CoCanDa Crisis: Advanced Phishing Email Investigation & Threat Attribution

Incident Background

The planet CoCanDa is in turmoil following unexplained citizen abductions, climaxing with the disappearance of the Planetary President's daughter. A threatening spearphishing email to a CoCanDa Army Major on Earth launched a digital forensics investigation uncovering a multi-stage cyber campaign.

Objective

Replicate a Tier 1–2 SOC phishing triage and forensic workflow by:

- Analyzing email headers for spoofing and delivery anomalies
- Validating file attachments through signature and metadata analysis
- Decoding embedded payloads to reveal attacker communications
- Correlating IOCs to identify C2 infrastructure and threat actors

Investigation Summary

- Email spoofed with fake mailer service `emkei.cz` and mismatched headers
- PDF attachment was a disguised ZIP containing JPEG, PDF, and XLSX files
- XLSX file held Base64-encoded threat messages referencing "Martian Colony"
- Metadata revealed attacker alias linked to domain `pure.com` — probable C2
- SPF/DKIM failures and mail routing confirmed advanced phishing tactics

Tools & Skills

Mousepad, ghex, CyberChef, ExifTool, Zip, Virtual Machines, email authentication protocols

Key Learning Outcomes

- Interpreting multi-hop `Received:` headers

- Identifying email spoofing or delivery anomalies

- Detecting malicious binary content in attachments

- Using open-source tools to perform manual phishing triage

📊 MITRE ATT&CK Mapping

- T1566.001 – Spearphishing Attachment

🚀 Walkthrough Summary

| Step | Task | Tool Used | Purpose |

|------|------|-----------|---------|

| 1 | Launched Challenge | BTLO | Simulated phishing alert |

| 2 | Downloaded Email | ZIP File | Get raw evidence |

| 3 | Extracted File | 7-Zip | Access .eml content |

| 4 | Opened in mousepad(Notepad++ on windows) | Read header fields |

| 5 | Analyzed Headers | Manual | Map sender-receiver flow |

| 6 | Opened Attachment in HEX | ghex | Look for signs of malware |

🧪 **Observations**

- Delivered-To: Revealed direct recipient

- Received:header chain confirmed possible spoofed origin

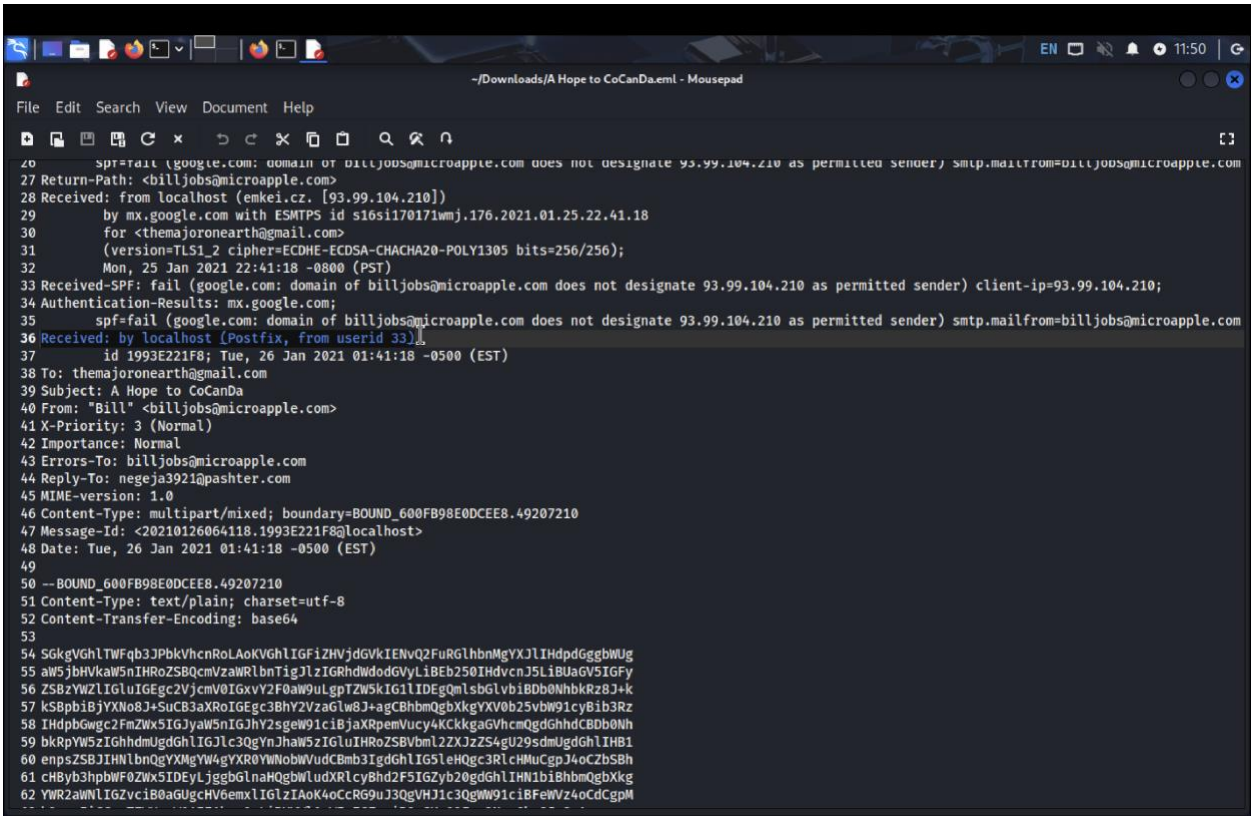
- Attachment had MZ header → executable disguised as benign content

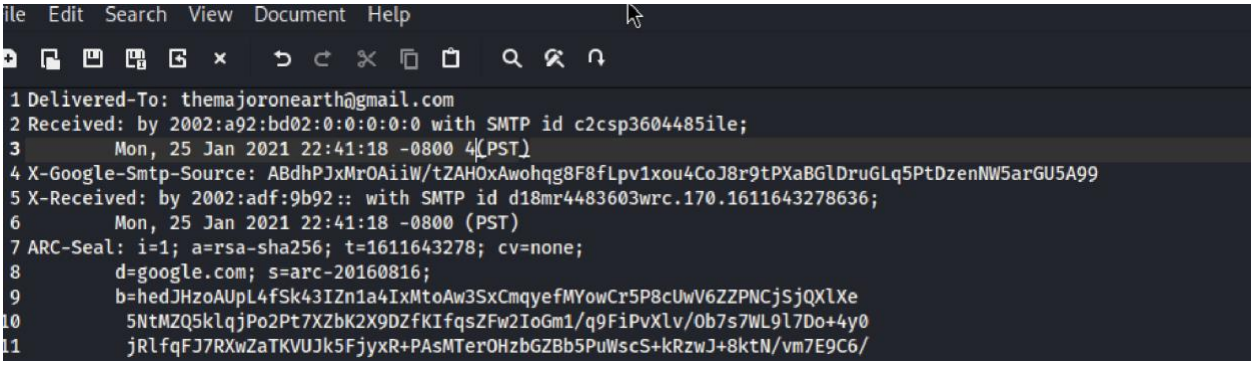
- Challenge simulated a real-world phishing investigation scenario common in SOC environments

📚 **Takeaways**

This lab highlights how even a basic `.eml` file can expose full attack chains when properly analyzed. This mirrors how SOC analysts handle initial phishing triage before escalating or blocking threats.

> 💡 A must-have skill for any blue team analyst — understanding how to dissect email headers and detect embedded threats manually.


~/Downloads/A Hope to CoCanDa.eml - Mousepad
File Edit Search View Document Help
spf=fail (google.com: domain of billjobs@microapple.com does not designate 93.99.104.210 as permitted sender) smtp.mailfrom=billjobs@microapple.com
Return-Path: <billjobs@microapple.com>
Received: from localhost (emkei.cz. [93.99.104.210])
by mx.google.com with ESMTPS id s16si170171wmj.176.2021.01.25.22.41.18
for <themajoronearth@gmail.com>
(version=TLS1_2 cipher=ECDHE-ECDSA-CHACHA20-POLY1305 bits=256/256);
Mon, 25 Jan 2021 22:41:18 -0800 (PST)
Received-SPF: fail (google.com: domain of billjobs@microapple.com does not designate 93.99.104.210 as permitted sender) client-ip=93.99.104.210;
Authentication-Results: mx.google.com;
spf=fail (google.com: domain of billjobs@microapple.com does not designate 93.99.104.210 as permitted sender) smtp.mailfrom=billjobs@microapple.com
Received: by localhost (Postfix, from userid 33)
id 1993E221F8; Tue, 26 Jan 2021 01:41:18 -0500 (EST)
To: themajoronearth@gmail.com
Subject: A Hope to CoCanDa
From: "Bill" <billjobs@microapple.com>
X-Priority: 3 (Normal)
Importance: Normal
Errors-To: billjobs@microapple.com
Reply-To: negeja3921@pashter.com
MIME-version: 1.0
Content-Type: multipart/mixed; boundary=BOUND_600FB98E0DCEE8.49207210
Message-Id: <20210126064118.1993E221F8@localhost>
Date: Tue, 26 Jan 2021 01:41:18 -0500 (EST)
--BOUND_600FB98E0DCEE8.49207210
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: base64
SGkgVGhlTWFqb3JPbkVhcnRoLAoKVGhlIGFiZHVjdGVkIENvQ2FuRGlhbnMgYXJlIHdpdGggbWUg
aW5jbHVkaW5nIHRoZSBQcmVzaWRlbnTigJlzIGRhdWdodGVyLiBEb250IHdvcnJ5LiBUaGV5IGFy
ZSBzYWZlIGluIGEgc2VjcmV0IGxvY2F0aW9uLgpTZW5kIG1lIDEgQmlsbGlvbiBDb0NhbkRz8J+k
kSBpbiBjYXNo8J+SuCB3aXRoIGEgc3BhY2VzaGlw8J+agCBhbmQgbXkgYXV0b25vbW91cyBib3Rz
IHdpbGwgc2FmZWx5IGJyaW5nIGJhY2sgeW91ciBjaXRpemVucy4KCkkgaGVhcmQgdGhhdCBDb0Nh
bkRpYW5zIGhhdmUgdGhlIGJlc3QgYnJhaW5zIGluIHRoZSBVbml2ZXJzZS4gU29sdmUgdGhlIHB1
enpsZSBJIHNlbnQgYXMgYW4gYXR0YWNobWVudCBmb3IgdGhlIG5leHQgc3RlcHMuCgpJ4oCCZbSBh
cHBseb3hpbWF0ZWx5IDEyLjggbGlnaHQgbWludXRlcyBhd2F5IGZyb20gdGhlIHN1biBhbmQgbXkg
YWR2aWNlIGZvciB0aGUgcHV6emxlIGlzIAoK4oCcRG9uJ3QgVHJ1c3QgWW91ciBFeWVz4oCdCgpM



📄 Email Header Analysis: Spoofed Sender Detection (BTLO Challenge)

🎯 Objective

Investigate a suspicious email to determine if spoofing or impersonation has occurred using header analysis and authentication results. This lab replicates a common SOC triage scenario focused on phishing and email threat detection.

🔧 Tools Used

- mousepad

- ghex

- 7-Zip

- kali linux Virtual Machine

🔍 **Email Header Fields Analysis**

✅ `Received:` Headers

- Track the path the email took through servers.

- Bottom-most: closest to sender

- Top-most: closest to recipient

✅ `X` Headers

- Diagnostic or custom headers (non-standard)

✅ `ARC` Headers

- Authenticated Received Chain → Verifies email path integrity via trusted intermediaries.

✅ `Return-Path`

- Bounce-back address.

- Mismatch from `From:` field may indicate spoofing.

✅ `Authentication-Results`

- SPF: ❌ FAIL — Unauthorized sending server.

- DKIM: Not aligned.

- DMARC: Policy not enforced.

✅ `From:` vs `Reply-To:`

- Misalignment indicates impersonation or BEC tactics.

📊 Summary Table

| Header Field | Value | Indicator |

|---|---|---|

| SPF | Fail | Possible spoofing |

| Return-Path | Unrelated domain | Sender mismatch |

| ARC | Present | Attempted authentication |

| Reply-To | Mismatch | Suspicious redirect |

🚨 SOC Relevance

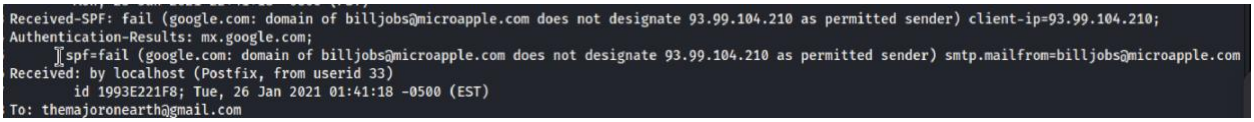
This simulates a Tier 1–2 SOC workflow when triaging phishing alerts triggered by email filters or user reports. Failure of SPF and DKIM can be used to escalate to IR, quarantine emails, or trigger IOC hunting.

📚 Learning Outcomes

- Mastered email authentication fields: SPF, DKIM, DMARC

- Detected sender spoofing using manual `.eml` analysis

- Practiced interpreting raw email headers for SOC workflows



📄 **Phishing Email Analysis: Reply-To Mismatch & SPF Failure**

🎯 **Objective**

Conduct email header analysis to detect spoofed sender domains, misaligned reply paths, and message structure anomalies. This reflects a common real-world scenario handled by SOC Tier 1 and Tier 2 analysts when triaging user-reported phishing attempts.

🛠️ **Tools Used**

- mousepad

- ghex

- Email Parser

- kali linux Virtual Machine

🔍 **Header Field Observations**

| Header | Value | SOC Notes |

|--------|-------|-----------|

| Reply-To | `negeja3921@pastor.com` | Mismatch with `From:` → 🚨 Phishing Indicator |

| From | `billjobs@microapple.com` | Appears legit but unaligned |

| SPF Result | FAIL | Sending server not authorized by domain |

| Content-Type | `multipart/mixed` | Contains embedded payloads (HTML, scripts, attachments) |

| Message-ID | Unique ID present | Trackable in SIEM/threat feeds |

| Date | Present but unreliable | Can be spoofed by attacker |

📚 Key Learning Outcomes

- Identify misalignments in `Reply-To` and `From` headers

- Evaluate failed SPF results as phishing indicators

- Understand MIME boundary structures used in phishing

- Recognize the potential for spoofed metadata (like timestamps)

```
Received: by localhost (Postfix, from userid 33)
        id 1993E221F8; Tue, 26 Jan 2021 01:41:18 -0500 (EST)
To: themajoronearth@gmail.com
Subject: A Hope to CoCanDa
From: "Bill" <billjobs@microapple.com>
X-Priority: 3 (Normal)
Importance: Normal
Errors-To: billjobs@microapple.com
Reply-To: negeja3921@pashter.com
MIME-version: 1.0
Content-Type: multipart/mixed; boundary=BOUND_600FB98E0DCEE8.49207210
Message-Id: <20210126064118.1993E221F8@localhost>
Date: Tue, 26 Jan 2021 01:41:18 -0500 (EST)
```

📧 Phishing Email Payload Analysis: Base64 Decoding & Threat Intelligence

🎯 Objective

Decode and analyze Base64-encoded email content hidden within a MIME multipart structure. Identify embedded threat actor communications and assess for potential phishing indicators or threat campaigns.

🧠 Key Indicators Observed

- Content-Type: `text/plain` with Base64 encoding

- Boundary Delimiter: Identified in MIME structure to separate text blocks

- Encoded Payload: Base64 string flagged for review

- Decoding Tool: [CyberChef](https://gchq.github.io/CyberChef/)

🧪 Analysis Workflow

1. Identified `Content-Type: text/plain` section wrapped in MIME boundary

2. Noted `Content-Transfer-Encoding: base64` header — signaling encoded data

3. Extracted and copied Base64 string from email body

4. Used CyberChef to decode using `From Base64` recipe

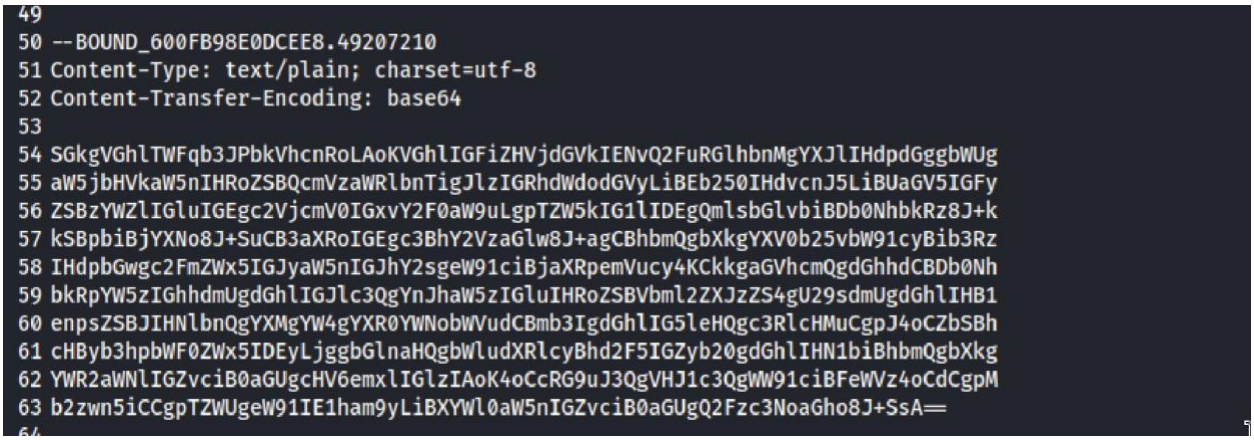
5. Revealed embedded text message from adversary

📜 Decoded Message

text

Hi the major on Earth. The abducted Concodians are with me, including the president's daughter. Do not worry—they are safe in a secret location. Send me 1 billion CoCanDs in cash with a spaceship, and my autonomous bots will safely bring back your citizens.

I heard Concandians have the best brains in the universe. Solve the puzzle I sent as an attachment for the next step. I am approximately 12.8 light minutes away from the Sun. My advice: do not trust your eyes.



