answer: **It's-A-Me, Mario!**

The earth's rotation really makes my day.

Q: (9E0:D0E960A2DDH@C5

This clue is a cue for a brute-force rotation cipher. If you put it into an online tool, you will get the following: **Wht_is_the_password**

I like the trailer for this movie. Can't wait to see it in theaters!

See the resource file *movie.jpg*

A: Put this image into a Kali VM or hex editor and find that it has the following flag at the end.
I like the trailer for this movie. Can't wait to see it in theaters!

SomeTimes its nicE to just stop workinG and search the Internet for good mEmes.

See the file *challenge.jpg*

A: Reading the question for capital letters gives us a hint for using steghide. When we use steghide on Kali Linux, we find the following flag: **eleven_is_more_than_ten**

The command we use is "steghide extract -sf challenge.jpg -xf hi.txt"

As long as more than Zer0 people enjoy these challanges I'd be happy Width that!

I really enjoyed the BlueMonkey 4n6 video on the last cipher questions. If you enjoy these challenges let us know!

A: The problem gives us a hint that a zero width (something) is used. At this point we can look to "Blue Monkey 4n6" for a lead. There is nothing to find with this lead. Using a zero-width decoder will reveal this: **This_!\$theFullFLAG**

Sometimes I wish we could visualize music

Use *message.wav*

A: Open the file in Audacity. After doing so, switch to the spectral analyzer and then see the flag there. Enter **"Popcorn"** for the correct flag

wh1ter0se.m4v

Use the file whiter0se.m4v

A: You won't know off the bat what to do, but when you do a bit of research you will find this site:

https://mrrobot.fandom.com/wiki/Eps1.7_wh1ter0se.m4v

going down the page, you will find a line that talks about the software DeepSound. Download that software and open the file in DeepSound. Press the Extract button and it will write the following flag to a file WOW! You found another flag! Keep up the great work!

Cobalt Strike: A Necessary Evil?

U2V0LVN0cmljdE1vZGUgLVZlcnNpb24gMgoKZnVuY3Rpb24gZnVuY19nZXRfcHJvY19hZGRyZXNzIHsKCVBhcmFtIlgkdmFyX21vZHVzZSwgJHZhcl9wcm9jZWR1cmUpCQkKCSR2YXJfdW5zYWZlX25hdGl2ZV9tZXRob2RzID0gKFtBcHBEB21haW5dOjpDdXJyZW50RG9tYWluLkdldEFzc2VtYmxpZXM0KSB8IFdoZXJlLU9iamVjdCB7ICRfLkdsb2JhbEFzc2VtYmx5Q2FjaGUgLUFuZCAkXy5Mb2NhdGlubi5TcGxpdcGnXFwnKVstMV0uRXF1YWxzKCDtEXN0ZW0uZGxsJykgfSkur2V0VHlwZSgnTWljcm9zb2Z0LldpbjMyLlVuc2FmZU5hdGl2ZU1ldGhvZHMnKQoJJHZhcl9ncGEgPSAkdmFyX3Vuc2FmZV9uYXRpdMVfbWV0aG9kcy5HZXRNZXRob2QoJ0dlFByb2NBZGRyZXNzJywgW1R5cGVbXV0gQCgnU3lzdGVtLlJ1bnRpbWUuSW50ZXJvcFNlcnZpY2VzLkhhbmR5ZVJlZicsICdzdHJpbmcnKSkKCXJldHVybiAkdmFyX2dwYS5JbnZva2UoJG51bGwslEAoW1N5c3RibS5SdW50aW1lLkludGVyb3BTZXJ2aWNlcy5lYW5kbGVSWZdKE5ldy1PYmplY3QgU3lzdGVtLlJ1bnRpbWUuSW50ZXJvcFNlcnZpY2VzLkhhbmR5ZVJlZigoTmV3LU9iamVjdCBJbnRQdHlplCAoJHZhcl91bnNhZmVfbmF0aXZlX21ldGhvZHMuR2V0TWV0aG9kKCDHZXRNb2R1bGVlYW5kbGUuKSkusW52b2tIKCRudWxsLCBAKCR2YXJfbW9kdWxlKSkpKSwgJHZhcl9wcm9jZWR1cmUpKQp9CgpmcW5jdGlubiBmdW5jX2dlF9kZWxlZ2F0ZV90eXBIIHsKCVBhcmFtIlgKCQlUGFyYW1ldGVyKFBvc2l0aW9uID0gMCwgTWFuZGF0b3J5ID0gJFRydWUpXSBBvHlwZVtdXSAdmFyX3BhcmFtZXRlcnMsCgkKW1BhcmFtZXRlcihQb3NpdGlubiA9IDEpXSBbVHlwZV0gJHZhcl9yZXR1cm5fdHlwZSA9IFtWb2lkXQoJKQoKCSR2YXJfdHlwZV9idWlsZGVyID0gW0FwcERvbWVpbl06OkN1cnJlbnREb21haW4uRGVmaW5lRHluYW1pY0Fzc2VtYmx5KChOZXT2JqZWNOIFN5c3RibS5SZWZsZWNOaW9uLkFzc2VtYmx5TmFtZSgnUmVmbGVjdGVkRGVsZWdhdGUuKSkslFtEXN0ZW0uUmVmbGVjdGlubi5FbWl0LkFzc2VtYmx5QnVpbGRlckFjY2Vzc106OIJ1bikuRGVmaW5lRHluYW1pY01vZHVzSgnSW5NZW1vcnlnb2R1bGUuLCAkZmFsc2UpLkRlZmluZVR5cGUoJ015RGVsZWdhdGVUeXBlJywgJ0NsYXNzLCBQdWJsaWMslFNlYWxlZCwgQW5zaUNsYXNzLCBBdXRvQ2xhc3MnLCBBU3lzdGVtLk11bHRpY2FzdERlbGVnYXRlXSkKCSR2YXJfdHlwZV9idWlsZGVyLkRlZmluZUNvbnN0cnVjdG9yKCDsVFNwZWNPYWxOYW1lLCBlaWRIQnlTaWcslFB1YmxpYycslFtEXN0ZW0uUmVmbGVjdGlubi5DYWxsaW5nQ29udmVudGlbnNdOjpTdGFuZGFyZCwgJHZhcl9wYXJhbWV0ZXJzKS5TZXRJbXBsZW1lbnRhZGlubkZsYWdzKCDsSdW50aW1lLCBNYW5hZ2ZVkJyKCSR2YXJfdHlwZV9idWlsZGVyLkRlZmluZU1ldGhvZCgnSW52b2tJywgJ1B1YmxpYywgSGlkZUJ5U2lnLCBOZXdTbG90LCBWAxJ0dWFsJywgJHZhcl9yZXR1cm5fdHlwZSwgJHZhcl9wYXJhbWV0ZXJzKS5TZXRJbXBsZW1lbnRhZGlubkZsYWdzKCDsSdW50aW1lLCBNYW5hZ2ZVkJyKCGlyZXR1cm4gJHZhcl90eXBIX2J1aWxkZXluQ3JlYXRlVHlwZSgpCn0KCKlmlChbSW50UHRyXT06c2l6ZSAtdXEGOCkgewoJW0J5dGVbXV0kdmFyX2NvZGUgPSBBU3lzdGVtLkNvbnZlcnRdOjpGcm9tQmFzZTY0U3RyaW5nKCCzMnVneDIQTDZ3QUFBR0p5WW50eGNuVnJFdkZHYYTzoeFEydw9jVHRycUhFRGE2aFJjMnNzbEdscGJoTHFheExqang5Q1h5RVBBMkxpNmkaU1lTEJ6bkZpY211b2NRT29ZUjlySXZORm9sczdLQ0ZXVWFpanF3QUFBR3VtNDFkRWF5THpjNmhyTzJlbnJlbnRdJlBBZFd2YzZtS29GNnRySXZWdUV1cHJFdU9QWXVMcUxtSWk0aHZE VnRKdklHOEHLMlIlhOGxiN2UyZW9Zd2RzSXZORlIxZ3ZhMmVvWVXo5cUI2TmlxQ2VYyXIMelludGllMzE2ZVdKN1lucGllV3VnendOaWNnekRlMko2ZVd1b01jcHMzTnpjZmtrQWFwMVVtazFLVfVaWEFHsJfHcXJGYjZyU1lwbHZWQVVRm1BackV1cHJFdkZ1RXV0dUV1cGljMkp6WXBwRmRWcUuZUGJJVUhsCnF1SmltN00

