THE NATIONAL CYBERCHAMP COMPETITION 2023 (NCCC23)

FINAL CHALLENGE

DIGITAL FORENSICS

DATE: 1st , APRIL 2023.

THE NATIONAL CYBERCHAMP COMPETITION 2023 (NCCC23)

FINAL CHALLENGE

FORENSICS

GLAGO GIDEON ELORM

29 APRIL 2023.

FORENSIC CASE SCENARIO

CYBERGHANA has been contracted as a consultant to conduct an independent investigation into a computer related crime. The case involves a suspect, Kofi Koomson, an employee for Global Technology Ltd suspected of child pornography and drug related crimes and his employer. CYBERGHANA has designated you as the lead investigator to handle this case. You have appropriately secured images of Kofi's computer on which the suspected activity happened together with a seized USB drive found to be empty.

TASK REQUIREMENT

- *PART 1*

i. Determination of the filetypes of the 3 attachments in the 3 different messages the suspect sent.

ii. Autopsy report for your investigation

iii. Retrieval of hidden information in the attached files

iv. Computation of hash values for all 3 attachments

- *PART 2*

i. Recovery of deleted files on the USB drive (if any)

ii. Generation of autopsy report for your investigation

iii. Retrieval of hidden information in the files found on the USB drive

iv. Computation of hash values of files found on the USB drive

v. Comparison and contrasting of hash values and hidden information found in files from the suspect's computer and the ones found on the seized USB drive.

OUTLINE OF TASK

Step 1: Recovering the actual file type of attachments from the SYSTEM.

Step 2: Generating autopsy reports from analysis made from the SYSTEM.

Step 3: Retrieving information from the attachments recovered from the SYSTEM.

Step 4: Computation of hash values from the attachments.

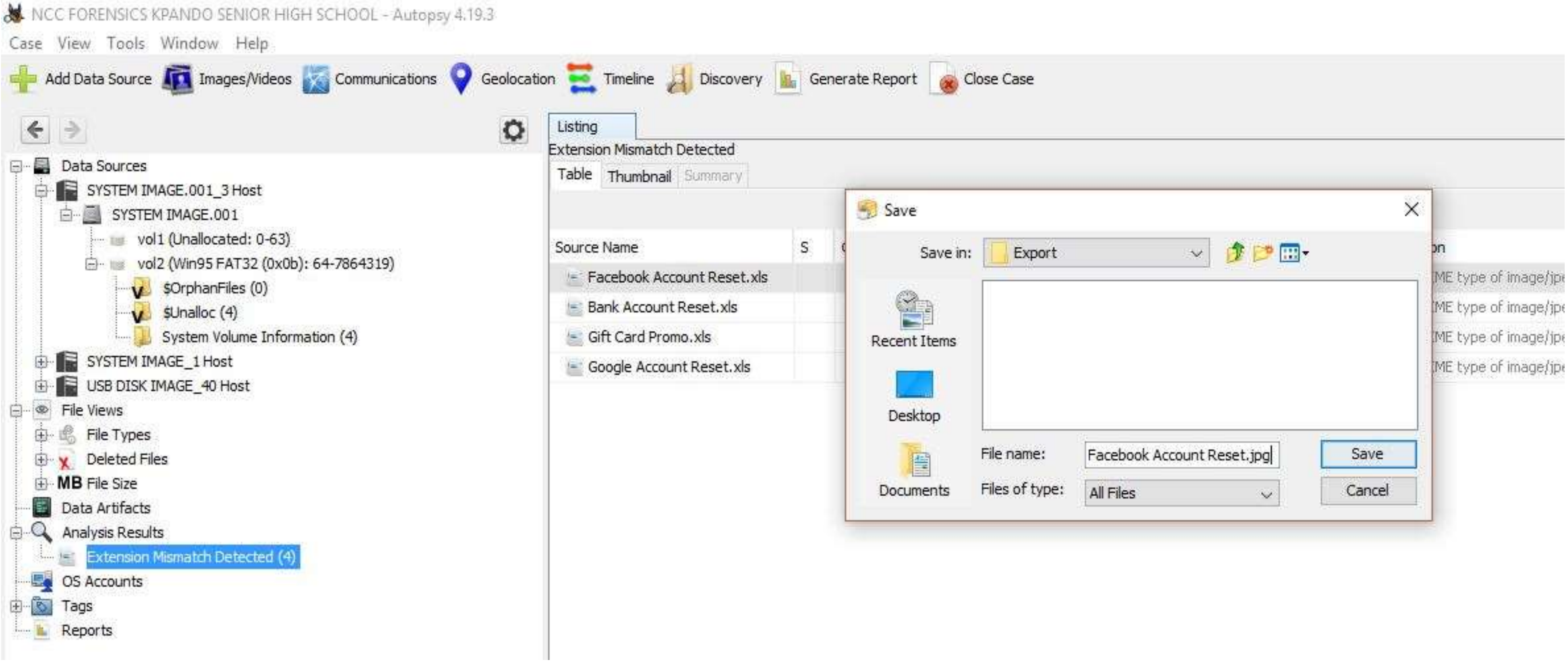
Step 5: Recovering deleted files from the USB disk image.

Step 6: Uncovering information from behind the recovered deleted files from the USB disk.

Step 7: Generating autopsy reports from analysis made from the USB disk.

Step 8:Observation, comparisons and conclusions from analysis and investigations carried out.

Screenshot showing how Actual and Perceived Files were Retrieved



NCC FORENSICS KPANDO SENIOR HIGH SCHOOL - Autopsy 4.19.3

- Data Sources
  - SYSTEM IMAGE.001_3 Host
    - SYSTEM IMAGE.001
      - vol1 (Unallocated: 0-63)
      - vol2 (Win95 FAT32 (0x0b): 64-7864319)
        - $OrphanFiles (0)
        - $Unalloc (4)
        - System Volume Information (4)
  - SYSTEM IMAGE_1 Host
  - USB DISK IMAGE_40 Host
- File Views
  - File Types
  - Deleted Files
  - MB File Size
- Data Artifacts
- Analysis Results
  - Extension Mismatch Detected (4)
- OS Accounts
- Tags
- Reports

Extension Mismatch Detected

Source Name	S	on
Facebook Account Reset.xls		ME type of image/jpe
Bank Account Reset.xls		ME type of image/jpe
Gift Card Promo.xls		ME type of image/jpe
Google Account Reset.xls		ME type of image/jpe

