UFO – BelkaCTF

Caos globale: aeroporti, ospedali e grandi organizzazioni vengono messi in ginocchio da improvvisi BSOD (schermi blu). il sospettato era un tempo un giornalista, ora apparentemente sostituito da... qualcosa di alieno.

Google account

Obiettivo: trovare l'account Google associato al dispositivo.

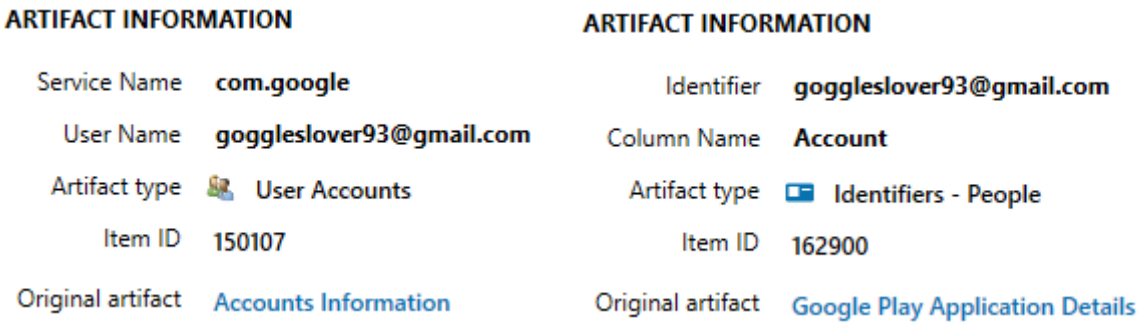


Figura 1 - Account Google

La mail dell'account Google associato al telefono è "***goggleslover93@gmail.com***".

Posizione

Obiettivo: trovare dove lavora il proprietario del telefono e la sua posizione.

Come prima cosa sono state analizzate le comunicazioni lavorative sia su WhatsApp che sulle e-mail. Si è notato come il nome del proprietario del telefono sia `Riley Stone`.

Dall'analisi delle e-mail di lavoro inviate da <`stonepresspa@runbox.com`> è possibile vedere come tutte le informazioni relative agli account degli utenti coinvolti e alle e-mail inviate e ricevute siano salvate all'interno del database denominato `EmailProvider.db`:

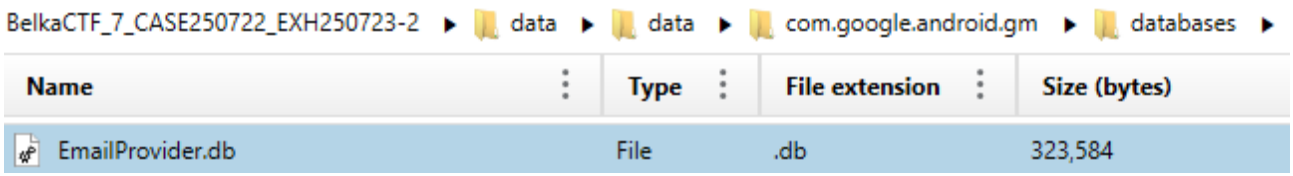


Figura 2 - Database da analizzare

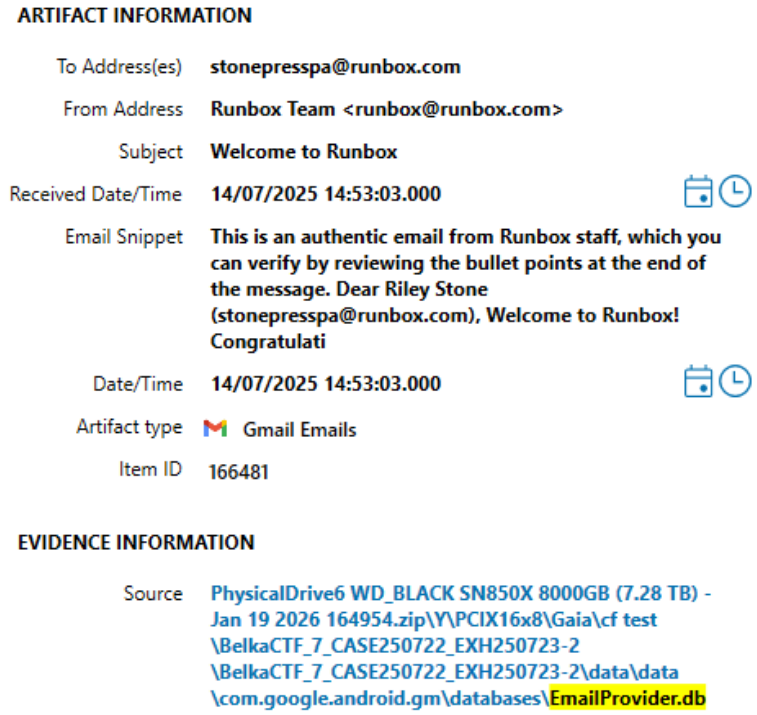


Figura 3 - E-mail esempio di lavoro

Andando ad analizzare il database con `DBrowser` o un altro tool per la visualizzazione (o anche nativamente da Magnet Axiom) si noterà una tabella denominata `Account`, nella quale sono presenti tutte le informazioni dell'account del proprietario del telefono, tra cui la firma preimpostata dall'utente:

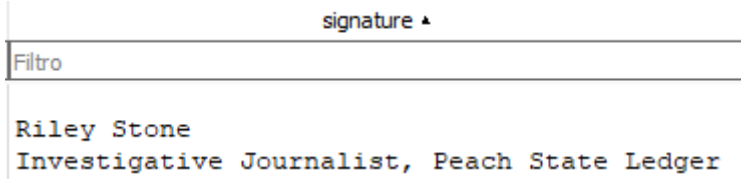


Figura 4 - Firma utente stonepresspa@runbox.com

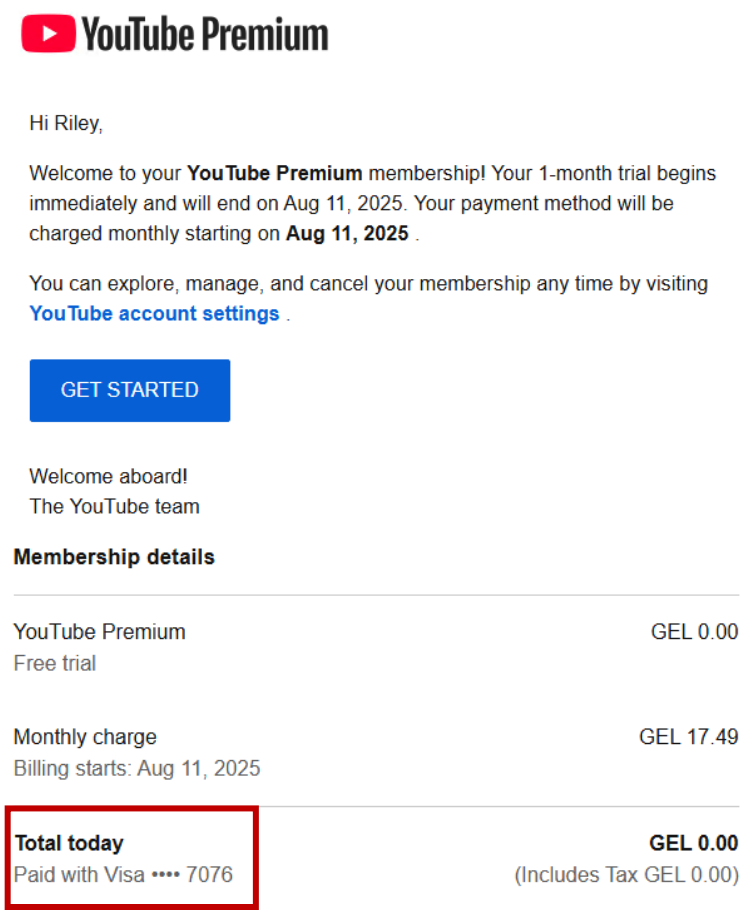
A questo punto è possibile afferma che lo stesso lavori presso **`Investigative Journalist`** a **`Peach State Ledger`**.

Banca

Obiettivo: trovare gli ultimi quattro numeri della carta della banca e il numero di telefono della banca.

Come prima cosa sono state analizzate le e-mail nelle quali si fa riferimento alla creazione di un account Google Wallet. Analizzando i file nella cartella del file system dedicata all'applicazione `<com.google.android.apps.walletnfcrel>` non sono stati trovati dati di interesse.

Si è proceduto dunque ad analizzare le e-mail relative ad un eventuale acquisto. Ne è stata trovata una riferibile all'acquisto di YouTube Premium. Dall'analisi della mail si è notato come il programma non abbia *parsato* correttamente l'`html` della mail, dunque risultava impossibile visualizzarla correttamente. Il codice è stato dunque copiato e aperto tramite browser:


YouTube Premium

Hi Riley,

Welcome to your **YouTube Premium** membership! Your 1-month trial begins immediately and will end on Aug 11, 2025. Your payment method will be charged monthly starting on **Aug 11, 2025** .

You can explore, manage, and cancel your membership any time by visiting **YouTube account settings** .

GET STARTED

Welcome aboard!
The YouTube team

Membership details

YouTube Premium Free trial	GEL 0.00
Monthly charge Billing starts: Aug 11, 2025	GEL 17.49
Total today Paid with Visa •••• 7076	**GEL 0.00** (Includes Tax GEL 0.00)

Figura 5 - YouTube Premium

Questa non era l'unica mail che si poteva prendere in considerazione per trovare le ultime cifre della carta; infatti, tra i messaggi di posta erano presenti più pagamenti:

Total charged 9.10€

PaymentIcon •••• 7076 9.10€

A temporary hold of 5€ was placed on •••• 7076 at the start of your ride. This is just used to verify your payment method and will be released once verification is complete. Learn more.

Payment Details

Card Issuer:	Visa
Authorization:	ef2d5c51-3d5d-4a69-97b3-a21bb0d65e4d - 12/07/25 17:48
Account/Card number:	**********7076

Figura 6 - Altri pagamenti trovati nella posta elettronica

Dall'immagine soprastante è possibile affermare che gli ultimi quattro numeri della carta della banca sono **7076**.