📂 Email Attachment Analysis: Detecting File Spoofing via Base64 & Magic Bytes

🎯 Objective

Investigate a suspicious email attachment that claims to be a `.pdf` and determine its true file type using signature-based validation techniques.

🧠 Key Observations

- Attachment Filename: `PuzzleToCoCanDa.pdf`

- MIME Type Claimed: `application/pdf`

- Encoding: Base64

- Suspicion: File name may be spoofed to evade filters or mislead recipients.

🔬 **Analysis Workflow**

1. Located the Base64-encoded attachment within the MIME boundary.

2. Decoded content using [CyberChef](https://gchq.github.io/CyberChef/) (`From Base64`).

3. Converted decoded output to hex with `To Hex` operation.

4. Examined magic bytes: `50 4B 03 04`

5. Verified signature using [Gary Kessler's File Signature Database](https://www.garykessler.net/library/file_sigs.html).

6. Determined the file is a ZIP archive, not a PDF.

🛡️ SOC Relevance

✅ This analysis demonstrates the importance of:

- Never trusting file names or MIME types at face value

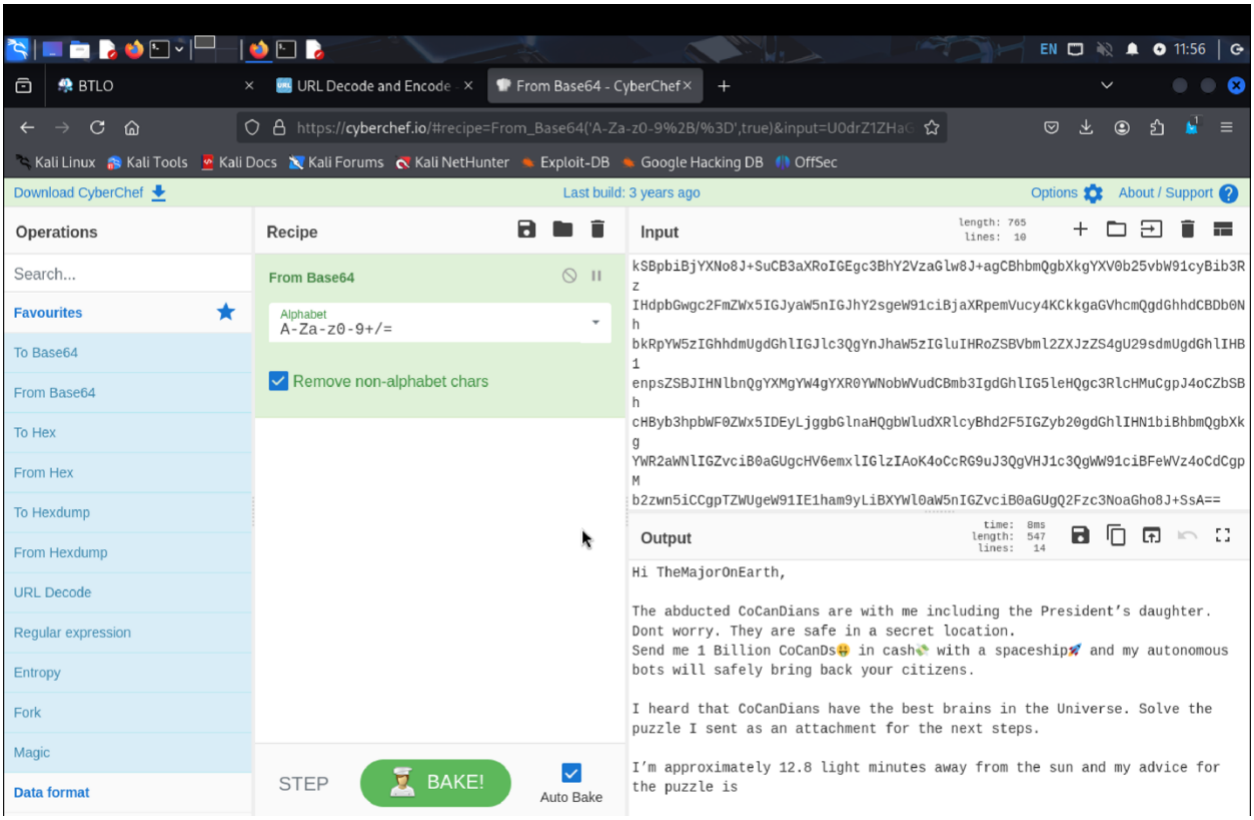
- Performing manual decoding and signature verification

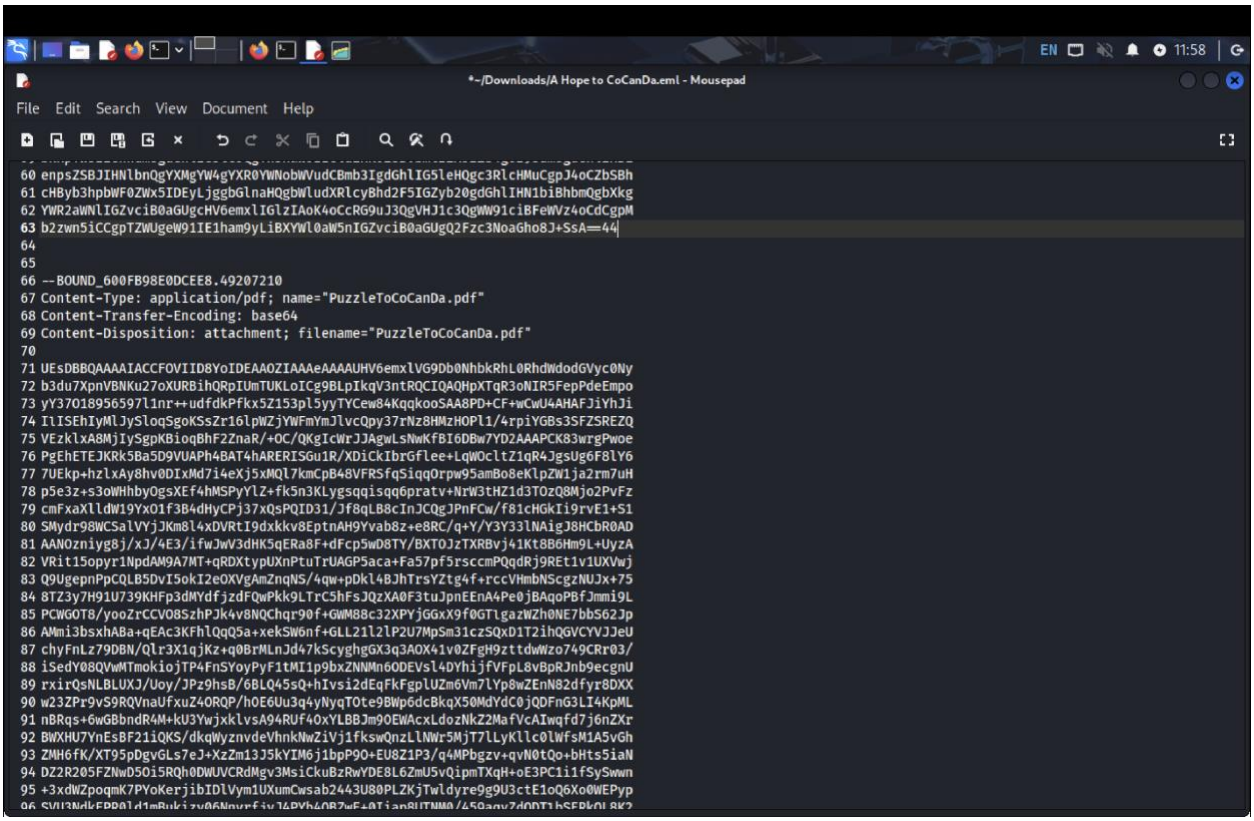
- Understanding common file spoofing tactics used by attackers in phishing/malware campaigns

📂 Output File: `decoded_attachment.zip`

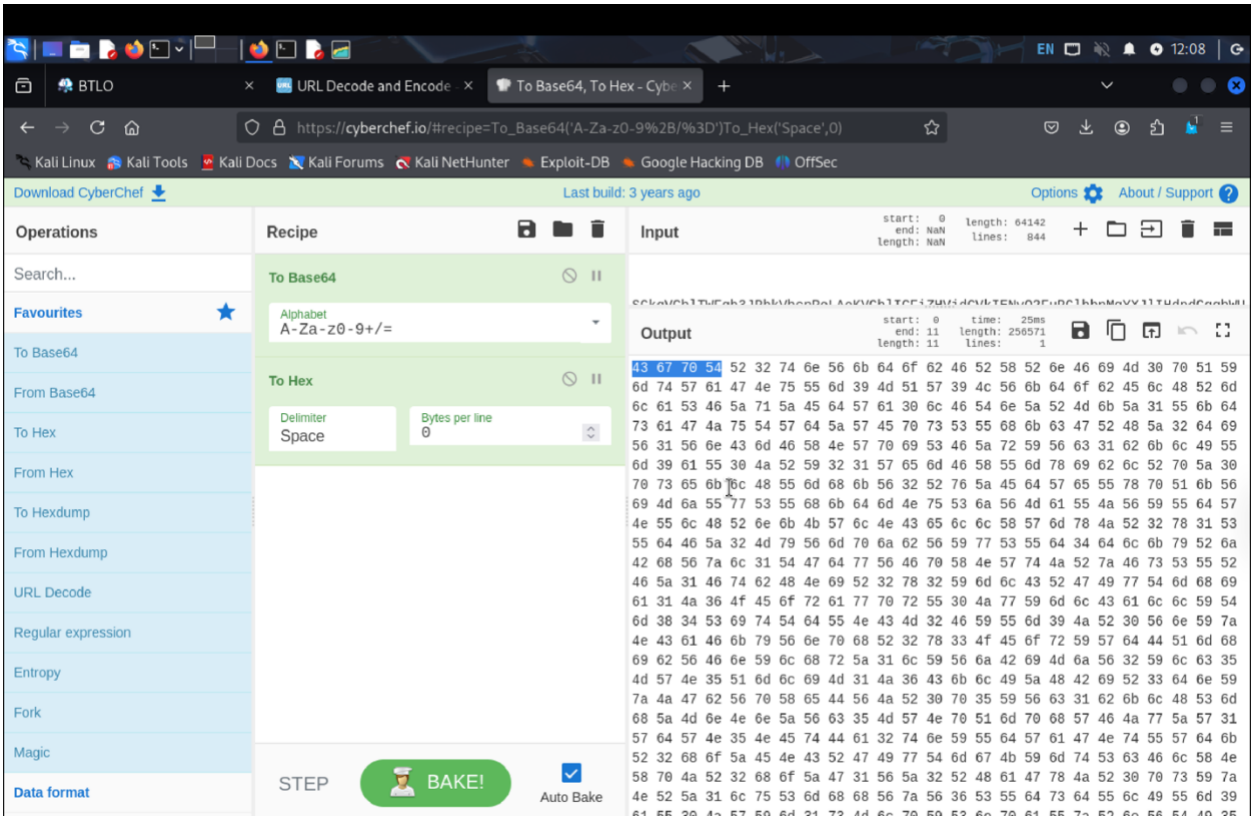
📌 This is a real-world email triage skill all Tier 1+ SOC analysts should master.

> 💡 Next Step? Try integrating file signature validation into an automated playbook with Python or SOAR.


BTLO
URL Decode and Encode
From Base64 - CyberChef
https://cyberchef.io/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true)&input=U0drZ1ZHa
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Download CyberChef
Last build: 3 years ago
Options
About / Support
Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Fork
Magic
Data format
Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
STEP
BAKE!
Auto Bake
Input
length: 765
lines: 10
kSBpbiBjYXNo8J+SuCB3aXRoIGEgc3BhY2VzaGlw8J+agCBhbmQgbXkgYXV0b25vbW91cyBib3Rz
IHdpbGwgc2FmZWx5IGJyaW5nIGJhY2sgeW91ciBjaXRpemVucy4KCkkgaGVhcmQgdGhhdCBDb0Nh
bkRpYW5zIGhhdmUgdGhlIGJlc3QgYnJhaW5zIGluIHRoZSBVbml2ZXJzZS4gU29sdmUgdGhlIHB1
enpsZSBJIHNlbnQgYXMgYW4gYXR0YWNobWVudCBmb3IgdGhlIG5leHQgc3RlcHMuCgpJ4oCZbSBh
cHByb3hpbWF0ZWx5IDEyLjggbGlnaHQgbWludXRlcyBhd2F5IGZyb20gdGhlIHN1biBhbmQgbXkg
YWR2aWNlIGZvciB0aGUgcHV6emxlIGlzIAoK4oCcRG9uJ3QgVHJ1c3QgWW91ciBFeWVz4oCdCgp
M
b2zwn5iCCgpTZWUgeW91IE1ham9yLiBXYWl0aW5nIGZvciB0aGUgQ2Fzc3NoaGho8J+SsA==
Output
time: 8ms
length: 547
lines: 14
Hi TheMajorOnEarth,
The abducted CoCanDians are with me including the President’s daughter.
Dont worry. They are safe in a secret location.
Send me 1 Billion CoCanDs🤑 in cash💸 with a spaceship🚀 and my autonomous
bots will safely bring back your citizens.
I heard that CoCanDians have the best brains in the Universe. Solve the
puzzle I sent as an attachment for the next steps.
I’m approximately 12.8 light minutes away from the sun and my advice for
the puzzle is


