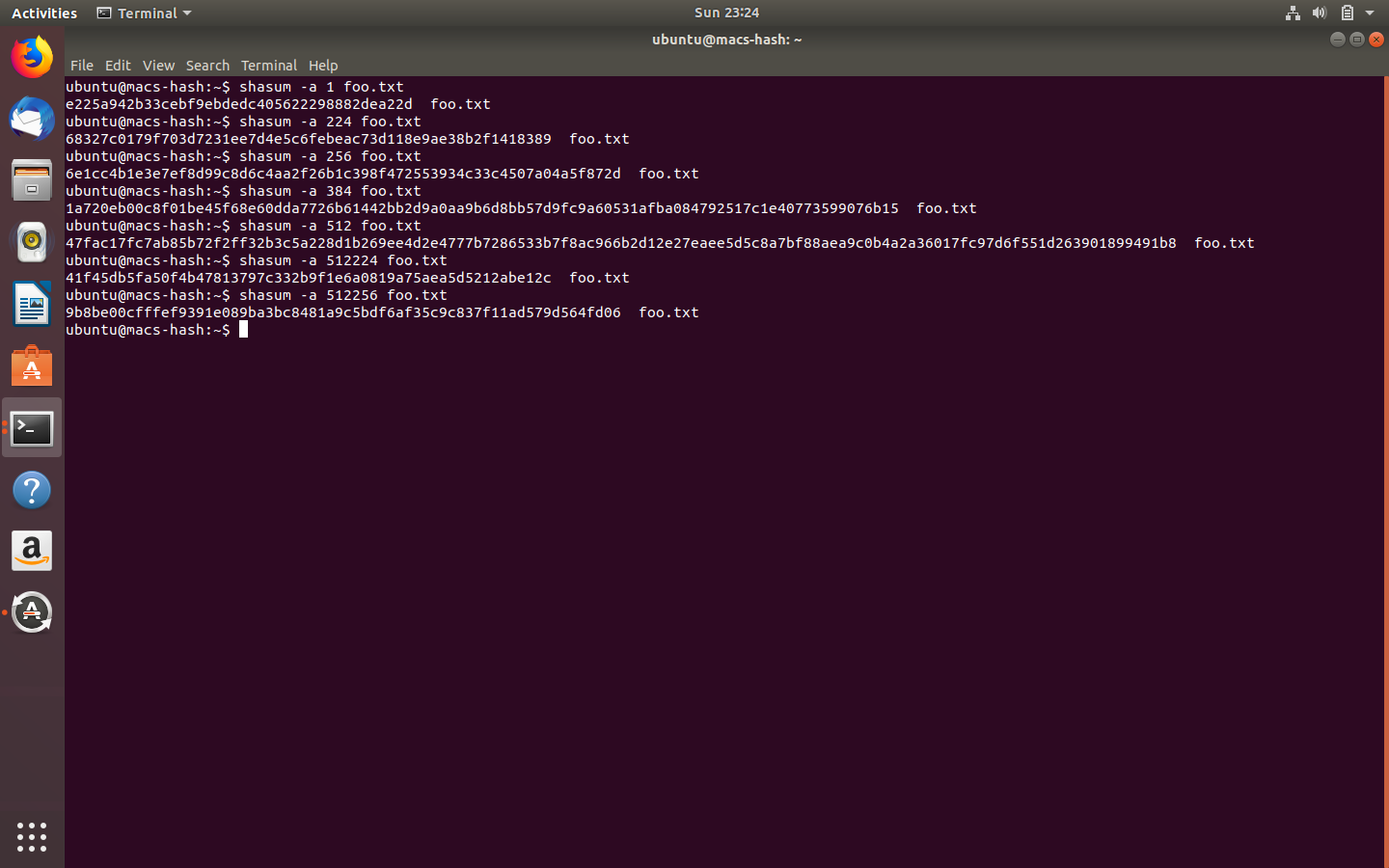
Lab Report

Exploring MACs and Hash Functions

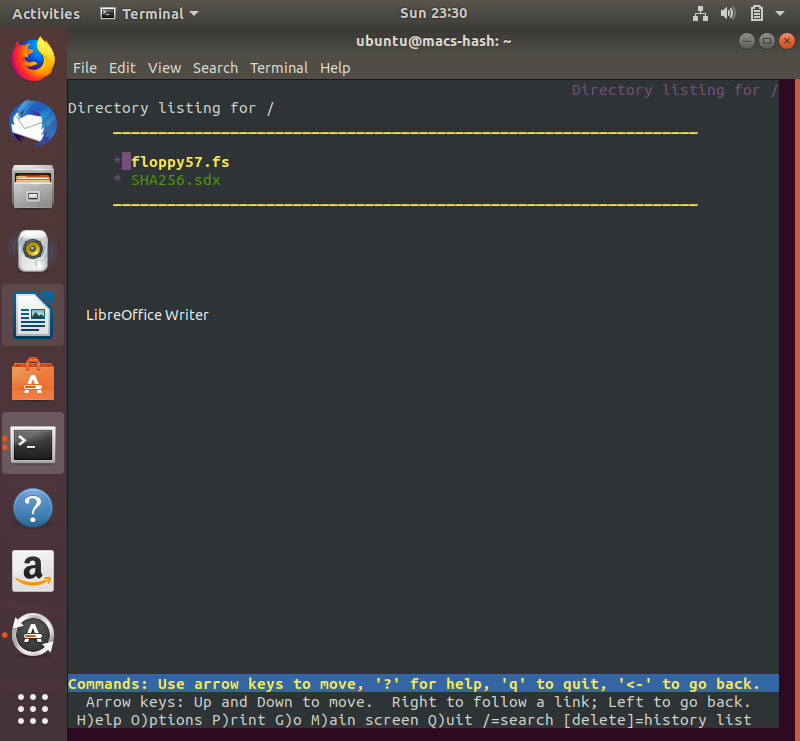