Dall'analisi delle ricerche web, è possibile affermare che la banca risulta essere `Liberty Bank`:

Web Related Potential Browser Activity	URL https://libertybank.ge/ka/agreements/liberti-angarishi
Web Related Potential Browser Activity	URL https://libertybank.ge
Web Related Potential Browser Activity	URL https://webchat.libertybank.ge
Web Related Potential Browser Activity	URL https://webchat.libertybank.ge/view/index.html
Web Related Potential Browser Activity	URL https://libertybank.ge/

Figura 7 - Info online Liberty Bank

È stato dunque esportato il database denominato `Pay` da Google Payments <`com.google.android.gms`>, ed è stato analizzato con un editor esadecimale. Si riporta di seguito quanto rinvenuto:

```
73 3a 2f 2f 77 77 77 2e 6c 69 62 65 72 74 79 62 s://www.libertyb
61 6e 6b 2e 67 65 2f 6b 61 2f 73 61 6d 61 72 74 ank.ge/ka/samart
6c 65 62 72 69 76 69 2d 69 6e 70 6f 72 6d 61 74 lebrivi-inpormat
73 69 61 2f 6d 6f 6e 61 74 73 65 6d 74 61 2d 64 sia/monatsemta-d
61 74 73 76 69 73 2d 70 6f 6c 69 74 69 6b 61 12 atsvis-politika.
0e 30 33 32 20 32 20 35 35 20 35 35 20 30 30 1a .032 2 55 55 00.
10 4c 69 62 65 72 74 79 20 42 61 6e 6b 20 4a 53 .Liberty Bank JS
43 22 36 68 74 74 70 73 3a 2f 2f 6c 69 62 65 72 C"6https://liber
74 79 62 61 6e 6b 2e 67 65 2f 6b 61 2f 61 67 72 tybank.ge/ka/agr
65 65 6d 65 6e 74 73 2f 6c 69 62 65 72 74 69 2d eements/liberti-
61 6e 67 61 72 69 73 68 69 32 12 0a 10 67 65 2e angarishi2...ge.
6c 62 2e 6d 6f 62 69 6c 65 62 61 6e 6b 3a 92 01 lb.mobilebank:'.
```

Figura 8 - Dati relativi alla banca

Il numero di telefono della banca è **032 255 5500**. Dato confermabile anche cercandola sul web.

Droga

Obiettivo: trovare una sostanza che crea dipendenza che viene menzionata nelle conversazioni.

È stato trovato un messaggio WhatsApp che è stato tradotto, al fine di verificarne il contenuto. Si riporta di seguito la traduzione:

Figura 9 - Conversazione di interesse

Controllando la formula chimica proposta all'interno del messaggio è evidente come l'elementi di cui si sta parlato sia la **caffeina**.

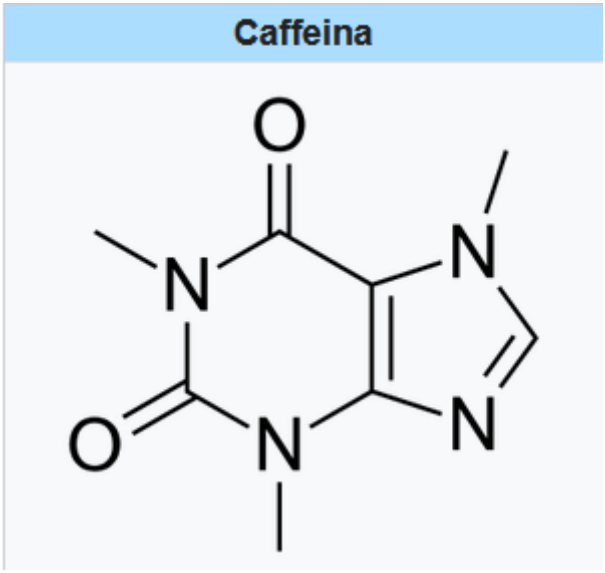


Figura 10 - Formula chimica della caffeina

Due persone scomparse

Obiettivo: trovare le due persone scomparse.

Sono state analizzate le note del dispositivo, in particolare è stato analizzato il database `keep.db` relativo all'applicazione Google Keep. Si riportano le note di interesse:

Source file	keep.db
Source file size	1,06 MB
Source table	text_search_tree_entities_content, text_search_sharing_content, text_search_note_content_content, text_search_labels_content
ID	12
Text	In Repubblica di Lirian un misterioso rapimento: agenti segreti portano la città sull'orlo delle proteste□Negli ultimi giorni, la Repubblica di Lirian è stata scossa da una notizia che ha rapidamente fatto il giro del paese. Secondo fonti non confermate, un gruppo di agenti segreti ha rapito un cittadino locale — noto attivista e figura pubblica.□Il rapimento è avvenuto il diciannove luglio alle ore sei e uno della sera, secondo l'ora locale di Lirian, che segue il fuso orario di due ore avanti rispetto all'orario di utc.□Questo evento ha suscitato un'ondata di indignazione tra la popolazione e ha portato a massicci appelli a proteste.□Secondo informazioni da familiari e conoscenti, la vittima è Ilai Jared, un uomo impegnato attivamente nella trasparenza del governo e nella lotta contro la corruzione. L'ultima volta è stato visto la scorsa settimana nel centro della capitale Lirian, dopodiché è scomparso senza lasciare tracce.□Sebbene non siano ancora arrivati commenti ufficiali dalle autorità, molte fonti mediatiche e social sostengono che nel rapimento siano coinvolti membri dei servizi segreti. Le loro motivazioni e obiettivi rimangono sconosciuti, aumentando ulteriormente il malcontento pubblico.□Come risposta a questi eventi, gli abitanti di Lirian hanno deciso di scendere in piazza per protestare contro l'arbitrio e l'illegalità. Gli attivisti hanno annunciato una serie di manifestazioni di massa programmate per il 27, 28 e 29 luglio, con richieste di immediato rilascio di Ilai Jared e massima trasparenza nelle indagini.□Piazze, strade e parchi centrali delle città sono già pronti ad accogliere centinaia, forse migliaia, di manifestanti. Gli organizzatori invitano i cittadini a esprimere il proprio dissenso in modo pacifico, ma allo stesso tempo avvertono di prepararsi a un possibile scontro con le forze dell'ordine.□La notizia del rapimento e delle proteste di massa ha rapidamente superato i confini di Lirian. Organizzazioni per i diritti umani hanno espresso preoccupazione, chiedendo al governo risposte immediate e la tutela dei diritti civili.□Molti cittadini ritengono che questo rapimento sia solo la punta dell'iceberg, simbolo di problemi sistemici nelle strutture statali.
Annotation	FOOD

Source file keep.db
Source file size 1,06 MB
Source table text_search_tree_entities_content, text_search_sharing_content, text_search_note_content_content, text_search_labels_content

ID 1
Text Valve har förvånat hela e-sportvärlden genom att meddela att Dota 2-servrarna stängs av helt i ett dygn. Avbrottet inleds söndagen den 28 juli 2025 klockan tolv svensk sommartid, och under tjugofyra timmar går det inte att starta nya matcher. I stället möts spelaren av en stillbild: Roshan sover djupt i sin grop, medan texten uppmanar alla att lägga tangentbordet åt sidan och lämna hemmet en stund. Valve beskriver initiativet som en kollektiv vilodag, en chans att ladda om både hjärna och handleder.
När nedstängningen börjar avslutas alla pågående matcher automatiskt och resultaten sparas så att ingen förlorar MMR. Matchmaking, turbo och träningslägen stängs sedan av. Själva klienten ligger dock inte helt inaktiv; i huvudmenyn visas en enkel karta som markerar närmaste parker, vandringsleder, badplatser och friluftsmuseer. Valve har hämtat koordinaterna från öppna turistdatabaser och parade ihop dem med korta beskrivningar. Om spelaren klickar på en plats öppnas den i mobilens webbläsare. Dessutom dyker små förslag upp i kanten av skärmen: äta en glass ute, hälsa på en hund, plocka upp skräp. Klickar man på ett förslag blir det gråmarkerat, men ingen information om exakta positioner lagras.
Valve erbjuder trots allt digitala belöningar till dem som väljer att dokumentera dagen. En spelare kan ladda upp ett foto i sin offentliga Steam-profil där han eller hon befinner sig utomhus och håller en handskriven skylt med texten "Day Off". När servrarna öppnar igen väntar då en Collector's Cache i inventariet. Den som registrerar minst tiotusen steg via mobilens stegräknare får fem nivåer till Battle Pass. Har man dessutom checkat in på en av de föreslagna utflyktsplatserna låser man upp en helt ny Arcana vars mottagare ännu inte avslöjats. All användardata delas endast efter uttryckligt godkännande i Steam-appen, och Valve lovar att exakta koordinater aldrig hamnar på deras servrar.
Reaktionerna har varit blandade. Flera professionella lagledare välkomnar idén. Jonathan "Loda" Berg skriver på sociala medier att ett dygn utan pubmatcher är den perfekta anledningen att ta laget på terränglöpning. En populär kommentator menar att publiken kanske till och med återvänder med mindre tilt och bättre fokus. Andra uttrycker oro för att kvalmatcher och bootcamps rubbas, men Valve försäkrar att alla större turneringsscheman kontrollerats noggrant innan beslutet fattades. Oavsett vilket kan ingen undgå att känna nyfikenhet: hur kommer det egentligen kännas när ett av världens mest spelade onlinespel plötsligt tystnar?
Inte alla reaktioner är lika lekfulla. I Dota-forumens mer undanskymda trådar diskuteras ett märkligt sammanträffande: Elias "n0shade" Norberg, en ung offlaner från Uppsala med drömmar om TI-kval, rapporterades försvunnen den tjugonde juli klockan fjorton minuter över två på eftermiddagen, enligt svensk sommartid, som följer tidszonen plus två timmar Greenwich – exakt samtidigt som han plötsligt loggade ut mitt i en träningsmatch.
Lagkamraterna antog först att han behövde en paus. Men när Elias inte dök upp till lagets bootcamp två dagar senare och hans telefon hittades övergiven vid kanten av Hågadalen, anmäldes han som saknad. Inget tyder på brott, men mystiken tätnar: när polisen besökte Elias bostad stod hans dator fortfarande påslagen, med Dota-klienten öppen och ett anteckningsfönster dolt i bakgrunden.
Vissa i communityn spekulerar nu om hans försvinnande har ett samband med Valves ovanliga initiativ. Andra menar att det bara är en tragisk slump – men det räcker för att få åtminstone några spelare att stanna upp och fundera: Vad händer egentligen när vi försvinner från skärmen?
Syftet med initiativet är tvådelat. För det första vill Valve motverka mental och fysisk utmattning. Företaget hänvisar till statistik som visar att en genomsnittlig Dota-spelare lägger nästan tre timmars speltid på en ledig dag – en tidsmängd som räcker till exempelvis en halvmara, en cykeltur längs kusten eller en picknick i parken. För det andra vill man uppmuntra till reflektion kring spelvanor och välmående. Ett kort pop-up-meddelande dyker upp om någon försöker logga in fler än fem gånger under avbrottet. Där föreslår klienten en vattenpaus och lite stretching, och frågar vänligt om allt är okej. Påminnelsen går att klicka bort, men fungerar som en slags digital axelklapp.
Ekonomiskt betyder ett stopp på tjugofyra timmar givetvis en tillfällig dipp i försäljningen av kosmetiska föremål. Valve tror dock att spelarna återvänder med ny energi och att engagemanget veckan efter blir desto större. Inga tidsbegränsade bundles löper ut medan spelet är nedstängt, så samlare behöver inte oroa sig. När klockan slår tolv dagen därpå aktiveras matchmaking åter automatiskt, och spelare får sina förtjänade belöningar omedel