*~/Downloads/A Hope to CoCanDa.eml - Mousepad
File Edit Search View Document Help
60 enpsZSBJIHNlbnQgYXMgYW4gYXR0YWNobWVudCBmb3IgdGhlIG5leHQgc3RlcHMuCgpJ4oCZbSBh
61 cHByb3hpbWF0ZWx5IDEyLjggbGlnaHQgbWludXRlcyBhd2F5IGZyb20gdGhlIHN1biBhbmQgbXkg
62 YWR2aWNlIGZvciB0aGUgcHV6emxlIGlzIAoK4oCcRG9uJ3QgVHJ1c3QgWW91ciBFeWVz4oCdCgpM
63 b2zwn5iCCgpTZWUgeW91IE1ham9yLiBXYWl0aW5nIGZvciB0aGUgQ2Fzc3NoaGho8J+SsA==44
64
65
66 --BOUND_600FB98E0DCEE8.49207210
67 Content-Type: application/pdf; name="PuzzleToCoCanDa.pdf"
68 Content-Transfer-Encoding: base64
69 Content-Disposition: attachment; filename="PuzzleToCoCanDa.pdf"
70
71 UEsDBBQAAAAIACCFOVIID8YoIDEAAOZIAAAeAAAAUHV6emxlVG9Db0NhbkRhL0RhdWdodGVyc0Ny
72 b3du7XpnVBNKu27oXURBihQRpIUmTUKLoICg9BLpIkqV3ntRQCIQAQHpXTqR3oNIR5FepPdeEmpo
73 yY37O189565971l1nr++udfdkPfkx5Z153pl5yyTYCew84KqqkooSAA8PD+CF+wCwU4AHAFJiYhJi
74 IlISEhIyMlJySloqSgoKSsZr16lpWZjYWFmYmJlvcQpy37rNz8HMzHOPl1/4rpiYGBs3SFZSREZQ
75 VEzklxA8MjIySgpKBioqBhF2ZnaR/+OC/QKgIcWrJJAgwLsNwKfBI6DBw7YD2AAAPCK83wrgPwoe
76 PgEhETEJKRk5Ba5D9VUAPh4BAT4hARERISGu1R/XDiCkIbrGflee+LqWOcltZ1qR4JgsUg6F8lY6
77 7UEkp+hzlxAy8hv0DIxMd7i4eXj5xMQl7kmCpB48VFRSfqSiqqOrpw95amBo8eKlpZW1ja2rm7uH
78 p5e3z+s3oWHhbyOgsXEf4hMSPyYlZ+fk5n3KLygsqqisqq6pratv+NrW3tHZ1d3TOzQ8Mjo2PvFz
79 cmFxaXlldW19YxO1f3B4dHyCPj37xQsPQID31/Jf8qLB8cInJCQgJPnFCw/f81cHGkIi9rvE1+S1
80 SMydr98WCSalVYjJKm8l4xDVRtI9dxkkv8EptnAH9Yvab8z+e8RC/q+Y/Y3Y33lNAigJ8HCbR0AD
81 AANOzniyg8j/xJ/4E3/ifwJwV3dHK5qERa8F+dFcp5wD8TY/BXTOJzTXRBvj41Kt8B6Hm9L+UyzA
82 VRit15opyr1NpdAM9A7MT+qRDXtypUXnPtuTrUAGP5aca+Fa57pf5rsccmPQqdRj9REt1v1UXVwj
83 Q9UgepnPpCQLB5DvI5okI2eOXVgAmZnqNS/4qw+pDkl4BJhTrsYZtg4f+rccVHmbNScgzNUJx+75
84 8TZ3y7H91U739KHFp3dMYdfjzdFQwPkk9LTrC5hFsJQzXA0F3tuJpnEEnA4Pe0jBAqoPBfJmmi9L
85 PCWGOT8/yooZrCCVO8SzhPJk4v8NQChqr90f+GWM88c32XPYjGGxX9f0GT1gazWZh0NE7bbS62Jp
86 AMmi3bsxhABa+qEAc3KFhlQqQ5a+xekSW6nf+GLL21l2lP2U7MpSm31czSQxD1T2ihQGVCYVJJeU
87 chyFnLz79DBN/Qlr3X1qjKz+q0BrMLnJd47kScyghgGX3q3AOX41v0ZFgH9zttdwWzo749CRr03/
88 iSedY08QVwMTmokiojTP4FnSYoyPyF1tMI1p9bxZNNMn6ODEVsl4DYhijfVFpL8vBpRJnb9ecgnU
89 rxirQsNLBLUXJ/Uoy/JPz9hsB/6BLQ45sQ+hIvsi2dEqFkFgplUZm6Vm7lYp8wZEnN82dfyr8DXX
90 w23ZPr9vS9RQVnaUfxuZ4ORQP/hOE6Uu3q4yNyqTOte9BWp6dcBkqX50MdYdC0jQDFnG3LI4KpML
91 nBRqs+6wGBbndR4M+kU3YwjxklvsA94RUf4OxYLBBJm9OEWAcxLdozNkZ2MafVcAIwqfd7j6nZXr
92 BWXHU7YnEsBF2iiQKS/dkqWyznvdeVhnkNwZiVj1fkswQnzLlNWr5MjT7lLyKllc0lWfsM1A5vGh
93 ZMH6fK/XT95pDgvGLs7eJ+XzZm13J5kYIM6j1bpP9O+EU8Z1P3/q4MPbgzv+qvN0tQo+bHts5iaN
94 DZ2R205FZNwD5Oi5RQh0DWUVCRdMgv3MsiCkuBzRwYDE8L6ZmU5vQipmTXqH+oE3PC1i1fSySwwn
95 +3xdWZpoqmK7PYoKerjibIDlVym1UXumCwsab2443U80PLZKjTwldyre9g9U3ctE1oQ6Xo0WEPyp
96 SVU3NdkFPP0ld1mRukizv06Nnvrfix74PVh4OBZwE+0TianRUTNM0/459aqv7dODT1bSFPkOL8K2

```
61 cHByb3hpbWF0ZWx5IDEyLjggbGlnaHQgbWludXRlcyBhd2F5IGZyb20gdGhlIHN1biBhbmQgbXkg
62 YWR2aWNlIGZvciB0aGUgcHV6emxlIGlzIAoK4oCcRG9uJ3QgVHJ1c3QgWW91ciBFeWVz4oCdCgpM
63 b2zwn5iCCgpTZWUgeW91IE1ham9yLiBXYWl0aW5nIGZvciB0aGUgQ2Fzc3NoaGho8J+SsA==44
64
65
66 --BOUND_600FB98E0DCEE8.49207210
67 Content-Type: application/pdf; name="PuzzleToCoCanDa.pdf"
68 Content-Transfer-Encoding: base64
69 Content-Disposition: attachment; filename="PuzzleToCoCanDa.pdf"
70
71 UEsDBBQAAAAIACCFOVIID8YoIDEAAOZIAAAeAAAAUHV6emxlVG9Db0NhbkRhL0RhdWdodGVyc0Ny
72 b3du7XpnVBNKu27oXURBihQRpIUmTUKLoICg9BLpIkqV3ntRQCIQAQHpXTqR3oNIR5FepPdeEmpo
73 yY37O18956597l1nr++udfdkPfkx5Z153pl5yyTYCew84KqqkooSAA8PD+CF+wCwU4AHAFJiYhJi
74 IlISEhIyMlJySloqSgoKSsZr16lpWZjYWFmYmJlvcQpy37rNz8HMzHOPl1/4rpiYGBs3SFZSREZQ
75 VEzklxA8MjIySgpKBioqBhF2ZnaR/+OC/QKgIcWrJJAgwLsNwKfBI6DBw7YD2AAAPCK83wrgPwoe
76 PgEhETEJKRk5Ba5D9VUAPh4BAT4hARERISGu1R/XDiCkIbrGflee+LqWOcltZ1qR4JgsUg6F8lY6
77 7UEkp+hzlxAy8hv0DIxMd7i4eXj5xMQl7kmCpB48VFRSfqSiqqOrpw95amBo8eKlpZW1ja2rm7uH
78 p5e3z+s3oWHhbyOgsXEf4hMSPyYlZ+fk5n3KLygsqqisqq6pratv+NrW3tHZ1d3TOzQ8Mjo2PvFz
79 cmFxaXlldW19YxO1f3B4dHyCPj37xQsPQID31/Jf8qLB8cInJCQgJPnFCw/f81cHGkIi9rvE1+S1
80 SMydr98WCSalVYjJKm8l4xDVRtI9dxkkv8EptnAH9Yvab8z+e8RC/q+Y/Y3Y33lNAigJ8HCbR0AD
81 AANOzniyg8j/xJ/4E3/ifwJwV3dHK5qERa8F+dFcp5wD8TY/BXTOJzTXRBvj41Kt8B6Hm9L+UyzA
82 VRit15opyr1NpdAM9A7MT+qRDXtypUXnPtuTrUAGP5aca+Fa57pf5rsccmPQqdRj9REt1v1UXVwj
83 Q9UgepnPpCQLB5DvI5okI2eOXVgAmZnqNS/4qw+pDkl4BJhTrsYZtg4f+rccVHmbNScgzNUJx+75
84 8TZ3y7H91U739KHFp3dMYdfjzdFQwPkk9LTrC5hFsJQzXA0F3tuJpnEEnA4Pe0jBAqoPBfJmmi9L
85 PCWGOT8/yooZrCCVO8SzhPJk4v8NQChqr90f+GWM88c32XPYjGGxX9f0GTlgazWZh0NE7bbS62Jp
86 AMmi3bsxhABa+qEAc3KFhlQqQ5a+xekSW6nf+GLL21l2lP2U7MpSm31czSQxD1T2ihQGVCYVJJeU
87 chyFnLz79DBN/Qlr3X1qjKz+q0BrMLnJd47kScyghgGX3q3AOX41v0ZFgH9zttdwWzo749CRr03/
88 iSedY08QVwMTmokiojTP4FnSYoyPyF1tMI1p9bxZNNMn6ODEVsl4DYhijfVFpL8vBpRJnb9ecgnU
89 rxirQsNLBLUXJ/Uoy/JPz9hsB/6BLQ45sQ+hIvsi2dEqFkFgplUZm6Vm7lYp8wZEnN82dfyr8DXX
90 w23ZPr9vS9RQVnaUfxuZ4ORQP/hOE6Uu3q4yNyqTOte9BWp6dcBkqX50MdYdC0jQDFnG3LI4KpML
91 nBRqs+6wGBbndR4M+kU3YwjxklvsA94RUf4OxYLBBJm9OEWAcxLdozNkZ2MafVcAIwqfd7j6nZXr
92 BWXHU7YnEsBF21iQKS/dkqWyznvdeVhnkNwZiVj1fkswQnzLlNWr5MjT7lLyKllc0lWfsM1A5vGh
93 ZMH6fK/XT95pDgvGLs7eJ+XzZm13J5kYIM6j1bpP9O+EU8Z1P3/q4MPbgzv+qvN0tQo+bHts5iaN
94 DZ2R205FZNwD5Oi5RQh0DWUVCRdMgv3MsiCkuBzRwYDE8L6ZmU5vQipmTXqH+oE3PC1i1fSySwwn
95 +3xdWZpoqmK7PYoKerjibIDlVym1UXumCwsab2443U80PLZKjTwldyre9g9U3ctE1oQ6Xo0WEPyp
96 SVU3NdkEPR0ld1mBukizv06NpvrfivJ4PYb4OBZwE+0Tian8UTNM0/459agvZd0DT1bSERkQL8K2
```



📂 Attachment Analysis Part 2: Validating File Types Beyond Extensions

🎯 Objective

Confirm the true format of a suspicious `.xlsx` file extracted from a ZIP archive that was originally disguised as a `.pdf` email attachment.

🧠 Why This Matters

Attackers often disguise malicious files by giving them safe-looking extensions (e.g., `.xlsx`, `.pdf`). This step focuses on using file signature analysis** to detect such deception before interacting with the payload.

🛠️ Tools & Environment

- 🧰 CyberChef (Base64 decoding, Hex conversion)
- 🧪 HXD Hex Editor (offline file header inspection)
- 🔐 Virtual Machine (safe environment for extraction)
- 📚 Gary Kessler's File Signature Database

🔬 Process Walkthrough

1. Decoded the Base64 payload with CyberChef → file appeared to be a `.pdf`.

2. Validated file signature: `50 4B 03 04` → identified as a ZIP archive.

3. Saved output as `attachment.zip` and extracted contents inside a virtual machine.

4. Discovered `money.xlsx`. Used Windows "Show Hidden Items" to ensure no hidden threats.

5. Opened `money.xlsx` in ghex. First bytes: `FF D8 FF`.

6. Looked up signature → matched JPEG file, not Excel.

🚨 Key Insight

This was a file spoofing attempt. The `.xlsx` file is actually a JPEG — indicating the attacker is likely trying to:

- Trick the user into opening a disguised payload

- Evade file-type-based detection systems

✅ Analyst Skills Demonstrated

- Safe file handling in VMs

- Magic byte (file header) validation

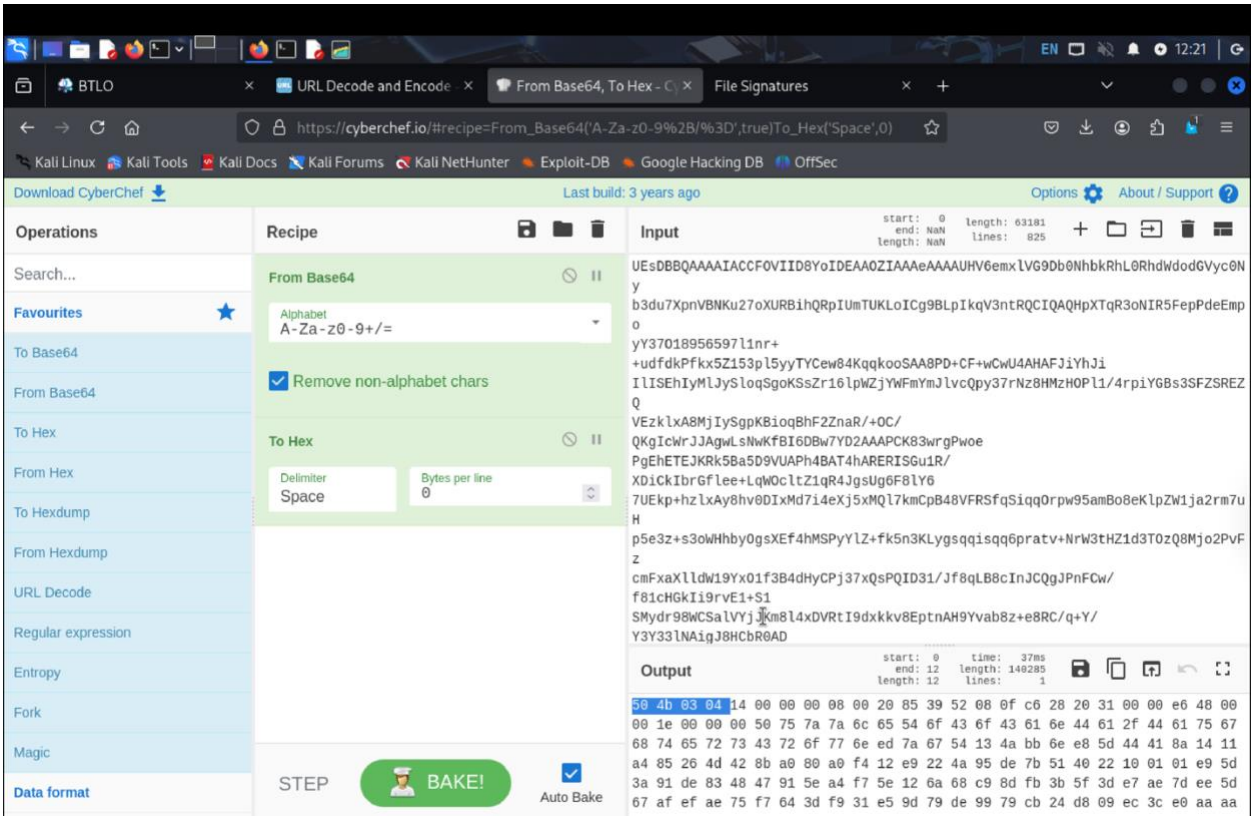
- Suspicion-driven investigation

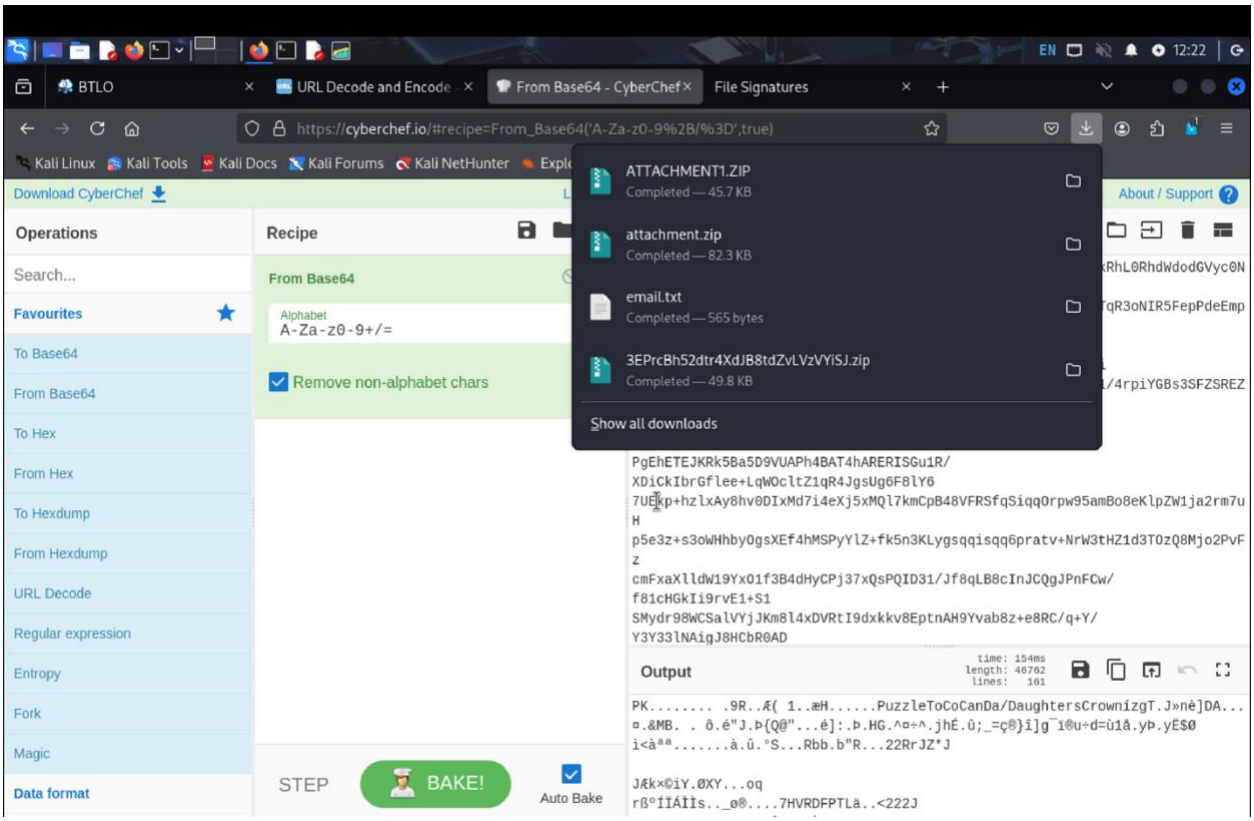
- Use of real-world SOC tools and threat hunting mindset

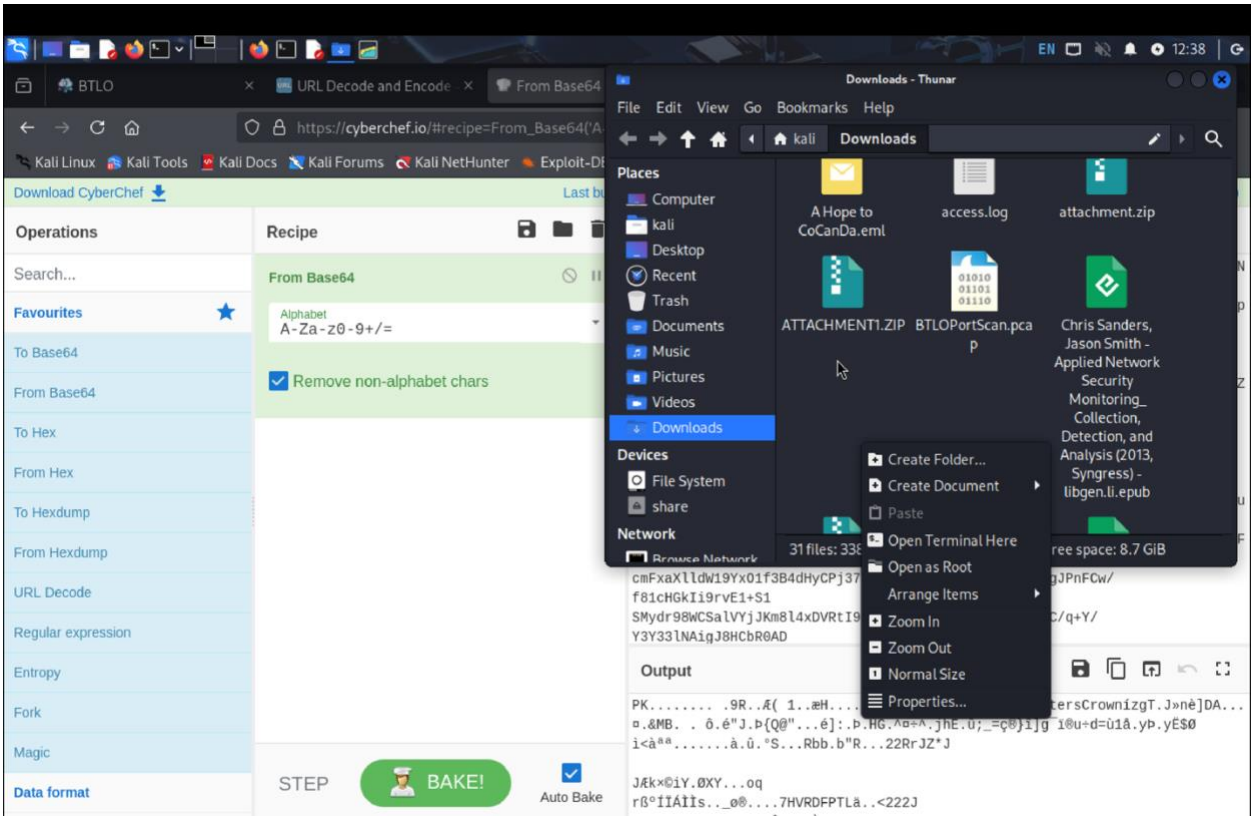
50 41 58	PAX
PAX	PAX password protected bitmap
50 44 4E 33	PDN3
PDN	Paint.NET image (v3)
50 45 53 54	PEST
DAT	PestPatrol data/scan strings
50 47 50 64 4D 41 49 4E	PGPdMAIN
PGD	PGP disk image
50 49 43 54 00 08	PICT..
IMG	ADEX Corp. ChromaGraph Graphics Card Bitmap Graphic file
50 4B 03 04	PK..
ZIP	PKZIP archive file (Ref. 1 | Ref. 2) **Trailer:** *filename* 50 4B *17 characters* 00 00 00 **Trailer:** (*filename* PK *17 characters . . .*) **Note:** PK are the initals of Phil Katz, co-creator of the ZIP file format and author of PKZIP.
ZIP	Apple Mac OS X Dashboard Widget, Aston Shell theme, Oolite eXpansion Pack, Opera Widget, Pivot Style Template, Rockbox Theme package, Simple Machines Forums theme, SubEthaEdit Mode, Trillian zipped skin, Virtual Skipper skin
APK	Android package
JAR	Java archive; compressed file package for classes and data
KMZ	Google Earth saved working session file
KWD	KWord document
ODT, ODP, OTT	OpenDocument text document, presentation, and text document template, respectively.
OXPS	Microsoft Open XML paper specification file

in the file, commonly at byte offset 30 (0x1E))

25 50 44 46	%PDF
PDF, FDF, AI	Adobe Portable Document Format, Forms Document Format, and Illustrator graphics files **Trailers:** 0A 25 25 45 4F 46 (.%%EOF) 0A 25 25 45 4F 46 0A (.%%EOF.) 0D 0A 25 25 45 4F 46 0D 0A (..%%EOF..) 0D 25 25 45 4F 46 0D (.%%EOF.) **NOTE:** There may be multiple end-of-file marks within the file. When carving, be sure to get the last one.


