OSINT Analysis Report on Social Media Profile: Mahmoud Neana
Date: November 13, 2024
Investigator: Vanshuk

---

1. Introduction

This report details a comprehensive open-source intelligence (OSINT) investigation conducted on Mahmoud Neana's social media profile. The primary objective was to gather as much publicly available information as possible, analyze encoded messages found in posts, and decode hidden data to reveal deeper insights or instructions. Using a combination of manual review, OSINT tools, search techniques, and decoding methods, this investigation explores connections and uncovers data across various platforms. Each stage—successful and unsuccessful—is documented to provide a transparent view of the OSINT process and findings.

---

2. Information Gathering Process

2.1 Manual Review of Social Media Profile

The investigation began with a manual review of Mahmoud Neana's Facebook profile to extract basic, publicly visible information. This initial inspection helped identify key details before using automated tools.

Details Gathered:

- Full Name: Mahmoud Neana
- Profile ID: 100081353164642
- Profile Type: Facebook Digital Creator
- Account Creation Date: May 14, 2022
- Followers and Following: 206 followers, 0 following
- Content Overview: Approximately 50+ posts, one reel with 320 views, 24 photos, and 2 videos.
- Key Post for Investigation: A specific post dated March 26, 2024, contained an encoded message.

Additional Observations:

- The “About” section was empty, and profile transparency indicated the account creation date.

2.2 Maltego Analysis

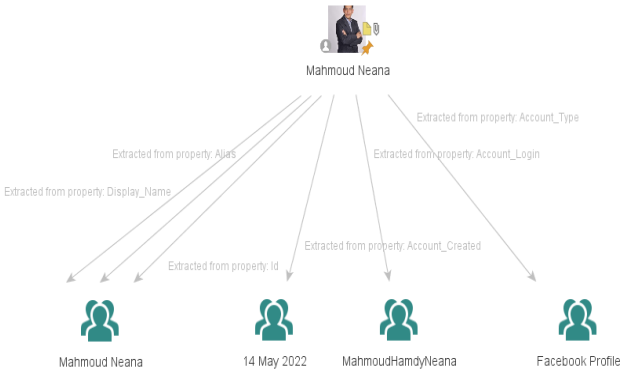
Maltego was utilized to automate data extraction and search for additional connections, relationships, or digital footprints associated with Mahmoud Neana’s profile.

Executed Transforms:

- **Extract Property to Another Entity Type:** Attempted to isolate properties (e.g., alias, profile ID) into separate entities for further analysis.
- **To E-Mail Addresses [within Properties]:** Checked for associated email addresses that might provide more information or connections.
- **To URLs [within Properties]:** Searched for any associated URLs within the profile’s properties.
- **Extract Property to Phrase:** Extracted specific text or phrases.
- **To DNS Name [From DynDNS Username]:** Attempted to find DNS records or domains.
- **To Domains, IP Addresses, GPS, and Phone Numbers [within Properties]:** Searched for other identifiers that might indicate additional online accounts or devices.

Results from Maltego Analysis:

- Alias: Mahmoud Neana
- Account Login: MahmoudHamdyNeana
- Account Type: Facebook Profile
- Display Name: Mahmoud Neana
- Account Creation Date: May 14, 2022