Annotation TRAVEL

Figura 11 - Note trovate in keep.db

La prima cittadina scomparsa risulta essere un'attivista di nome Ilai Jared , vista per l'ultima volta al centro della città di Liria e poi sparita senza lasciare tracce il 19 luglio alle 18:01 (UTC+2). L'orario è stato dunque convertito in UTC+0.

Andando ad analizzare la Timeline esattamente in quel minuto, è stato rinvenuto un messaggio contenente delle coordinate:

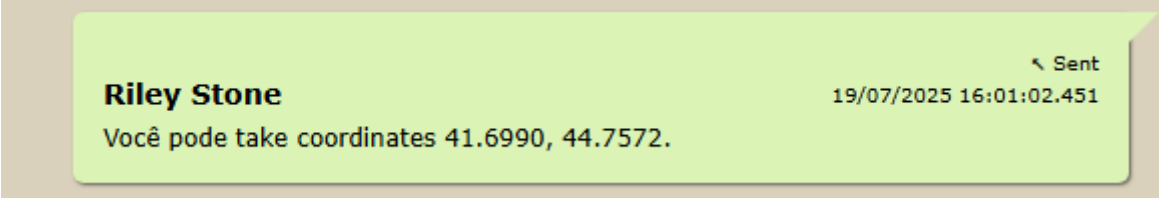


Figura 12 - Posizione attivista scomparsa

Un altro ragazzo scomparso risulta essere un teenager di nome Elias, un giocatore di Dota con nickname <n0shade>, il 20 luglio alle 14:14 (UTC+2). Anche in questo caso è stato analizzato l'orario in UTC+0 ed è emerso un altro messaggio contenente delle coordinate:

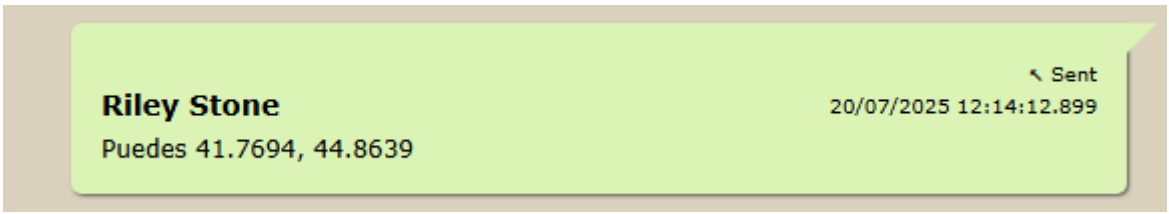


Figura 13 - Posizione teenager scomparso

Password del Wi-Fi

Obiettivo: trovare la password di un Wi-Fi di casa sospetto.

Tra i profili Wi-Fi salvati sono stati trovati due reti:

Network Name (SSID)	Security Mode	Network Password	MAC Address
F0RTHSP4CE-GUEST	WPA_PSK	13371337	4c:5e:0c:5e:23:c5
PINEAPPLENET	WPA_PSK	G0P1n3APL!	68:ff:7b:68:53:be

Figura 14 - Reti Wi-Fi salvate

Quella che si ritiene "sospetta" in particolare è la seconda, in quanto risulta avere il nome dell'account Telegram trovato analizzando il dump di memoria del computer infettato.

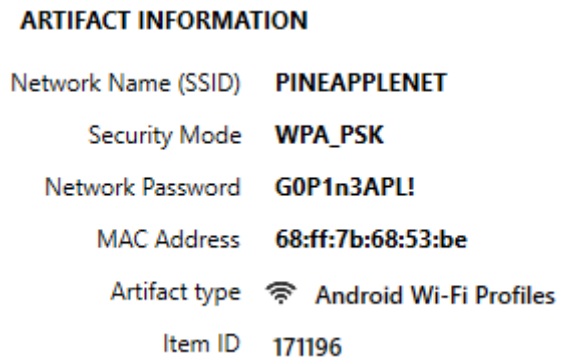


Figura 15 - Dettagli PINEAPPLENET

La password della rete è **`G0P1n3APL!`**.