Save

Save in: Export

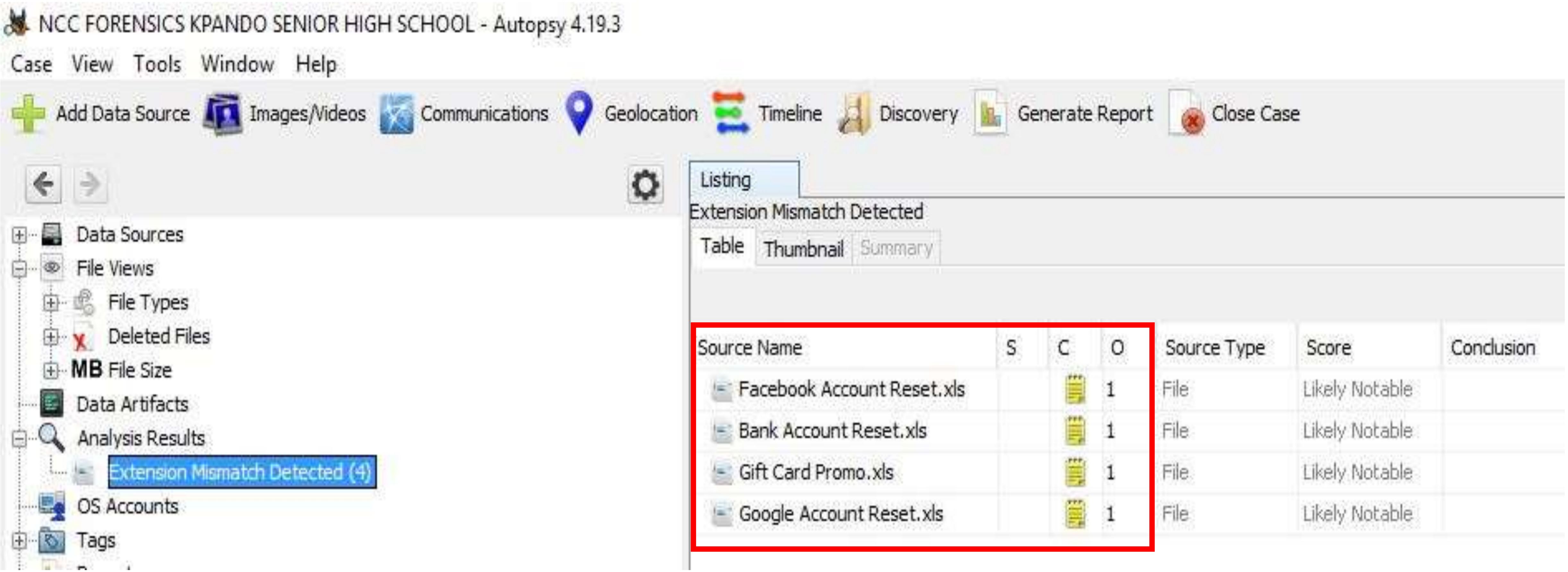
File name: Facebook Account Reset.jpg

Files of type: All Files

Actual Filetypes & Extensions

Perceived File Type	Actual File Type
Bank Account Reset.xls	Bank Account Reset.jpg
Facebook Account Reset.xls	Facebook Account Reset.jpg
Google Account Reset.xls	Google Account Reset.jpg

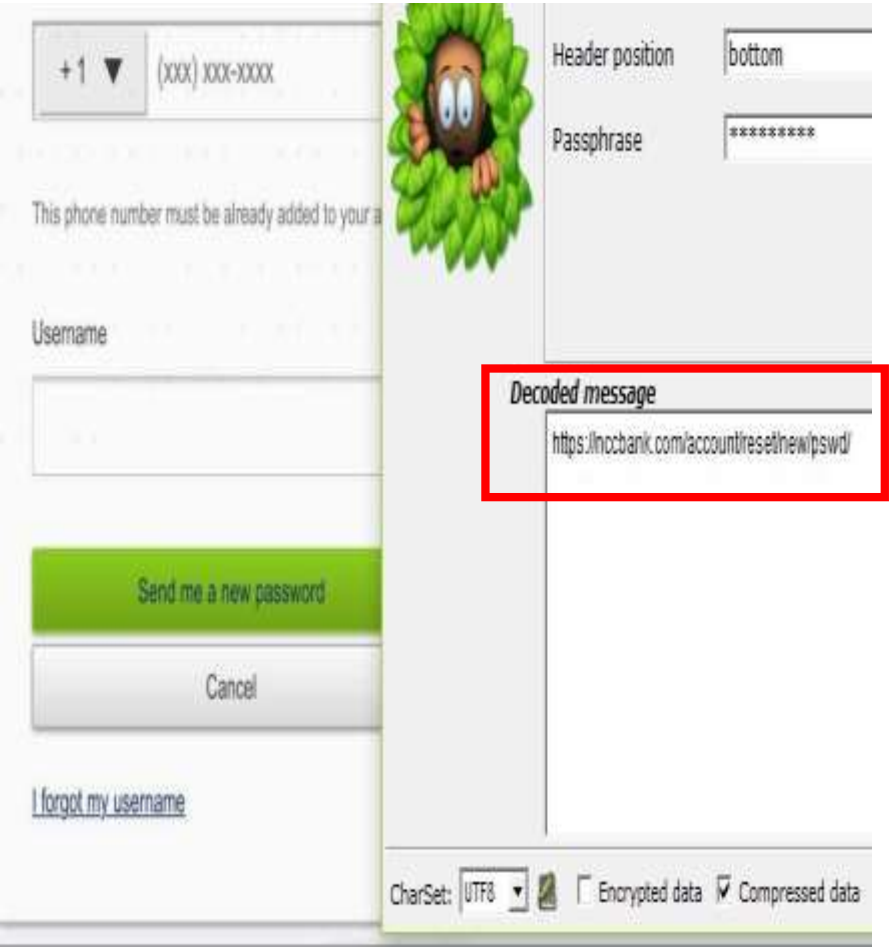
Screenshot of Actual Files and extensions on System Image in Autopsy (Extension Mismatch)



Extension Mismatch Detected

Source Name	S	C	O	Source Type	Score	Conclusion
Facebook Account Reset.xls		🗒	1	File	Likely Notable	
Bank Account Reset.xls		🗒	1	File	Likely Notable	
Gift Card Promo.xls		🗒	1	File	Likely Notable	
Google Account Reset.xls		🗒	1	File	Likely Notable	

Screenshot Showing how Hidden Information in Files on System Image were Retrieved