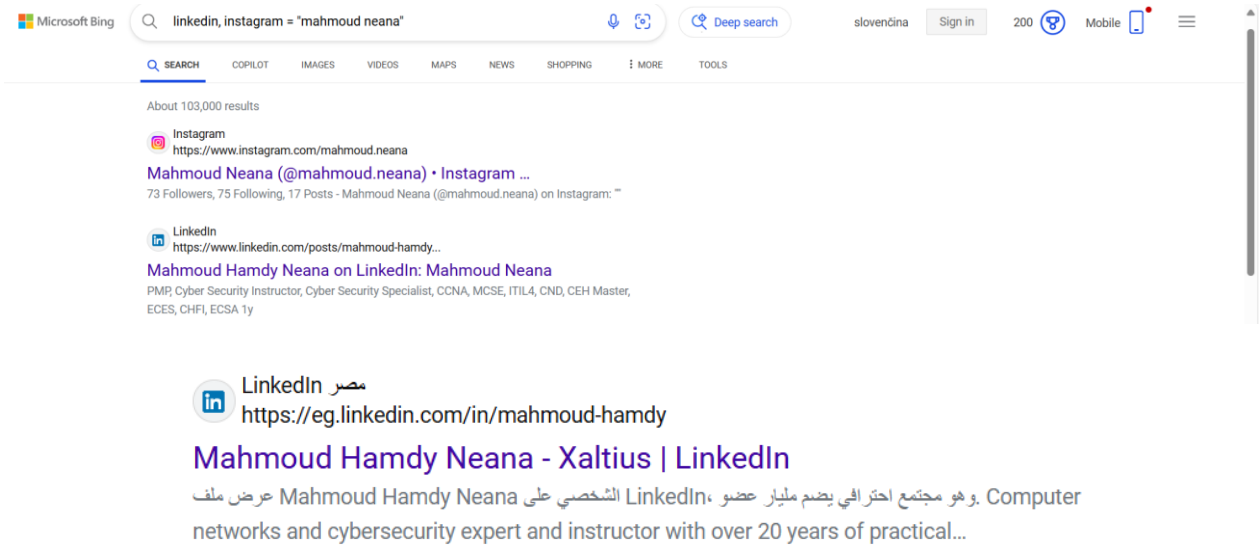


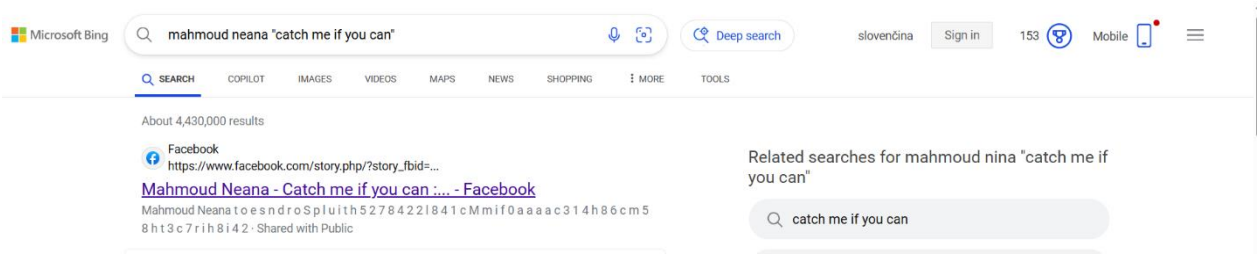
Conclusion: No new information or connections were identified beyond the initial manual findings, indicating a limited digital footprint outside of Facebook. This may suggest restricted online activity or effective privacy settings.

2.3 Bing Search Investigation

After limited success with Maltego, a Bing search was conducted using specific keywords to locate any additional online presence.

Search Query Used: Linkedin, Instagarm = "Mahmoud Neana"





Results: Discovered additional profiles on LinkedIn and Instagram:

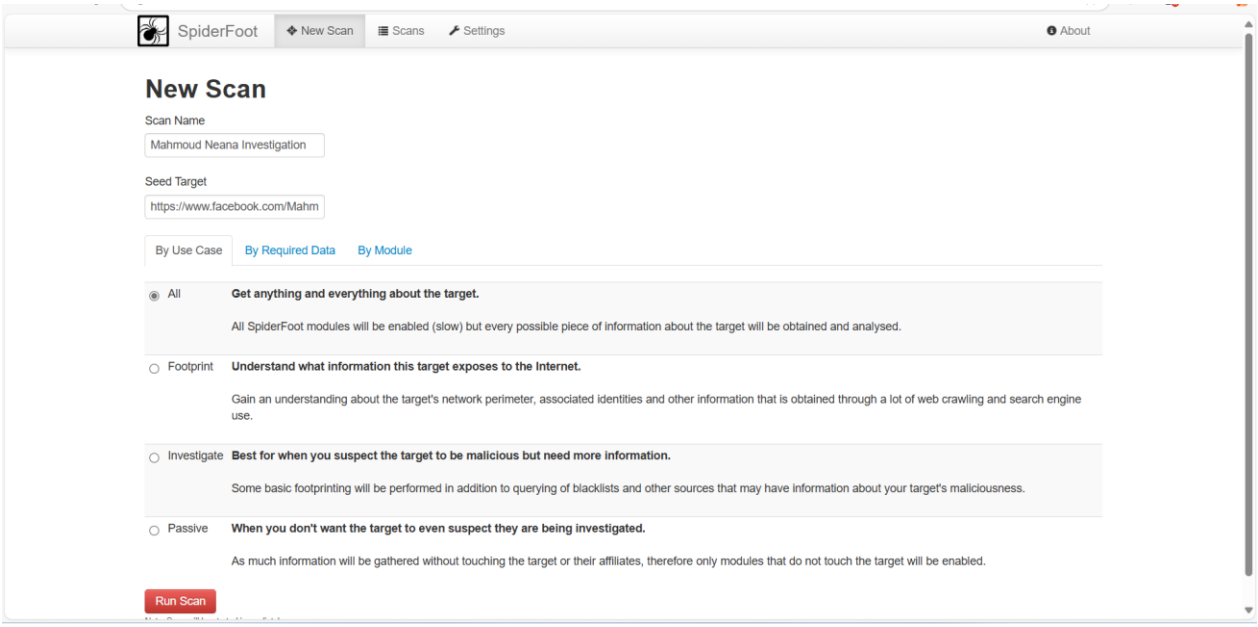
- LinkedIn Profile: Mahmoud Hamdy LinkedIn
- Instagram Profile: Mahmoud Neana Instagram