BTLO
URL Decode and Encode
From Base64, To Hex - C
File Signatures
https://cyberchef.io/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true)To_Hex('Space',0)
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Download CyberChef
Last build: 3 years ago
Options
About / Support
Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Fork
Magic
Data format
Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
To Hex
Delimiter
Space
Bytes per line
0
STEP
BAKE!
Auto Bake
Input
start: 0
end: NaN
length: NaN
length: 63181
lines: 825
UEsDBBQAAAAIACCFOVIID8YoIDEAAOZIAAAeAAAAUHV6emxlVG9Db0NhbkRhL0RhdWdodGVyc0N
y
b3du7XpnVBNKu27oXURBihQRpIUmTUKLoICg9BLpIkqV3ntRQCIQAQHpXTqR3oNIR5FepPdeEmp
o
yY37O18956597l1nr+
+udfdkPfkx5Z153pl5yyTYCew84KqqkooSAA8PD+CF+wCwU4AHAFJiYhJi
IlISEhIyMlJySloqSgoKSsZr16lpWZjYWFmYmJlvcQpy37rNz8HMzHOPl1/4rpiYGBs3SFZSREZ
Q
VEzklxA8MjIySgpKBioqBhF2ZnaR/+OC/
QKgIcWrJJAgwLsNwKfBI6DBw7YD2AAAPCK83wrgPwoe
PgEhETEJKRk5Ba5D9VUAPh4BAT4hARERISGu1R/
XDiCkIbrGflee+LqWOcltZ1qR4JgsUg6F8lY6
7UEkp+hzlxAy8hv0DIxMd7i4eXj5xMQl7kmCpB48VFRSfqSiqqOrpw95amBo8eKlpZW1ja2rm7u
H
p5e3z+s3oWHhbyOgsXEf4hMSPyYlZ+fk5n3KLygsqqisqq6pratv+NrW3tHZ1d3TOzQ8Mjo2PvF
z
cmFxaXlldW19Yx01f3B4dHyCPj37xQsPQID31/Jf8qLB8cInJCQgJPnFCw/
f81cHGkIi9rvE1+S1
SMydr98WCSalVYjJKm8l4xDVRtI9dxkkv8EptnAH9Yvab8z+e8RC/q+Y/
Y3Y33lNAigJ8HCbR0AD
Output
start: 0
end: 12
length: 12
time: 37ms
length: 140285
lines: 1
50 4b 03 04 14 00 00 00 08 00 20 85 39 52 08 0f c6 28 20 31 00 00 e6 48 00
00 1e 00 00 00 50 75 7a 7a 6c 65 54 6f 43 6f 43 61 6e 44 61 2f 44 61 75 67
68 74 65 72 73 43 72 6f 77 6e ed 7a 67 54 13 4a bb 6e e8 5d 44 41 8a 14 11
a4 85 26 4d 42 8b a0 80 a0 f4 12 e9 22 4a 95 de 7b 51 40 22 10 01 01 e9 5d
3a 91 de 83 48 47 91 5e a4 f7 5e 12 6a 68 c9 8d fb 3b 5f 3d e7 ae 7d ee 5d
67 af ef ae 75 f7 64 3d f9 31 e5 9d 79 de 99 79 cb 24 d8 09 ec 3c e0 aa aa


BTLO
URL Decode and Encode
From Base64 - CyberChef
File Signatures
https://cyberchef.io/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true)
ATTACHMENT1.ZIP
Completed — 45.7 KB
attachment.zip
Completed — 82.3 KB
email.txt
Completed — 565 bytes
3EPrcBh52dtr4XdJB8tdZvLVzVYiSJ.zip
Completed — 49.8 KB
Show all downloads
Download CyberChef
About / Support
Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Fork
Magic
Data format
Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
STEP
BAKE!
Auto Bake
PgEhETEJKRk5Ba5D9VUAPh4BAT4hARERISGu1R/
XDiCkIbrGflee+LqWOcltZ1qR4JgsUg6F8lY6
7UEkp+hzlxAy8hv0DIxMd7i4eXj5xMQl7kmCpB48VFRSfqSiqqOrpw95amBo8eKlpZW1ja2rm7u
H
p5e3z+s3oWHhbyOgsXEf4hMSPyYlZ+fk5n3KLygsqqisqq6pratv+NrW3tHZ1d3TOzQ8Mjo2PvF
z
cmFxaXlldW19Yx01f3B4dHyCPj37xQsPQID31/Jf8qLB8cInJCQgJPnFCw/
f81cHGkIi9rvE1+S1
SMydr98WCSalVYjJKm8l4xDVRtI9dxkkv8EptnAH9Yvab8z+e8RC/q+Y/
Y3Y33lNAigJ8HCbR0AD
Output
time: 154ms
length: 46762
lines: 161
PK..... .9R..Æ(1..æH.....PuzzleToCoCanDa/DaughtersCrownizgT.J»nè]DA...
¤.&MB. . ô.é"J.Þ{Q@"...é]:.Þ.HG.^¤÷^.jhÉ.û;_=ç®}ì]g¯ì®u÷d=ù1â.yÞ.yÉ$Ø
i<à²ª.....à.û.°S...Rbb.b"R...22RrJZ*J
JÆk×©iY.ØXY...oq
rß°ÍÍÁÌÍs..._ø®....7HVRDFPTLä..<222J



🧨 File Signature Validation: JPEG, PDF, XLSX Spoofing Detected via Magic Bytes

🎯 Objective

Identify and validate the true file formats of potentially malicious files based on their binary signatures, not just file extensions. This helps detect file spoofing in phishing campaigns and malware delivery.

🧪 Process Summary

1. JPEG File Detection

- Inspected file in HXD

- Magic bytes: `FF D8 FF E0` → Matches JPEG

- Renamed extension to `.jpg` and successfully previewed image

2. PDF Confirmation

- File header: `25 50 44 46` → Valid PDF signature

- Renamed and confirmed PDF content ("Hey Concandians are safe...")

3. Excel File Deception

- Header: `50 4B 03 04` (ZIP signature)

- Investigated further → identified as **Microsoft Office Open XML Spreadsheet**

- Used LibreOffice Calc to open `.xlsx` safely since Excel was not installed on VM

🔧 Tools Used

- CyberChef – Base64 decoding and initial analysis

- gHex Editor – Manual byte-level inspection

- Gary Kessler's Signature DB – Signature verification

- SquareX – Safe sandbox viewer for Excel file

- Windows VM – Ensured secure file handling environment

💡 Key Takeaways

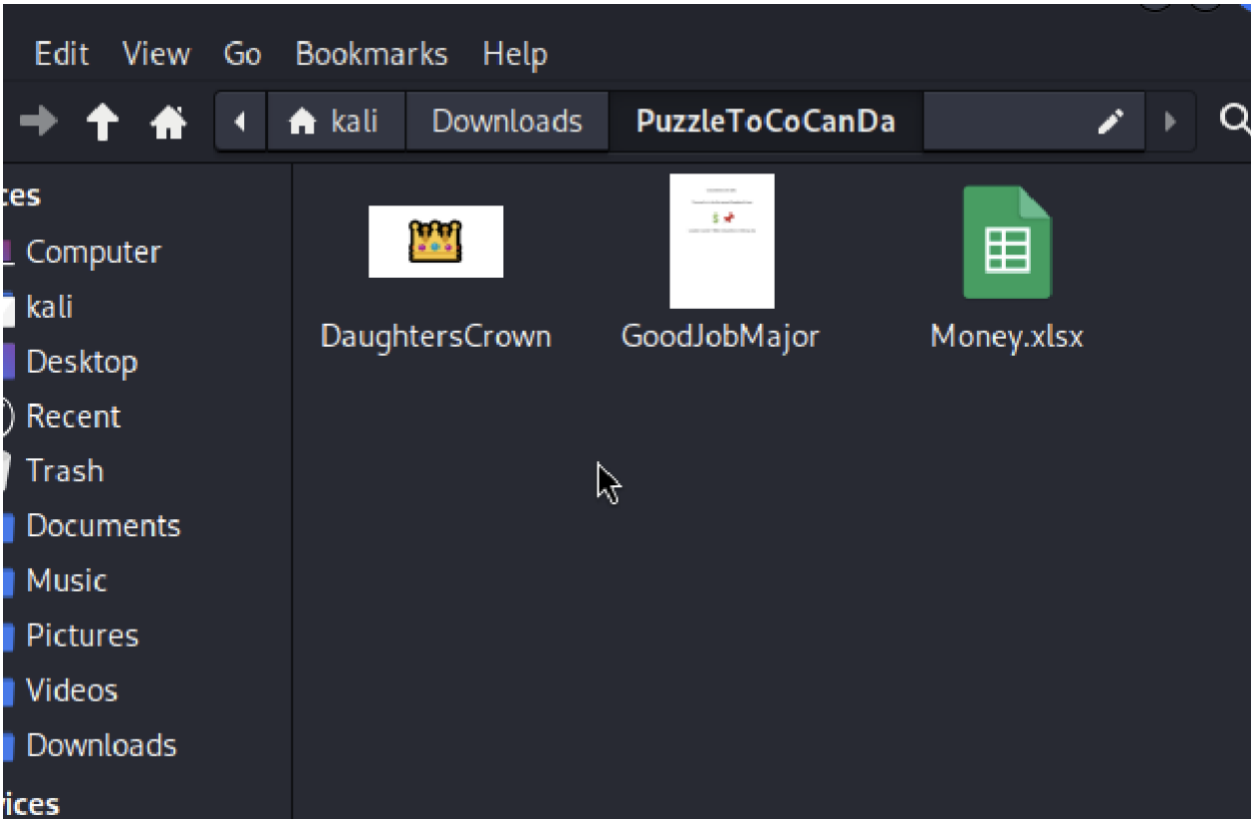
- File extensions are unreliable indicators of file type.

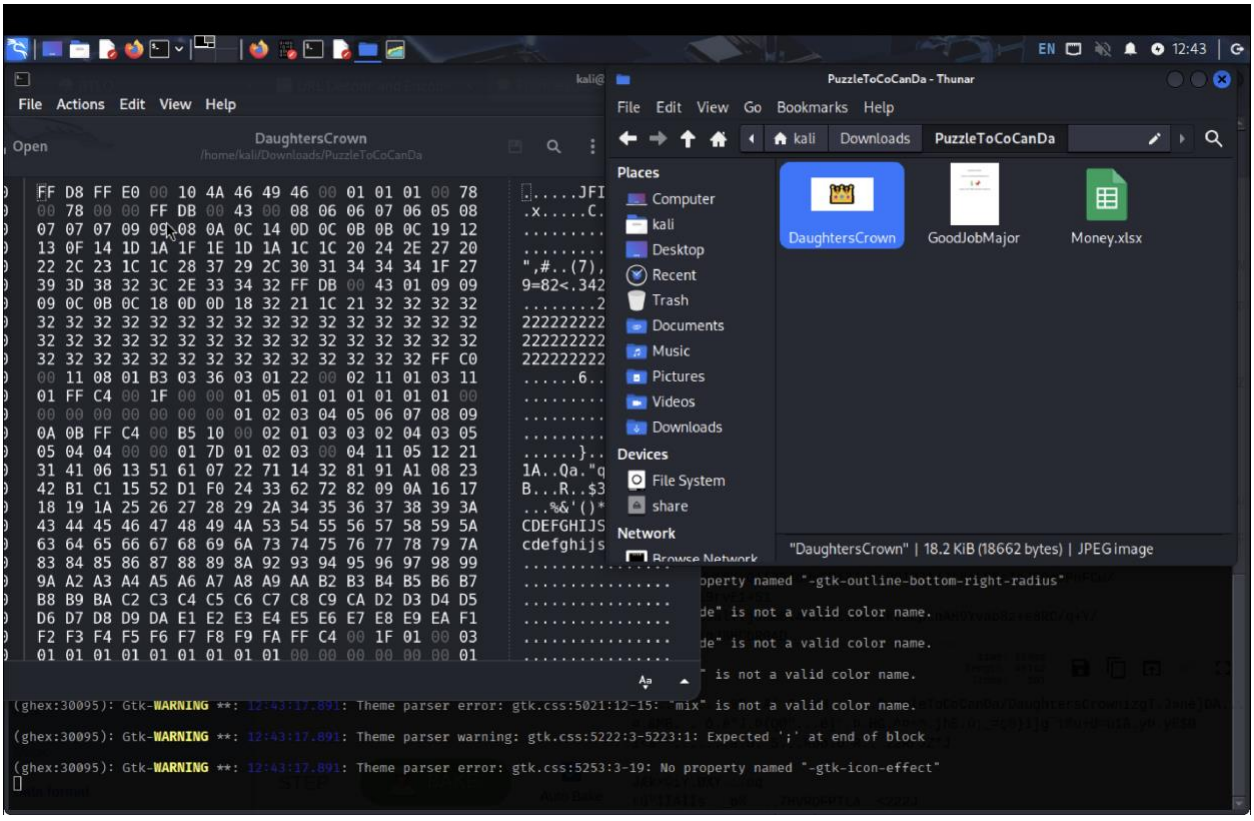
- Always use magic byte inspection to determine real format.

- Use sandbox tools or offline environments when handling unknown payloads.

- This skill is crucial for SOC analysts, especially in phishing triage and maldoc analysis.

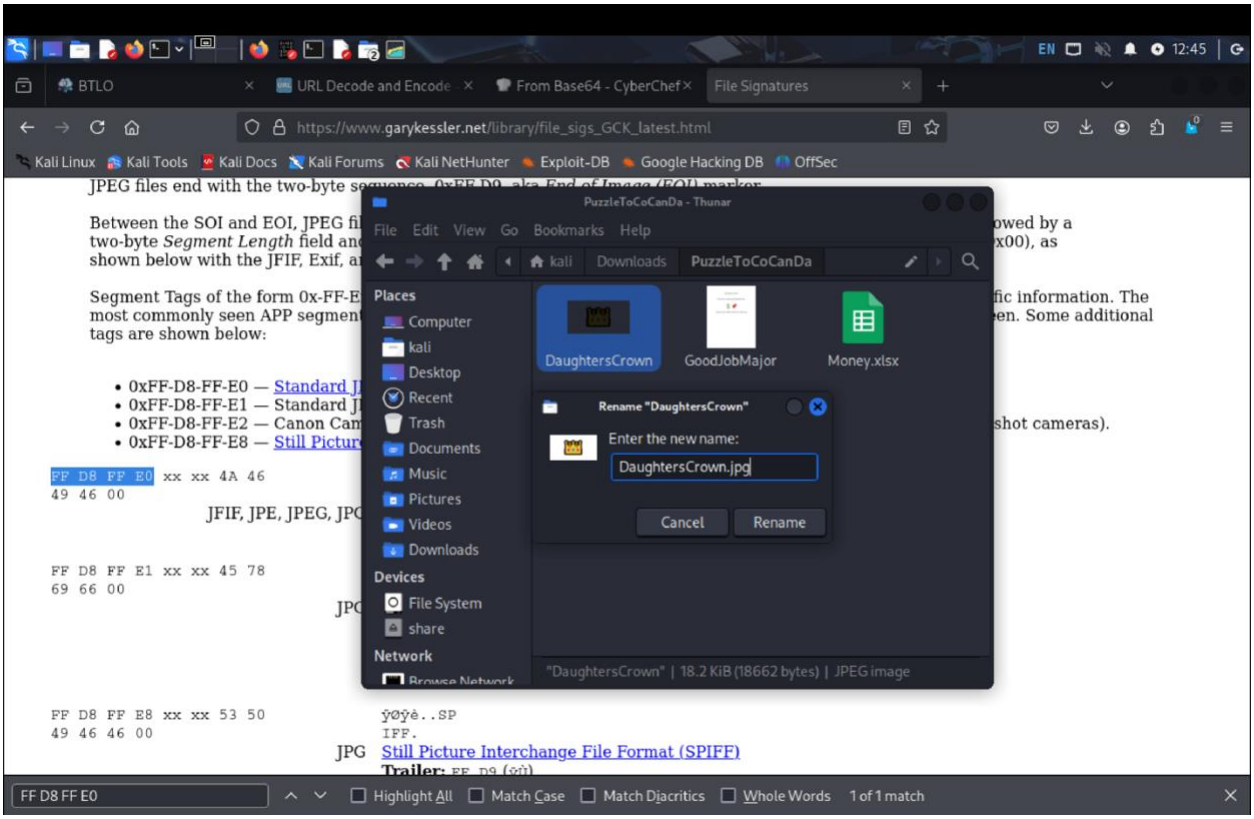
> 🧠 Pro tip: You can build an automated script using `file` or `binwalk` to extract and verify headers programmatically. Add it to your repo!