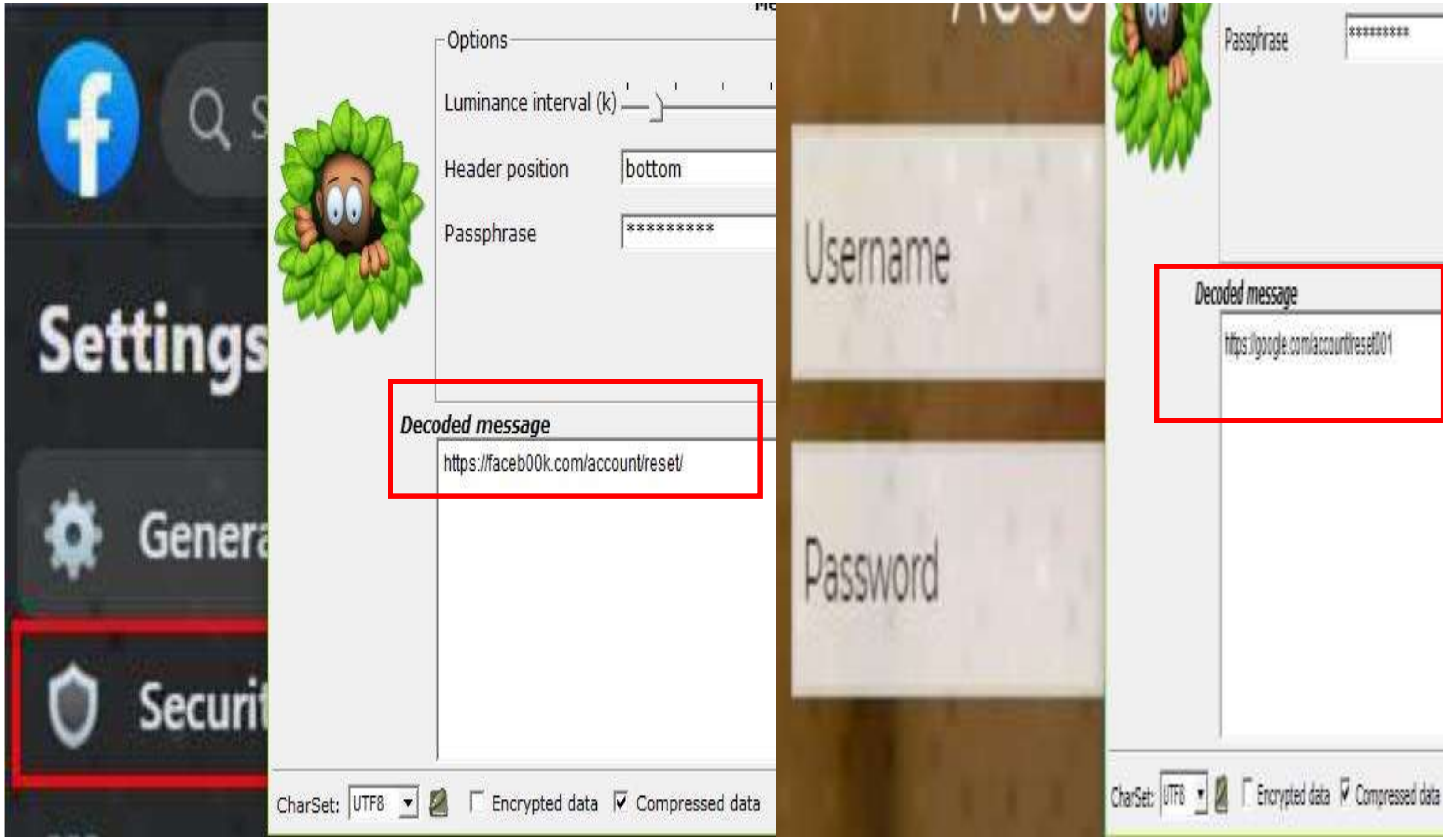
Header position: bottom

Passphrase: *********

Decoded message

https://nccbank.com/account/reset/new/pswd/

CharSet: UTF8 □ Encrypted data ☑ Compressed data



Options

Luminance interval (k)