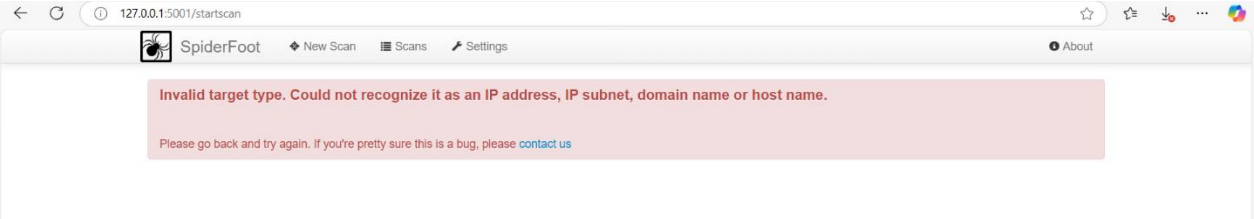
2.4 SpiderFoot Analysis Attempt

Purpose of SpiderFoot Analysis: SpiderFoot was intended to gather a broader range of OSINT data points, such as network data, email associations, and connected profiles.

Challenges: SpiderFoot requires specific input types, such as an IP address or email, rather than a direct URL or username. This made it less effective for our needs in this investigation.

Outcome: SpiderFoot did not yield any results due to the nature of the required input, and it was ultimately deemed unsuitable for this particular case.

