

# 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.

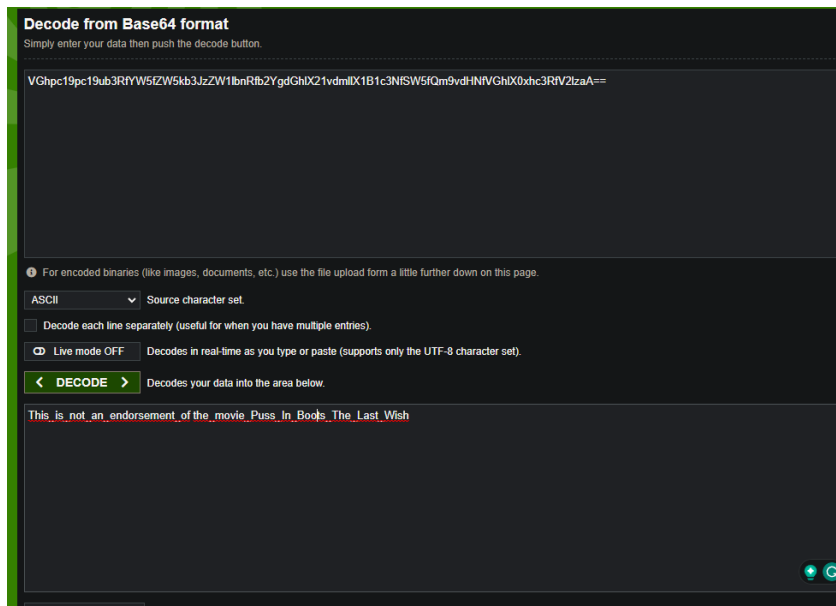
Q: (9E0:D0E960A2DDH@C5

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!

A: Put this image into a Kali VM or hex editor and find that it has the following flag at the end. Decode frn base64 first.



## SomeTimes its nicE to just stop workinG and searchH 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!

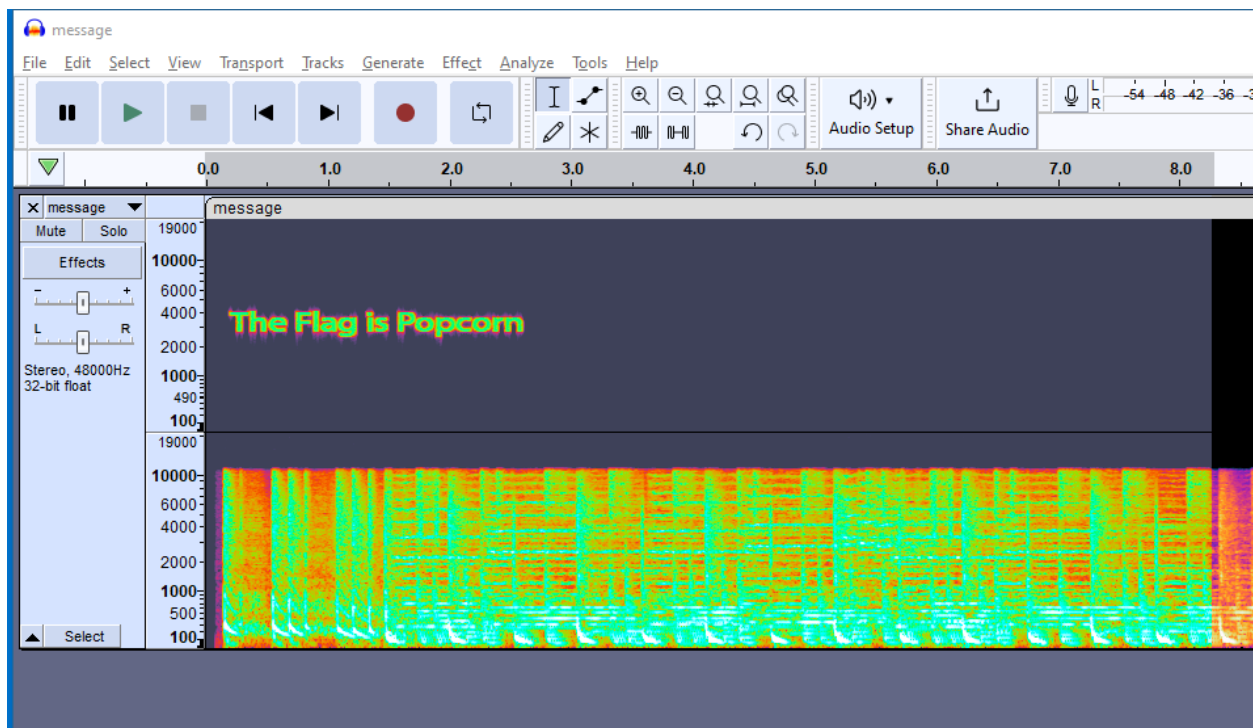
I really enjoyed the BlueMonkey 4n6 video on the last cipher questions. If you enjoy these challenges let us know!