32uxg9PL6wAAAGJyYnNxcnVrEvFGa6hxQ2uocTtrqHEDa6hRc2sslGlpbhLqaxLjjx9CXyEPA2Li6i5ilulBznFic
muocQOoYR9rlvNFols7KCFWUaijqwAAAGum41dEayLzc6hrO2eoYwNqlvPAdWvc6mKoF6trlvVuEuprEuOP
YuLqLmli4hvdVtJvIG8HK2Ya8lb7e2eoYwdqlvNFYqgva2eoYz9qlvNiqCeraYlZyntie316eWJ7YnpieWugzwN
cdzDe2J6eWuoMcps3NzcfcAap1Usk1KTUZXAGJ1aqrFb6rSYplvVAUk3PZrEuprEvFuEuNuEupic2JzYpkZdV
qE3PbiUHLrqJum7M8AABuEupicmJySSBicmKZdKq85dz2yHp4a6riaxLxaqr7bhLqcUsAIWOncXFimch2DRjc
9muq5Wug4HNJKXxrqtJrqvlq5OPc3NzcbhLqcXFimQ4IO1jc9qbjLKa+IgAAa9zsLkevlGAAyPDKxyIAAMuB3N
zcDBFFUncAijb/JdOBccoNCFrt/gYE1C5KBfph47IcCRbhkDT/M/HH9TaPwbugyN0Hk5C7ZdVaogVoUoMzA/
7VhgWCqlRmzKkHroKnePbfWQB2UEZRDmJERk1XGQNuTFIKT09CDBcNEwMLQExOU0JXSkFPRhgDbnBqZ
gMUDRMYA3RKTUdMVfADbXcDFQ0TCi4pAED4ETbyn30sxC5WfeAk/O6zzJxBKD2hmdj0Tlx7EWIveSMpd
5mSzwclaPpoAqvEFO3nCppyVcu7DYvCY4xpACyNaR3ZHustK/fU5pDVszT+Gzt1Pf9l/ybwhvmif1EQaA+
wGPlwio/AMbNhgIHxKWb7Dgl7Gfi5yXtgXqilsezEfPKxaB9Ltr5NXLIolvj3JK9s8beuLUw8Whx1L3gbAqGO
F320Fc2T88oRDJrdz8A3WASvTwA3xlkgN7B9QtB0Rnb16X+wMXWoIuyxGyZNcdUeuFwwrScbulKx8qaRhC
aXzWSChFrPnoHtgDqCAyp3TloF13PZrEuqZAABjAGKbADMAAGKaYwAAAGKZe4dwxtz2a7BwcGuqxGuq0
muq+WKBaMAAGqq2mKZMbWqwdz2a6DnA6bjV5VFqCRrluCm41b0e3t7ayYAAAAAc+DLvN7c3HpMVn
xITFZNR3x3S0Z8YBEAMRd1Ww==

and then put that into cyberchef with the following parameters

The screenshot shows the CyberChef web interface. The 'From Base64' section is active, with the 'Alphabet' dropdown set to 'A-Za-z0-9+/' and the 'Remove non-alphabet chars' checkbox checked. The 'Strict mode' checkbox is unchecked. Below this, the 'XOR' section is visible, with the 'Key' dropdown set to '35', the 'Scheme' dropdown set to 'DECIMAL', and the 'Null preserving' checkbox unchecked.

You will receive this output:

The screenshot shows the 'Output' section of CyberChef, displaying a large block of obfuscated text. The text is a mix of uppercase and lowercase letters, numbers, and special characters, including symbols like \$, %, ^, &, and ~. It appears to be a base64-encoded string that has been XOR'd with the key 35. The text is wrapped in a dark-themed window with standard OS window controls (minimize, maximize, close) in the top right corner.

(Note: Use the following resource to see a better explanation of my method:

<https://michaelkoczvara.medium.com/cobalt-strike-powershell-payload-analysis-eecf74b3c2f7>)

typing out all these questions...

****Question Name:** **

typing out all these questions is starting to hurt my Fingers, maybe I should Shift my thinking.

