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.

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

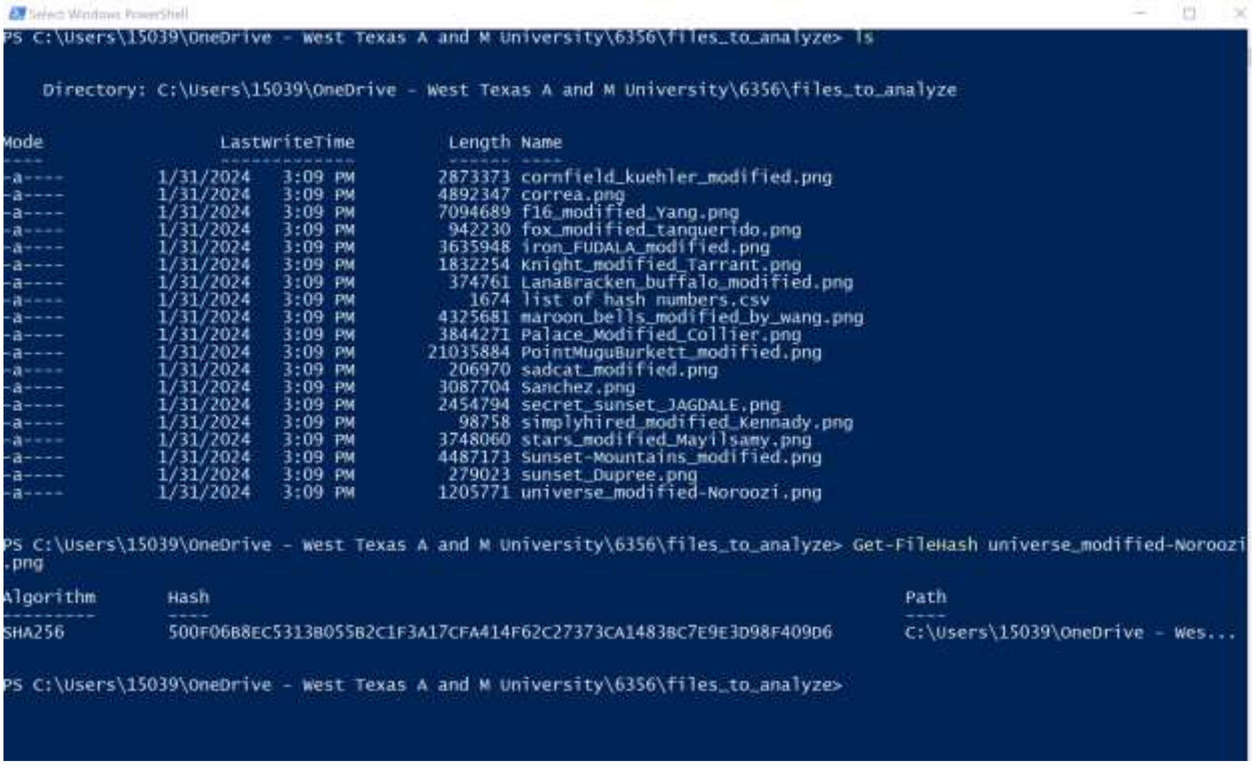
File Name	Date of File	Date Received	Dr. Humpherys' Hash Number	My Hash Number
universe_modified-Noroozi.png	1/31/2024 3:09 PM PST	1/31/2024 11:49:42AM CST	500f06b8ec5313b055b2c1f3a17cfa414f62c27373ca1483bc7e9e3d98f409d6	500F06B8EC5313B055B2C1F3A17CFA414F62C27373CA1483BC7E9E3D98F409D6

Table 1. List of Hash Numbers

The purpose of Figure 1 (See Figure 1) is to provide a visual representation of the hash numbers associated with the digital file "universe_modified-Noroozi.png." This table serves as a reference for the chain of custody, displaying key information such as file names, dates, and hash numbers, ensuring transparency and traceability in the analysis process. The Chain of Custody table serves as our structured guide to ensure accuracy and control throughout the analysis process.

Comparison of Hash Numbers

The comparison involves checking if our generated hash (fingerprint) matches the one provided by Dr. Humpherys. If they match, it signifies that the image hasn't undergone any changes, ensuring data integrity. This verification step is crucial for maintaining the reliability of the digital evidence.



```
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>
```

Figure 1. PowerShell Outcome

Figure 1 illustrates the outcome of executing the PowerShell command within the project repository. The displayed information showcases the result of hashing the file "universe_modified-Noroozi.png," providing a unique cryptographic fingerprint (hash) represented in hexadecimal format. This visual representation serves as a record of the file's integrity verification through the SHA-256 checksum process, ensuring data integrity and aiding in the chain of custody documentation for digital forensic analysis.

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."