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



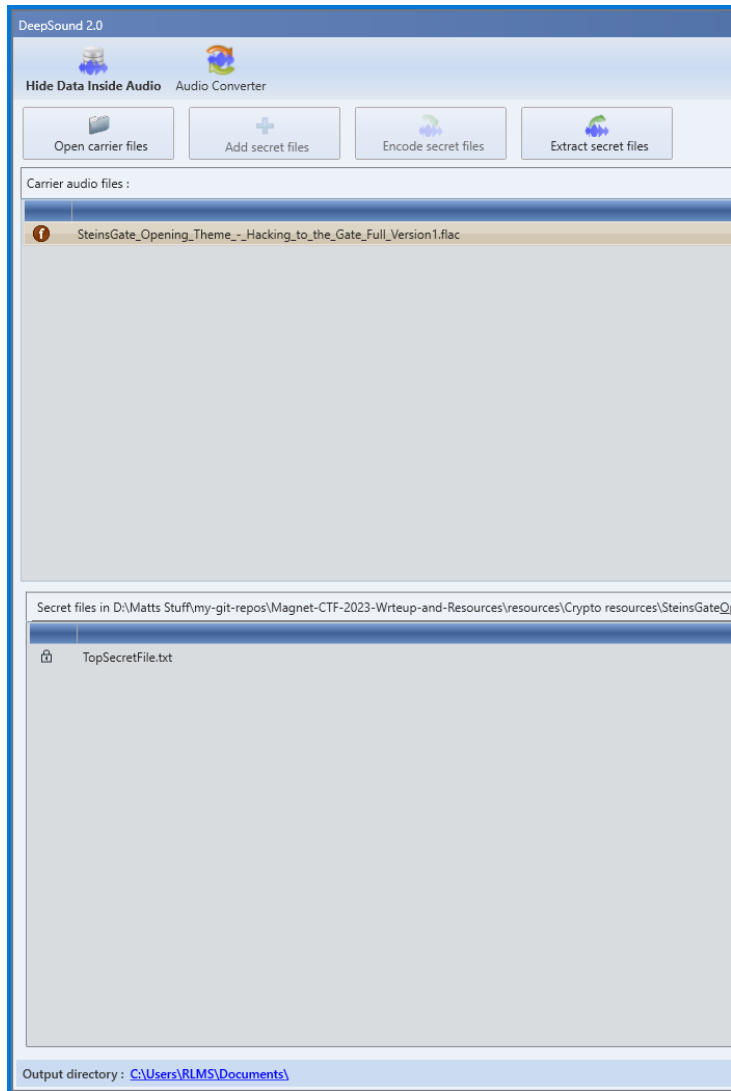
## wh1ter0se.m4v

*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](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**



File Edit Format View Help

WOW! You found another flag! Keep up the great work!

**WOW! You found another flag! Keep up the great work!**

## Cobalt Strike: A Necessary Evil?

[illegible]