****Challenge:** **

yjdodyjrg;sh

*Look at your keyboard. Move all of the letters in the clue off by one. After doing that you will see that the flag is **thisistheflag***

ANDROID (Unanswered: 8)

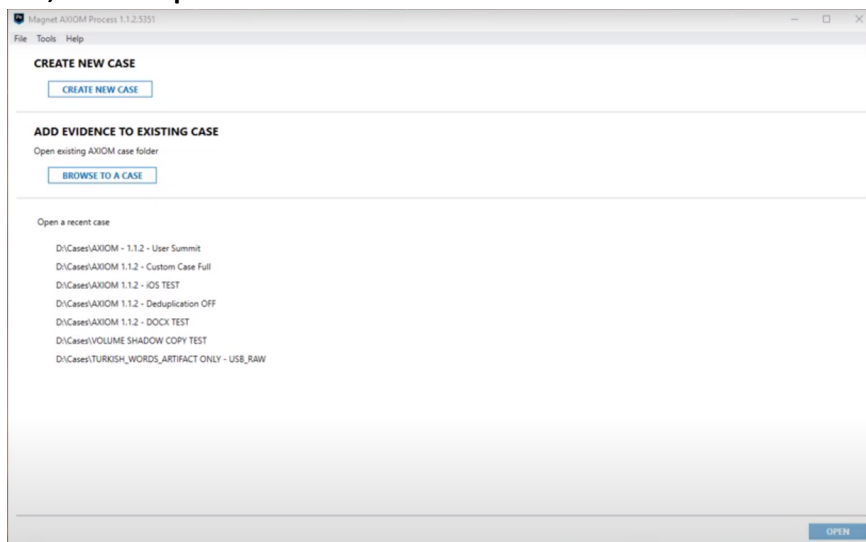
Process

Tools used

- **Magne Axiom**
- **ALEAPP**
- **Autopsy**

How I started:

As soon as I received the image in my emails, I began processing it with Magnet Axiom Process. To do so, I opened Magnet Axiom Process and began a new case. This is the first screen you see, on startup.



Once you press the “New Case” button, you will be taken to a screen where you can enter the details of your case. This is the min detail of the Case Details screen. Write as much or as little as you need to to start. Press Next to continue,

CASE INFORMATION

Case number

Case type

Other

LOCATION FOR CASE FILES

Folder name

AXIOM - May 06 2023 185223

File path

D:\Matts Stuff\Axiom Cases\Pixel Case

BROWSE

Available space:

947.79 GB

LOCATION FOR ACQUIRED EVIDENCE

Folder name

AXIOM - May 06 2023 185223

File path

D:\Matts Stuff\Magnet Forensics\MWS In Person

BROWSE

Available space:

947.79 GB

SCAN INFORMATION

SCAN 1

Scanned by

Description

REPORT OPTIONS

Cover logo

BROWSE

Image resized to:

150x150 pixels

COMPUTER

MOBILE

CLOUD

VEHICLE

REMOTE COMPUTER

EVIDENCE SOURCES ADDED TO CASE

Type	Image - location name	Evidence number	Search type	Status
------	-----------------------	-----------------	-------------	--------

EVIDENCE SOURCES

MOBILE
SELECT EVIDENCE SOURCE



ANDROID



IOS



WINDOWS PHONE



KINDLE FIRE



MEDIA DEVICE (MTP)



SIM CARD

Load the evidence

EVIDENCE SOURCES

ANDROID
LOAD OR ACQUIRE



LOAD EVIDENCE



ACQUIRE EVIDENCE

Image

EVIDENCE SOURCES

ANDROID

SELECT EVIDENCE TO LOAD



IMAGE



FILES & FOLDERS

In the file manager window that pops up, find the tar file of the image you downloaded and select it. Once it loads fully, click next. You will be taken back to the first evidence source selection screen. Select Go to Processing Details. Clicking will take you to this screen.

CASE DETAILS

EVIDENCE SOURCES1

PROCESSING DETAILS

Search archives and mobile backupsOn

Decode file-based encryption

Add keywords to search

Extract text from files (OCR)On

Calculate hashes and find matchesOn

Analyze chats with Magnet.AI

Analyze pictures with Magnet.AI

Search with YARA rulesOn

Find more artifacts

ARTIFACT DETAILS256

Mobile artifacts256 of 269

Cloud artifacts

Computer artifacts

Vehicle artifacts

Parse and carve artifacts

Privileged content

Date range filter

ANALYZE EVIDENCE

PROCESSING DETAILS

SEARCH ARCHIVES AND MOBILE BACKUPS

Container files such as archives and mobile backups can be found within other evidence sources. Configure options on this page to search any containers found during your search.

SEARCH ARCHIVES AND MOBILE BACKUPS

ADD KEYWORDS TO SEARCH

Provide the keywords and regular expressions that you want to include in your search. If a keyword gets a hit during the search, it's added to a Keywords filter in AXIOM Examine.

ADD KEYWORDS TO SEARCH

PROCESS FILES USING OPTICAL CHARACTER RECOGNITION

During a scan, Magnet AXIOM can extract text from certain files using optical character recognition (OCR). AXIOM Examine displays the extracted text in its own card, called Text extracted using OCR.

PROCESS FILES USING OPTICAL CHARACTER RECOGNITION

DECODE FILE-BASED ENCRYPTION

Evidence sources can contain files that have been encrypted. Provide decryption keys so that AXIOM Process can decode the data for you.

DECODE FILE-BASED ENCRYPTION

CALCULATE HASHES AND FIND MATCHES

AXIOM Process can calculate hash values for each file in an evidence source. You can add hash sets from local .JSON or text files, or from a central Hash Sets Manager in your lab, so that AXIOM Process searches for files in the evidence with matching hash values.

CALCULATE HASHES AND FIND MATCHES

ANALYZE CHATS WITH MAGNET.AI

Enable chat categories so that Magnet.AI automatically categorizes chat conversations, based on the categories you select, and tags them in AXIOM Examine.

ANALYZE CHATS WITH MAGNET.AI

BACK

GO TO ARTIFACT DETAILS

Here you can tweak all properties for what the software will look for when it scans the image file system/

After clicking the Go to Analyze Evidence button, you will be taken to this screen.