Header position: bottom

Passphrase: *********

Decoded message

https://faceb00k.com/account/reset/

CharSet: UTF8 □ Encrypted data ☑ Compressed data

Passphrase: *********

Decoded message

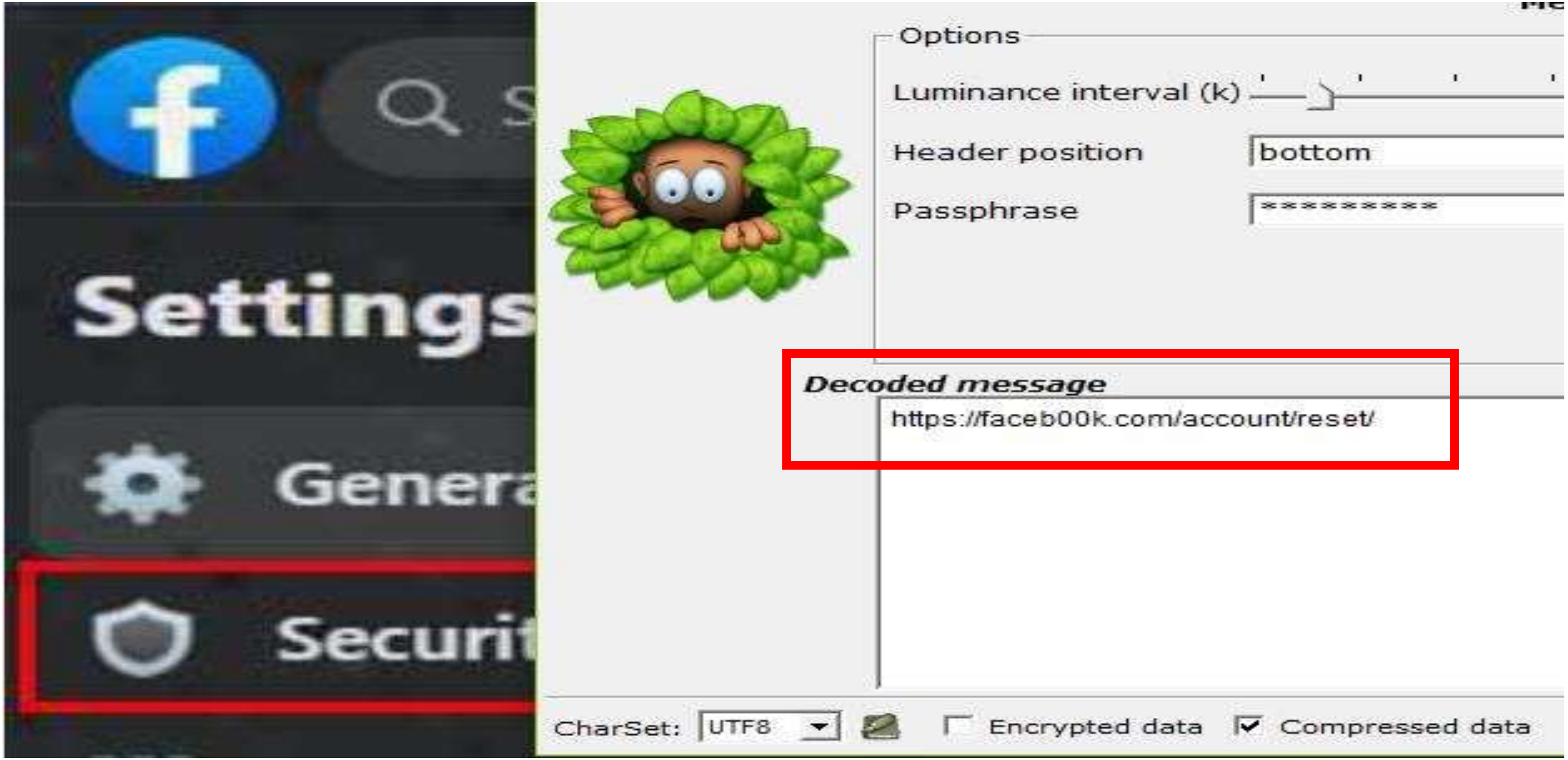
https://google.com/account/reset001

CharSet: UTF8 □ Encrypted data ☑ Compressed data

Hidden Information in Files on System Image

File	Hidden Information
Bank Account Reset.jpg	https://nccbank.com/account/reset/new/pswd/
Facebook Account Reset.jpg	https://faceb00k.com/account/reset/
Google Account Reset.jpg	https://google.com/account/reset001

Sample Screenshot of How Hidden Information was Retrieved using Silent Eye



Options

Luminance interval (k)

Header position: bottom

Passphrase: **********

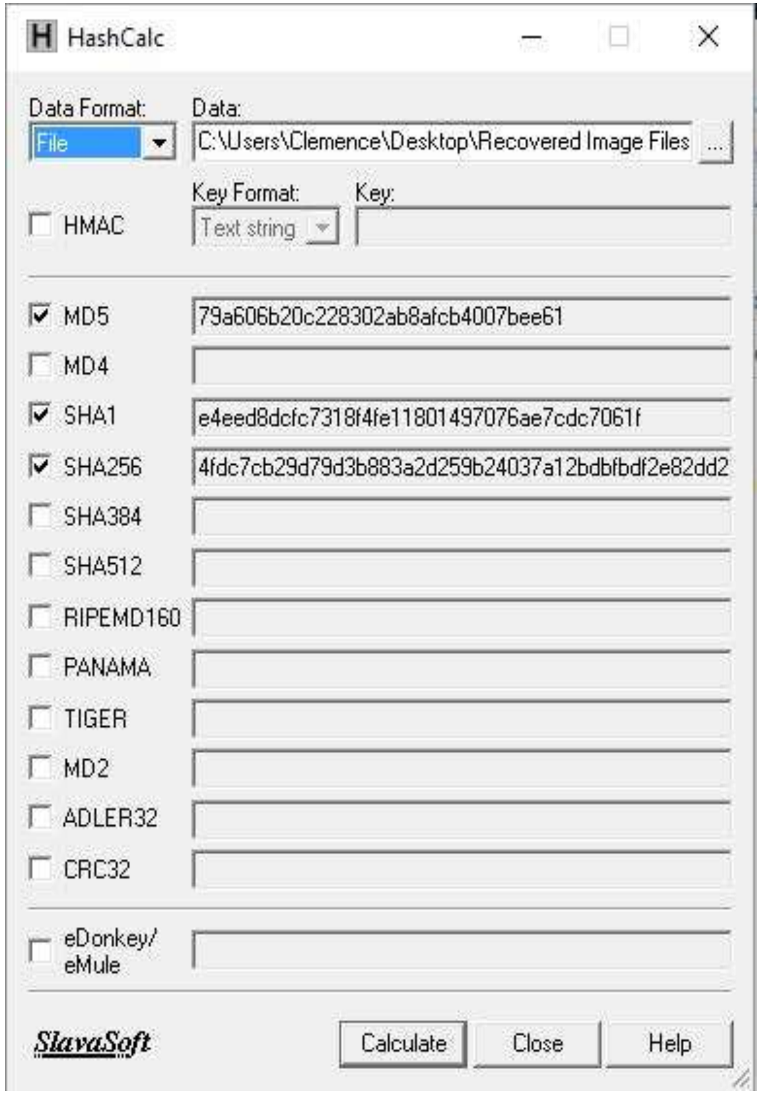
Decoded message

https://faceb00k.com/account/reset/

CharSet: UTF8 □ Encrypted data ☑ Compressed data

Sample Screenshot of Computing Hash values using HashCalc

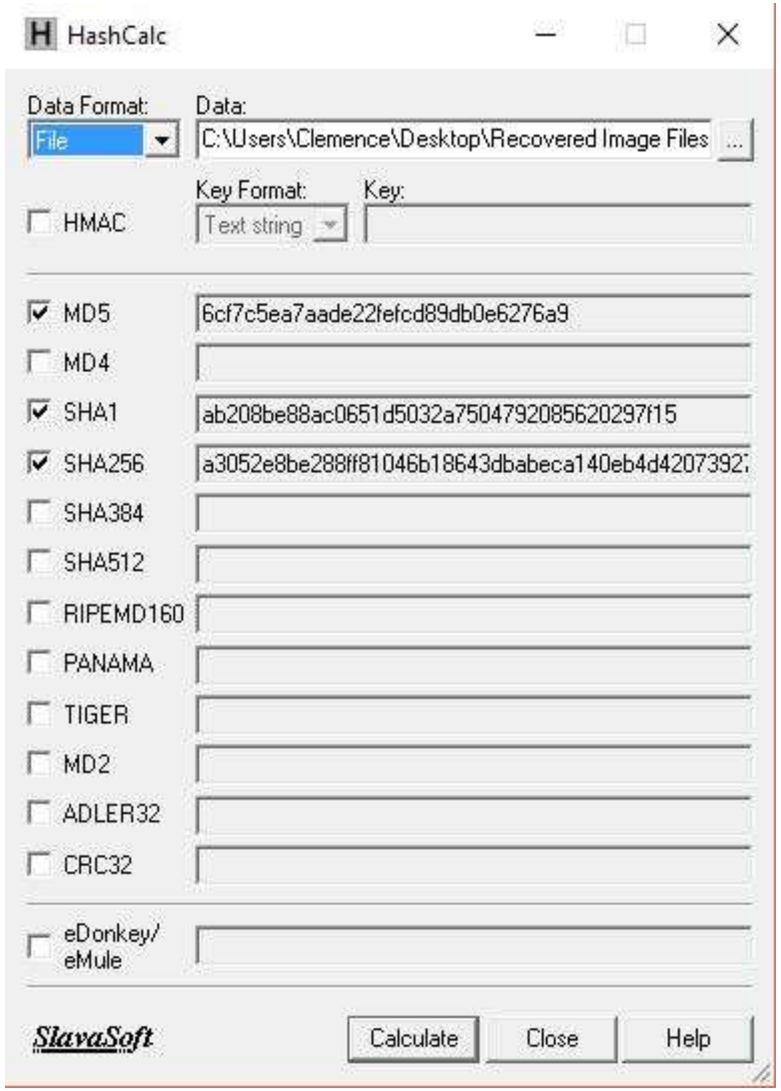
Bank Account Reset.jpg hash values



Data Format: File
Data: C:\Users\Clemence\Desktop\Recovered Image Files
□ HMAC Key Format: Text string Key:

☑ MD5 79a606b20c228302ab8afcb4007bee61
□ MD4
☑ SHA1 e4eed8dcfc7318f4fe11801497076ae7cdc7061f
☑ SHA256 4fdc7cb29d79d3b883a2d259b24037a12bdbfbdf2e82dd2
□ SHA384
□ SHA512
□ RIPEMD160
□ PANAMA
□ TIGER
□ MD2
□ ADLER32
□ CRC32
□ eDonkey/ eMule

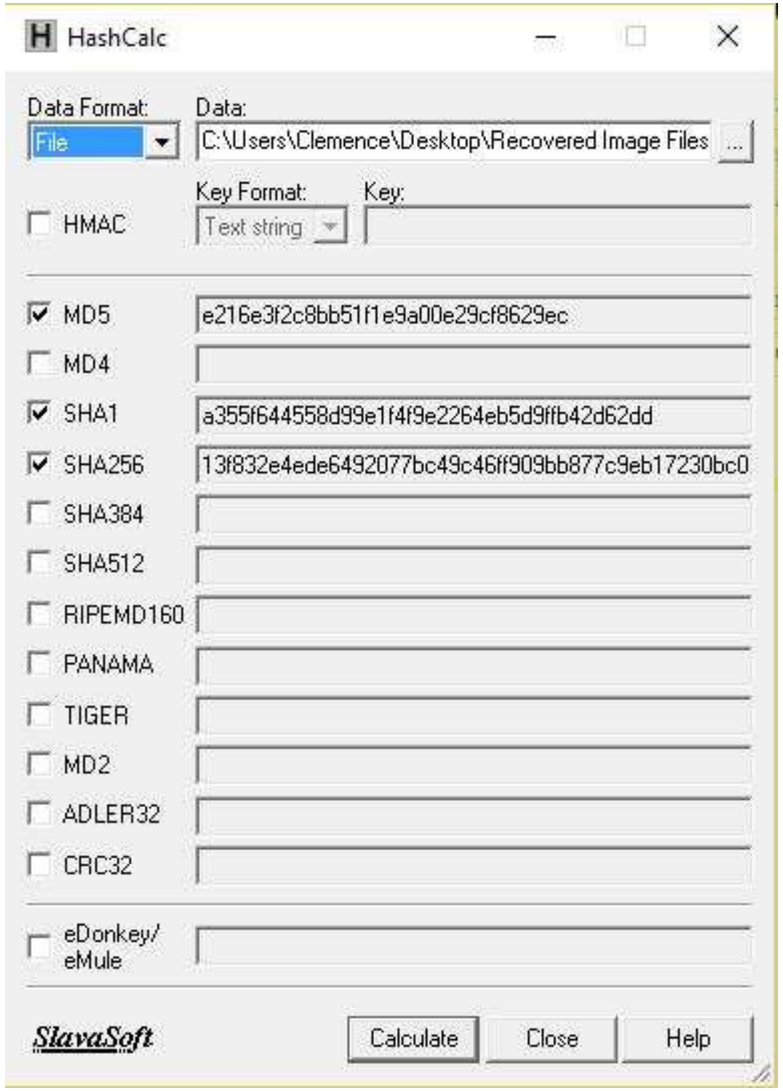
Facebook Account Reset.jpg hash values



Data Format: File
Data: C:\Users\Clemence\Desktop\Recovered Image Files
□ HMAC Key Format: Text string Key:

☑ MD5 6cf7c5ea7aade22fefcd89db0e6276a9
□ MD4
☑ SHA1 ab208be88ac0651d5032a7504792085620297f15
☑ SHA256 a3052e8be288ff81046b18643dbabeca140eb4d4207392
□ SHA384
□ SHA512
□ RIPEMD160
□ PANAMA
□ TIGER
□ MD2
□ ADLER32
□ CRC32
□ eDonkey/ eMule

Google Account Reset.jpg hash values



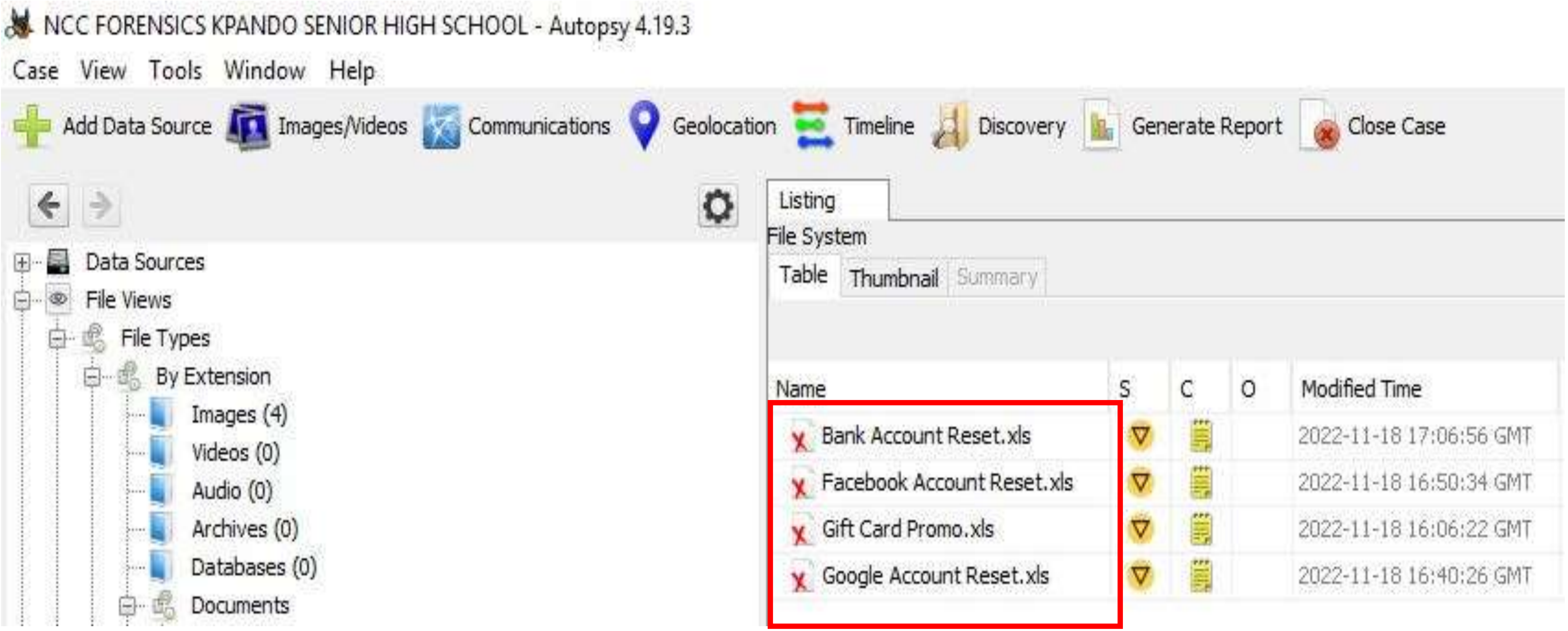
Data Format: File
Data: C:\Users\Clemence\Desktop\Recovered Image Files
□ HMAC Key Format: Text string Key:

☑ MD5 e216e3f2c8bb51f1e9a00e29cf8629ec
□ MD4
☑ SHA1 a355f644558d99e1f4f9e2264eb5d9ffb42d62dd
☑ SHA256 13f832e4ede6492077bc49c46ff909bb877c9eb17230bc0
□ SHA384
□ SHA512
□ RIPEMD160
□ PANAMA
□ TIGER
□ MD2
□ ADLER32
□ CRC32
□ eDonkey/ eMule

Hash Values of Files on System Image

File	Hash Value
Bank Account Reset.jpg	**SHA 256:** 4fdc7cb29d79d3b883a2d259b24037a12bdbfbdf2e82dd2
Facebook Account Reset.jpg	**SHA 256:** a3052e8be288ff81046b18643dbabeca140eb4d42073927f5ec2fa189fe68aaa
Google Account Reset.jpg	**SHA256:** 13f832e4ede6492077bc49c46ff909bb877c9eb17230bc09e0dcac3fec1e5fa4

Screenshot of Recovered Deleted Files on USB Image using Autopsy

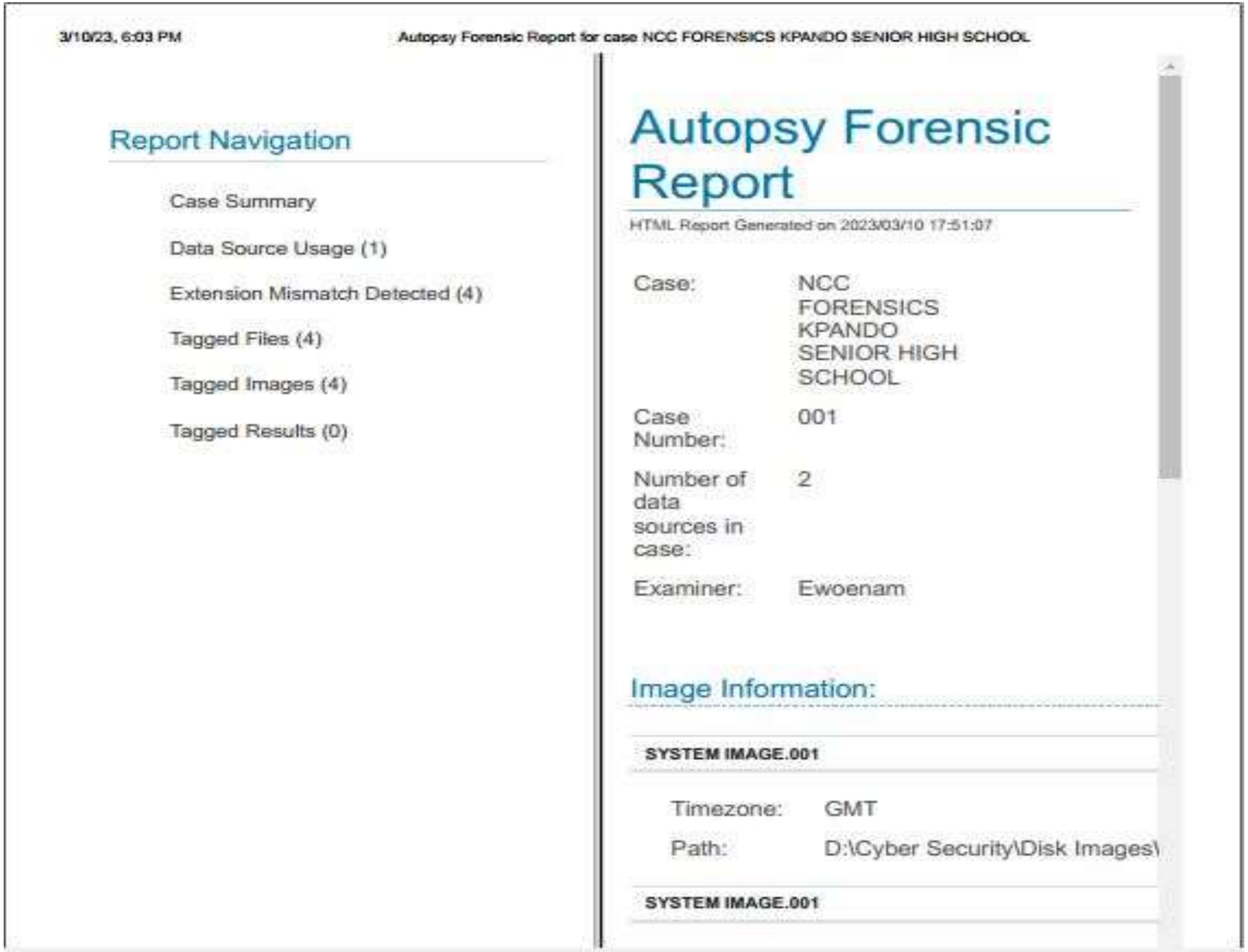


Name	S	C	O	Modified Time
Bank Account Reset.xls	▽	📝		2022-11-18 17:06:56 GMT
Facebook Account Reset.xls	▽	📝		2022-11-18 16:50:34 GMT
Gift Card Promo.xls	▽	📝		2022-11-18 16:06:22 GMT
Google Account Reset.xls	▽	📝		2022-11-18 16:40:26 GMT

RECOVERED DELETED FILES AND HIDDEN INFORMATION

File	Hidden Information
Bank Account Reset	https://nccbank.com/account/reset/new/pswd/
Facebook Account Reset	https://faceb00k.com/account/reset/
Google Account Reset	https://google.com/account/reset001

Screenshot of Autopsy Generated Report for both System and USB Images



3/10/23, 6:03 PM Autopsy Forensic Report for case NCC FORENSICS KPANDO SENIOR HIGH SCHOOL

Report Navigation

- Case Summary
- Data Source Usage (1)
- Extension Mismatch Detected (4)
- Tagged Files (4)
- Tagged Images (4)
- Tagged Results (0)

Autopsy Forensic Report

HTML Report Generated on 2023/03/10 17:51:07

Case:	NCC FORENSICS KPANDO SENIOR HIGH SCHOOL
Case Number:	001
Number of data sources in case:	2
Examiner:	Ewoenam