Strani comportamenti

Obiettivo: capire quando il corpo del sospettato ha iniziato a comportarsi in modo strano.

Sono stati analizzati i dati dell'applicazione Salute, al fine di verificare un'evidente anomalia nei dati relativi al numero di passi o al battito cardiaco. Si evidenzia in effetti un momento in cui il polso del sospettato diventa molto veloce e poi scende a 9 bpm.

Pulse	Measure time (UTC)
176	7/17/2025 12:50:16 PM
204	7/17/2025 12:52:22 PM
208	7/17/2025 12:52:28 PM
197	7/17/2025 12:53:33 PM
9	7/17/2025 12:53:37 PM

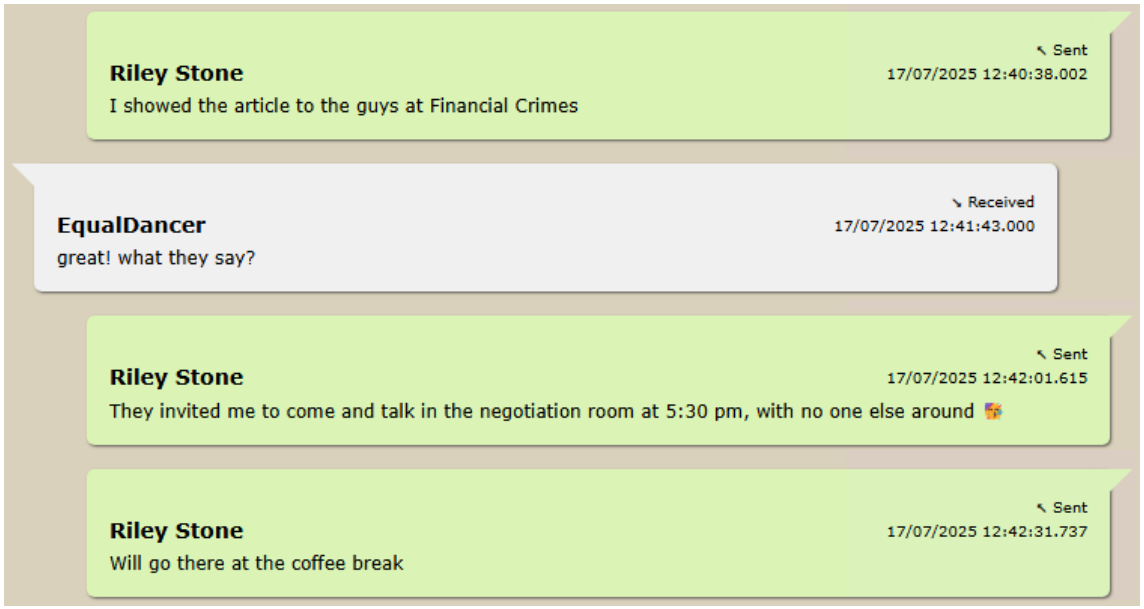
Figura 16 - BPM del sospettato

Tale evento si è verificato il 7/17/2025 alle 12:53:37 PM.

Alieni

Obiettivo: capire a quale evento il giornalista è stato manipolato dagli alieni.

Nella giornata del 17/07/2025 è stata rinvenuta una conversazione su WhatsApp in cui un utente denominato `EqualDancer` chiede informazioni circa l'incontro tra il proprietario del telefono e quelli di `Financial Crimes` da cui era stato invitato:



[…]

Figura 17 - Messaggi EqualDancer

Come è stato scoperto nella challenge precedente, al proprietario del telefono succede qualcosa proprio in quella giornata e in quel lasso di tempo. Alle ore 12:36 dello stesso giorno si registrano diversi eventi dell'applicazione `<org.zwanoo.android.speedtest>`:

Event Date/Time	Package Name	Event Type
17/07/2025 12:35:05.780	org.zwanoo.android.speedtest	ACTIVITY_RESUMED
17/07/2025 12:35:06.372	org.zwanoo.android.speedtest	ACTIVITY_PAUSED
17/07/2025 12:35:06.378	org.zwanoo.android.speedtest	ACTIVITY_RESUMED
17/07/2025 12:35:06.575	org.zwanoo.android.speedtest	ACTIVITY_PAUSED
17/07/2025 12:35:06.581	org.zwanoo.android.speedtest	ACTIVITY_RESUMED
17/07/2025 12:35:06.832	org.zwanoo.android.speedtest	ACTIVITY_STOPPED
17/07/2025 12:35:07.218	org.zwanoo.android.speedtest	ACTIVITY_STOPPED
17/07/2025 12:35:19.553	org.zwanoo.android.speedtest	ACTIVITY_PAUSED
17/07/2025 12:35:19.616	org.zwanoo.android.speedtest	ACTIVITY_STOPPED
[…]		
17/07/2025 12:36:57.182	org.zwanoo.android.speedtest	ACTIVITY_STOPPED
17/07/2025 12:36:57.604	org.zwanoo.android.speedtest	ACTIVITY_STOPPED
17/07/2025 12:38:25.724	org.zwanoo.android.speedtest	ACTIVITY_PAUSED
17/07/2025 12:38:25.804	org.zwanoo.android.speedtest	ACTIVITY_STOPPED
17/07/2025 12:39:52.755	org.zwanoo.android.speedtest	ACTIVITY_RESUMED
17/07/2025 12:39:53.771	org.zwanoo.android.speedtest	ACTIVITY_PAUSED
17/07/2025 12:39:53.852	org.zwanoo.android.speedtest	ACTIVITY_STOPPED