# **Task 1. Practice Generating Digests**

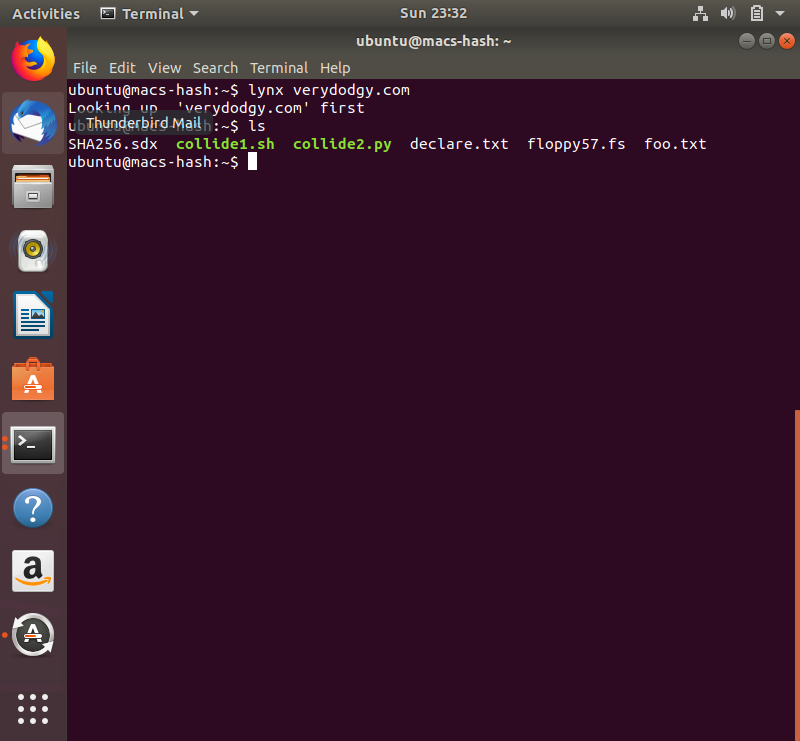
**Please include your commands, screenshots, and explanation for task 1 here:**