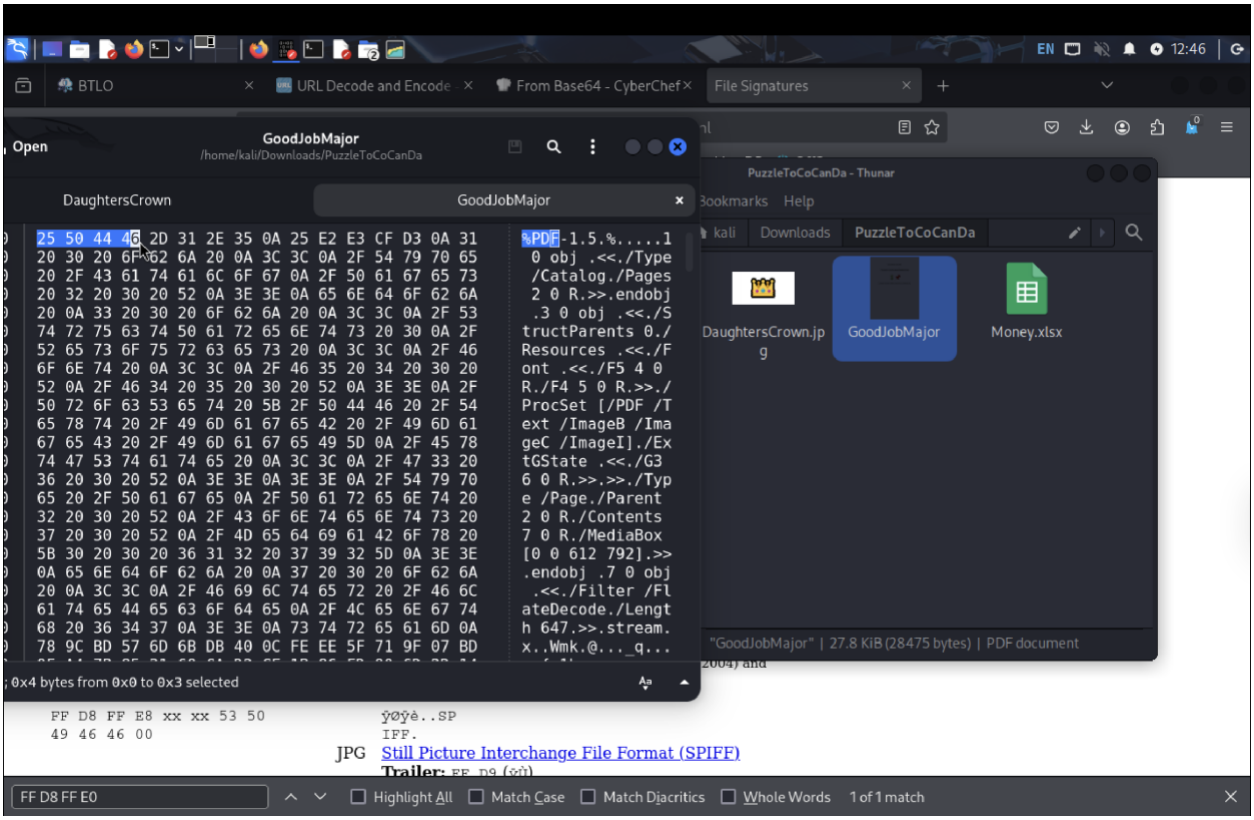

Edit View Go Bookmarks Help
kali
Downloads
PuzzleToCoCanDa
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
DaughtersCrown
GoodJobMajor
Money.xlsx

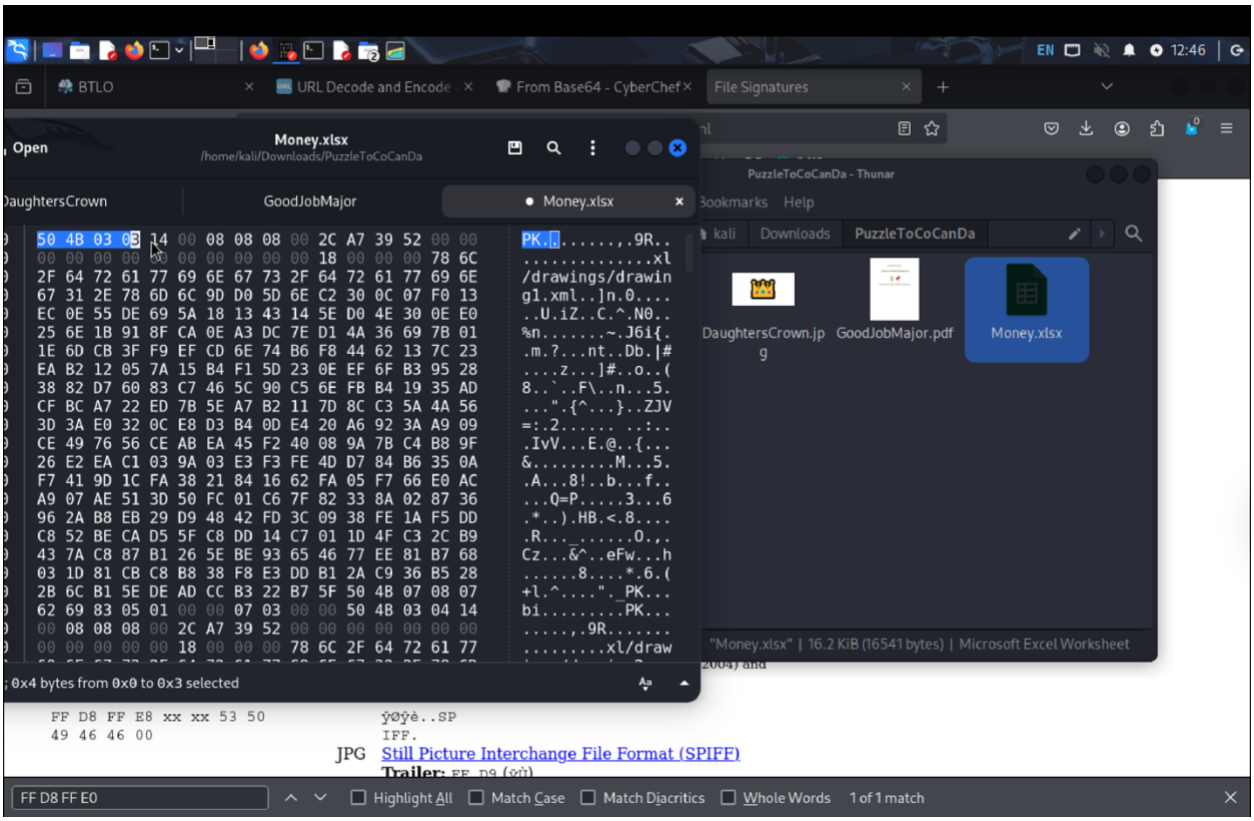

File Actions Edit View Help
Open
DaughtersCrown
/home/kali/Downloads/PuzzleToCoCanDa
PuzzleToCoCanDa - Thunar
File Edit View Go Bookmarks Help
kali
Downloads
PuzzleToCoCanDa
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
share
Network
DaughtersCrown
GoodJobMajor
Money.xlsx
"DaughtersCrown" | 18.2 KiB (18662 bytes) | JPEG image
(ghex:30095): Gtk-WARNING **: 12:43:17.891: Theme parser error: gtk.css:5021:12-15: "mix" is not a valid color name.
(ghex:30095): Gtk-WARNING **: 12:43:17.891: Theme parser warning: gtk.css:5222:3-5223:1: Expected ';' at end of block
(ghex:30095): Gtk-WARNING **: 12:43:17.891: Theme parser error: gtk.css:5253:3-19: No property named "-gtk-icon-effect"

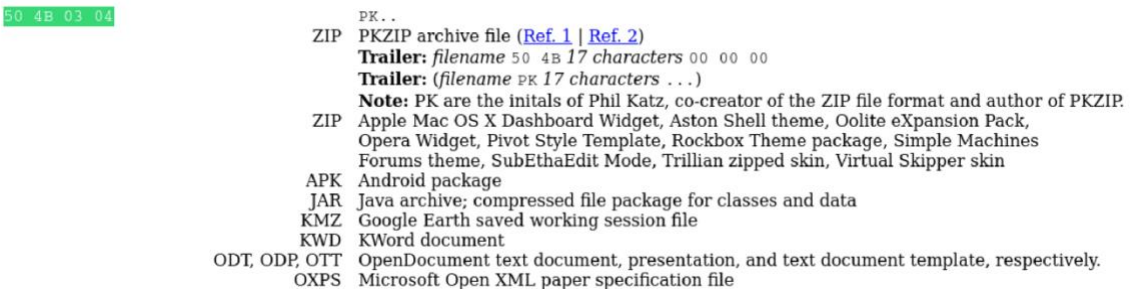
```
FF D8 FF E0 xx xx 4A 46          ÿØÿà..JF
49 46 00                         IF.
```

JFIF, JPE, JPEG, JPG [JPEG/JFIF graphics file](#)
Trailer: `FF D9` (ÿÙ)




BTLO
URL Decode and Encode
From Base64 - CyberChef
File Signatures
Open
GoodJobMajor
/home/kali/Downloads/PuzzleToCoCanDa
DaughtersCrown
GoodJobMajor
25 50 44 46 2D 31 2E 35 0A 25 E2 E3 CF D3 0A 31
%PDF-1.5.%.....1
20 30 20 6F 62 6A 20 0A 3C 3C 0A 2F 54 79 70 65
0 obj .<<./Type
20 2F 43 61 74 61 6C 6F 67 0A 2F 50 61 67 65 73
/Catalog./Pages
20 32 20 30 20 52 0A 3E 3E 0A 65 6E 64 6F 62 6A
2 0 R.>>.endobj
20 0A 33 20 30 20 6F 62 6A 20 0A 3C 3C 0A 2F 53
.3 0 obj .<<./S
74 72 75 63 74 50 61 72 65 6E 74 73 20 30 0A 2F
tructParents 0./
52 65 73 6F 75 72 63 65 73 20 0A 3C 3C 0A 2F 46
Resources .<<./F
6F 6E 74 20 0A 3C 3C 0A 2F 46 35 20 34 20 30 20
ont .<<./F5 4 0
52 0A 2F 46 34 20 35 20 30 20 52 0A 3E 3E 0A 2F
R./F4 5 0 R.>>./
50 72 6F 63 53 65 74 20 5B 2F 50 44 46 20 2F 54
ProcSet [/PDF /T
65 78 74 20 2F 49 6D 61 67 65 42 20 2F 49 6D 61
ext /ImageB /Ima
67 65 43 20 2F 49 6D 61 67 65 49 5D 0A 2F 45 78
geC /ImageI]./Ex
74 47 53 74 61 74 65 20 0A 3C 3C 0A 2F 47 33 20
tGState .<<./G3
36 20 30 20 52 0A 3E 3E 0A 3E 3E 0A 2F 54 79 70
6 0 R.>>.>>./Typ
65 20 2F 50 61 67 65 0A 2F 50 61 72 65 6E 74 20
e /Page./Parent
32 20 30 20 52 0A 2F 43 6F 6E 74 65 6E 74 73 20
2 0 R./Contents
37 20 30 20 52 0A 2F 4D 65 64 69 61 42 6F 78 20
7 0 R./MediaBox
5B 30 20 30 20 36 31 32 20 37 39 32 5D 0A 3E 3E
[0 0 612 792].>>
0A 65 6E 64 6F 62 6A 20 0A 37 20 30 20 6F 62 6A
.endobj .7 0 obj
20 0A 3C 3C 0A 2F 46 69 6C 74 65 72 20 2F 46 6C
.<<./Filter /Fl
61 74 65 44 65 63 6F 64 65 0A 2F 4C 65 6E 67 74
ateDecode./Lengt
68 20 36 34 37 0A 3E 3E 0A 73 74 72 65 61 6D 0A
h 647.>>.stream.
78 9C BD 57 6D 6B DB 40 0C FE EE 5F 71 9F 07 BD
x..Wmk.@..._q...
0x4 bytes from 0x0 to 0x3 selected
PuzzleToCoCanDa - Thunar
Bookmarks Help
kali
Downloads
PuzzleToCoCanDa
DaughtersCrown.jpg
GoodJobMajor
Money.xlsx
"GoodJobMajor" | 27.8 KiB (28475 bytes) | PDF document
FF D8 FF E8 xx xx 53 50
ÿØÿè..SP
49 46 46 00
IFF.
JPG Still Picture Interchange File Format (SPIFF)
Trailer: FF D9 (ÿÙ)
FF D8 FF E0
Highlight All
Match Case
Match Diacritics
Whole Words
1 of 1 match


BTLO
URL Decode and Encode
From Base64 - CyberChef
File Signatures
Open
Money.xlsx
/home/kali/Downloads/PuzzleToCoCanDa
DaughtersCrown
GoodJobMajor
Money.xlsx
50 4B 03 04 14 00 08 08 08 00 2C A7 39 52 00 00
PK.....,.9R..
00 00 00 00 00 00 00 00 00 00 18 00 00 00 78 6C
..............xl
2F 64 72 61 77 69 6E 67 73 2F 64 72 61 77 69 6E
/drawings/drawin
67 31 2E 78 6D 6C 9D D0 5D 6E C2 30 0C 07 F0 13
g1.xml..]n.0....
EC 0E 55 DE 69 5A 18 13 43 14 5E D0 4E 30 0E E0
..U.iZ..C.^.N0..
25 6E 1B 91 8F CA 0E A3 DC 7E D1 4A 36 69 7B 01
%n.......~.J6i{.
1E 6D CB 3F F9 EF CD 6E 74 B6 F8 44 62 13 7C 23
.m.?...nt..Db.|#
EA B2 12 05 7A 15 B4 F1 5D 23 0E EF 6F B3 95 28
....z...]#..o..(
38 82 D7 60 83 C7 46 5C 90 C5 6E FB B4 19 35 AD
8..`..F\..n...5.
CF BC A7 22 ED 7B 5E A7 B2 11 7D 8C C3 5A 4A 56
..."{^...}..ZJV
3D 3A E0 32 0C E8 D3 B4 0D E4 20 A6 92 3A A9 09
=:.2..... ..:..
CE 49 76 56 CE AB EA 45 F2 40 08 9A 7B C4 B8 9F
.IvV...E.@..{...
26 E2 EA C1 03 9A 03 E3 F3 FE 4D D7 84 B6 35 0A
&.........M...5.
F7 41 9D 1C FA 38 21 84 16 62 FA 05 F7 66 E0 AC
.A...8!..b...f..
A9 07 AE 51 3D 50 FC 01 C6 7F 82 33 8A 02 87 36
...Q=P.....3...6
96 2A B8 EB 29 D9 48 42 FD 3C 09 38 FE 1A F5 DD
.*..).HB.<.8....
C8 52 BE CA D5 5F C8 DD 14 C7 01 1D 4F C3 2C B9
.R..._.....O.,.
43 7A C8 87 B1 26 5E BE 93 65 46 77 EE 81 B7 68
Cz...&^..eFw...h
03 1D 81 CB C8 B8 38 F8 E3 DD B1 2A C9 36 B5 28
......8....*.6.(
2B 6C B1 5E DE AD CC B3 22 B7 5F 50 4B 07 08 07
+l.^....".._PK...
62 69 83 05 01 00 00 07 03 00 00 50 4B 03 04 14
bi.........PK...
00 08 08 08 00 2C A7 39 52 00 00 00 00 00 00 00
.....,.9R.......
00 00 00 00 00 18 00 00 00 78 6C 2F 64 72 61 77
.........xl/draw
0x4 bytes from 0x0 to 0x3 selected
PuzzleToCoCanDa - Thunar
Bookmarks Help
kali
Downloads
PuzzleToCoCanDa
DaughtersCrown.jpg
GoodJobMajor.pdf
Money.xlsx
"Money.xlsx" | 16.2 KiB (16541 bytes) | Microsoft Excel Worksheet
FF D8 FF E8 xx xx 53 50
ÿØÿè..SP
49 46 46 00
IFF.
JPG Still Picture Interchange File Format (SPIFF)
Trailer: FF D9 (ÿÙ)
FF D8 FF E0
Highlight All
Match Case
Match Diacritics
Whole Words
1 of 1 match



🧠 XLSX Threat Payload Discovery – Obfuscated Sheet & Base64 Hidden Message

🎯 Objective

Perform deep inspection of a suspicious `.xlsx` file to uncover hidden messages or data potentially used in phishing or C2 communication.