ARTIFACT DETAILS

CASE DETAILS

EVIDENCE SOURCES 1

PROCESSING DETAILS

- Search archives and mobile backups On
- Decode file-based encryption On
- Add keywords to search On
- Extract text from files (OCR) On
- Calculate hashes and find matches On
- Analyze chats with Magnet.AI On
- Analyze pictures with Magnet.AI On
- Search with YARA rules On
- Find more artifacts

ARTIFACT DETAILS 256

- Mobile artifacts 256 of 269
- Cloud artifacts
- Computer artifacts
- Vehicle artifacts
- Parse and carve artifacts
- Privileged content
- Date range filter

ANALYZE EVIDENCE

COMPUTER ARTIFACTS

0 of 263 apps are included in the case

[CUSTOMIZE COMPUTER ARTIFACTS](#)

MOBILE ARTIFACTS

256 of 269 apps are included in the case

[CUSTOMIZE MOBILE ARTIFACTS](#)

CLOUD ARTIFACTS

0 of 123 apps are included in the case

[CUSTOMIZE CLOUD ARTIFACTS](#)

VEHICLE ARTIFACTS

0 of 1 apps are included in the case

[CUSTOMIZE VEHICLE ARTIFACTS](#)

PARSE AND CARVE ARTIFACTS

By default, AXIOM will parse and carve all selected artifacts

[SELECT PARSING AND CARVING OPTIONS](#)

PRIVILEGED CONTENT

Exclude or tag privileged content using keywords

[SELECT PRIVILEGED CONTENT OPTIONS](#)

DATE RANGE FILTER

Filter artifact hits based on date range window

[SELECT DATE RANGE FILTER](#)

[BACK](#) [GO TO ANALYZE EVIDENCE](#)

Here you can tweak what the software does with parsing the artifacts in the image.

The next screen verifies that you have the data that you want. Click the Analyze Evidence button to process the data.

After the software successfully processes the image, you will be taken to Magnet AXIOM Examine. This is where you can get all of the info you need.

File Tools Process Help

Case dashboard

CASE OVERVIEW

EVIDENCE SOURCES 1

Google Pixel 3a XL Logical Image - Data.tar

INSIGHTS

Potential Cloud Evidence Leads 3

CASE SUMMARY NOTES

Record your case summary notes here. These notes will appear in the case report when the setting is enabled.

Examiner name

Case summary

CASE PROCESSING DETAILS

CASE NUMBER

SCAN 1

Scanned by

Scan date/time - local time 2023-04-28 21:36:03

Scan description

[VIEW SCAN SUMMARY](#)

PROJECT REVIEW ONLINE

You can integrate Magnet AXIOM with the Project REVIEW Online beta, a SaaS platform that allows users to review and collaborate with important stakeholders. [SHOW MORE](#)

CASE INFORMATION

The Case Information.txt file contains information about how the case was processed. For example, the file includes the settings that were applied to the search, search type, number of artifacts discovered, and more.

[OPEN CASE INFORMATION FILE](#)

The AXIOMExamine.log file contains information about any errors encountered, jobs that were run, and general debugging information.

[OPEN LOG FILE](#)

EVIDENCE OVERVIEW

[ADD NEW EVIDENCE](#)

GOOGLE PIXEL 3A XL LOGICAL IMAGE - DATA... (42,797)

[VIEW EVIDENCE FOR THIS SOURCE ONLY](#)

Evidence number Google Pixel 3a XL Logical Image - Data.tar

Description

Location Google Pixel 3a XL Logical Image - Data.tar

Platform Mobile

Process method Parsing and carving

[CHANGE PICTURE](#)

PLACES TO START

ARTIFACT CATEGORIES

[VIEW ALL ARTIFACT CATEGORIES](#)

Evidence source Google Pixel 3a XL Logical Image - Data.tar

Number of artifacts 42,797

Media 28,640

Application Usage 9,321

Web Related 2,927

Refined Results 496

Social Networking 318

Custom 245

TAGS AND COMMENTS

IDENTIFIER MATCHES

Magnet AXIOM can compare identifiers found in this case with identifiers from other cases that your organization has uploaded to the Magnet Prague database. These identifiers can include people identifiers, such as email addresses or phone numbers, and device identifiers, such as camera serial numbers or phone IMEI.

For more information and to download a beta copy of the Magnet Prague server software, visit Magnet Idea Lab.

<https://magnetideallab.com/> COPY URL

Once you have installed the Magnet Prague server software, configure product integration settings to connect Magnet AXIOM to Magnet Prague.

[CONFIGURE PRODUCT INTEGRATIONS](#)

MAGNET.AI CATEGORIZATION

KEYWORD MATCHES

POTENTIAL CLOUD EVIDENCE LEADS (3)

Magnet AXIOM discovered the following cloud accounts in the evidence. With AXIOM Cloud, you can attempt to access accounts using available credentials to acquire cloud evidence. Alternatively, you can try other methods such as public data acquisition, processing user-downloaded packages, or warrant returns.

Time zone UTC+000

On this screen you can start by going through any of the artifact categories. For instance, you can check the Media Files to view all of the media files on the device. This is what your screen might look like.

The screenshot displays the Magnet Axiom interface. On the left, a sidebar lists artifact categories with their counts: MATCHING RESULTS (42,797), REFINED RESULTS (496), CLASSIFIEDS (10), CLOUD SERVICES (5), FACEBOOK (22), GOOGLE SEARCHES (68), IDENTIFIERS - DEVICE (27), IDENTIFIERS - PEOPLE (233), PASSWORDS AND TOKENS (93), REBUILT WEBSITES (2), SOCIAL MEDIA (4), USER ACCOUNTS (24), WEB CHAT (6), WEB RELATED (2,927), COMMUNICATION (102), SOCIAL NETWORKING (318), MEDIA (28,640), EMAIL & CALENDAR (237), and DOCUMENTS (171). The 'MEDIA' category is expanded, showing sub-categories like AMR Files (22), Audio (8), Carved Audio (58), Photoshop Files (9), Pictures (28,311), and Videos (232). The main panel shows 'MATCHING RESULTS (28,311 of 28,311)' with a table of artifacts. The table has columns for Image, File, File..., Crea..., Last..., Last..., Size..., Skin..., Orig..., Orig..., Exif..., and Crea... The table lists various image files with their sizes, skin tones, and extraction status. On the right, a detailed view of artifact 1096 is shown, titled 'Google Pixel 3a XL Logical Image - Data.tar'. It includes a preview, details, and evidence information.