VnRKdkIHoeHLMlIHOGxiN2UyZW9Zd2RxSXZORllxZ3ZhMmVvWXo5cUI2TmlxQ2VyYXIMelludGllMzE2Z  
VdKN1lucGllV3VnendOaWNkekRlMko2ZVd1b01jcHMzTnpjZmtrQWFwMVVTazFLVFVaWEFHSjFhcXJGY  
jZyU1lwbHZZWQVVRm1BackV1cHJFdkZ1RXVODuV1cGljMkp6WXBrWmRWcUUzUGJJVUhsnf1SmltN00  
4QUFCdUV1cGljBU5U1NCaWNtS1pkS3E4NWR6MnllcDRhNnJpYXhMeGFxcjdiaExxY1VzQUiXT25jWEZ  
pbWNoMkRSamM5bXVxNVd1ZzRITkpLWHhycXRKcnF2bHE1T1BjM056Y2JoTHFjWEZpbVE0bE8xamM5  
cWJqTEthK0lnQUFHoxpzTEtldklNQUF5UERLeHIJQUFNdUizTnpjREJGRlVuY0FpamIvSmRPQmNjb05DZlJ  
OL2dZRTFDNUtCZnBoNDdJY0NSYmhrRFQvTS9ISDIUYVB3YnVneU4wSGs1QzdaZFZh2dWb1VvTXpBLzd  
WaGdXQ3FsUm16S2tlcm9LbmVQYmZXUUIyVUVaUkRtSkVSazFYR1FOdVRGbEtUMDIDREJTkV3TUxRR  
XhPVTBKWfNRIBSaGdEYm5CcVpnTVVEUk1ZQTNSS1RVZE1WRkFEYlhjREZRMFRDaTRwQUVENEVUYnl  
uMzBzeEM1V2ZlQWsvTzZ6ekp4QktEMmhtZGowVGx4N0VXSXZIU01wZDVtU3p3Y0lhUHBvQXF2RUZP  
M25DcHB5VmN1N0RZdkNZNHhwQUUNZbkFSM1pldXN0Sy9mVTvWRFZzdXpUK0dadDFQZjlsL3l5Yndod  
m1pZjFFUWFBK3dHUGx3aW8vQU1iTmhnEbEhYS1dCN0RnbDdHZmk1eVh0Z1hRaWxzZXpFRnBLUXhhQjI  
MdHI1TlhMSW9sdmozSks5cchiZXVMVXc4V2h4MUwzZ2JBcUdPRjMyMEZjMIQ4OG9SREpyZHo4QTNXQ  
VN2VHdBm3hJa2dON0I5UXRCMFJuYjE2Wct3TVhXb0l1eXhHeVpOY2RVZXVGd3dyU2NidWxLeDhxYVJo  
Q2FYeldTQ2hGclBub0h0Z2RRY0FZcDNUbG9GMTNQWnJFdXFaQUFCakFHS2JBRE1BQUdLYVI3QUFBR0t  
aZTRkd3h0ejJhN0J3Y0d1cXhHdXEWbXVxK1dLYkFBTUFBR3FxmM1LWk1iV3F3ZHoyYTZEbkE2YmpWNVZ  
GcUNScKl1Q200MWlWZTN0N2F5WUFBQUFBYytETHZON2MzSHBNVm54bFRGWk5SM3gzUzBaOFICRUf  
NUmQxV3c9PScpCgoJZm9yICgkeCA9IDA7ICR4IC1sdCAkdmFyX2NvZGUuQ291bnQ7ICR4KysplHsKCQkk  
dmFyX2NvZGVbJHhdID0gJHZhcl9jb2RIWYr4XSAtYnhvciAzNQoJfQoKCSR2YXJfdmEgPSBbU3lzdGVtLlJl1b  
nRpbWUuSW50ZXJvcFNlcnZpY2VzLk1hcnNoYWxdOjPHZXREZWxlZ2F0ZUZvckZ1bmN0aW9uUG9pbmRI  
cigoZnVuY19nZXRfCHJvY19hZGRyZXNzIGtldm5lbnRsbCBWbWwXJ0dWFsQWxsb2MplCAoZnVuY19n  
ZXRfZGVsZWdhbGVfdHlwZSBAKFtJbnRQdHJdLCBbVUludDMYXSwgW1VJbnQzMl0siftVSW50MzJdKSA  
oW0ludFB0cl0pKSkKCSR2YXJfYnVmZmVYID0gJHZhcl92Y5SjbnZva2UoW0ludFB0cl06Olplcm8sICR2YXJf  
Y29kZS5MZW5ndGgsIDB4MzAwMwMwMHg0MCKKCVtTeXN0ZW0uUnVudGltZS5JbnRlcm9wU2VydmljZ  
XMuTWfYc2hhbF06OkNvcHkoJHZhcl9jb2RILCAwLCAkdmFyX2J1ZmZlciwgJHZhcl9jb2RILmXlbnmd0aCkKC  
gkKdmFyX3J1bm1lID0gW1N5c3RlbS5SdW50aW1lLkludGVyb3BTZXJ2aWNlcy5NYXJzaGFsXT06R2V0RG  
VsZWdhbGVGb3JGdW5jdGlvbIBvaW50ZXIoJHZhcl9idWZmZXIsICmdW5jX2dlldF9kZWxlZ2F0ZV90eXBII  
EAoW0ludFB0cl0pIChbVm9pZf0pKSkKfQ==

**You\_Found\_The\_C2.** Plug the base64 into a base64 decoder. You will get a powershell program. Find the following:

32ugx9PL6wAAAGJyYnNxcnVrEvFGa6hxQ2uocTtrqHEDa6hRc2sslGlpbhLqaxLjx9CXyEPA2Li6i5iluLBznFic  
muocQOoYR9rlvNFols7KCFWUaijqwAAAGum41dEayLzc6hrO2eoYwNqlvPAdWvc6mKoF6trlvVuEuprEuOP  
YuLqLmli4hvDVtJvIG8HK2Ya8lb7e2eoYwdqlvNFYqgva2eoYz9qlvNiqCeraYzYntie316eWJ7YnpieWugzwNi  
cdzDe2J6eWuoMcps3NzcfkAap1USk1KTUZXAGJ1aqrFb6rSYplvVAUk3PZrEuprEvFuEuNuEupic2JzYpkZdV  
qE3PblUHLrquJim7M8AABuEupicmJySSBicmKZdKq85dz2yHp4a6riaxLxaqr7bhLqcUsAlWOnCXfimch2DRjc  
9muq5Wug4HNJKXxrqtJrqlvq5OPc3NzcbhLqcXFimQ4lO1jc9qbjLKa+IgAAa9zsLKevlgAAyPDKxyIAAMuB3N  
zcDBFFUncAijb/JdOBccoNCFrt/gYE1C5KBfph47lcCRbhkDT/M/HH9TaPwbugyN0Hk5C7ZdVaogVoUoMzA/  
7VhgWCqlRmzKkHroKnePbfWQB2UEZRDmJERk1XGQNuTFIKT09CDBcNEwMLQExOU0JXSkfPRhgDbnBqZ  
gMUDRMYA3RKTUdMVfADbXcDFQ0TCi4pAED4ETbyn30sxCS5WfeAk/O6zzJxBKD2hmdj0Tlx7EWlveSMpd  
5mSzwclaPpoAqvEFO3nCppyVcu7DYvCY4xpACyNAR3ZHustK/fU5pDVsuZT+GZt1Pf9l/yybwhvmif1EQaA+  
wGPlwio/AMbNhgIHXXKB7Dgl7Gfi5yXtgXQilsezEFpKQxaB9Ltr5NXLlolvj3JK9s8beuLUw8Whx1L3gbAqGO  
F320Fc2T88oRDJrdz8A3WASvTwA3xlkgN7B9QtB0Rnb16X+wMXWoluyxGyZncdUeuFwwrScbulKx8qaRhC  
aXzWSChFrPnoHtgDQcAYp3TloF13PZrEuqZAABjAGKbADMAAGKaYwAAAGKZe4dwxtz2a7BwcGuqxGuq0  
muq+WKBAAAGq2mKZMbWqwdz2a6DnA6bjV5VFqCRluCm41b0e3t7ayAAAAAc+DLvN7c3HpMVn