🧪 Methodology

1. Opened file in SquareX sandbox to prevent local macro execution

2. Identified visible message referencing the Cocandians war escalation

3. Inspected all sheets → Sheet3 appeared blank

4. Applied "Clear Formatting" to uncover hidden white-on-white text

5. Located a Base64-encoded string embedded in cell data

6. Decoded using CyberChef → revealed `The Martian Colony, Beside Interplanetary spaceport`

🧰 Tools Used

- 📄 LibreOffice Calc – Secure viewer

- 🧬 CyberChef – Payload decoding

- 🧠 Manual Excel review with formatting reset

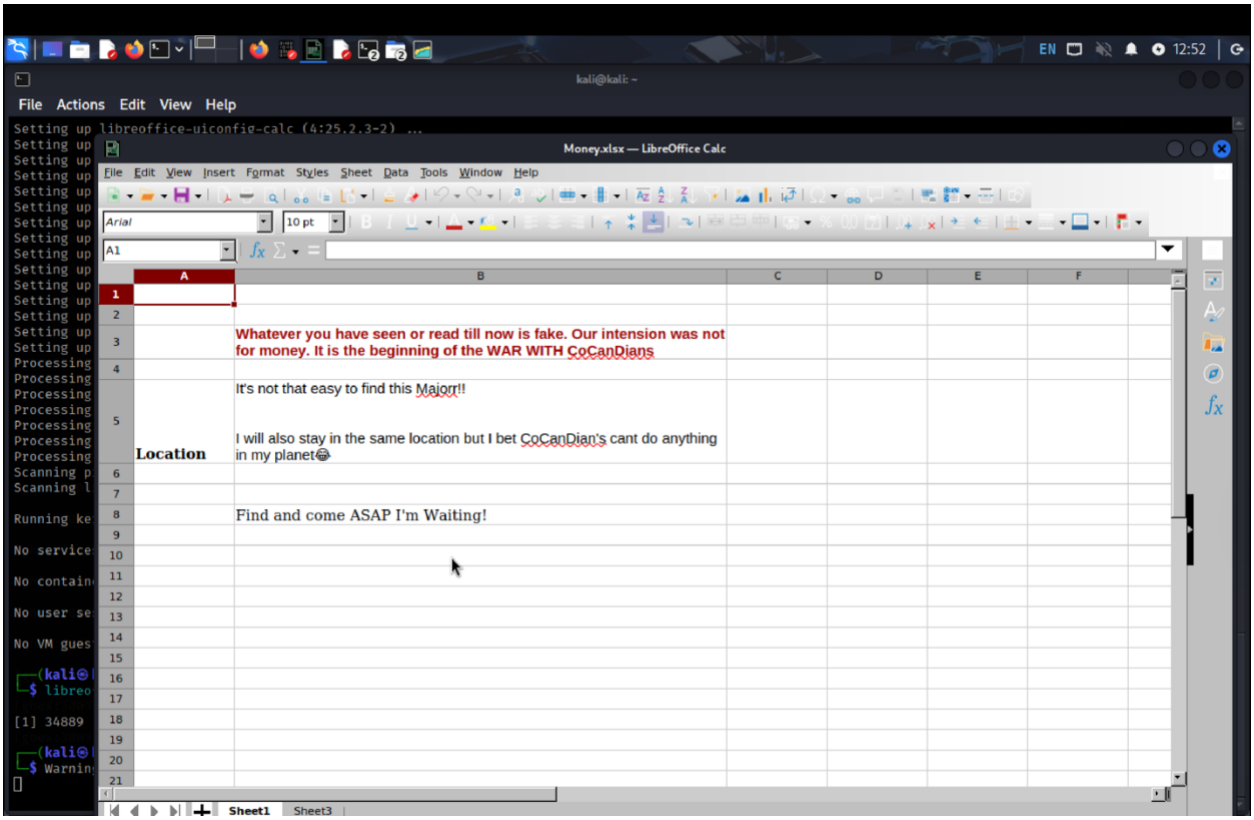
💡 Observations & TTPs

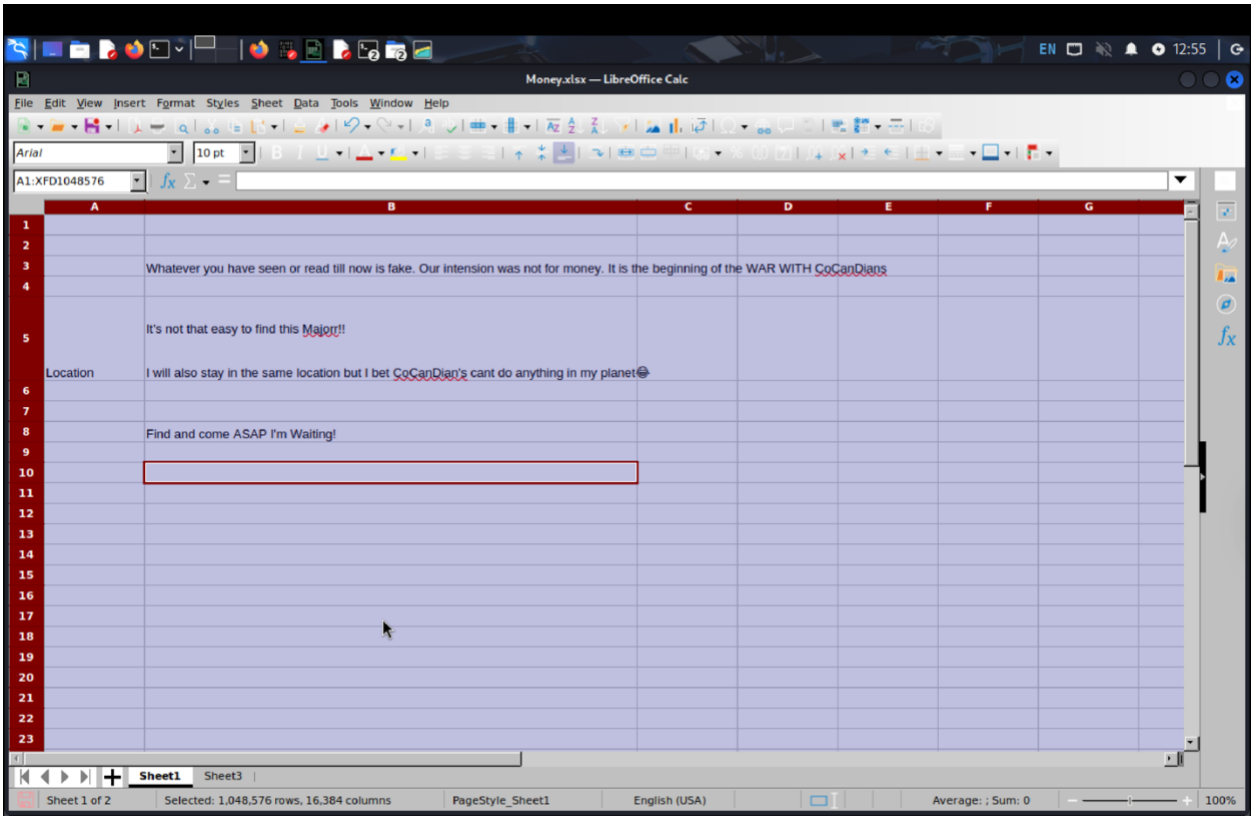
- Adversary used Excel formatting obfuscation

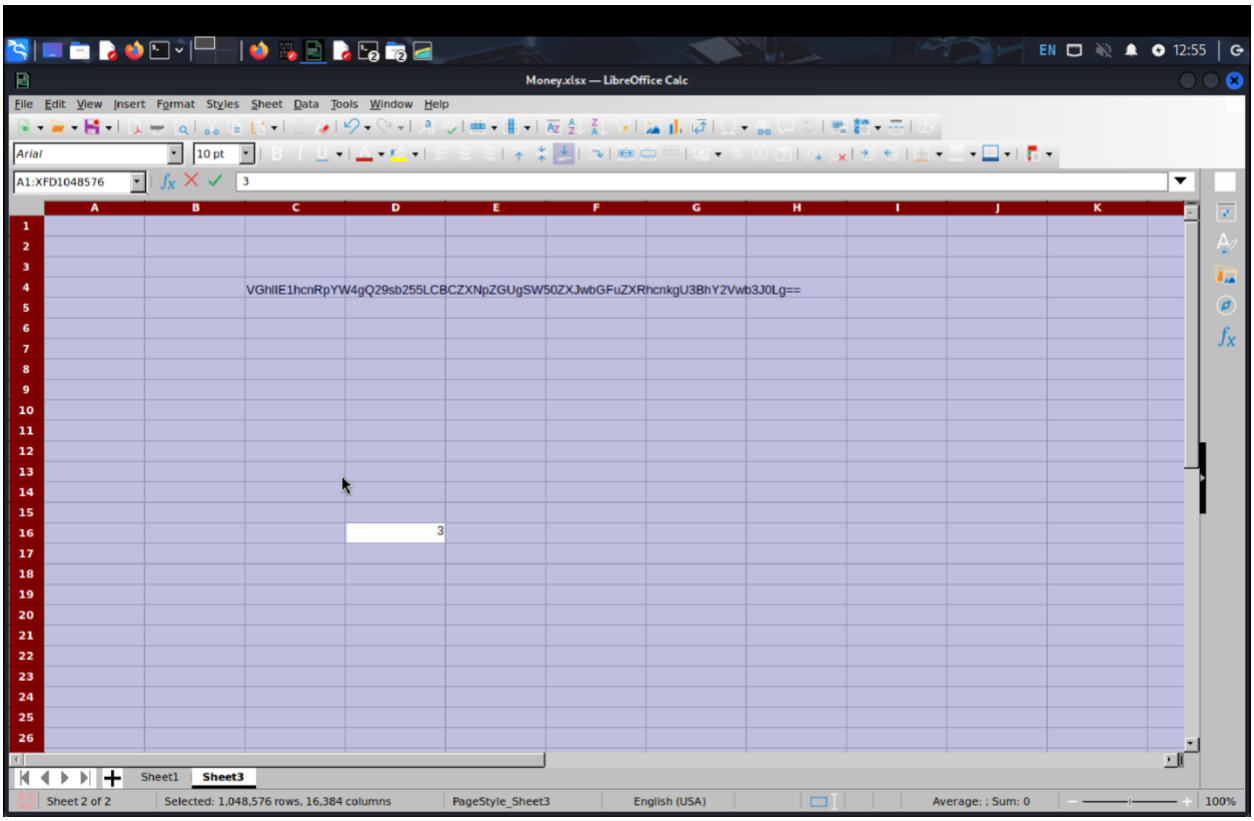
- Payload embedded via Base64, common in phishing campaigns

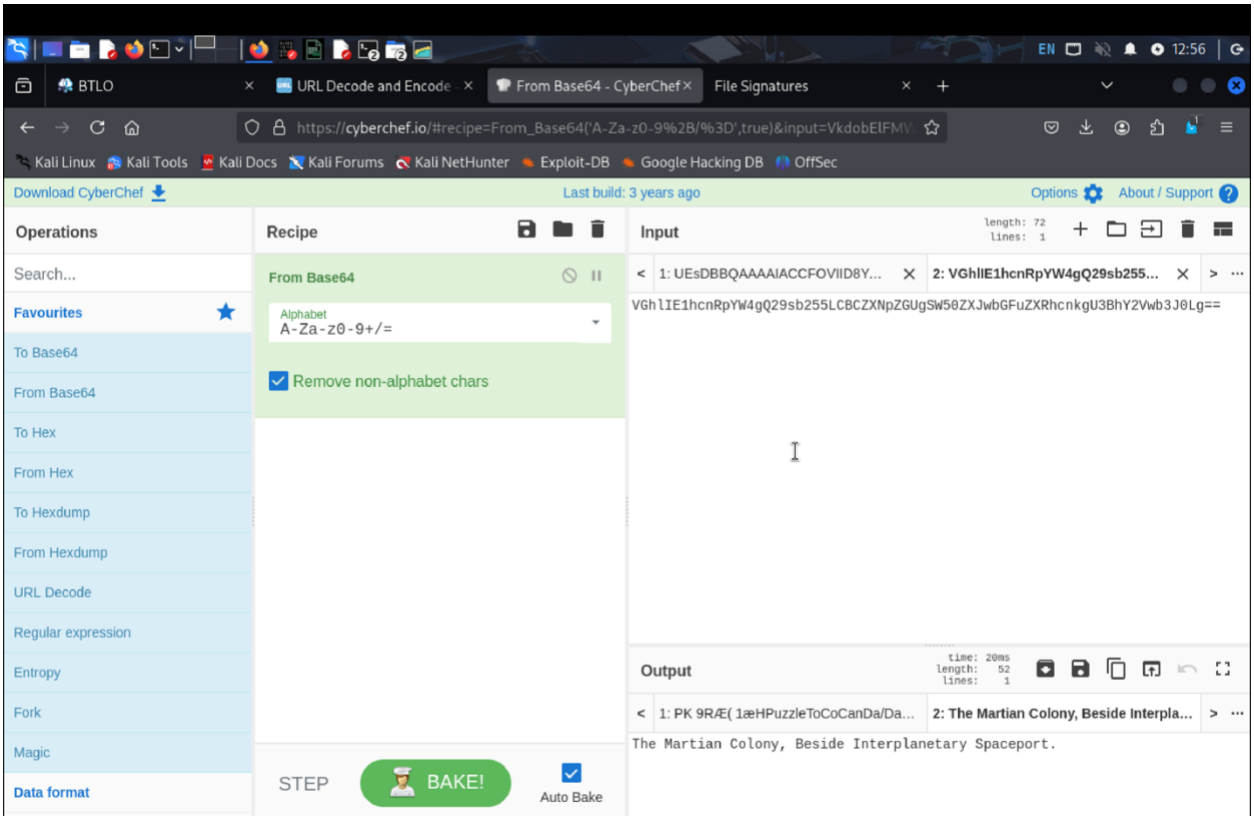
- Demonstrates a CTF-like use of deception, but directly maps to real-world tactics used by APTs

> 📌 Lesson: Analysts should always check for hidden sheets, clear formatting, and decode suspect text blocks when reviewing document-based threats.




Money.xlsx — LibreOffice Calc
File Edit View Insert Format Styles Sheet Data Tools Window Help
Arial
10 pt
A1:XFD1048576
Whatever you have seen or read till now is fake. Our intension was not for money. It is the beginning of the WAR WITH CoCanDians
It's not that easy to find this Majorr!!
Location
I will also stay in the same location but I bet CoCanDian's cant do anything in my planet
Find and come ASAP I'm Waiting!
Sheet1
Sheet3
Sheet 1 of 2
Selected: 1,048,576 rows, 16,384 columns
PageStyle_Sheet1
English (USA)
Average: ; Sum: 0
100%


Money.xlsx — LibreOffice Calc
File Edit View Insert Format Styles Sheet Data Tools Window Help
Arial
10 pt
A1:XFD1048576
3
VGhlIE1hcnRpYW4gQ29sb255LCBCZXNpZGUgSW50ZXJwbGFuZXRhcnkgU3BhY2Vwb3J0Lg==
3
Sheet1
Sheet3
Sheet 2 of 2
Selected: 1,048,576 rows, 16,384 columns
PageStyle_Sheet3
English (USA)
Average: ; Sum: 0
100%



🧠 Phishing Email Analysis – Spoofing via MK Mailer & Malicious Archive

🎯 Objective

Analyze a phishing email that used spoofing tactics and a disguised payload to lure the victim. Focused on email header inspection and payload triage.

📭 Metadata Breakdown

Field	Value	Observation
From	billjobs@microapple.com	Claims Microsoft affiliation
Return-Path	billjobs@microapple.com	🧨 Spoofed domain
Reply-To	negeja3921@pashter.com	🧨 Unrelated email domain used
Mail Service	`emkei.cz`	❗ Identified as fake mailer

📎 Payload Contents

- Attachment posed as `.pdf` but was actually a `.zip` file

- ZIP included:

 - 🖼️ A JPEG decoy

 - 📄 A PDF threat message

 - 📊 An Excel sheet analyzed separately (see XLSX section)

🔍 **Key Takeaways**

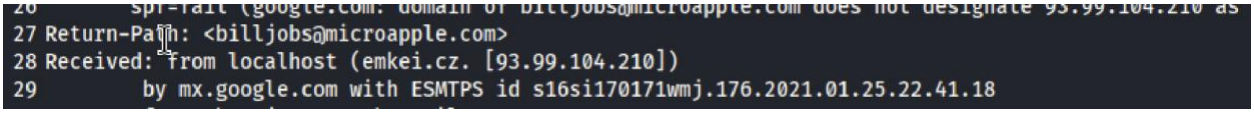
- Spoofing often involves manipulating multiple headers (`From`, `Reply-To`, `Return-Path`)

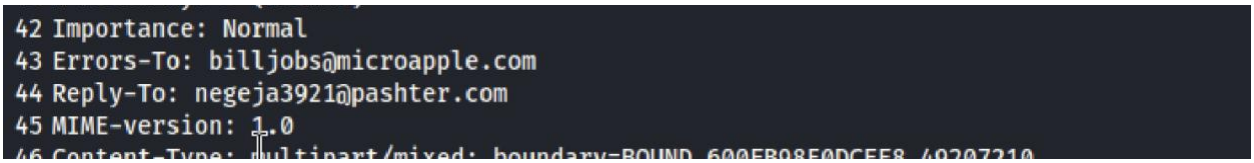
- Tools like `emkei.cz` are publicly available and often abused in phishing

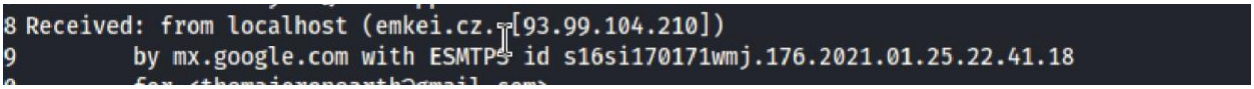
- Attachments may misrepresent file types — always verify actual MIME and content

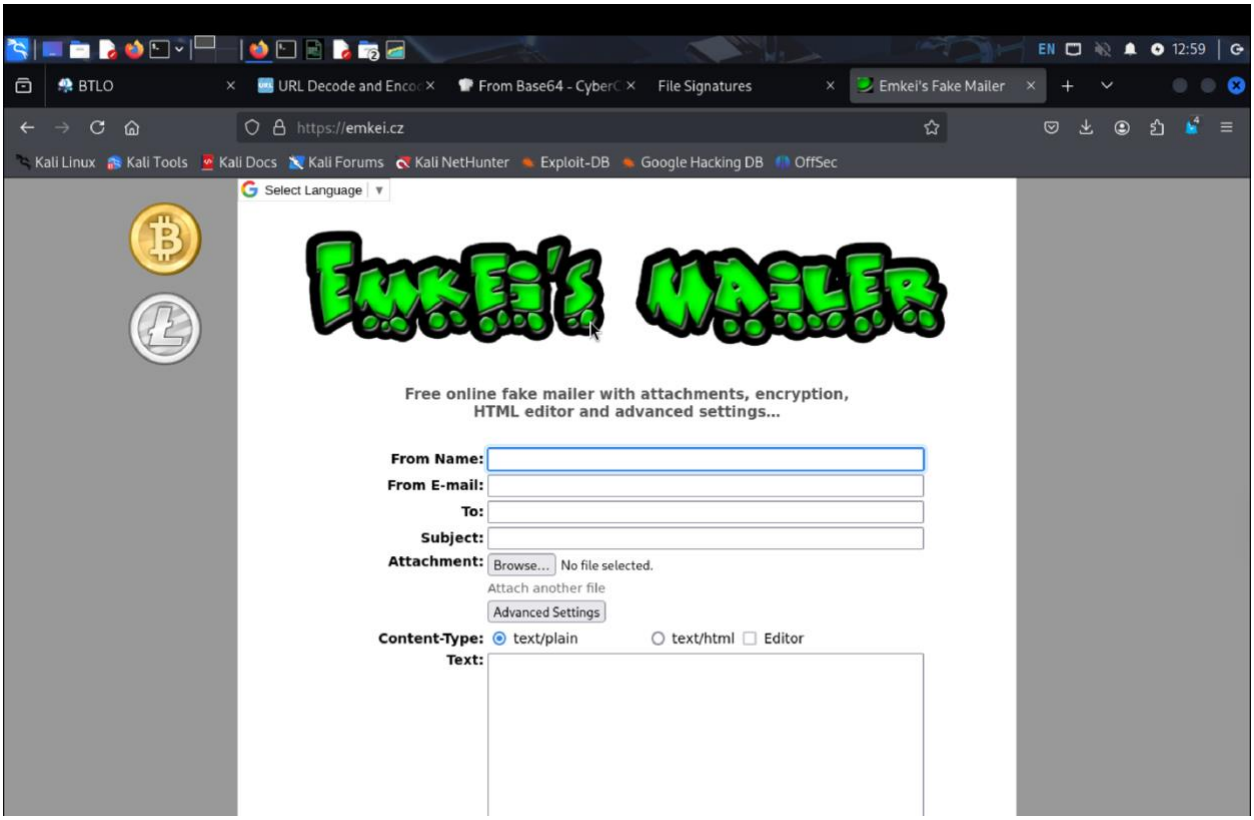
- Analysts must inspect email paths, perform OSINT on headers, and correlate payload behavior

> 📌 This case emulates real-world phishing campaigns used in BEC and ransomware initial access. Practicing these techniques sharpens SOC response skills.