Image	File	File...	Crea...	Last...	Last...	Size...	Skin...	Orig...	Orig...	Exif...	Crea...
1096	0.0	41	41	Complete							
1243	0.0	41	41	Complete							
1098	0.0	96	48	Complete							
2119	0.0	180	180	Complete							
1605	0.0	84	84	Complete							
1520	0.0	120	120	Complete							
1731	0.0	54	54	Complete							
1544	0.0	128	64	Complete							
1526	0.0	54	54	Complete							
1036	0.0	56	56	Complete							
3415	0.0	121	131	Complete							
1500	0.0	62	70	Complete							
2310	0.0	112	112	Complete							
2787	0.0	240	240	Complete							
1096	0.0	41	41	Complete							
1243	0.0	41	41	Complete							
1098	0.0	96	48	Complete							
1208	0.0	96	96	Complete							
2463	0.0	81	81	Complete							
2834	0.0	81	81	Complete							
1779	0.0	192	72	Complete							
2572	0.0	360	360	Complete							
1526	0.0	54	54	Complete							
2305	0.0	192	96	Complete							
1166	0.0	144	60	Complete							
1731	0.0	54	54	Complete							
3917	0.0	168	168	Complete							
2505	0.0	108	108	Complete							
2816	0.0	108	108	Complete							
170132	4.7	300	300	Complete							
1208	0.0	96	96	Complete							

1096
Google Pixel 3a XL Logical Image - Data.tar

PREVIEW

EXPAND PREVIEW ZOOM 100%

DETAILS

ARTIFACT INFORMATION

Size (Bytes) 1096
Skin Tone Percentage 0.0
Original Width 41
Original Height 41
Exif Extraction Status Complete
Exif Data
Extraction Result: Complete
ImageWidth: 41
ImageHeight: 41
MDS Hash 96b0718bc8767424182c8982a67b3
SHA1 Hash 3457dbcf56efdd13bd658a038c93c9be1ef7ce5
Artifact type Pictures
Item ID 23

EVIDENCE INFORMATION

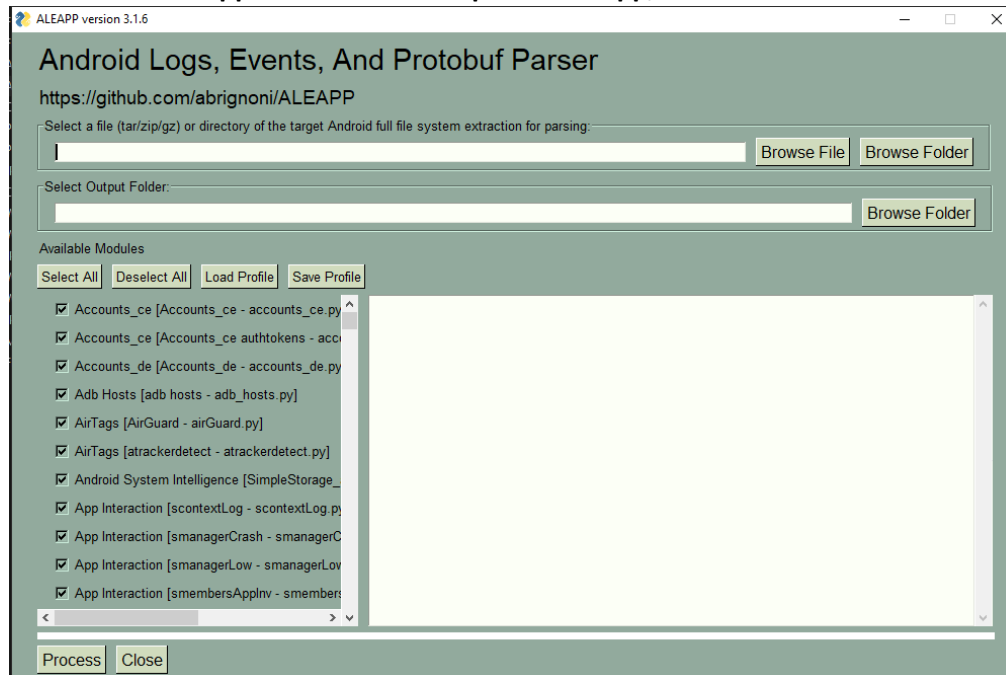
Source Google Pixel 3a XL Logical Image - Data.tar\data
Recovery method Carving
Deleted source
Location File Offset 6254796
Evidence number Google Pixel 3a XL Logical Image - Data.tar

From this screen you can filter all of the artifacts the software found. Expand/contract any of the categories on the left to see more/less data from each category.

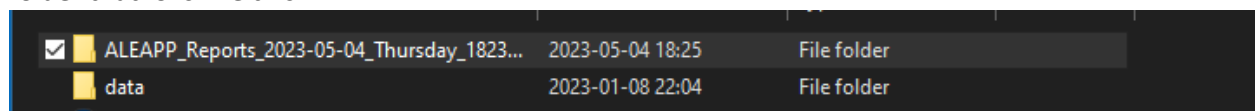
At this point, you have all of the basics you need to navigate Magnet Axiom. There are a few advanced techniques that I learned, but you can get by without them since most data is better found through the files or ALEAPP,

Android Logs Events And Protobuf Parser (ALEAPP)







































To download AEAPP, I went to <https://github.com/abrignoni/ALEAPP/releases> and downloaded aleappGUI.exe. When I opened the app, I saw this screen



Now select your tar file and a folder to output the results to. Press Process. It will spit out a folder that looks like this



Opening it reveals this:

	_elements	2023-05-04 18:25	File folder	
	_KML Exports	2023-05-04 18:24	File folder	
	_Timeline	2023-05-04 18:25	File folder	
	_TSV Exports	2023-05-04 18:25	File folder	
	Browser Cache	2023-05-04 18:25	File folder	
	Call Logs	2023-05-04 18:24	File folder	
	Cast	2023-05-04 18:24	File folder	
	Contacts	2023-05-04 18:24	File folder	
	Gboard Keyboard	2023-05-04 18:24	File folder	
	Google Call Screen	2023-05-04 18:24	File folder	
	Google Chat	2023-05-04 18:24	File folder	
	Google Now & QuickSearch	2023-05-04 18:25	File folder	
	Google Photos	2023-05-04 18:25	File folder	
	Image Manager Cache	2023-05-04 18:25	File folder	
	Offline Pages	2023-05-04 18:25	File folder	
	RCS Chats	2023-05-04 18:25	File folder	
	Recent Activity	2023-05-04 18:25	File folder	
	Script Logs	2023-05-04 18:23	File folder	
	SQLite Journaling	2023-05-04 18:25	File folder	
	temp	2023-05-04 18:24	File folder	
	Usage Stats	2023-05-04 18:25	File folder	
	User Dictionary	2023-05-04 18:25	File folder	
	WiFi Profiles	2023-05-04 18:25	File folder	
	Account Data.html	2023-05-04 18:25	Firefox HTML Doc...	31 KB
	accounts_ce_0.html	2023-05-04 18:25	Firefox HTML Doc...	29 KB
	accounts_de_0.html	2023-05-04 18:25	Firefox HTML Doc...	29 KB
	ADB Hosts.html	2023-05-04 18:25	Firefox HTML Doc...	29 KB
	Android 11 Roles_0.html	2023-05-04 18:25	Firefox HTML Doc...	31 KB
	App Icons.html	2023-05-04 18:25	Firefox HTML Doc...	1,699 KB
	App Updates (Frosting.db).html	2023-05-04 18:25	Firefox HTML Doc...	70 KB
	Appops.xml Setup Wizard.html	2023-05-04 18:25	Firefox HTML Doc...	30 KB
	Appops.xml.html	2023-05-04 18:25	Firefox HTML Doc...	130 KB
	Authtokens_0.html	2023-05-04 18:25	Firefox HTML Doc...	90 KB
	Bluetooth Adapter Information.html	2023-05-04 18:25	Firefox HTML Doc...	29 KB
	Bluetooth Connections.html	2023-05-04 18:25	Firefox HTML Doc...	29 KB
	Calendar - Calendars.html	2023-05-04 18:25	Firefox HTML Doc...	29 KB
	Cello.html	2023-05-04 18:25	Firefox HTML Doc...	31 KB
	Chrome - Autofill - Entries.html	2023-05-04 18:25	Firefox HTML Doc...	29 KB

