Digital Forensic Analysis of Hidden Messages in Images

By: **Farzaneh Noroozi**

Digital Forensic Analysis Report

Summary of Analysis

This digital forensic analysis involves the extraction of hidden messages from a collection of images provided by Dr. Humpherys. The process includes performing SHA-256 checksums on each image to ensure data integrity, creating a chain of custody by recording file details and hash numbers and extracting hidden messages using steganography techniques.

Objectives

1. Download and unzip image files provided by Dr. Humpherys.
2. Perform SHA-256 checksum on each image and record hash numbers.
3. Create a chain of custody table with the file name, date of the file, date received, Dr. Humpherys' hash number, and your hash number.
4. Extract hidden messages from each image using steganography techniques.
5. Write a report on how we did the stenographic file.

Chain of Custody (Table of Hash Numbers)

File Name	Date of File	Date Received	Dr. Humpherys' Hash Number	My Hash Number
universe_modified-Noroozi.png	1/31/2024 3:09 PM PST	1/31/2024 11:49:42AM CST	500f06b8ec5313b055b2c1f3a17cfa414f62c27373ca1483bc7e9e3d98f409d6	500F06B8EC5313B055B2C1F3A17CFA414F62C27373CA1483BC7E9E3D98F409D6

The chain of Custody table is like our organized roadmap to keep things in check during our analysis.

Digital Forensic Analysis of Hidden Messages in Images

By: **Farzaneh Noroozi**

1. **File Name:** We're just jotting down the names of each image. Helps us know which image we're talking about.
2. **Date of the File:** This is just about timing – when I get the Hash number from PowerShell.
3. **Date Received:** This shows the time that I received the file from Dr. Humpherys.
4. **Dr. Humpherys' Hash Number:** It was written in the homework guide page and It's like a fingerprint for the original image, and we're noting it down.
5. **My Hash Number:** Now it's our turn. We're using the same math to get our own unique number for each image. It's like our fingerprint for the image.

Comparison of Hash Numbers:

Now, here's the interesting part. We're checking if our fingerprint matches Dr. Humpherys'. Why? Because if they match, it means the image hasn't changed. No funny business.

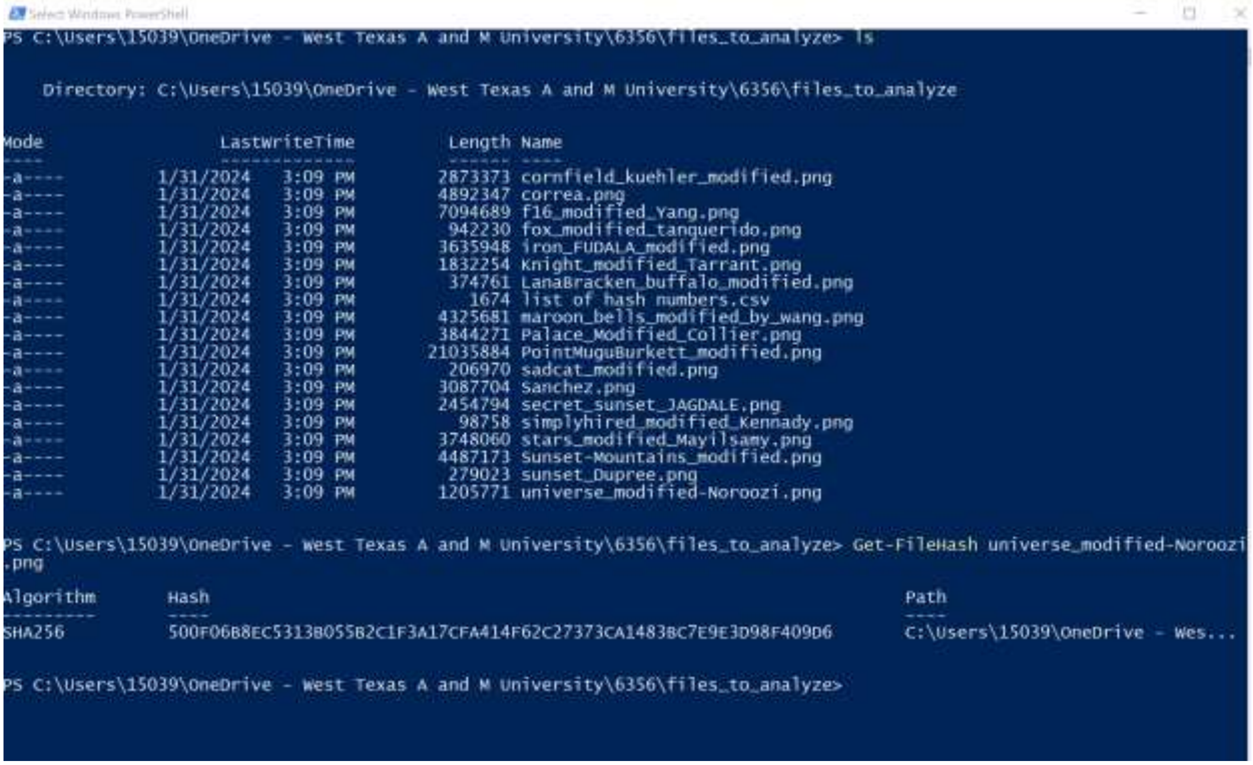
Explanation:

- If our fingerprint matches Dr. Humpherys', it's like a digital high-five. It means the image we got is the same as the one he provided. No sneaky stuff happened.
- The math we're using is pretty cool. Even tiny changes to the image make the fingerprint totally different. So, if the fingerprints match, we can trust that the image is exactly as it should be.
- This whole comparison thing is crucial. It's our way of saying, "Hey, we're keeping an eye on things, and nothing fishy is going on." It's a solid way to make sure the images stay the way they were when we started.