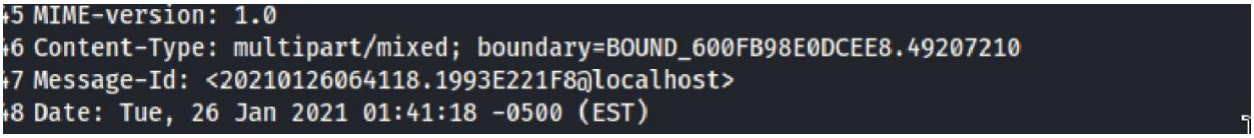









```
3 Received-SPF: fail (google.com: domain of billjobs@microapple.com does not designate 93.99.104.210 as permitted sender) client-ip=93.99.104.210;
4 Authentication-Results: mx.google.com;
5       spf=fail (google.com: domain of billjobs@microapple.com does not designate 93.99.104.210 as permitted sender) smtp.mailfrom=billjobs@microapple.com
6 Received: by localhost (Postfix, from userid 33)
7         id 1993E221F8; Tue, 26 Jan 2021 01:41:18 -0500 (EST)
8 To: themajoronearth@gmail.com
9 Subject: A Hope to CoCanDa
0 From: "Bill" <billjobs@microapple.com>
1 X-Priority: 3 (Normal)
```



🛡️ Email Phishing Triage: Header & Metadata Forensics

🎯 Objective

Perform a complete SOC-style triage on a phishing email — identify spoofed headers, extract hidden metadata, and determine potential C2 communications.

🕵️ Step 1: Header Investigation

Field	Action	Indicator of Spoof
Received	IP/domain reputation lookup	✔
Return-Path	Bounce address – should match sender	Mismatch detected
SPF/DKIM/DMARC	Examine authentication results	SPF FAILED
From vs Reply-To.	Compare email addresses	Mismatch detected
Subject / Message-ID	Org-wide search for related emails	✔

🔗 Step 2: Attachment Metadata & C2 Discovery

- ExifTool Analysis:

bash

```
exiftool money.xlsx
```

Revealed `Author: pestero Negeja` → undocumented actor info

- **Embedded C2 Domain**:
  Found `pashter.com` in email body/attachments → flagged as potential command & control

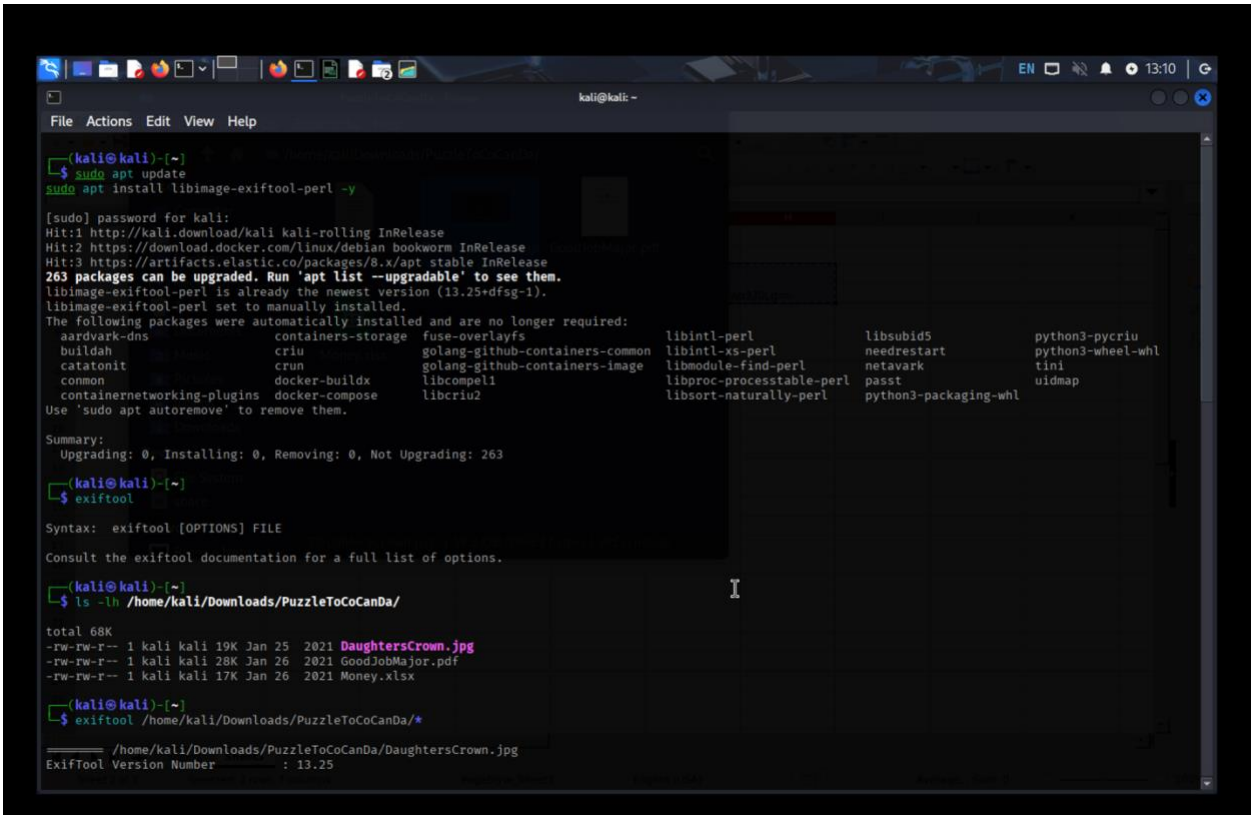
---

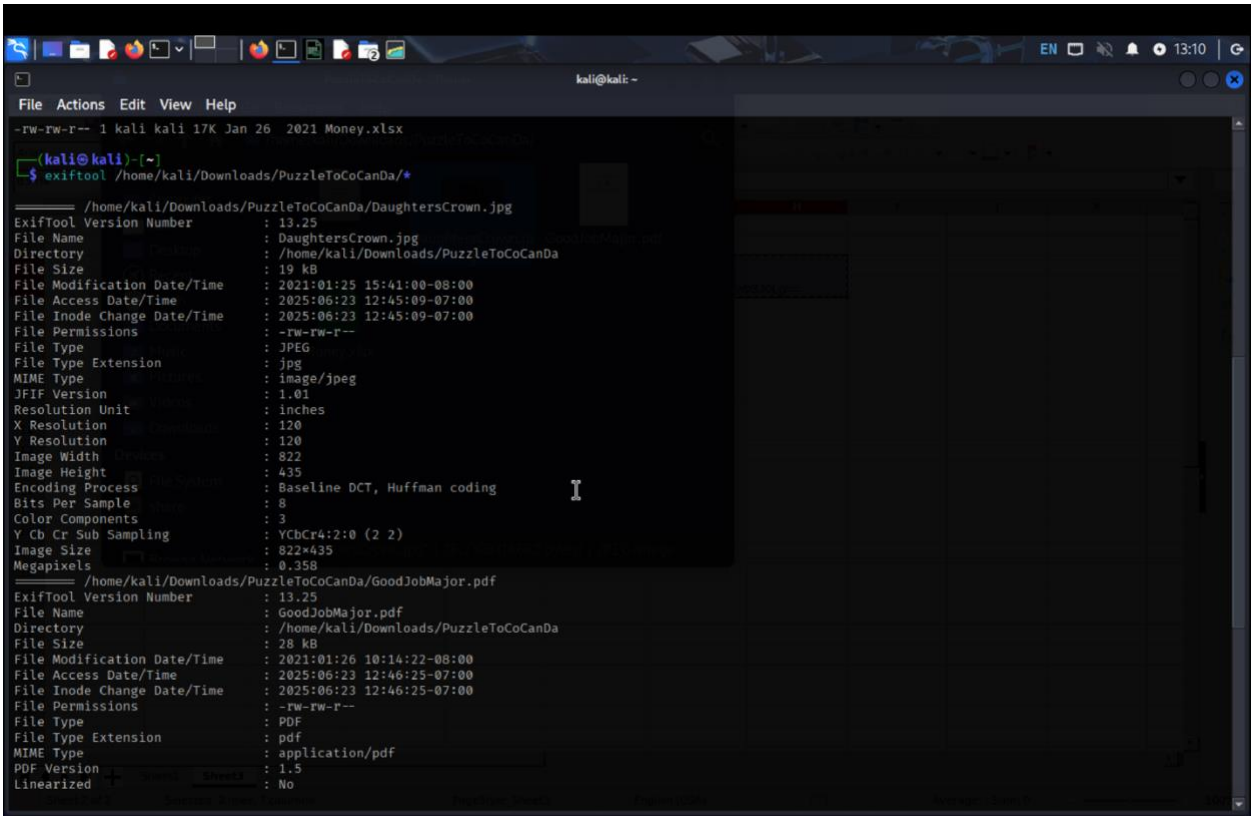
🛠 Tools Utilized

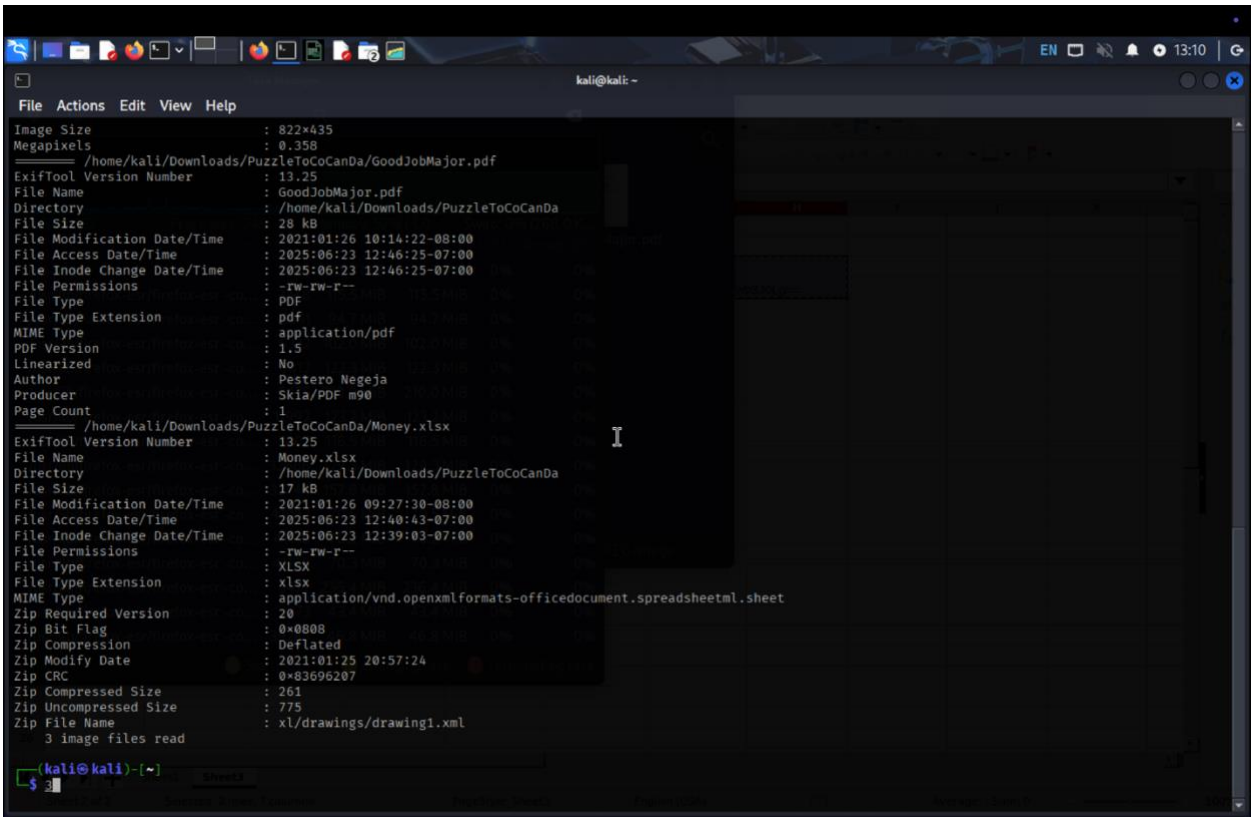
- Email gateway logs
- Threat intel lookups (IP/domain)
- **ExifTool** – metadata extraction
- Manual text scanning (for URL/domain discovery)

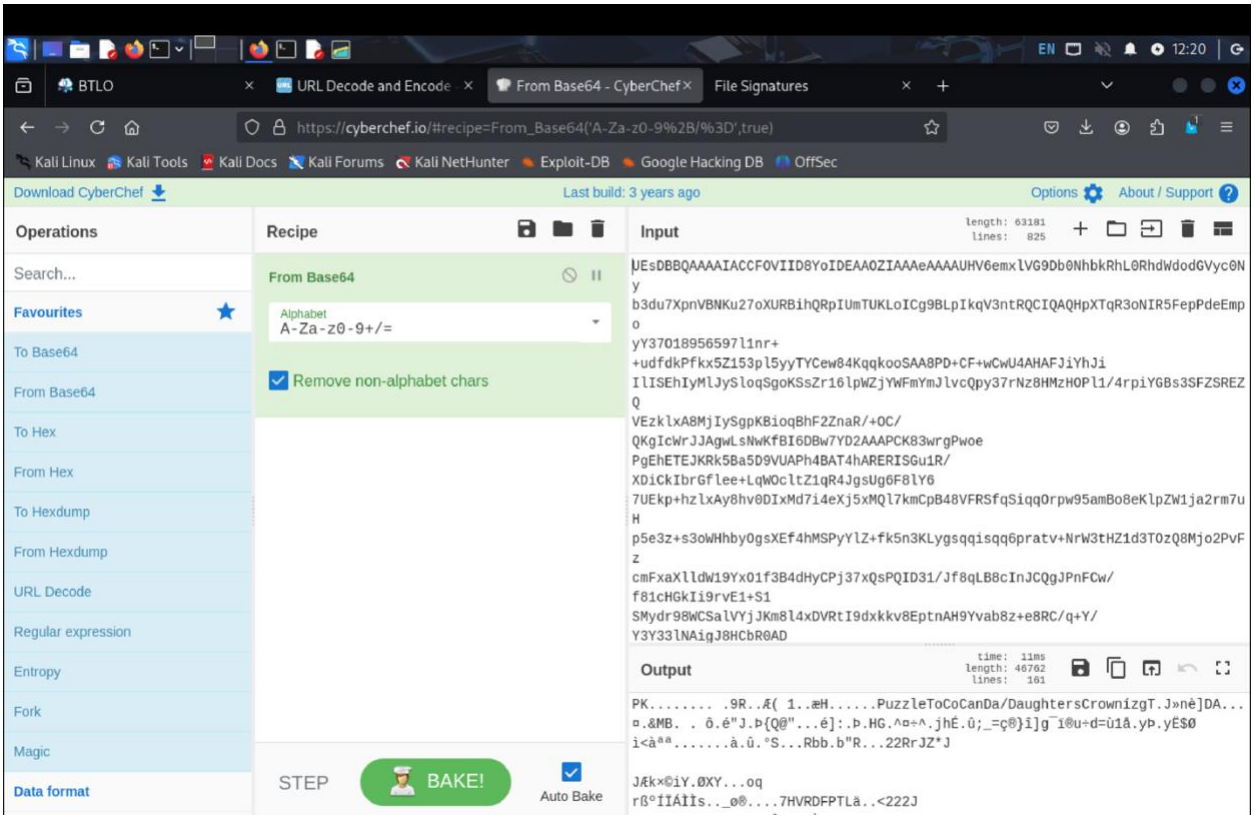
🧠 SOC Analyst Takeaways

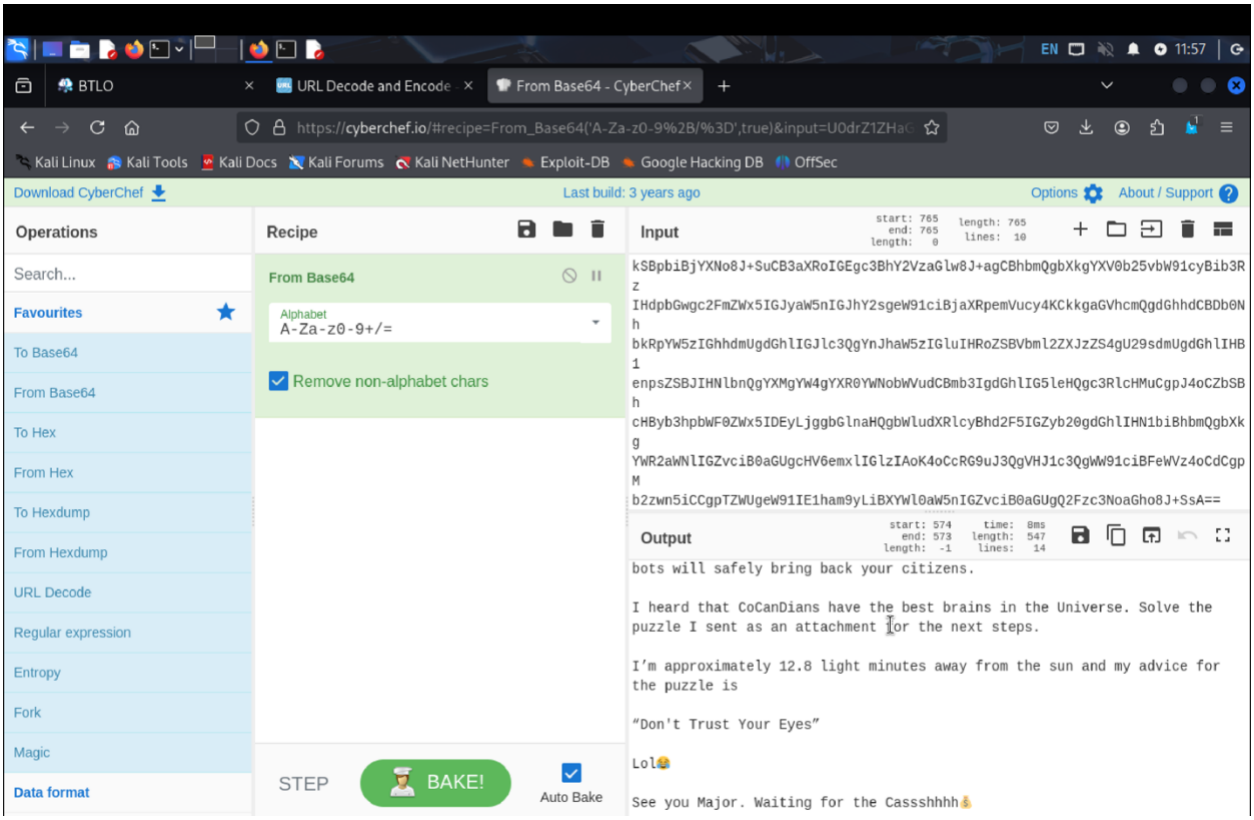
- Pay close attention to header fields — early indicators of spoofing
- Use metadata analysis to uncover hidden threat details
- Search text/attachments for unknown domains to identify C2
- Rinse-and-repeat workflow maps perfectly to real SOC triage procedures