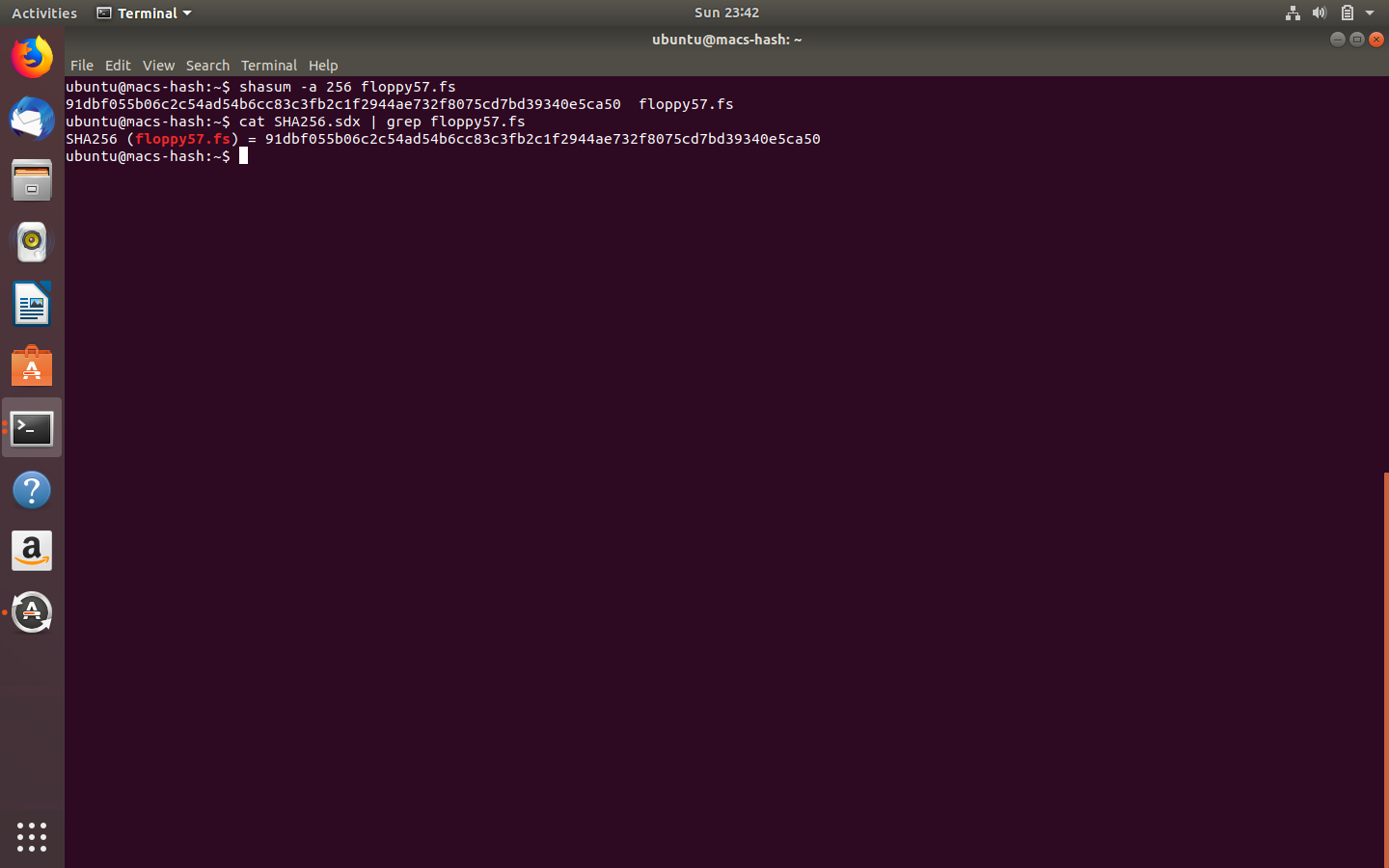
****

**Checking Software Digests**

**Please include your commands, screenshots, and explanation for task 2 here:**

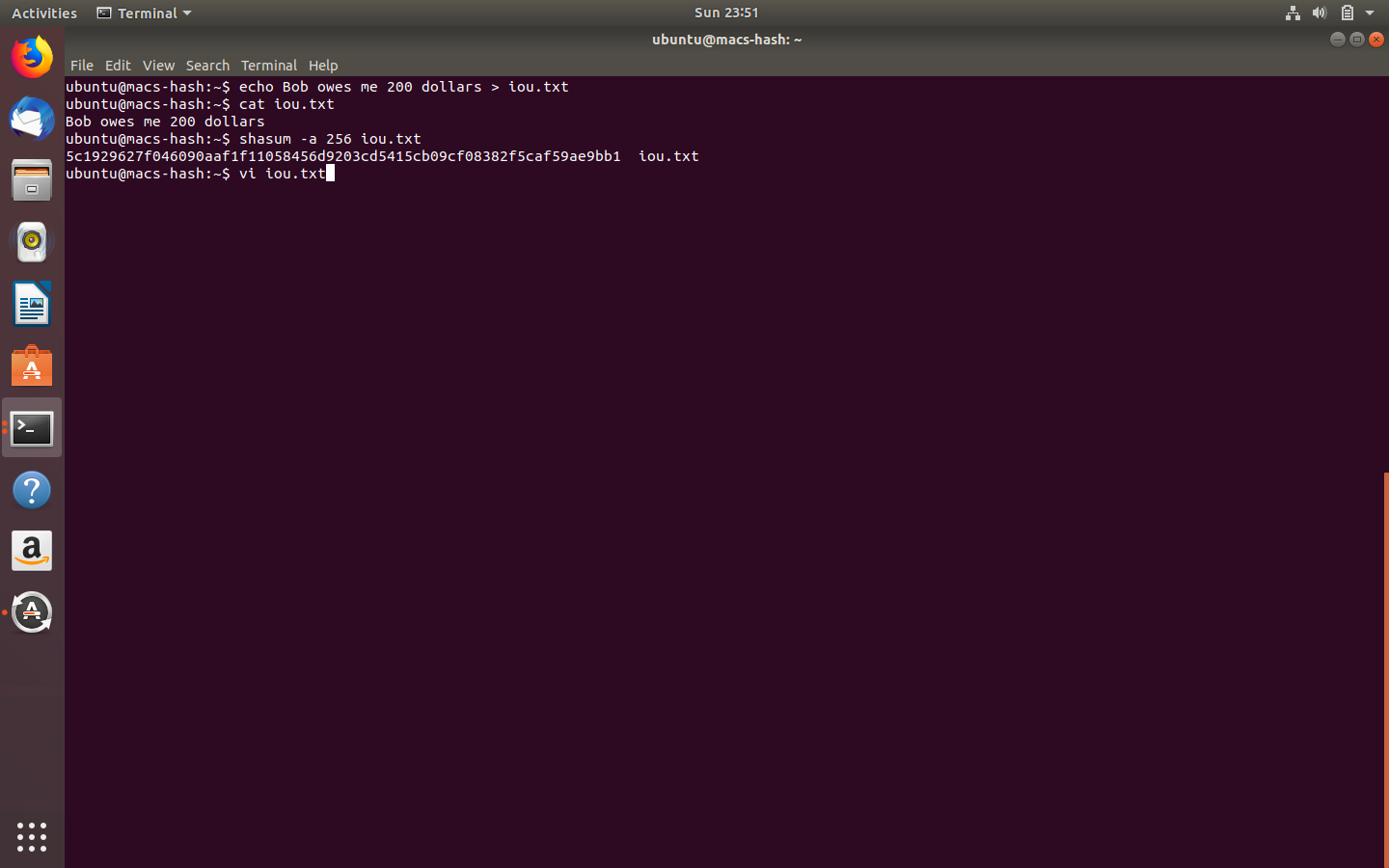


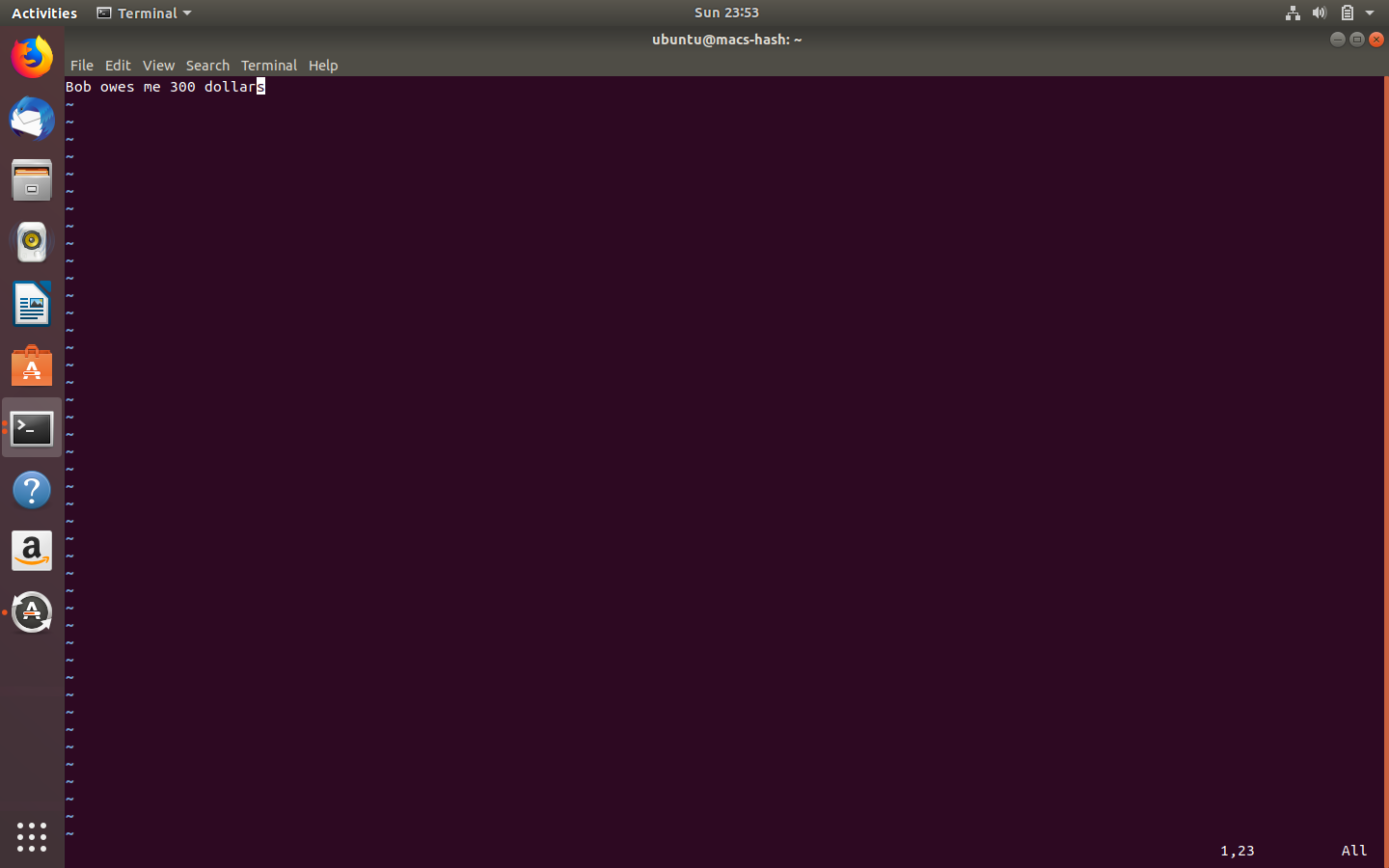


