

# File forensics

## CSC-160 Spring 2021

You and your friends are freelance data detectives, decoding the binary debris of everyone from wealthy eccentrics to desperate losers for a few lousy bucks a week on your Patreon. This morning an envelope is on your chair when you come in. As you pick it up, a text message flashes across your display.

“\$1k if you can read the first one—we think it’s text. Another \$5k if you can read the second file.”

The message metadata simply reads “Sender unknown”. You delete the message.

The envelope holds a folded piece of paper, whose contents are reproduced below.

```
54 68 65 72 65 20 61 72 65 20 61 20 67 72 65 61 74 20 6d 61 6e 79
20 64 69 66 66 65 72 65 6e 74 20 77 61 79 73 20 74 6f 20 65 6e 63
6f 64 65 20 65 76 65 6e 20 73 6f 6d 65 74 68 69 6e 67 20 61 73 20
73 69 6d 70 6c 65 20 61 73 20 61 20 74 65 78 74 20 73 74 72 69 6e
67 2e
```

The back of the paper contains merely the incantation

```
hexdump mystery | head
```

Perhaps if you chant it the right way, the data will reveal themselves to you.

Your task is to determine what information these files contain. Probably, the best first step will be to guess the data format. The only clues you have, as always, are the values themselves, which look like they might be hexadecimal bytes.