x|TFZNR3x3S0Z8YBEAMRd1Ww==

and then put that into cyberchef with the following parameters

From Base64

Alphabet  
A-Za-z0-9+/=

☒ Remove non-alphabet chars

☐ Strict mode

XOR

Key  
35

DECIMAL

Scheme  
Standard

☐ Null preserving

You will receive this output:

**Output**

```
UH•ãðÈè###AQAPRQVH1ðEH•R`H•RcAH•R H•rPH$•JJM1ÉH1À~<a|STX, AÁÉ Ck ASonÁâiRAQH•R •B<H$onDf•XcAnVTSTXur•••###H•ÁtgH$onDP•HcAND•@ ISon
ðÄVHyÉA•4•H$onÔM1ÉH1À~AÁÉ Ck ASonÁ8uñLEtH L$ B$ E9Ñu0XD•@ $I$onDfA• FF HD•@ P$ I$onDA•EOT•H$onDAXAX•YZAXAYAZH•î ARy•XAYAZH•DC2
éOÿÿÿ]jI$Xwininet#AVI•æL•ñA•Lw&BELyÖH1ÉH1ÔM1ÂM1ÉAPAPA•Vy$ÿðèsZH•ÁA. •U$ ##M1ÉAQAQjETXAQA•W•ÆyÖEY[H•ÁH1ÔI•ÔM1ÉRH#STX•@
RRRæEU. ;yÖH•ÄH•ÄPj
_H•ñH•UÎCâyÿÿÿm1ÉRRRæ•ACKCAn{yÖ•$I **$on##HyÎ $I **$on##eðèöäson##eçÿÿÿ/2fqT#ÔNAKÜACKÖçRé.*xNÝ'÷ Ck I&ÜBÀ•?•5A³ ETDÜL$ðäÖNAK~â••ep$°•3•
&Kq ðLE Yô&ÿ;•wEÎ•$•ÿ•[Öüz#User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0) CR
#cÜ2NANX•$I Ck Ck U•ÄN&ßÎ•I•ÿbVT RS•qÜxm•X2A PFZMUL
T°±i$+KÜK! (C7Ä1)³Qvè••. "ã~J#ENQEOT" >Ü=È $O RS•ÖZ•Ä³ö•IäÜEN•ôP•B•+L¹ EOTÖ2%£Ö"~•+•B 8NAK;ACK>Qm$•Ä•%•¿•&óX=ibJ
/y$ñî•°t $IÖVÖH•$E RS ÖU$ NÈ~p, S#>hy$ÿä•@|ÜN&PGßÑ$ ENQ•PÖ.ö" B$ ðä.Ü$onK.Î<S>2X•Y|Î/~I+•S I E°•Vd•4/ B$ jãî•_ •B*•DZETX•S•Ä•
XCV$#AXÖQÜVYÖH1É•##@#A. #DLE##A•@###A°X$SâyÖH•SSH•çH•ñH•ÚA. # ##I•ÜA•DC2••âyÖH•Ä •ÄTgJf•BELH$onÄ•ÄÜxXXXH ENQ####PÄè•
ÿÿÿYou_Found_The_C2#DC34Vx
```

**(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: \*\***

yjododyjrg;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)

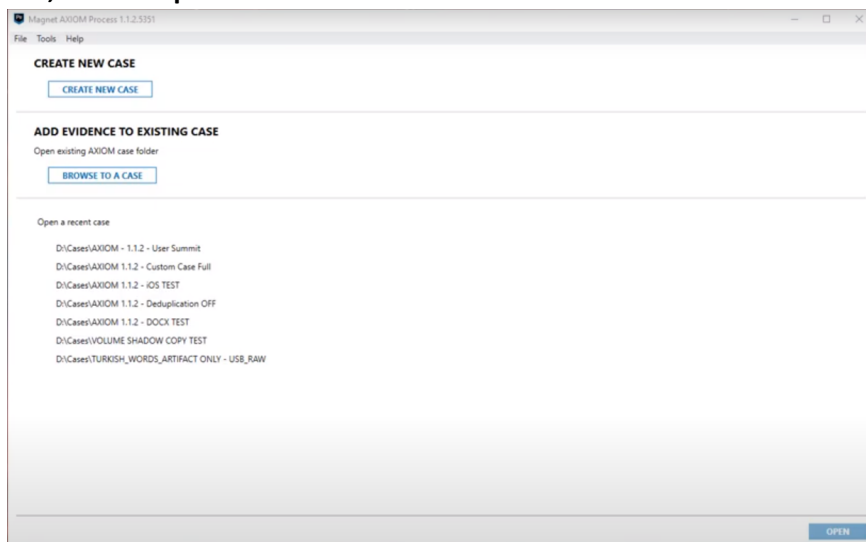
## **Process**

### **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


SELECT EVIDENCE SOURCE




COMPUTER




MOBILE



CLOUD



VEHICLE



REMOTE COMPUTER

EVIDENCE SOURCES ADDED TO CASE

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

BACK

GO TO PROCESSING DETAILS

Next you will be taken to a screen where you select the type of OS you are looking at. Select **Android**.