Image Information:

SYSTEM IMAGE.001

Timezone:	GMT
Path:	D:\Cyber Security\Disk Images\

SYSTEM IMAGE.001

RECOVERED DELETED FILES AND HASH VALUES

File	Hash Values
Bank Account Reset.jpg	**SHA 256:** 4fdc7cb29d79d3b883a2d259b24037a12bdbfbdf2e82dd2
Facebook Account Reset.jpg	**SHA 256:** a3052e8be288ff81046b18643dbabeca140eb4d42073927f5ec2fa189fe68aaa
Google Account Reset.jpg	**SHA256:** 13f832e4ede6492077bc49c46ff909bb877c9eb17230bc09e0dcac3fec1e5fa4

COMPARISON OF HIDDEN INFORMATION

Hidden Information Found on System Image	Hidden Information on the USB Image used for Analysis
Bank Account Reset.jpg https://nccbank.com/account/reset/new/pswd/	**Bank Account Reset.jpg** https://nccbank.com/account/reset/new/pswd/
Facebook Account Reset.jpg https://faceb00k.com/account/reset/	**Facebook Account Reset.jpg** https://faceb00k.com/account/reset/
Google Account Reset.jpg https://google.com/account/reset001	**Google Account Reset.jpg** https://google.com/account/reset001

COMPARISON OF HASH VALUES

HASH VALUES OF FILES ON SYSTEM IMAGE	HASH VALUES OF FILES ON USB IMAGE
Bank Account Reset.jpg SHA 256: 4fdc7cb29d79d3b883a2d259b24037a12bdbfbdf2e82dd2	**Bank Account Reset.jpg** SHA 256: 4fdc7cb29d79d3b883a2d259b24037a12bdbfbdf2e82dd2
Facebook Account Reset.jpg SHA256: a3052e8be288ff81046b18643dbabeca140eb4d42073927f5ec2fa189fe68aaa	**Facebook Account Reset.jpg** SHA 256: a3052e8be288ff81046b18643dbabeca140eb4d42073927f5ec2fa189fe68aaa
Google Account Reset.jpg SHA256: 13f832e4ede6492077bc49c46ff909bb877c9eb17230bc09e0dcac3fec1e5fa4	**Google Account Reset.jpg** SHA256: 13f832e4ede6492077bc49c46ff909bb877c9eb17230bc09e0dcac3fec1e5fa4

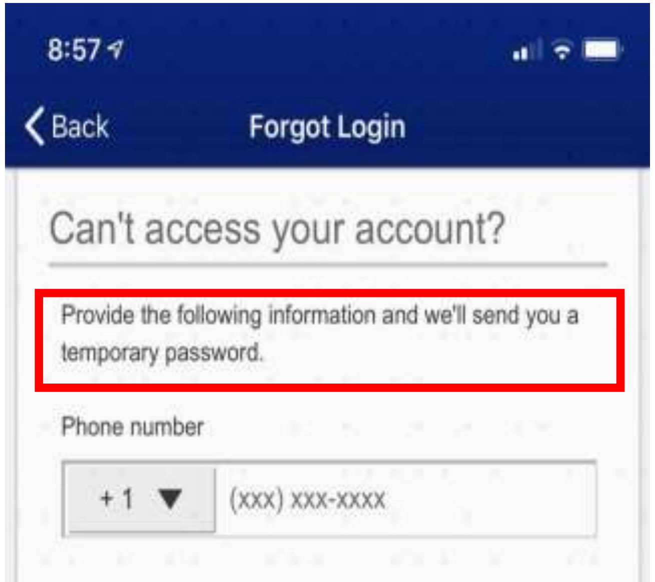
ANY OTHER RELEVANT INFORMATION ON THE USB IMAGE (IF ANY)

- The suspected employee used phishing to make the victim think he had a legitimate email from an organization. From that technique, the suspect was able to get access to the client's bank account, the client's Facebook account and the client's google account. All the information that were retrieved from the attachments were links to websites. The main aim was bent towards getting clients to reset their passwords.

- From the image; "Facebook Account Reset.jpg", it indicates that the file was created at 8:57 but the metadata that was generated from the autopsy report indicates that it was created on the 11th of November, 2022 at 5:20PM GMT.

Screenshot of Any other Relevant Data Found on USB Image

1.



8:57

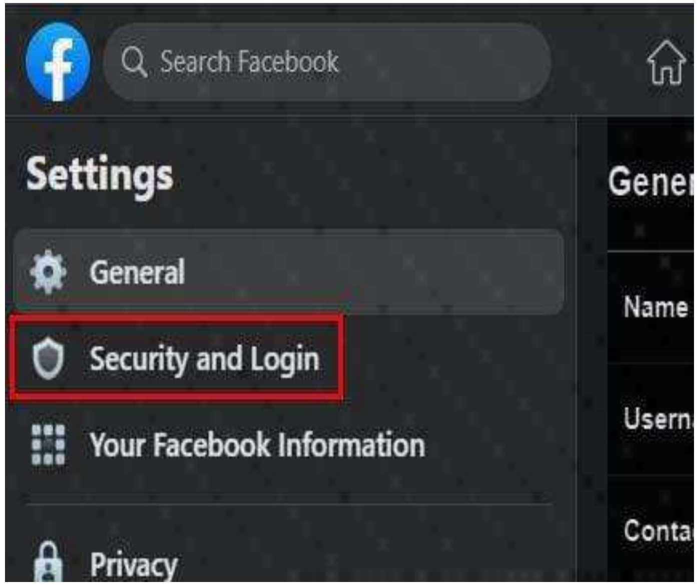
Back Forgot Login

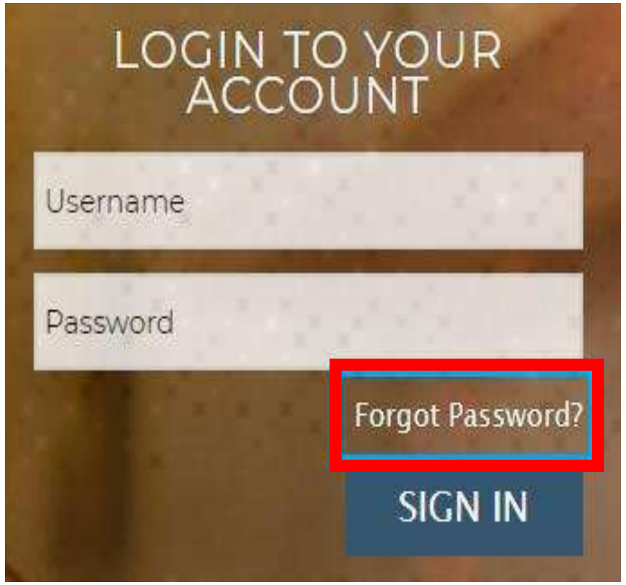
Can't access your account?