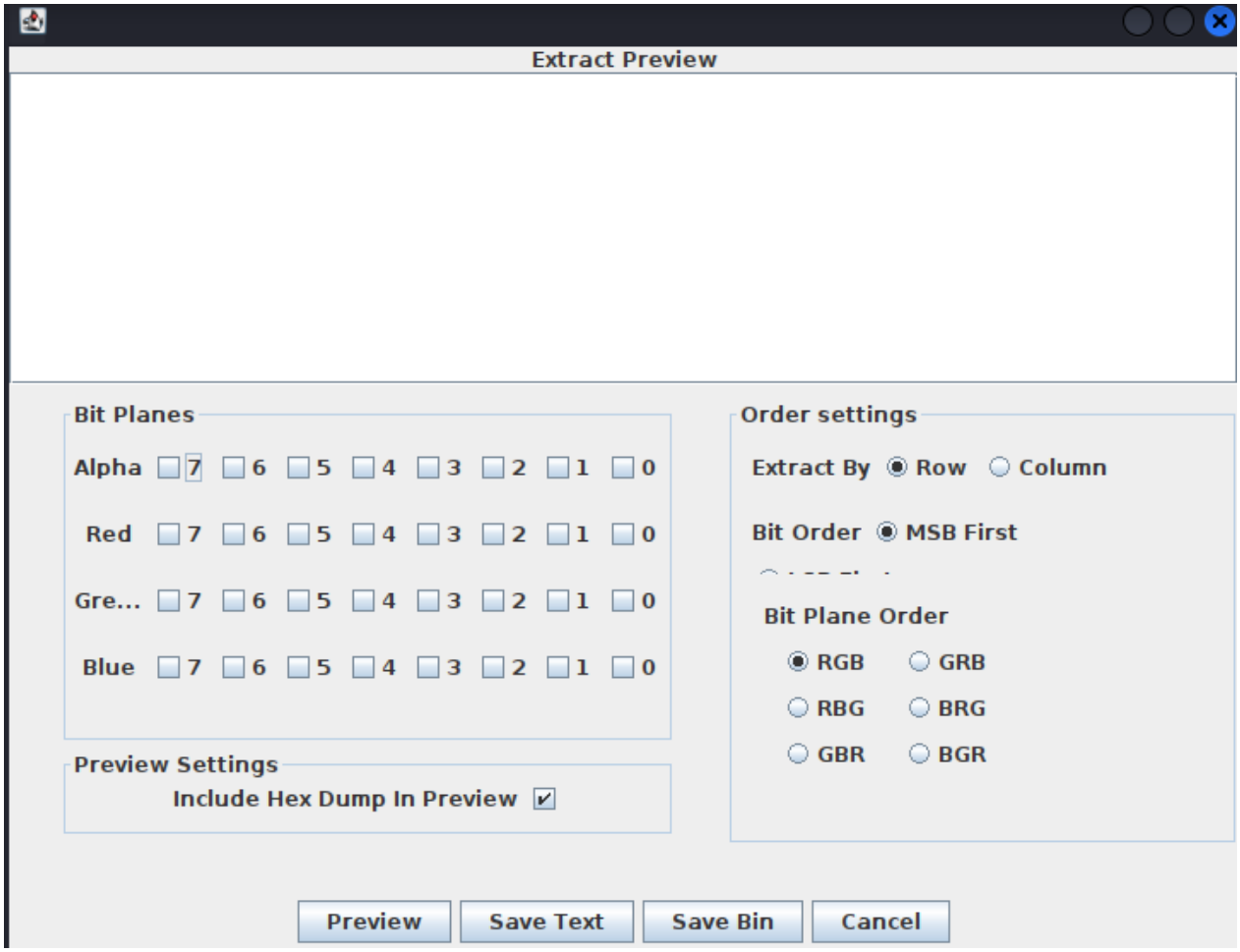




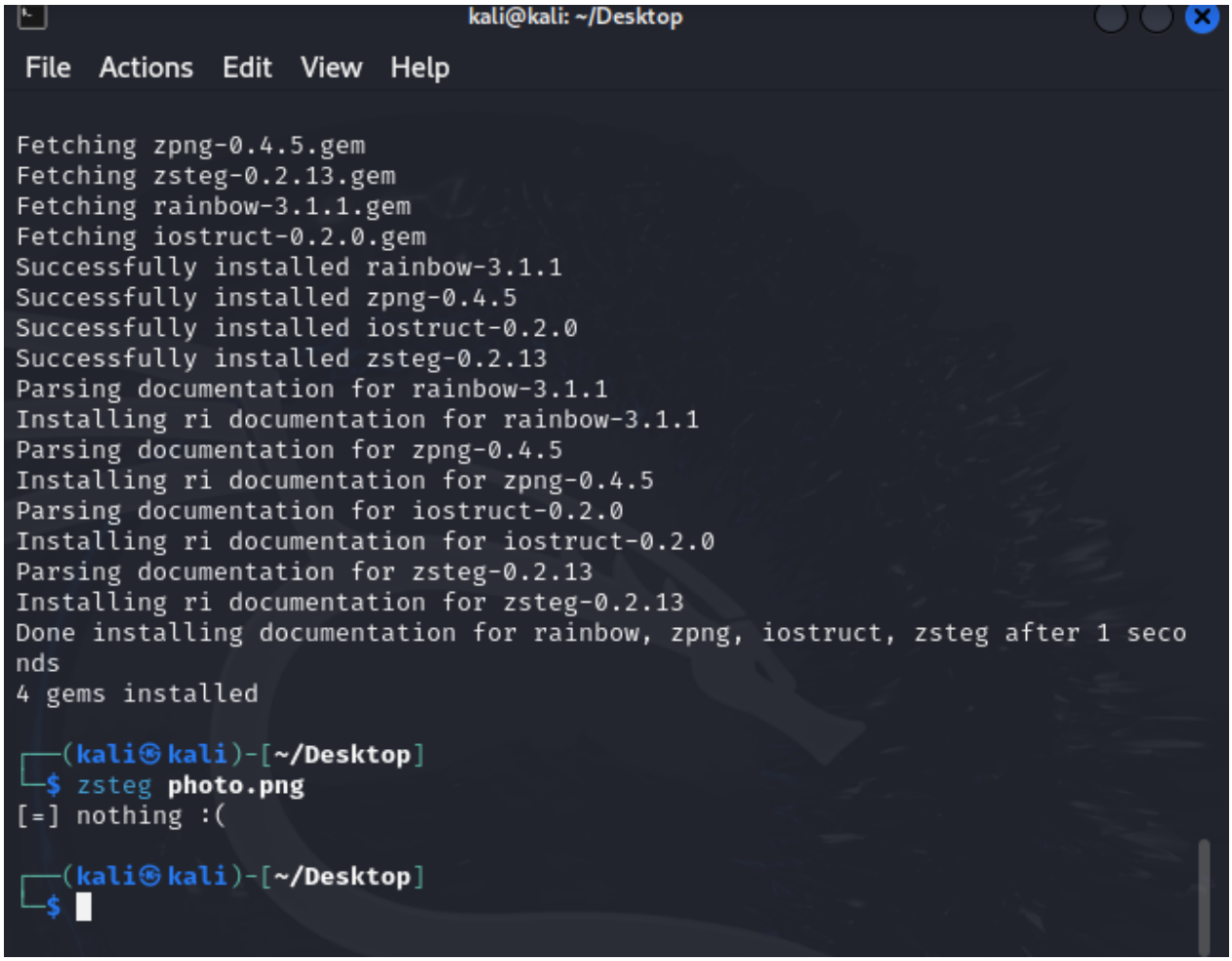
2.5 Alternative OSINT Tools and Unsuccessful Attempts