## 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), **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, Audio, Carved Audio, Photoshop Files, Pictures (28,311), and Videos. The main panel shows **MATCHING RESULTS (28,311 of 28,311)** in a table with columns for Image, File, File..., Crea..., Last..., Last..., Size..., Skin..., Orig..., Orig..., Exif..., and Crea... The table lists various image files with their sizes and extraction status. On the right, a detailed view for artifact **1096** is shown, titled **Google Pixel 3a XL Logical Image - Data.tar**. It includes a **PREVIEW** section with a zoomed-in image and a **DETAILS** section with **ARTIFACT INFORMATION** and **EVIDENCE INFORMATION**.

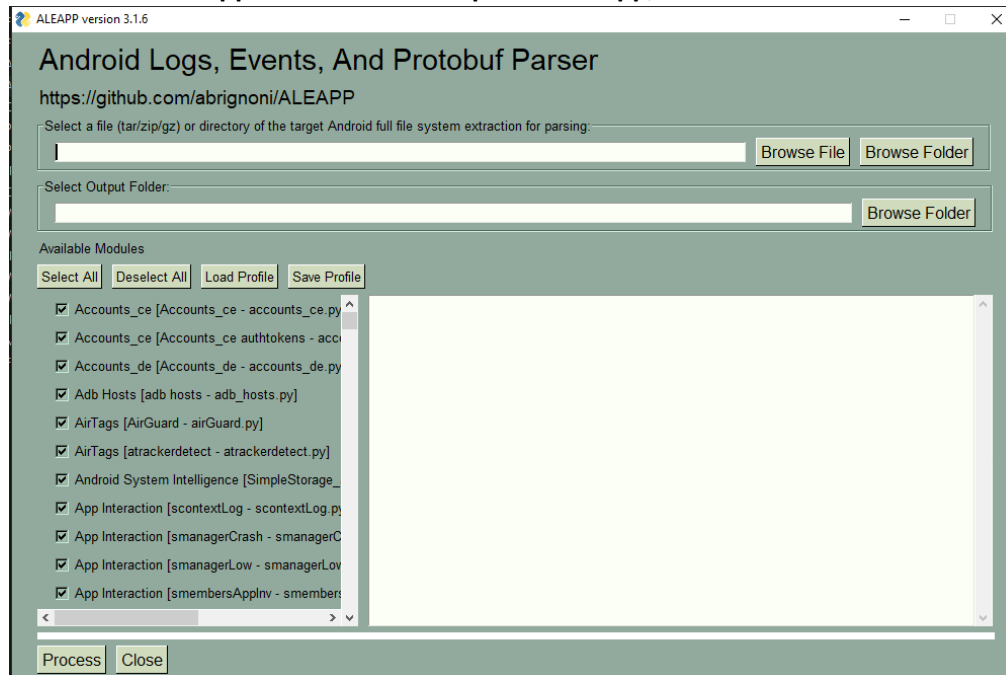
| Image  | File | File... | Crea... | Last...  | Last... | Size... | Skin... | Orig... | Orig... | Exif... | Crea... |
|--------|------|---------|---------|----------|---------|---------|---------|---------|---------|---------|---------|
| 1096   | 0.0  | 41      | 41      | Complete |         |         |         |         |         |         |         |
| 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 |         |         |         |         |         |         |         |

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.

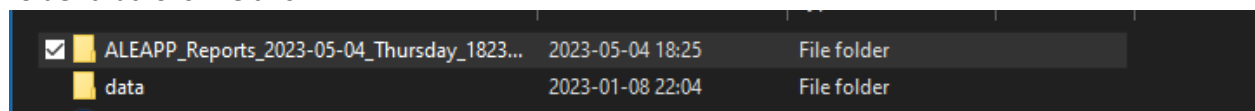
At this point, you have all of the basics you need to navigate Magnet Axiom. There are a few advanced techniques that I learned, but you can get by without them since most data is better found through the files or ALEAPP,

## 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 android 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?

b00fd41a87f574ce. Find in ALEAPP Settings Secure report

| Name              | Value             |
|-------------------|-------------------|
| android_id        | b00fd41a87f574ce  |
| bluetooth_address | 58:CB:52:4E:67:55 |
| bluetooth_name    | Pixel 3a XL       |
| mock_location     | 0                 |
| Name              | Value             |

Showing 1 to 4 of 4 entries

Previous1Next

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 4 of 4 entries

Previous1Next

Never track a user by their username...