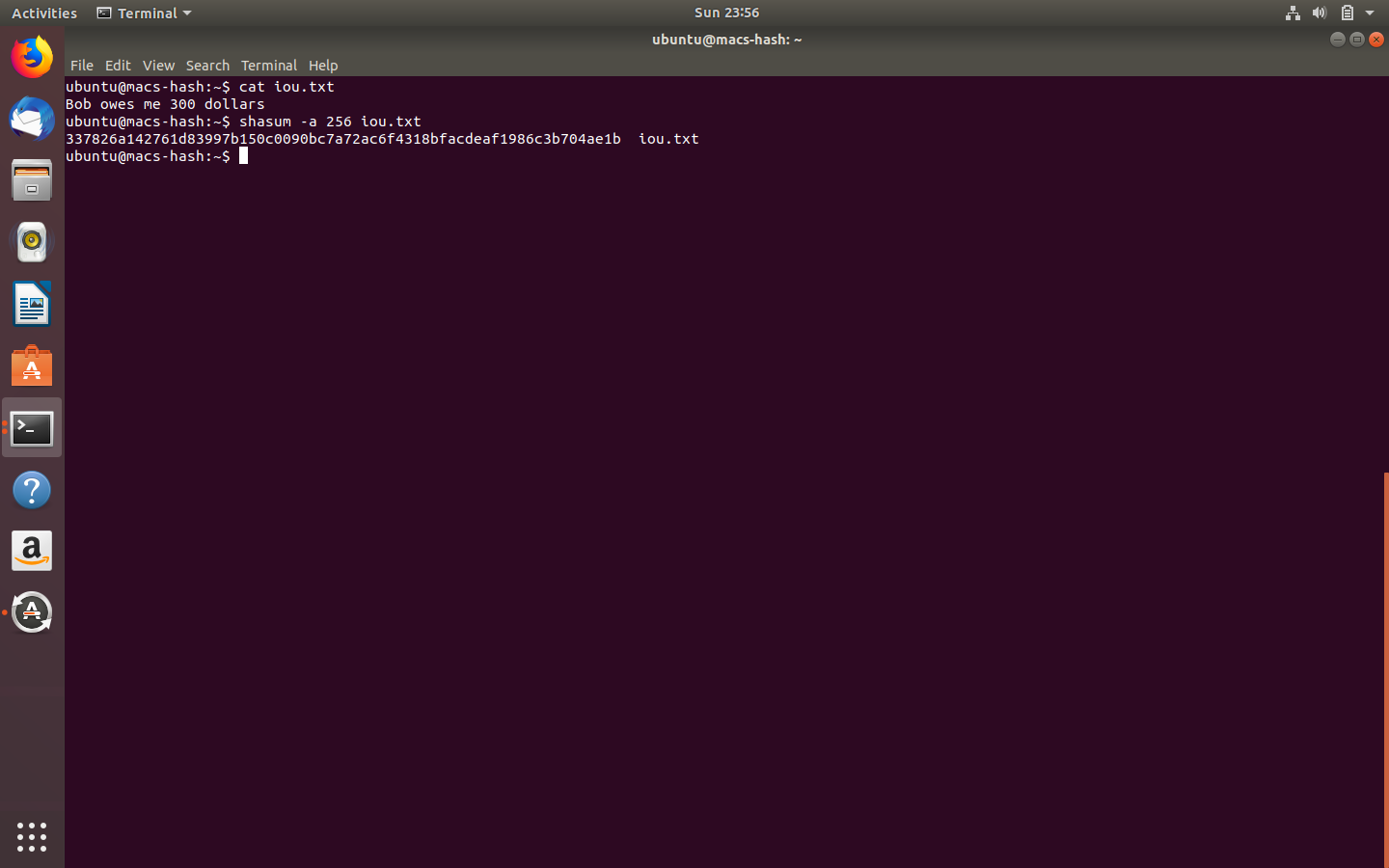


# **Exploring the “Avalanche Effect”**

**Screenshots:**







**Exploring Second Pre-Image Resistance**

1. The last four hex digits of the SHA256 digest of declare.txt: 7bc8

2. The number of attempts to match on **the last hex digit** of the digest for declare.txt.

|  |  |
| --- | --- |
| Attempt | # Tries |
| 1 | 30 |
| 2 | 10 |
| 3 | 16 |
| 4 | 10 |
| 5 | 31 |
| 6 | 7 |
| 7 | 13 |
| 8 | 7 |
| 9 | 1 |
| 10 | 2 |

3. The number of attempts to match on the last **two** hex digits of the digest for declare.txt.

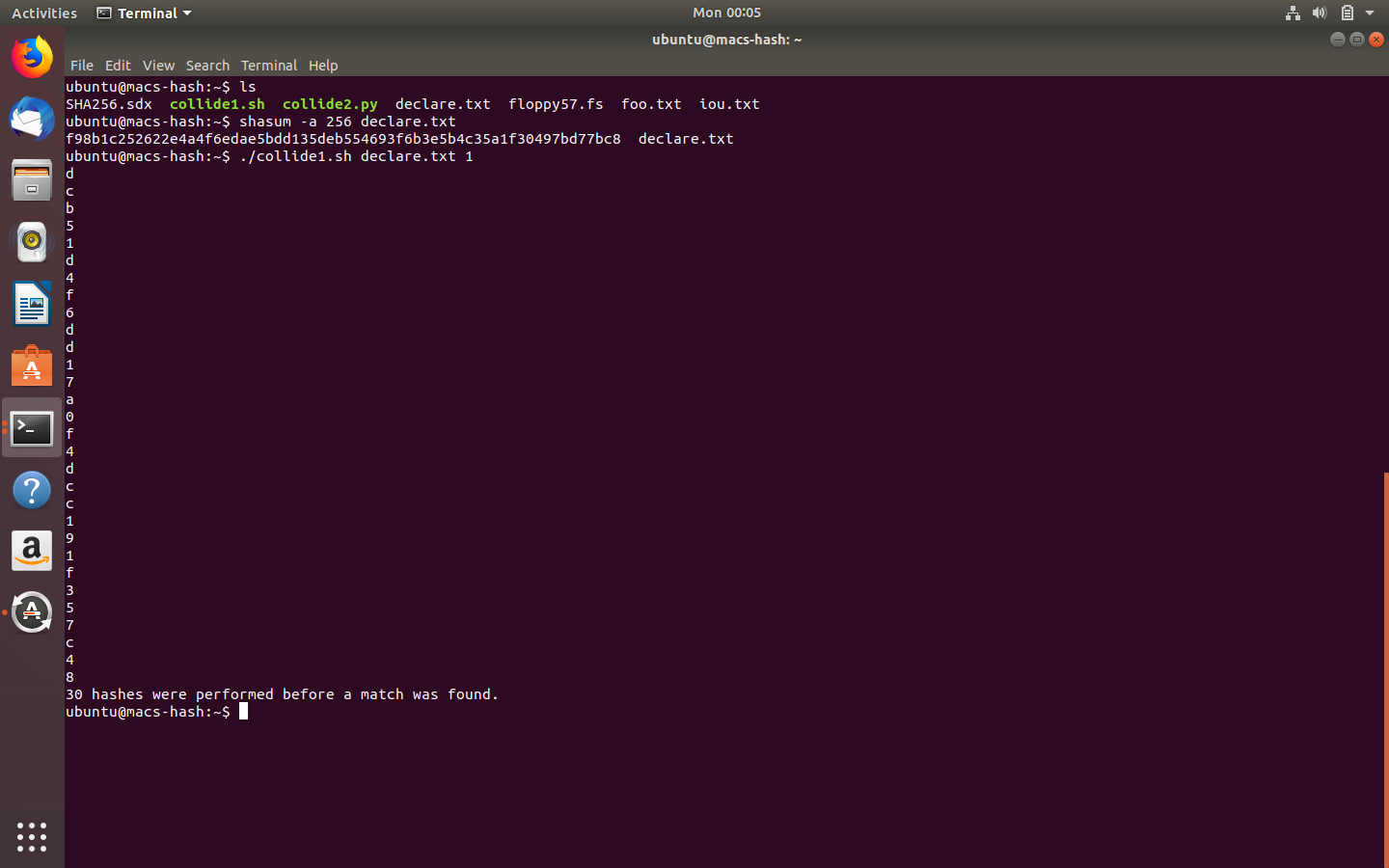
|  |  |
| --- | --- |
| Attempt | # Tries |
| 1 | 150 |
| 2 | 250 |
| 3 | 120 |
| 4 | 198 |
| 5 | 449 |
| 6 | 141 |
| 7 | 334 |
| 8 | 117 |
| 9 | 51 |
| 10 | 31 |