For most of the data needs, you can find in the HTML files. Start with the Account Data.html file. This is what you will see first.

272023204347291. Find this easily on the ALEAPP device info report.

Case Information

Details

Device details

Script run log

Processed files list

Android version per Usagestats: 12
Codename per Usagestats: REL
Build version per Usagestats: 8177914
Bluetooth name: Pixel 3a XL
Bluetooth address: 58:CB:52:4E:67:55
SIM Number & IMSI: None - None
SIM Display Name: CARD
SIM Number & IMSI: - 272023204347291
SIM Display Name: 3
Last Boot Timestamp: 2023-01-09 06:04:28

Out with the old and in with the new!

What version of andriod was on the system?

12. If you use ALEAPP, find this artifact in the OS Version report.

Key	Value
Android Version	12
Build version	8177914
Codename	REL
Key	Value

Showing 1 to 2 of 2 entries

Let's address this question

What is the bluetooth mac address of this device?

58:cb:52:4e:67:55. Find this in the ALEAPP Bluetooth Adapter Information Report.

Key	Value
Address	58:cb:52:4e:67:55
DiscoveryTimeout	120
FileSource	Empty
LE_LOCAL_KEY_DHK	dc16a18b0d9a166d8aeadea7effeadc5
LE_LOCAL_KEY_ER	e2edf47b90b567a0455072582cca2faa
LE_LOCAL_KEY_IR	caf320a1fd72b343b767ca0742f57bbe
LE_LOCAL_KEY_IRK	678309337de9184877dbce2cf783ccff
Salt256Bit	113b013352dd03a6810e234ea355eb0616806f6e3d4837ea8df4f38165e07015
ScanMode	0
TimeCreated	2022-11-30 22:37:01
Key	Value

Somebody is picky!

What timezone was selected for the users Calendar?

UTC. Find this in the ALEAPP Calendar-calendars report

Created Timestamp	Calendar Name	Calendar Display Name	Account Name	Account Type	Visible	Calendar Location	Timezone	Owner Account	Is Primary	Color	Color Index
2022-11-30 22:53:55	tlouis@kurvalis.com	tlouis@kurvalis.com	tlouis@kurvalis.com	com.google	Yes		UTC	tlouis@kurvalis.com	Yes	-6299161	14
Created Timestamp	Calendar Name	Calendar Display Name	Account Name	Account Type	Visible	Calendar Location	Timezone	Owner Account	Is Primary	Color	Color Index

Wa-was that a gh-gh-ghost?

What is the android id of this device?

Key	Value
Android Version	12
Build version	8177914
Codename	REL
Key	Value

Showing 1 to 5 of 5 entries

Built Different

What is the build version of this device?

8177914. This can be found in the OS Version report of ALEAPP

Key	Value
Android Version	12
Build version	8177914
Codename	REL
Key	Value

Showing 1 to 5 of 5 entries

Never track a user by their username...

What was the GUID for the primary account registered to this device?

Let me [auto]fill you in on the deets

What name is set in chrome autofil entries?

Operation Outsource. Found in the ALEAPP Chrome Autofill entries report

Date Created	Field	Value	Date Last Used	Count
2022-12-15 02:49:26	name	Operation Outsource	2022-12-15 02:49:26	1
2022-12-22 02:52:36	username	wilts1991@protonmail.com	2022-12-22 02:52:36	1
Date Created	Field	Value	Date Last Used	Count

This one is plain and simple!

What was the password of the hotspot on this device?

enc8px7tpftac4c. Find this in the WiFi Hotspot report of ALEAPP

Who needs user privileges?

What software that may aid in privilege escalation exists on this device?

Magisk. This is the easiest thing to find. It's right in front of you when you unpack the files.

incremental	2022-11-30 14:36	File folder
local	2022-11-30 14:36	File folder
lost+found	2022-11-30 14:36	File folder
magisk_backup_3d9a9efa20ddafed407...	2023-01-08 21:59	File folder
media	2022-11-30 14:37	File folder
mediadrms	2022-11-30 14:36	File folder

My favorite kind of boot, other than cowboy boots of course

What is the last boot time in UTC associated with this device? (FORMAT YYYY-MM-DD HH:MM:SS based on 24 hour clock)

2023-01-09 06:04:28: Found in Last Boot Time Report from ALEAPP.

Timestamp	File Name
2023-01-09 06:04:28	last_boot_time_utc
Timestamp	File Name

What time is it? Twitter time!

When was the last time in UTC the twitter account typed their password? (FORMAT YYYY-MM-DD HH:MM:SS based on 24 hour clock)

2022-12-18 09:42:51. Found in the ALEAPP Accounts_de report

Last password entry	Name	Type
2022-11-30 22:53:13	tlouis@kurvalis.com	com.google
2022-12-18 09:42:51	LTina1900	com.twitter.android.auth.login

Com with me on an adventure

What is the application package name of the messaging app with the most number of messages received?

In Magnet Axion Examine, go to the communications tab within your case. After that notice that the second subcategory has the most. Find the package name by scrolling down the details panel at the right. You will find the following

com.google.android.apps.messaging

That is your answer!