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

102066635235203906215

Found in this bit from the Wellbeing report from ALEAPP

```

    "02:02:embedded message": {
      "01:00:Varint": 2,
      "02:01:embedded message": {
        "01:00:Varint": 2,
        "02:01:embedded message": {
          "01:00:string": "102066635235203906215",
          "02:01:string": "Tina Louis",
          "03:02:string": "tlouis@kurvalis.com",
          "05:03:Varint": 0,
          "07:04:string": "google",
          "08:05:string": "Tina",
          "09:06:string": "Louis",
          "1000:07:embedded message": {
            "01:00:Varint": 0,
            "03:01:Varint": 2
          }
        },
        "03:02:Varint": 1
      }
    }
  }
}

```

**This may be incorrect, as I cannot find any direct mention of it easily. I think I guessed on this one.**

## Let me [auto]fill you in on the deets

**What name is set in chrome autofill 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

| SSID        | Passphrase      | SecurityType |
|-------------|-----------------|--------------|
| PixieL_1463 | enc8px7tpftac4c | 1            |
| SSID        | Passphrase      | SecurityType |

## 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 Axiom 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!

|                                  |   |   |
|----------------------------------|---|---|
| <b>COMMUNICATION</b> 102         | 50333 Local User <Google Pixel 3a XL Logical Image - Data... From Three: 4G voice calling and WiFi calling has be... 2022-12-25 11:30:29 2022-12- | 3Plus and enter now at 3plus.ie/nkt. To optout of marketing messages, text OPTOUT to 50333. |
| Android Messages 23              | 50232 Local User <Google Pixel 3a XL Logical Image - Data... From Three: Welcome to United States of America... 2022-12-25 23:13:05 2022-12-      | Received Date/Time 2022-12-05 16:09:06  |
| Android Sim Card Information 2   | Google Local User <Google Pixel 3a XL Logical Image - Data... Your Messenger verification code is G-059086 2022-12-29 00:38:45 2022-12-           | Original Transmit Date/Time 2022-12-05 16:08:58   |
| Android SMS/MMS 38               | Three Local User <Google Pixel 3a XL Logical Image - Data... From Three: Your balance is low. Check options at w... 2022-12-29 17:36:25 2022-12-  | Direction Incoming  |
| Google Hangouts Cached Images 32 | 50333 Local User <Google Pixel 3a XL Logical Image - Data... From Three: Success! Go. You! Thanks for topping u... 2022-12-13 11:25:02 2022-12-   | Status Read   |
| LINE Messages 4                  | Three Local User <Google Pixel 3a XL Logical Image - Data... From Three: Your 10,000Minutes NATIONAL/ROAM... 2023-01-09 04:31:06 2023-01-         | Type SMS  |
| TextPlus Calls 3                 | Three Local User <Google Pixel 3a XL Logical Image - Data... From Three: Thanks for topping up EUR20 using Onl... 2022-12-12 01:41:23 2022-12-    | Application com.google.android.apps.messaging   |
|                                  | 50232 Local User <Google Pixel 3a XL Logical Image - Data... From Three: Welcome to Denmark. Your base rates a... 2022-12-03 20:50:24 2022-12-    | Date/Time 2022-12-05 16:09:06   |

## PineappleOnPizzalsGreat!

What WiFi network was the registered user connected to at the time the document "Banana\_split\_(1).pdf" was added to google drive?

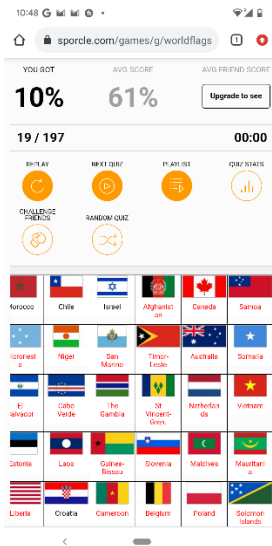
**Abo South.** A guess that was the right one. This is the final entry of the WiFi Profiles report on ALEAPP

|              |            |                 |         |          |          |                     |                 |               |                   |               |    |
|--------------|------------|-----------------|---------|----------|----------|---------------------|-----------------|---------------|-------------------|---------------|----|
| WPA_PSK      | ATT4xPB84I | "pqj37rg57t+="+ |         |          |          | 94:8f:cf:02:07:70   |                 |               |                   |               |    |
| WPA_PSK      | Abo South  | "Pepperoni"     |         |          |          |                     |                 |               |                   |               |    |
| SecurityMode | SSID       | PreSharedKey    | WEPKeys | Password | Identity | DefaultGwMacAddress | semCreationTime | semUpdateTime | LastConnectedTime | CaptivePortal | Lo |

## How many flags can you find?

At 10:48, How many flags did Tina get correct?

19. There is an image within/data/media/0/Pictures/Screenshots with some flags on it. Specifically Screenshot\_20221206-104819.png. This one has the answer on it.



## We've GotTa change the password

What was the password that the user used to log into fiver with?