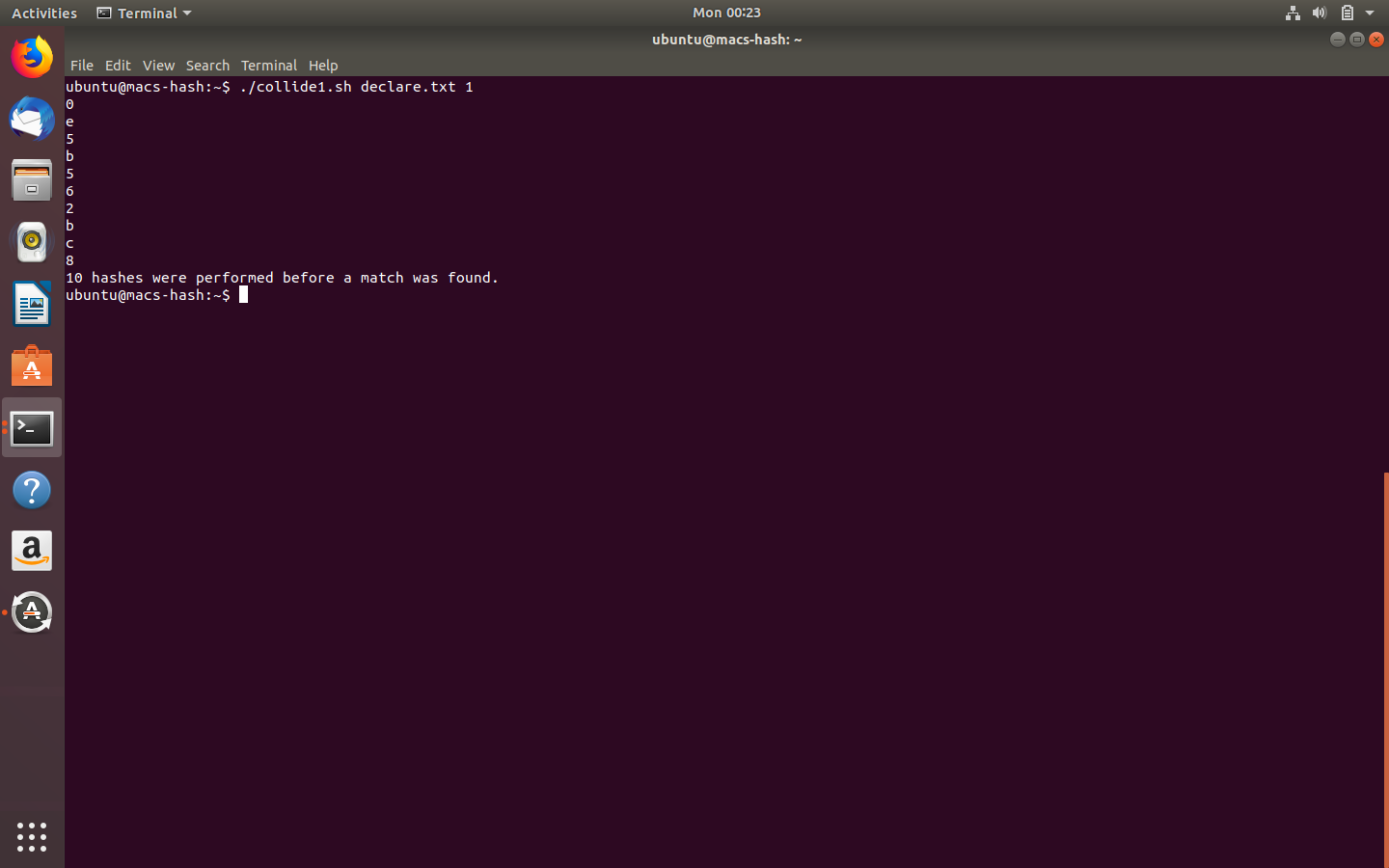
4. The number of attempts to match on the last **three** hex digits of the digest for declare.txt.