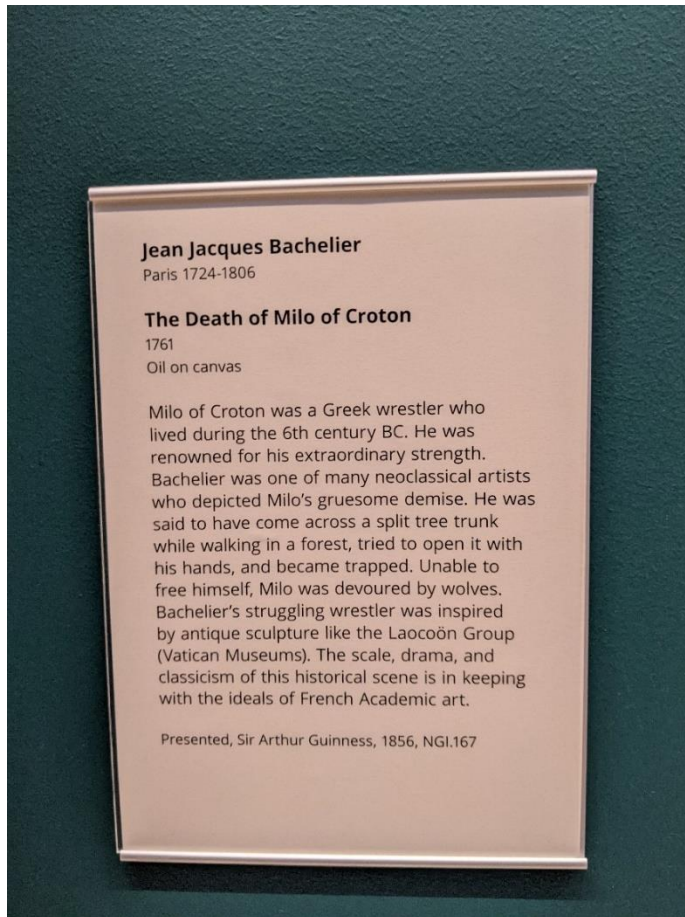
Got2Sell. Go to *ALEAPP Chrome Login data report*

Created Time	Username	Password	Origin URL	Blacklisted by User	Browser Name
2022-12-03 03:01:20	Wilts1991@protonmail.com	Got2Sell	android://iUMtL0i8Zd1gBiZHTUebf0hT1dohNEYVhkbrvIM_X55_1mD3J8zoSHMmsS6CcWlJ76DDWAdcUF7H8YDRYWtw==@com.fiverr.fiverr/	0	Chrome
2022-12-03 03:04:09	wilts1991@protonmail.com	Suam6is3eik	android://aOxyoiW7Q5diMxdB7TEKZ9q_kJ_UL8rTVs9BnD_7hyIAHM1G4FevHZuieXyRu7MgvoQwnB6pUY-CW26fHe0ZQw==@ch.protonmail.android/	0	Chrome
Created Time	Username	Password	Origin URL	Blacklisted by User	Browser Name

Italian beast!

What animals killed the figure who was renowned for his strength?

Wolves. Find the answer in /data/media/0/DCIM/Camera. This is the image you are looking for



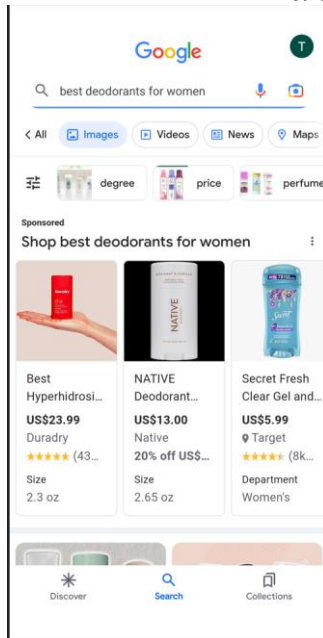
You always forget something when traveling...

This user seems to have been shopping for some sort of personal hygiene item, what was the price of the red item?

\$23.99. Find this evidence in the location

/data/dat/com.google.android.googlequicksearchbox/files/recently/tlouis@kurvalis.com-

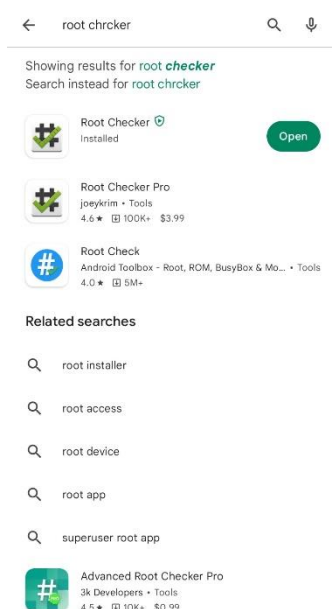
7133291355466100338.jpg



Thr answrr is right infront of you!

This user installed an app on the phone relating checking privledges. What did the user specifically search for in the appstore when lookingnng for it?

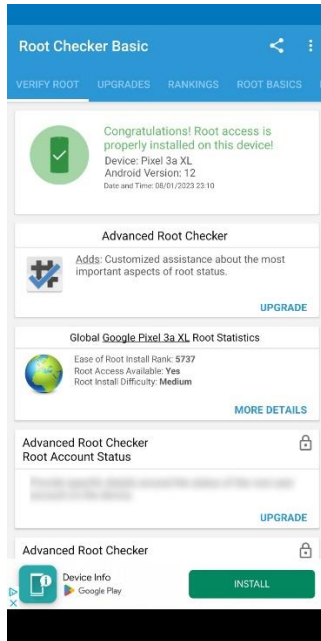
root chrcker. See the image at /data/system_ce/snapshots/121.jpg



Easy Peasy

What was the "Ease of Root Install Rank" of this device?

5737. See this image from /data/system_ce/snapshots/134.jpg



These new phones battery life can sure last a long time...

What was Tinas battery % when she entered the Copenhagen timezone?

83. Find this in the Turbo - Phone Battery report in ALEAPP. Modify the Show: filter to "All" and scroll down till you see 2022-12-04 18:03:57 on the time column. You will see that the column directly to the left of the time shows 83. That is our answer.

2022-12-04 12:07:55	84			Europe/Dublin
2022-12-04 18:03:57	83			Europe/Copenhagen
2022-12-04 18:07:17	82			Europe/Copenhagen
2022-12-05 01:37:55	81			Europe/Copenhagen
2022-12-05 04:37:55	80			Europe/Copenhagen

How low did we go?

It seems Tina did a lot of traveling. What was Tinas battery percentage when she left the Copenhagen timezone?