Provide the following information and we'll send you a temporary password.

Phone number

+1 ▼ (xxx) xxx-xxxx





LOGIN TO YOUR ACCOUNT

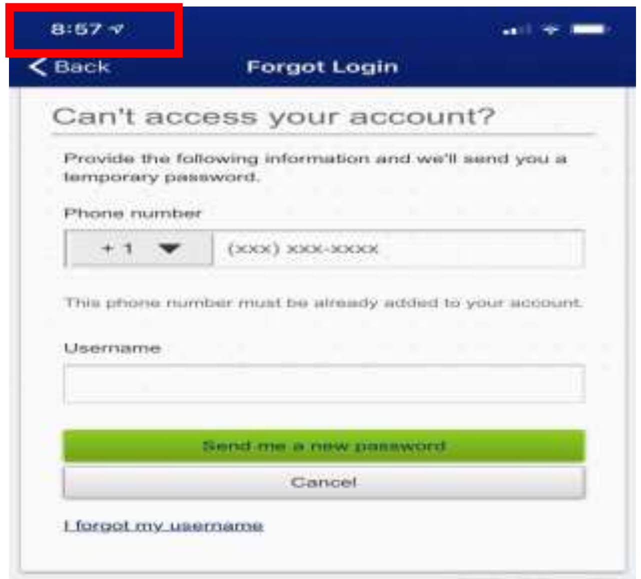
Username

Password

Forgot Password?

SIGN IN

2.



8:57

Back Forgot Login

Can't access your account?

Provide the following information and we'll send you a temporary password.

Phone number

+1 ▼ (xxx) xxx-xxxx

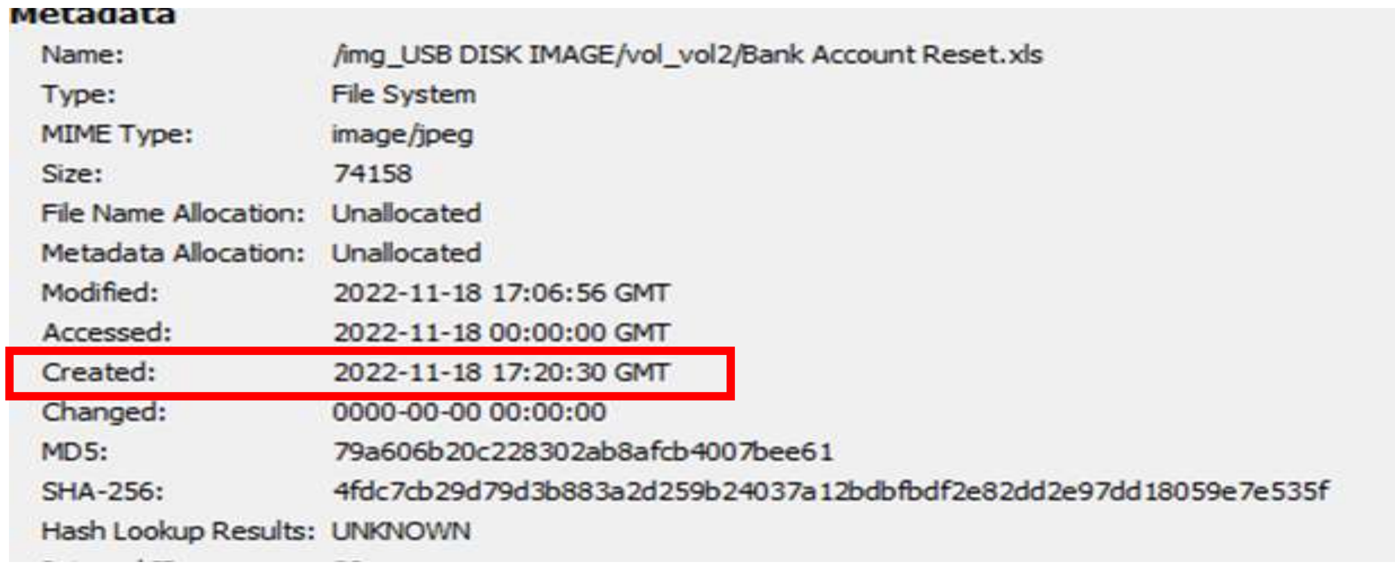
This phone number must be already added to your account.

Username

Send me a new password

Cancel

I forgot my username



Metadata

```
Name:                    /img_USB DISK IMAGE/vol_vol2/Bank Account Reset.xls
Type:                    File System
MIME Type:               image/jpeg
Size:                    74158
File Name Allocation:    Unallocated
Metadata Allocation:     Unallocated
Modified:                2022-11-18 17:06:56 GMT
Accessed:                2022-11-18 00:00:00 GMT
Created:                 2022-11-18 17:20:30 GMT
Changed:                 0000-00-00 00:00:00
MD5:                     79a606b20c228302ab8afcb4007bee61
SHA-256:                 4fdc7cb29d79d3b883a2d259b24037a12bdbfbdf2e82dd2e97dd18059e7e535f
Hash Lookup Results:     UNKNOWN
```

SUMMARY OF OBSERVATION1/2

1. The System image and USB image contain a total of 6 images, all with mismatched extensions.(.xls).
2. An anti-forensics step had been taken to cover up the actual file types of images on the system image.
3. All the images contained links to sites where the reset of password was required.
4. The deleted files were images but had been changed to Microsoft excel spreadsheet files with extension ".xls".
5. The image files on the SYSTEM IMAGE corresponds to the recovered deleted image files on the USB IMAGE.
6. The retrieved links from the system image were the same as the retrieved links from the USB drive image.
7. The hash values (or the finger prints) of extracted images from the system were same as the recovered images from the USB drive image.

SUMMARY OF OBSERVATION 2/2

From all investigations that were carried out, we observed that the suspect changed the extensions for all the attachments because if he did not do that, then the files he was working with could have just been read by anyone. For this reason, he changed them into a format that was unreadable for the actual file type.

Before changing the extensions of the files, the suspect hid phishing links behind the images so that a third party would just see the file without knowing what it actually contained.

Further investigations indicated that, the suspect worked the files on his computer system then later transferred them to his USB drive. After which, he deleted them because he realized he could soon be caught.

CONCLUSIONS

- There can be only two reasons for changing the file extension of all the attachments recovered from the suspect’s computer and deleting the attachments on the USB drive;
- i. either the suspect wants to cover up a crime
- ii. Or the suspect does not want anybody to know what he has been up to.

- With the evidences that were procured, we suggest that the suspect did send phishing messages with links to malicious sites because, all the hidden links which were uncovered from all the attachments seemed to aim at one thing, that is, to get clients’ personal information.

- Whoever the suspect sent the phishing message to must be aware some information has been encoded into the attachments therefore receiver is not a victim but an accomplice.

End of Presentation

THANK YOU