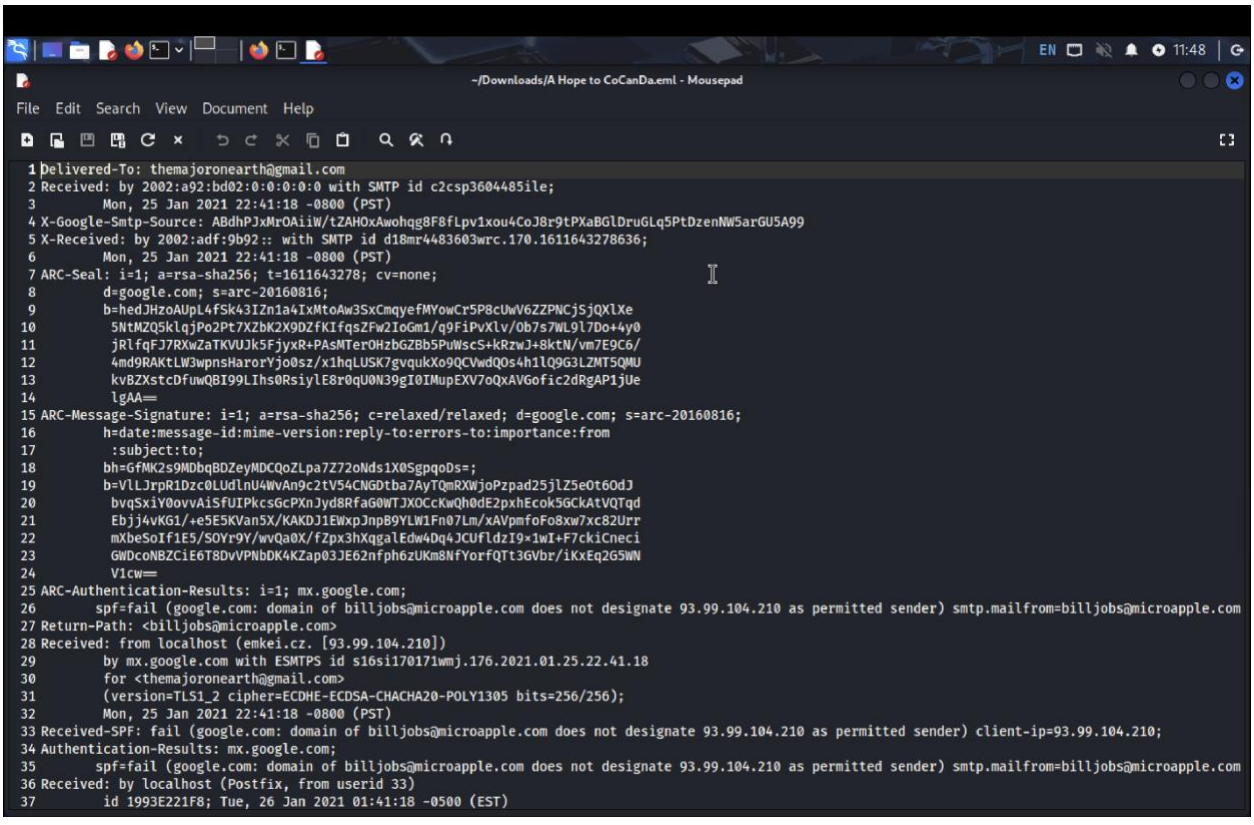



kali@kali: ~
File Actions Edit View Help
-rw-rw-r-- 1 kali kali 17K Jan 26 2021 Money.xlsx
(kali㉿kali)-[~]
$ exiftool /home/kali/Downloads/PuzzleToCoCanDa/*
======== /home/kali/Downloads/PuzzleToCoCanDa/DaughtersCrown.jpg
ExifTool Version Number : 13.25
File Name : DaughtersCrown.jpg
Directory : /home/kali/Downloads/PuzzleToCoCanDa
File Size : 19 kB
File Modification Date/Time : 2021:01:25 15:41:00-08:00
File Access Date/Time : 2025:06:23 12:45:09-07:00
File Inode Change Date/Time : 2025:06:23 12:45:09-07:00
File Permissions : -rw-rw-r--
File Type : JPEG
File Type Extension : jpg
MIME Type : image/jpeg
JFIF Version : 1.01
Resolution Unit : inches
X Resolution : 120
Y Resolution : 120
Image Width : 822
Image Height : 435
Encoding Process : Baseline DCT, Huffman coding
Bits Per Sample : 8
Color Components : 3
Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2)
Image Size : 822×435
Megapixels : 0.358
======== /home/kali/Downloads/PuzzleToCoCanDa/GoodJobMajor.pdf
ExifTool Version Number : 13.25
File Name : GoodJobMajor.pdf
Directory : /home/kali/Downloads/PuzzleToCoCanDa
File Size : 28 kB
File Modification Date/Time : 2021:01:26 10:14:22-08:00
File Access Date/Time : 2025:06:23 12:46:25-07:00
File Inode Change Date/Time : 2025:06:23 12:46:25-07:00
File Permissions : -rw-rw-r--
File Type : PDF
File Type Extension : pdf
MIME Type : application/pdf
PDF Version : 1.5
Linearized : No


kali@kali: ~
File Actions Edit View Help
Image Size : 822×435
Megapixels : 0.358
======== /home/kali/Downloads/PuzzleToCoCanDa/GoodJobMajor.pdf
ExifTool Version Number : 13.25
File Name : GoodJobMajor.pdf
Directory : /home/kali/Downloads/PuzzleToCoCanDa
File Size : 28 kB
File Modification Date/Time : 2021:01:26 10:14:22-08:00
File Access Date/Time : 2025:06:23 12:46:25-07:00
File Inode Change Date/Time : 2025:06:23 12:46:25-07:00
File Permissions : -rw-rw-r--
File Type : PDF
File Type Extension : pdf
MIME Type : application/pdf
PDF Version : 1.5
Linearized : No
Author : Pestero Negeja
Producer : Skia/PDF m90
Page Count : 1
======== /home/kali/Downloads/PuzzleToCoCanDa/Money.xlsx
ExifTool Version Number : 13.25
File Name : Money.xlsx
Directory : /home/kali/Downloads/PuzzleToCoCanDa
File Size : 17 kB
File Modification Date/Time : 2021:01:26 09:27:30-08:00
File Access Date/Time : 2025:06:23 12:40:43-07:00
File Inode Change Date/Time : 2025:06:23 12:39:03-07:00
File Permissions : -rw-rw-r--
File Type : XLSX
File Type Extension : xlsx
MIME Type : application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
Zip Required Version : 20
Zip Bit Flag : 0×0808
Zip Compression : Deflated
Zip Modify Date : 2021:01:25 20:57:24
Zip CRC : 0×83696207
Zip Compressed Size : 261
Zip Uncompressed Size : 775
Zip File Name : xl/drawings/drawing1.xml
3 image files read
(kali㉿kali)-[~]
$ 3


EN 12:20
BTLO
URL Decode and Encode
From Base64 - CyberChef
File Signatures
https://cyberchef.io/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true)
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Download CyberChef
Last build: 3 years ago
Options
About / Support
Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Fork
Magic
Data format
Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
STEP
BAKE!
Auto Bake
Input
length: 63181
lines: 825
UEsDBBQAAAAIACCFOVIID8YoIDEAAOZIAAAeAAAAUHV6emxlVG9Db0NhbkRhL0RhdWdodGVyc0N
y
b3du7XpnVBNKu27oXURBihQRpIUmTUKLoICg9BLpIkqV3ntRQCIQAQHpXTqR3oNIR5FepPdeEmp
o
yY37O18956597l1nr+
+udfdkPfkx5Z153pl5yyTYCew84KqqkooSAA8PD+CF+wCwU4AHAFJiYhJi
IlISEhIyMlJySloqSgoKSsZr16lpWZjYWFmYmJlvcQpy37rNz8HMzHOPl1/4rpiYGBs3SFZSREZ
Q
VEzklxA8MjIySgpKBioqBhF2ZnaR/+OC/
QKgIcWrJJAgwLsNwKfBI6DBw7YD2AAAPCK83wrgPwoe
PgEhETEJKRk5Ba5D9VUAPh4BAT4hARERISGu1R/
XDiCkIbrGflee+LqWOcltZ1qR4JgsUg6F8lY6
7UEkp+hzlxAy8hv0DIxMd7i4eXj5xMQl7kmCpB48VFRSfqSiqqOrpw95amBo8eKlpZW1ja2rm7u
H
p5e3z+s3oWHhbyOgsXEf4hMSPyYlZ+fk5n3KLygsqqisqq6pratv+NrW3tHZ1d3TOzQ8Mjo2PvF
z
cmFxaXlldW19Yx01f3B4dHyCPj37xQsPQID31/Jf8qLB8cInJCQgJPnFCw/
f81cHGkIi9rvE1+S1
SMydr98WCSalVYjJKm8l4xDVRtI9dxkkv8EptnAH9Yvab8z+e8RC/q+Y/
Y3Y33lNAigJ8HCbR0AD
Output
time: 11ms
length: 46762
lines: 161
PK..... .9R..Æ(1..æH.....PuzzleToCoCanDa/DaughtersCrownízgT.J»nè]DA...
¤.&MB. . ô.é"J.Þ{Q@"...é]:.Þ.HG.^¤÷^.jhÉ.û;_=ç®}ì]g¯ï®u÷d=ù1â.yÞ.yÉ$Ø
i<à ª ª.....à.û.°S...Rbb.b"R...22RrJZ*J
JÆk×©ïY.ØXY...oq
rß°ÍÍÁÍÌs..¸ø®....7HVRDFPTLä..<222J


BTLO
URL Decode and Encode
From Base64 - CyberChef
https://cyberchef.io/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true)&input=U0drZ1ZHa
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Download CyberChef
Last build: 3 years ago
Options
About / Support
Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Fork
Magic
Data format
Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
STEP
BAKE!
Auto Bake
Input
kSBpbiBjYXNo8J+SuCB3aXRoIGEgc3BhY2VzaGlw8J+agCBhbmQgbXkgYXV0b25vbW91cyBib3Rz
IHdpbGwgc2FmZWx5IGJyaW5nIGJhY2sgeW91ciBjaXRpemVucy4KCkkgaGVhcmQgdGhhdCBDb0N
h
bkRpYW5zIGhhdmUgdGhlIGJlc3QgYnJhaW5zIGluIHRoZSBVbml2ZXJzZS4gU29sdmUgdGhlIHB
1
enpsZSBJIHNlbnQgYXMgYW4gYXR0YWNobWVudCBmb3IgdGhlIG5leHQgc3RlcHMuCgpJ4oCZbSB
h
cHByb3hpbWF0ZWx5IDEyLjggbGlnaHQgbWludXRlcyBhd2F5IGZyb20gdGhlIHN1biBhbmQgbXk
g
YWR2aWNlIGZvciB0aGUgcHV6emxlIGlzIAoK4oCcRG9uJ3QgVHJ1c3QgWW91ciBFeWVz4oCdCgp
M
b2zwn5iCCgpTZWUgeW91IE1ham9yLiBXYWl0aW5nIGZvciB0aGUgQ2Fzc3NoaGho8J+SsA==
Output
bots will safely bring back your citizens.
I heard that CoCanDians have the best brains in the Universe. Solve the puzzle I sent as an attachment for the next steps.
I'm approximately 12.8 light minutes away from the sun and my advice for the puzzle is
"Don't Trust Your Eyes"
Lol
See you Major. Waiting for the Cassshhhh


~/Downloads/A Hope to CoCanDa.eml - Mousepad
File Edit Search View Document Help
1 Delivered-To: themajoronearth@gmail.com
2 Received: by 2002:a92:bd02:0:0:0:0:0 with SMTP id c2csp3604485ile;
3 Mon, 25 Jan 2021 22:41:18 -0800 (PST)
4 X-Google-Smtp-Source: ABdhPJxMrOAiiW/tZAHOxAwohqg8F8fLpv1xou4CoJ8r9tPXaBGlDruGLq5PtDzenNW5arGU5A99
5 X-Received: by 2002:adf:9b92:: with SMTP id d18mr4483603wrc.170.1611643278636;
6 Mon, 25 Jan 2021 22:41:18 -0800 (PST)
7 ARC-Seal: i=1; a=rsa-sha256; t=1611643278; cv=none;
8 d=google.com; s=arc-20160816;
9 b=hedJHzoAUpL4fSk43IZn1a4IxMtoAw3SxCmqyefMYowCr5P8cUwV6ZZPNCjSjQXlXe
10 5NtMZQ5klqjPo2Pt7XZbK2X9DZfKIfqsZFw2IoGm1/q9FiPvXlv/Ob7s7WL9l7Do+4y0
11 jRlfqFJ7RXwZaTKVUJk5FjyxR+PAsMTerOHzbGZBb5PuWscS+kRzwJ+8ktN/vm7E9C6/
12 4md9RAKtLW3wpnsHarorYjo0sz/x1hqLUSK7gvqukXo9QCVwdQOs4h1lQ9G3LZMT5QMU
13 kvBZXstcDfuwQBI99LIhs0RsiylE8r0qU0N39gI0IMupEXV7oQxAVGofic2dRgAP1jUe
14 lgAA==
15 ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
16 h=date:message-id:mime-version:reply-to:errors-to:importance:from
17 :subject:to;
18 bh=GfMK2s9MDbqBDZeyMDCQoZLpa7Z72oNds1X0SgpqoDs=;
19 b=VlLJrpR1Dzc0LUdlnU4WvAn9c2tV54CNGDtba7AyTQmRXWjoPzpad25jlZ5eOt6OdJ
20 bvqSxiY0ovvAiSfUIPkcsGcPXnJyd8RfaG0WTJXOCcKwQh0dE2pxhEcok5GCkAtVQTqd
21 Ebjj4vKG1/+e5E5KVan5X/KAKDJ1EWxpJnpB9YLW1Fn07Lm/xAVpmfoFo8xw7xc82Urr
22 mXbeSoIf1E5/SOYr9Y/wvQa0X/fZpx3hXqgalEdw4Dq4JCUfldzI9+1wI+F7ckiCneci
23 GWDcoNBZCiE6T8DvVPNbDK4KZap03JE62nfph6zUKm8NfYorfQTt3GVbr/iKxEq2G5WN
24 V1cw==
25 ARC-Authentication-Results: i=1; mx.google.com;
26 spf=fail (google.com: domain of billjobs@microapple.com does not designate 93.99.104.210 as permitted sender) smtp.mailfrom=billjobs@microapple.com
27 Return-Path: <billjobs@microapple.com>
28 Received: from localhost (emkei.cz. [93.99.104.210])
29 by mx.google.com with ESMTPS id s16si170171wmj.176.2021.01.25.22.41.18
30 for <themajoronearth@gmail.com>
31 (version=TLS1_2 cipher=ECDHE-ECDSA-CHACHA20-POLY1305 bits=256/256);
32 Mon, 25 Jan 2021 22:41:18 -0800 (PST)
33 Received-SPF: fail (google.com: domain of billjobs@microapple.com does not designate 93.99.104.210 as permitted sender) client-ip=93.99.104.210;
34 Authentication-Results: mx.google.com;
35 spf=fail (google.com: domain of billjobs@microapple.com does not designate 93.99.104.210 as permitted sender) smtp.mailfrom=billjobs@microapple.com
36 Received: by localhost (Postfix, from userid 33)
37 id 1993E221F8; Tue, 26 Jan 2021 01:41:18 -0500 (EST)

Conclusion

This project demonstrates comprehensive SOC analyst skills in phishing triage, payload forensics, and threat intelligence — critical for defending against sophisticated phishing campaigns and supporting incident response operations.