44. Keep scrolling down on the report from the result of the previous question. Look at the entry to the right of 2022-12-07 08:27:53. Find this answer to the right of that time.

2022-12-07 07:17:53	45			Europe/Copenhagen
2022-12-07 08:27:53	44			Europe/Copenhagen
2022-12-07 10:27:22	43			Europe/Dublin
2022-12-07 10:28:37	42			Europe/Dublin

One email isn't enough...

What email address is associated with this device that is NOT a gmail account?

I used Magnet Axiom Examine for this one. I looked at the protonmail contacts and found this one wilts1991@protonmail.com . Entering it was the correct answer

	From	To	Subject	Date/Time	Type	Body
	MAILER-DAEMON@protonmail.com	Wilts1991@protonmail.com	Undelivered Mail Returned to Sender	2022-12-04 00:52:17	Incoming	
	info@twitter.com	wilts1991@protonmail.com	B/R Football Tweeted: Bryan Mbeumo finishes off Li...	2023-01-02 20:51:58	Incoming	
	info@twitter.com	wilts1991@protonmail.com	abigail thaw Tweeted: Would have been 81 today. H...	2023-01-04 05:42:07	Incoming	
	no-reply@notify.proton.me	Wilts1991@protonmail.com	Get more out of your inbox	2022-12-21 19:23:34	Incoming	
	info@twitter.com	wilts1991@protonmail.com	Sarah McInerney Tweeted: Actual tears.	2022-11-19 02:36:39	Incoming	
	workspace-noreply@google.com	wilts1991@protonmail.com	Your Google Account password for kurvalis.com has...	2022-12-08 03:09:11	Incoming	
	no-reply@news.proton.me	Wilts1991@protonmail.com	Win a Lifetime account in Proton's Charity Fundraiser!	2022-12-22 23:14:18	Incoming	
	info@twitter.com	wilts1991@protonmail.com	PSG Report Tweeted: Neymar's reaction to Leo Mess...	2023-01-05 00:21:15	Incoming	
	info@twitter.com	wilts1991@protonmail.com	Independent.ie Tweeted: Two teens and a woman in...	2022-12-21 03:37:51	Incoming	
	notify@twitter.com	wilts1991@protonmail.com	@LTina1900, check out the notifications you have o...	2022-12-30 07:06:50	Incoming	
	no-reply@notify.proton.me	Wilts1991@protonmail.com	Improve your account security	2022-11-18 19:23:33	Incoming	

How many is too many...

It seems that this user may have recieved a document with some PII. How many different individuals are listed in this document.

A: 5. Look in banana_split(1).pdf. There is XML code in it that shows 5 objects that are people

```

[
  {
    "SammyCare": "Reagan Conley",
    "date": "Dec 26, 2007",
    "email": "aliquet.sem@protonmail.couk",
    "company": "BH11712842341853418751"
  },
  {
    "SammyCare": "Edward Sykes",
    "date": "Dec 26, 2007",
    "email": "auctor@protonmail.org",
    "company": "AD5822625809122233483518"
  },
  {
    "SammyCare": "Constance Joseph",
    "date": "Dec 26, 2007",
    "email": "vel@icloud.edu",
    "company": "MK15177498541079748"
  },
  {
    "SammyCare": "Flynn Pollard",
    "date": "Dec 26, 2007",
    "email": "psum.sodales@yahoo.com",
    "company": "KW6825896229234874757444413396"
  },
  {
    "SammyCare": "McKenzie Rodgers",
    "date": "Dec 26, 2007",
    "email": "vehicula.pellentesque@outlook.edu",
    "company": "SA4476857582675731568062"
  }
]

```

Danger is my middle name

What was the danger type of magisk?

Dangerous But User Validated. Navigate to the ALEAPP Chrome - Downloads report and see that the "Danger Type" column says "Dangerous But User Validated".

Start Time	End Time	Last Access Time	URL	Target Path	State	Danger Type	Interrupt Reason	Opened?	Received Bytes	Total Bytes
2022-11-30 22:54:59	2022-11-30 22:55:32	2022-11-30 22:55:36	https://en.softonic.com/download/magisk-manager/android/post-download	content://media/external/downloads/19	Complete	Dangerous But User Validated		1	11278270	11278270
Start Time	End Time	Last Access Time	URL	Target Path	State	Danger Type	Interrupt Reason	Opened?	Received Bytes	Total Bytes

Quite a leniant game!

It seems this user downloaded a game. How many hints were they allowed in the game?

57. This was a random guess. I did not know where to look for this one.

A love story?

It seems that Tina had intentions of spawning some sort of office romance, as she searched for the legality behind it. What was the article called that gave her the answer to her question?

Can an Employer Prohibit Workplace Dating?. Find this in ALEAPP chrome Web History report.

2022-12-23 20:44:51	https://www.rocketlawyer.com/business-and-contracts/employers-and-hr/company-policies/legal-guide/can-an-employer-prohibit-workplace-dating#:~:text=Although%20employers%20may%20implement%20policies,coworker%20out%20on%20a%20date.	Can an Employer Prohibit Workplace Dating? - Rocket Lawyer	1	0	58	
---------------------	---	--	---	---	----	--

UNSOLVED:

CIPHER

people Online keep telling me my Style Suxx

uses cat2.png

Rapidly making my way through the Machete Order

IkImIHlvdSBvbmX5IGtuZXcgdGhlIHVvd2VyIG9mIHRoZSBkYXJrIHNPZGUiDigJQoVGhIEVtcGlyZSBTdHJpa2VzIEJhY2spCgo=

CIPHER

What is three's address?

What phone number sent the most andriod SMS messages?

(3/3 attempts used)

50333

Just a second

How many motion photos were taken with the devices own camera?

(3/3 Attempts used)

Would you like a free battery? Free of charge.

When was the FIRST time in UTC this phone shut down because it ran out of battery? (FORMAT YYYY-MM-DD HH:MM:SS based on 24 hour clock)

Shhhhhh it's a secret

It seems that Tina wants to avoid mentioning something shes doing with Shawn. What is this?

Secret plans...

"It seems that Tina has been having conversations with someone she's working with. On 12/28/2022, it seems they made plans for a video call. When is this call in UTC? (FORMAT YYYY-MM-DD HH:MM:SS based on 24 hour clock)"

I am feeling thirsty...

What popular destination spot did Tina visit on 12/04/2022?

Old mans geolocation

This user traveled to Denmark, and downloaded a few applications on the same day. Of these applications, only one has a UTM_campaign parameter set in google searches relating to the application. What is the user's AppUserID for this application?