Got2Sell. Go to ALEAPP Chrome Login data report

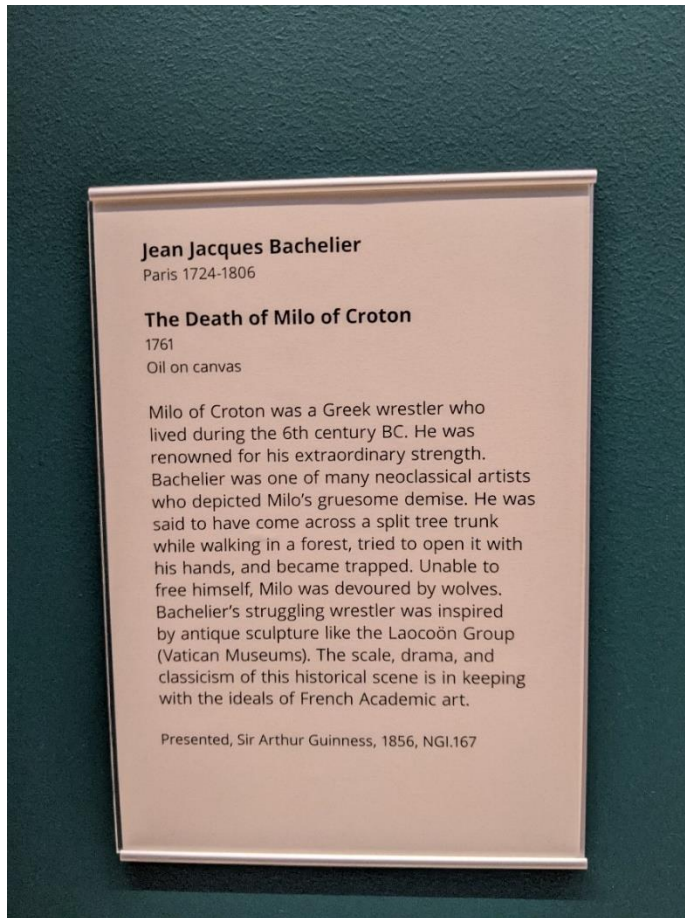
| Created Time        | Username                 | Password    | Origin URL   | Blacklisted by User | Browser Name |
|---------------------|--------------------------|-------------|--|---------------------|--------------|
| 2022-12-03 03:01:20 | Wilts1991@protonmail.com | Got2Sell    | android:///IUMtL0i8Zd1gBiZHTUebf0hT1dohNEVvhkbrvIM_X55_1mD3J8zoSHMmsS6CcWUJ76DDWAdoUF7H8YDRYWtw==@com.fiverr.fiverr/       | 0                   | Chrome       |
| 2022-12-03 03:04:09 | wilts1991@protonmail.com | Suam6is3eik | android:///aQxyoiW7Q5diMxdB7TEKZ9q_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



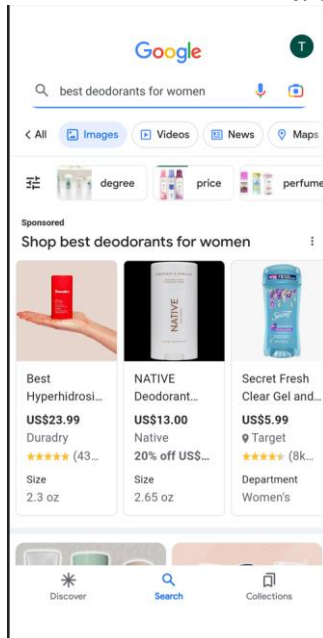
**You always forget something when traveling...**

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-

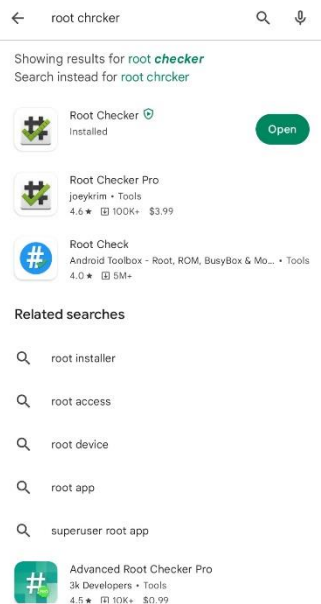
7133291355466100338.jpg



**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?**

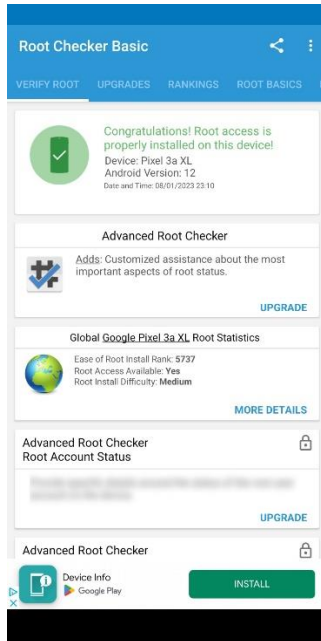
***root chrcker. See the image at /data/system\_ce/snapshots/121.jpg***