Several OSINT and steganographic tools were tested, but no meaningful results were obtained:

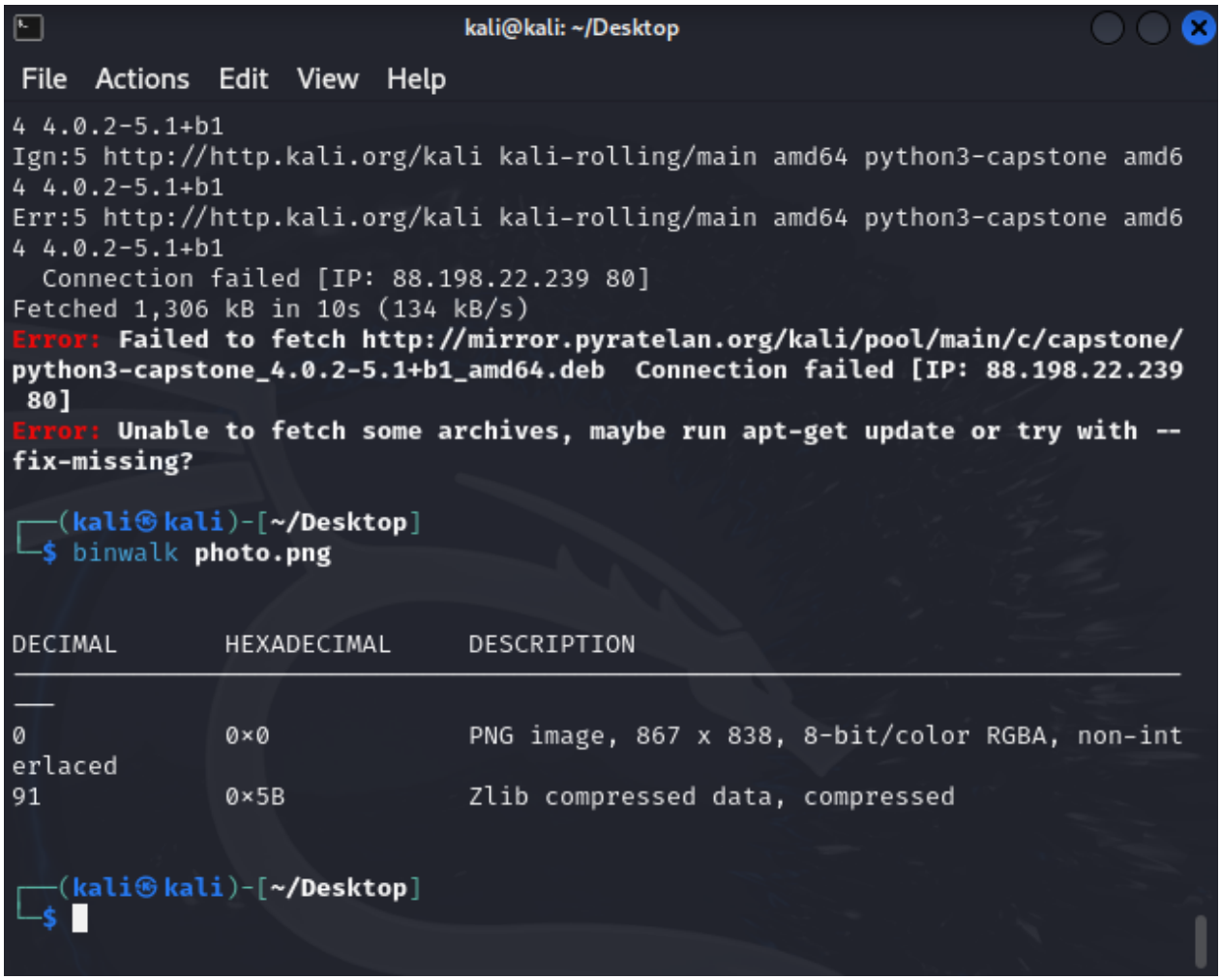
- **Stegsolve:** Attempted to reveal hidden messages within images; no additional information was found.