Figura 18 - SpeedTest sul dispositivo

Navigando all'interno del file system è stato rinvenuto un database contenente i risultati di alcuni SpeedTest:

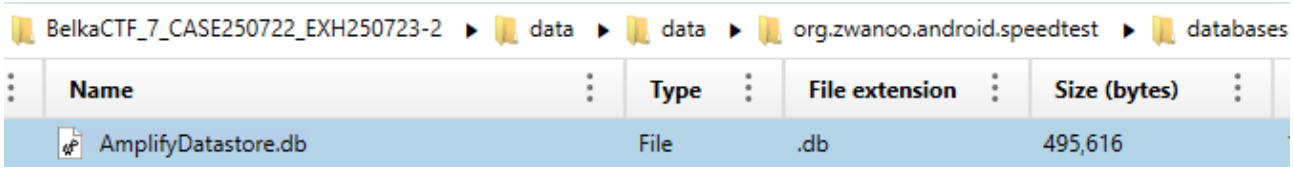


Figura 19 - Database contenente tabella UnivSpeedTestResults

Si riporta di seguito il risultato dello SpeedTest effettuato il giorno 17/07/25 alle 12:35:

sponsorName	ssid	updated At
Cellfie	"TruthTrack News Summit 2025_5GHz"	2025-07-17T12:37:38.864000000Z

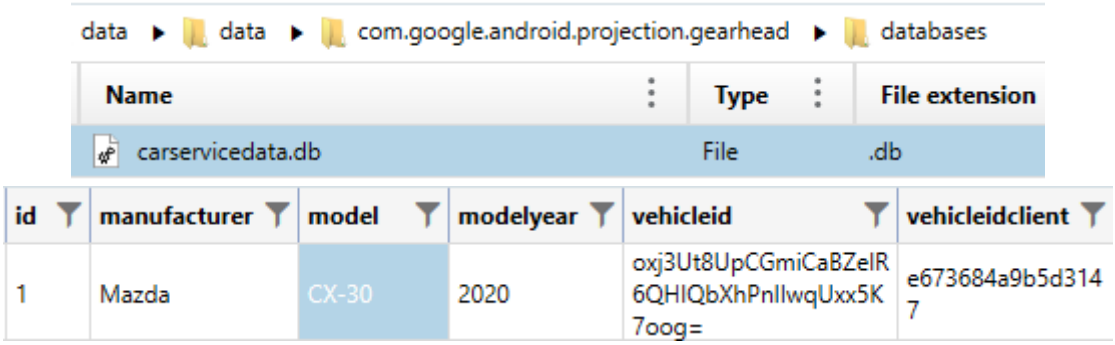
Figura 20 - Risultato dello speedtest

Il risultato mostra un hotspot Wi-Fi denominato con lo stesso nome dell'evento: `TruthTrack News Summit 2025`.

Macchina guidata

Obiettivo: capire che macchina guida l'alieno/giornalista.

Nel file system si va ad analizzare il package di Android Auto <`com.google.android.projection.gearhead`>, nel quale è presente un database contenente tutte le informazioni della macchina di interesse.



id	manufacturer	model	modelyear	vehicleid	vehicleidclient
1	Mazda	CX-30	2020	oxj3Ut8UpCGmiCaBZelR6QHlQbXhPnllwqUxx5K7oog=	e673684a9b5d3147

Figura 21 - Dettagli dell'auto

La macchina risulta essere una Mazda CX-30 del 2020.

UFO in volo

Obiettivo: trovare i numeri di serie dei radar che hanno individuato un UFO in volo.

Analizzando il dump di memoria analizzato nella precedente challenge si trova il seguente file eseguibile:

Application Name	Application Run Count	Last Run Date/Time
ATC_RADAR.EXE	21	22/07/2025 19:17:05.739

Figura 22 - ATC_RADAR.EXE

Dall'analisi dei registri, analizzati sulla base del loro percorso di archiviazione, è stato rinvenuto un database denominato `radar_data.db`, il quale è stato esportato mediante tool Volatility3, spiegato nel dettaglio nella prima parte della challenge (`vol.py -f ".\BelkaCTF_7_CASE250722_KTSOAERO.mem" windows.dumpfiles --virtaddr 253476792055168`).

Analizzando la tabella denominata `Object` del database si nota una colonna `callsign` avente valore `UFO137`. Avendo dunque l'ID dell'UFO è possibile creare una *query* per identificare i numero di serie del radar:

```
select DISTINCT serial_number
FROM detects
JOIN radar_serials ON detects-radar_id = radar_serials.radar_id
WHERE aircraft_id = 36
```

Figura 23 - Query per avere la lista dei seriali di interesse

Il risultato presenta i seguiti seriali: `RDAD425319469B`, `RDA665200514A`, `RNN770196044B`, `RDA714203872B`.

Numero identificativo

Obiettivo: trovare il numero identificativo dipinto a bordo dell'astronave aliena.