Digital Forensic Analysis of Hidden Messages in Images

By: **Farzaneh Noroozi**

……………………………………………………………………………………………………



```
PS C:\Users\15039\OneDrive - West Texas A and M University\6356\files_to_analyze> ls


    Directory: C:\Users\15039\OneDrive - West Texas A and M University\6356\files_to_analyze


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         1/31/2024   3:09 PM        2873373 cornfield_kuehler_modified.png
-a----         1/31/2024   3:09 PM        4892347 correa.png
-a----         1/31/2024   3:09 PM        7094689 f16_modified_Yang.png
-a----         1/31/2024   3:09 PM         942230 fox_modified_tanquerido.png
-a----         1/31/2024   3:09 PM        3635948 iron_FUDALA_modified.png
-a----         1/31/2024   3:09 PM        1832254 Knight_modified_Tarrant.png
-a----         1/31/2024   3:09 PM         374761 LanaBracken_buffalo_modified.png
-a----         1/31/2024   3:09 PM           1674 list of hash numbers.csv
-a----         1/31/2024   3:09 PM        4325681 maroon_bells_modified_by_wang.png
-a----         1/31/2024   3:09 PM        3844271 Palace_Modified_Collier.png
-a----         1/31/2024   3:09 PM       21035884 PointMuguBurkett_modified.png
-a----         1/31/2024   3:09 PM         206970 sadcat_modified.png
-a----         1/31/2024   3:09 PM        3087704 Sanchez.png
-a----         1/31/2024   3:09 PM        2454794 secret_sunset_JAGDALE.png
-a----         1/31/2024   3:09 PM          98758 simplyhired_modified_Kennady.png
-a----         1/31/2024   3:09 PM        3748060 stars_modified_Mayilsamy.png
-a----         1/31/2024   3:09 PM        4487173 Sunset-Mountains_modified.png
-a----         1/31/2024   3:09 PM         279023 sunset_Dupree.png
-a----         1/31/2024   3:09 PM        1205771 universe_modified-Noroozi.png


PS C:\Users\15039\OneDrive - West Texas A and M University\6356\files_to_analyze> Get-FileHash universe_modified-Noroozi
.png

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          500F06B8EC5313B055B2C1F3A17CFA414F62C27373CA1483BC7E9E3D98F409D6       C:\Users\15039\OneDrive - Wes...


PS C:\Users\15039\OneDrive - West Texas A and M University\6356\files_to_analyze>
```

Methods and Tools Used

The SHA-256 checksums were calculated using PowerShell. The Python code for extracting hidden messages is executed in Google Colab. The analysis code can be found here.

PowerShell Code Example:

```
Get-FileHash universe_modified-Noroozi.png
```

Python Code for Hidden Messages:

```
!pip install stegano
from stegano import lsb
from PIL Import Image

image_name_with_message = "universe_modified-Noroozi.png"
hidden_message = lsb.reveal(image_name_with_message)
```

```
print(hidden_message)
Image.open(image_name_with_message)
```

Relevant Findings

1. **universe_modified-Noroozi.png: Hidden Message** "life is full of surprises"
2. **correa.png Hidden Message** "Domingo is the best student in this class"
3. **f16_modified_Yang.png: Hidden Message** "Generation Four"
4. **fox_modified_tanquerido.png: Hidden Message** "What does the fox say?"
5. **iron_FUDALA_modified.png: Hidden Message** "Don't meddle with things, you don't understand"
6. **Knight_modified_Tarrant.png: Hidden Message** "He who kneels before God can stand before anyone"
7. **LanaBracken_buffalo_modified.png: Hidden Message** "On, on Buffaloes... we'll bring home the victory! W-T-A-M-, WTAM, Fight! Fight! Fight!"
8. **maroon_bells_modified_by_wang.png: Hidden Message** "404"
9. **Palace_Modified_Collier.png: Hidden Message** "The idyllic city of Beauclair and its palace at night."
10. **PointMuguBurkett_modified.png: Hidden Message** "These trails are by the beach."
11. **sadcat_modified.png: Hidden Message** "My Monday Mood"
12. **Sanchez.png: Hidden Message** "Do I really look like a guy with a plan? You know what I am? I'm a dog chasing cars. I wouldn't know what to do with one if I caught it!"
13. **secret_sunset_JAGDALE.png: Hidden Message** "I <3 Chai"
14. **simplyhired_modified_Kennady.png: Hidden Message** "Capture Flag event is my first assignment in Digital Forensics"

15. **stars_modified_Mayilsamy.png: Hidden Message** "Hi!! My name is Priya. Nice to meet you!"

16. **Sunset-Mountains_modified.png: Hidden Message** "May the force be with you."

17. **sunset_Dupree.png: Hidden Message** "Just like the moons and the suns, With the certainty of the tides, Just like the hopes springing high, Still I rise."