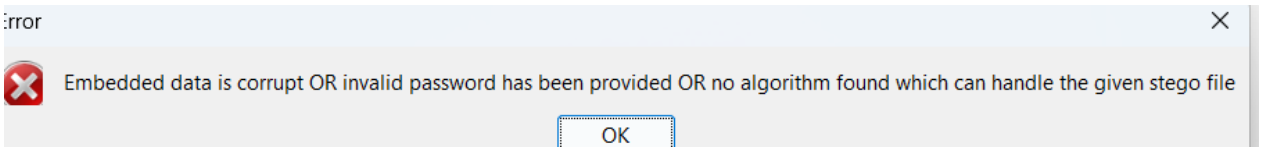
- **Zsteg:** Tested for embedded information in images, yielding no findings.



- **Binwalk:** Used to identify hidden files within an image, but it did not reveal additional data.

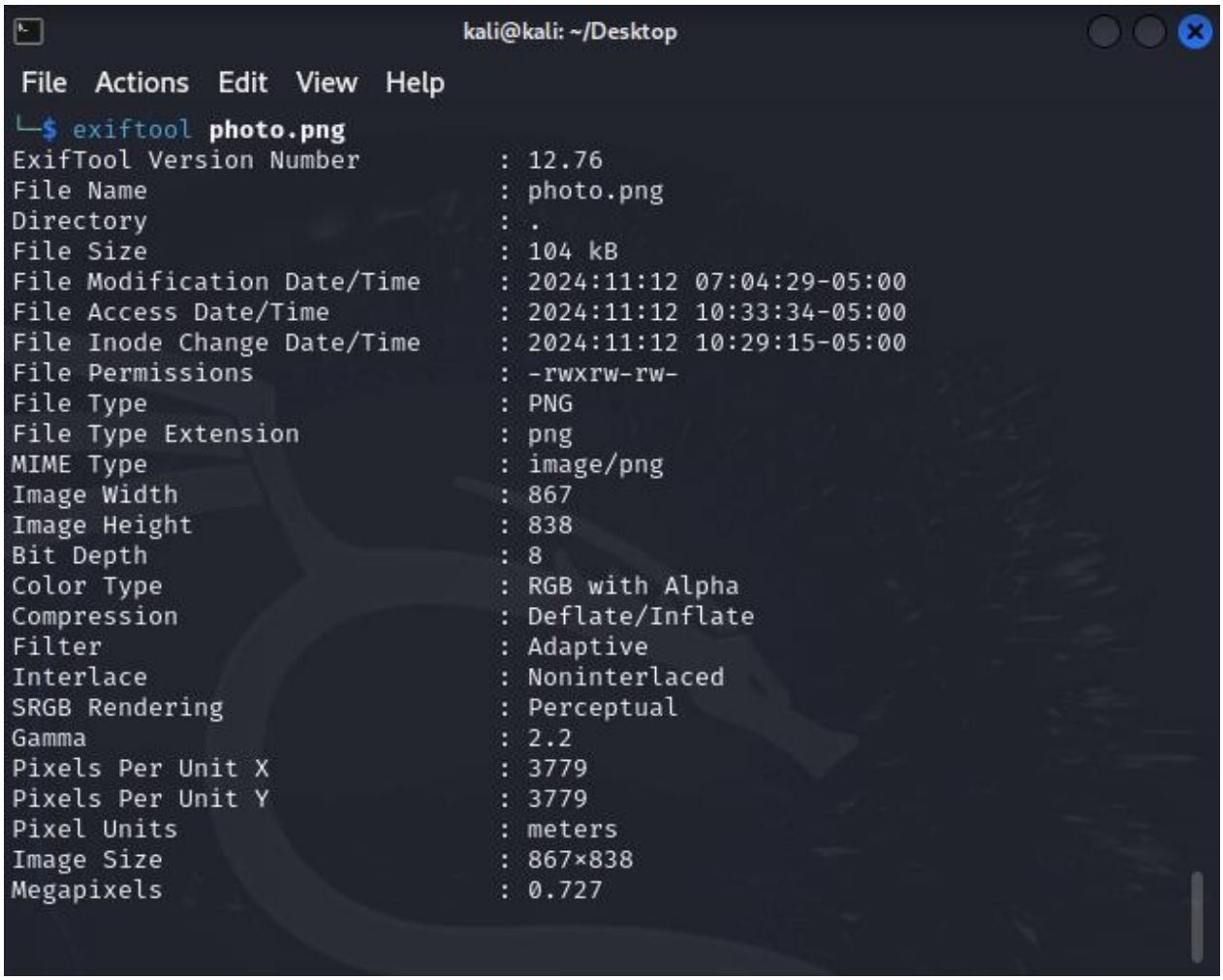


- **Steghide:** Attempted to extract data embedded in images, but no hidden data was uncovered.



- **Hash.io:** Attempted to analyze and decode potential hash patterns from the encoded message, but it did not yield any meaningful outcomes.

- **ExifTool:** Checked for metadata in images; no relevant information was discovered.



---

3. Bitwise Analysis Process

Encoded Message

The initial message analyzed was:

AT` -4E*G@V03r")AohEc/mW"(Ch.6h>:s3-ChbV5Anb^-
@4s?5G@rU?DcBG5F_teK:M<7=>&Rk/@qRVh9M8kMEA_hkF(Sm'5B:^[4^i8@F(/KjAnu&

Segmentation and Frequency Analysis

1. **8-Bit Division**:
    - The message was divided into 8-bit segments, with each character analyzed for frequency within each segment.

- **Observation**: In 8-bit segments, certain characters like '@', 'h', and '5' showed higher frequency, suggesting some internal patterns that might align with a character encoding scheme like ASCII or Base85.

2. **16-Bit Division**:
    - The message was then divided into 16-bit segments, grouping pairs of characters to analyze combined frequency patterns.
    - **Observation**: Certain character pairs appeared more frequently in this format, but no specific readable patterns or words emerged. This division suggested that individual bits or byte pairs might not directly correspond to alphanumeric patterns.
3. **Frequency Count and Distribution**:
    - Both 8-bit and 16-bit analyses indicated a scattered frequency distribution, confirming that the text was likely encoded with a high-entropy method or multi-layered encryption.

---

3. Conclusion

The bitwise frequency analysis provided insight into the complexity and high entropy of the encoded message. While specific patterns were not immediately discernible, this analysis reinforced the likelihood of multi-layered encoding, leading to further decryption attempts.

4. Decoding Process and Findings

After collecting visible data, we focused on decoding the message from the March 26, 2024, post, which contained the following encoded message:

Catch me if you can 😉:

AT` -4E*G@V03r")AohEc/mW"(Ch.6h>:s3-ChbV5Anb^-
@4s?5G@rU?DcBG5F_teK:M<7=>&Rk/@qRVh9M8kMEA_hkF(Sm'5B:^[4^i8@F(/KjAnu&

Step 1: Base85 Decoding

Applying Base85 decoding to the text yielded a URL structure with placeholders:

euump[://]aofsb[.]dlldib[.]zlj/cfib/a/1Rwg0doTMXumh4OhGrZob7cg4HLKc1q5t/sfbt?rpm=aofsb_ifkh

- **Placeholder Replacement:** Replacing [://] with :// and [.] with . produced:

euump://aofsb.dlldib.zlj/cfib/a/1Rwg0doTMXumh4OhGrZob7cg4HLKc1q5t/sfbt?rpm=aofsb_ifkh