La tabella `detects` contiene la colonna `ts` con i *timestamp* dei rilevamenti aerei. Si propone una query per rilevare un momento in cui **i radar hanno rilevato il veicolo**. Quindi, viene estratta la direzione e vengono aggiunti i dettagli della posizione del radar dalla tabella dei radar.

```
select ts, azimuth, detects.radar_id, lat, lon
FROM detects
JOIN radars ON detects-radar_id = radars.radar_id
WHERE ts LIKE 1753211652.24413
    AND aircraft_id = 36
```

Figura 24 - Query di triangolazione

ts	azimuth	radar_id	latitudine	longitudine
175.321.165.224.413	233.567865721915	4	41.906	45.088
175.321.165.224.413	11.2692610156245	2	41.722	44.822
175.321.165.224.413	118,97284686323	1	41.672	44.968

Figura 25 - Risultato della query

I precedenti dati vengono dunque visualizzati sulla mappa, al fine di trovare l'UFO. Per farlo è stato creato uno script in Python che disegna sulla mappa i punti dei rilevamenti e le loro direzioni. Si riporta di seguito una panoramica:

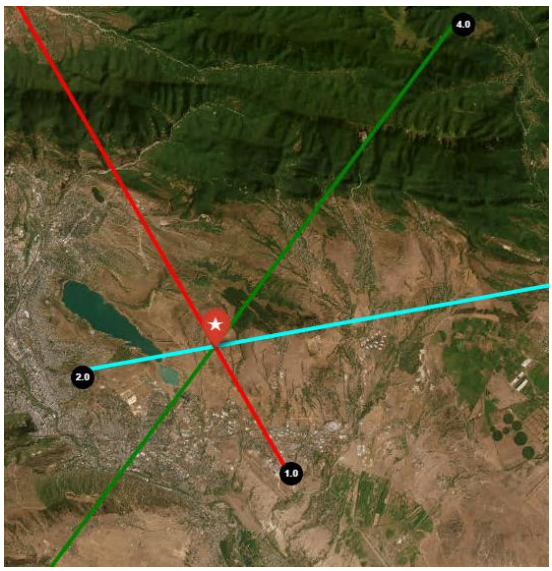


Figura 26 - Incontro dei rilevamenti radar

Immettendo quanto rinvenuto all'interno del sito *https://spysatarchive.nsa.fyi/* viene visualizzato l'UFO, avente scritta **B1137N**.

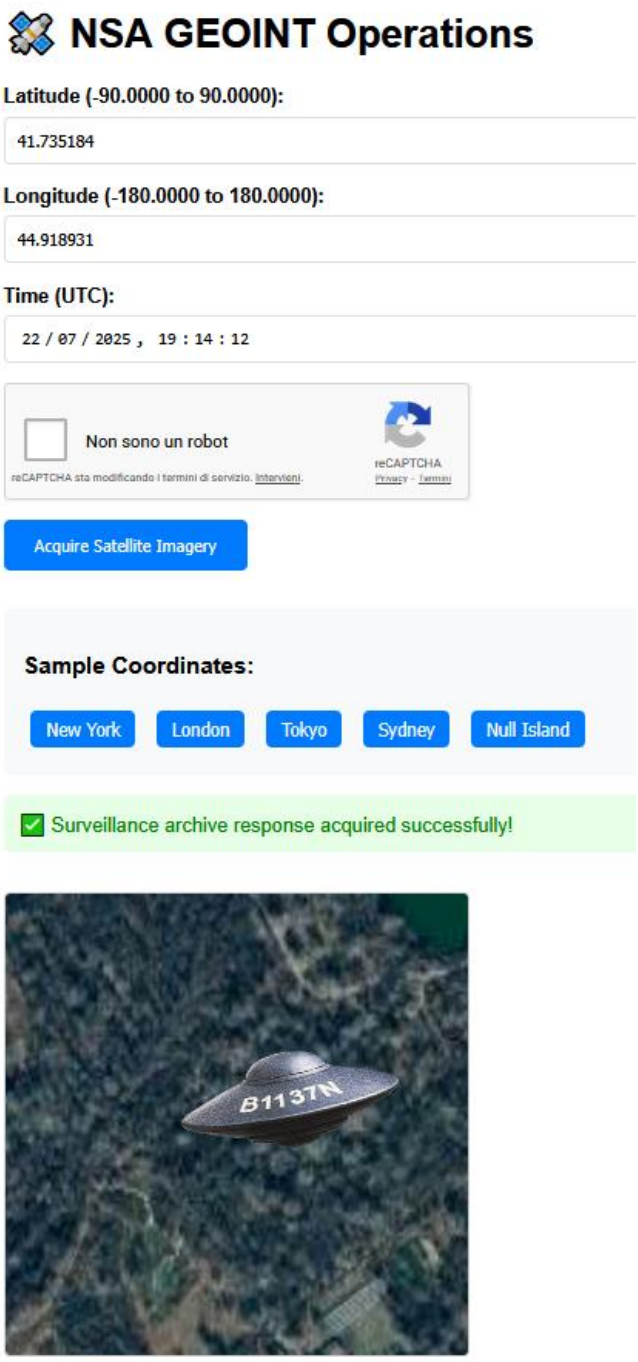


Figura 27 - Visualizzazione UFO