Task 1 - What's On the Drive?

(Computer Forensics, Command Line, Encryption Tools)

Points: 10

In accordance with USSID18, a collection on an American citizen is permitted in cases where the person is reasonably believed to be held captive by a group engaged in international terrorism. As a result, we have obtained a copy of the home directory from the journalist's laptop and are hoping it will contain information that will help us to locate and rescue the hostage. Your first task is to analyze the data and files available in the journalist's home directory.

Provided files

- Archive of data from journalist's computer (for tasks 1-3) (`home.zip`)

Prompt

- What is the journalist's username on their computer?
- Enter the file name for the encrypted file on the journalist's computer.

Prerequisites

```
~$ apt install unzip tree file
```

Solution

We start by extracting the ZIP archive.

```
~$ unzip home.zip
~$ ls
home  home.zip
```

We may then inspect the extracted contents.

```
~$ tree home
home
└── JadeOrchids745
    ├── credentials
    ├── Documents
    │   └── Blog-Articles
    │       ├── blogEntry1.txt
    │       ├── blogEntry2.txt
    │       └── blogIntro.txt
    ├── Downloads
    ├── Pictures
    │   ├── Pets
    │   │   ├── couchChillin.jpg
    │   │   ├── loaf.jpg
    │   │   └── shenanigans.jpg
    │   └── Travels
    │       ├── Malta
    │       │   ├── BlueGrotto.jpg
    │       │   ├── MostaDome.jpg
    │       │   └── TritonFountain.jpg
    │       └── Wales
    │           ├── heatherFields.jpg
    │           └── horseFeeding.jpg
```

```
    └── pwHints.txt
```

We may infer that the journalist's username is `JadeOrchids745` since that is the only directory under the `home` directory.

We proceed to inspect the files under the `JadeOrchids745` directory.

```
~$ cd home/JadeOrchids745
~/home/JadeOrchids745$ file credentials
credentials: GPG symmetrically encrypted data (AES256 cipher)
```

We see that `credentials` is the encrypted file.

Results

- What is the journalist's username on their computer?
  - `JadeOrchids745`
- Enter the file name for the encrypted file on the journalist's computer.
  - `credentials`

Author

- **Aviv Brook**