**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 Bt 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

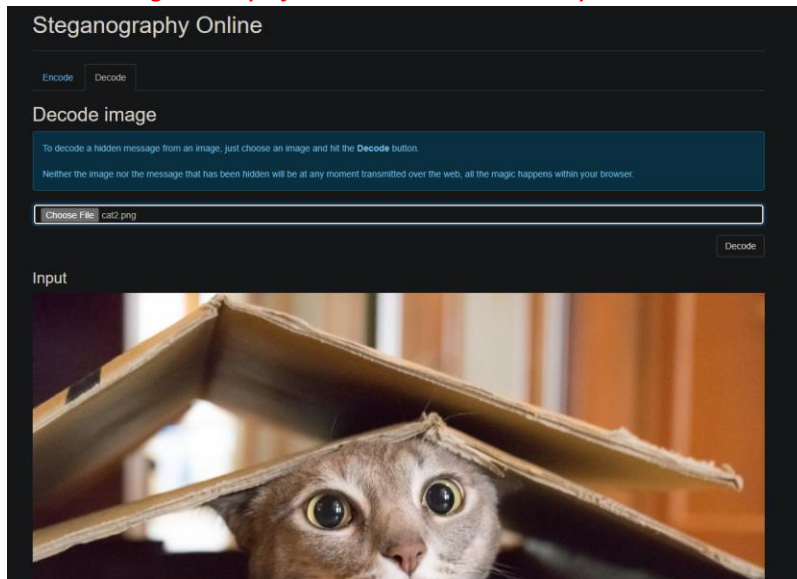
Found answers to this section from this video: <https://www.youtube.com/watch?v=KtdQyuhAZAs>

people Online keep telling me my Style Suxx

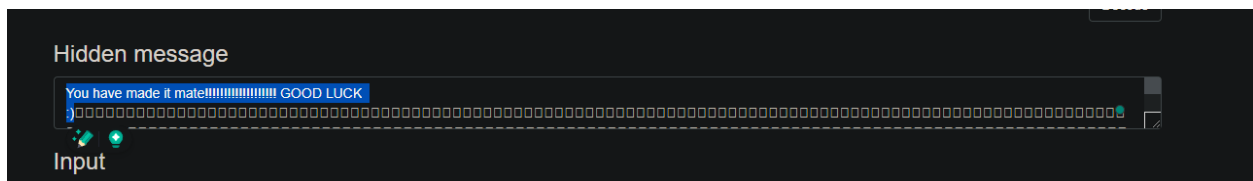
uses cat2.png

Pecial thanks to BlueMonkey 4n6 for the video!

**You have made it mate!!!!!!!!!!!!!!!!!!!! GOOD LUCK :)** For this one, look up “Style Suxx steganography online” and go to any of the tools that decode style suxx. This is an example.



*After decoding, you will see the flag.*



*Why I didn't solve: I did not realize that style suxx was a thing and thus did not get the question*

## Rapidly making my way through the Machete Order

IkImIHvdSBvbmX5IGtuZXcgdGhlIHbvd2VyIG9mIHRobSBkYXJrIHNPZGUuliDigJQoVGhIEVtcGlyZSBTdHJpa2VzIEJhY2spCgo=

**"If you only knew the power of the dark side." —(The Empire Strikes Back)** Pluc the clue into a Base64 decoder. You will see that it spits out that.

*Why I did not solve: I had that answer off the bat, but I overthought and tried cross-referencing quotes. I found nothing. When I tried entering the quote as is, It was not right.*

## FORENSICS

### What is three's address?

What phone number sent the most andriod SMS messages?

(3/3 attempts used)

50333.

Why I didn't solve: I didn't realize I was making a mistake until I had wasted all of my tries.

### Just a second

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

(3/3 Attempts used)

Why I did not solve: Parsed the clue incorrectly and did not look for the right information

### 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)

Why I did not solve: Could not find in the Battery logs or anywhere I'd thought of looking

### Shhhhhh it's a secret

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

Why I did not solve: Simply had no idea where to find

### 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)"

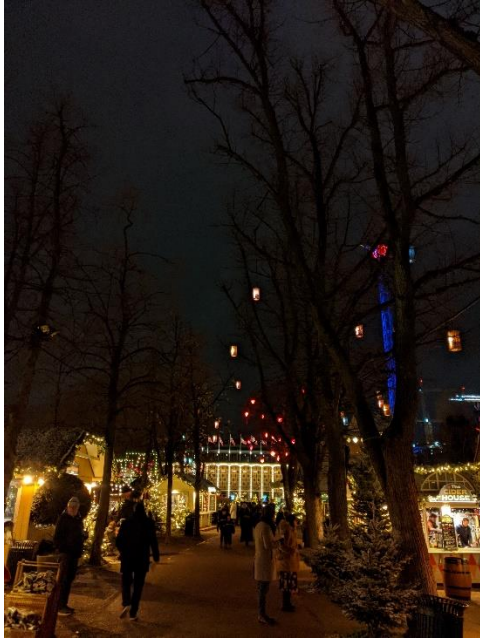
Why I did not solve: Simply had no idea where to find

### I am feeling thirsty...

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

Why I did not solve: Had no idea where to find. This image was my only lead, but it was not correct





*Specifically, this part of it*



### 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?

*Why I didn't solve: I didn't know where to find this. Given that Tina was in Denmark from 4Dec-7 Dec, I thought Fiverr and Twitter were possible matches, but I couldn't find a matching UID.*