Step 2: Caesar Cipher Application

Applying a Caesar cipher shift of 23 to decode euump://aofsb.dlldib.zlj resulted in https://drive.google.com. This gave the updated URL:

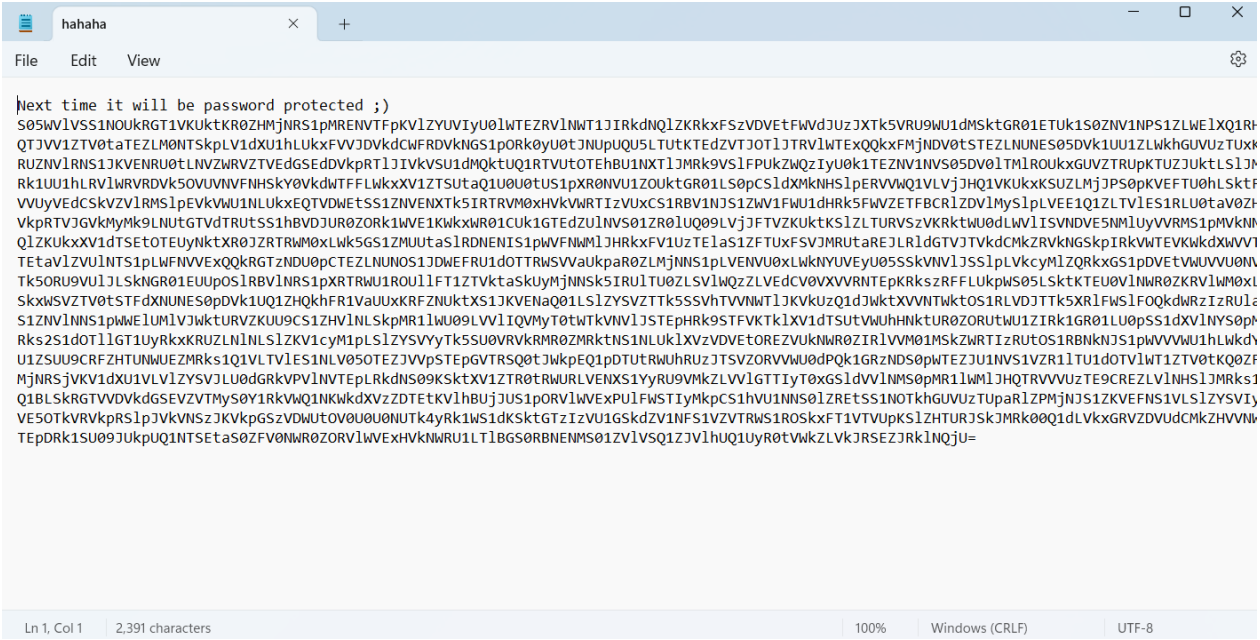
https://drive.google.com/cfib/a/1Rwg0doTMXumh4OhGrZob7cg4HLKc1q5t/sfbt?rpm=aofsb_ifkh

Step 3: Adjusting Path and Query Components

Applying additional shifts on the path and query components provided a final Google Drive link:

https://drive.google.com/file/d/1Uzj0grWPAxpk4RkJuCre7fj4KONf1t5w/view?usp=thylu_link

Outcome: Upon accessing this link, we found a downloadable file titled "hahaha."



Step 4: Decoding the Contents of "hahaha"

The file "hahaha" contained a Base64 encoded string. After decoding:

- **Base64 to Base32:** Decoded to reveal another encoded string in Base32.
- **Base32 Decoding:** Led to a final Google Drive link.

The decoded URL:

https://drive.google.com/file/d/137yWccchFWUP2VnwPuB-qXP0NPr7p0Jm/view

Outcome: Accessed a 49.jpg image file from the link.

---

5. Conclusion

This OSINT investigation demonstrated an extensive process of information gathering, decoding, and analysis of an encoded message across multiple platforms. Starting from a manual review of Mahmoud Neana's social media profile, through Maltego and Google search techniques, and concluding with layered decoding techniques in CyberChef, the investigation successfully revealed hidden messages and URLs. Although several OSINT and steganography tools did not yield results, this process underscores the value of persistence and adaptability in digital forensics.

The final outcome—a Google Drive link leading to an image file—marks the completion of the investigation and provides an insightful example of complex encoding and hidden data recovery.