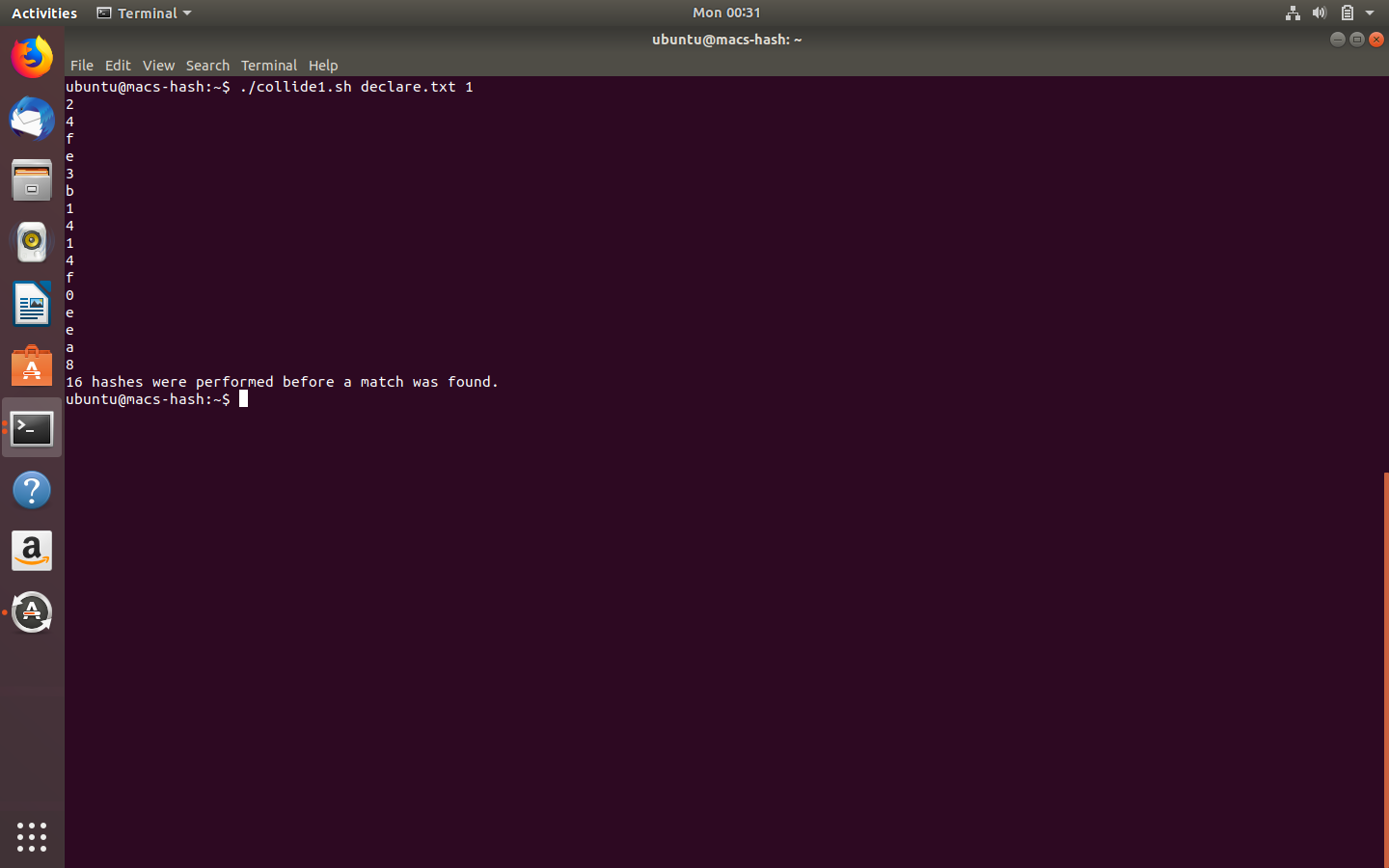
|  |  |
| --- | --- |
| Attempt | # Tries |
| 1 | 249 |
| 2 | 5972 |
| 3 | 1228 |
| 4 | 2273 |
| 5 | 15616 |
| 6 | 1203 |
| 7 | 4017 |
| 8 | 913 |
| 9 | 5318 |
| 10 | 4732 |

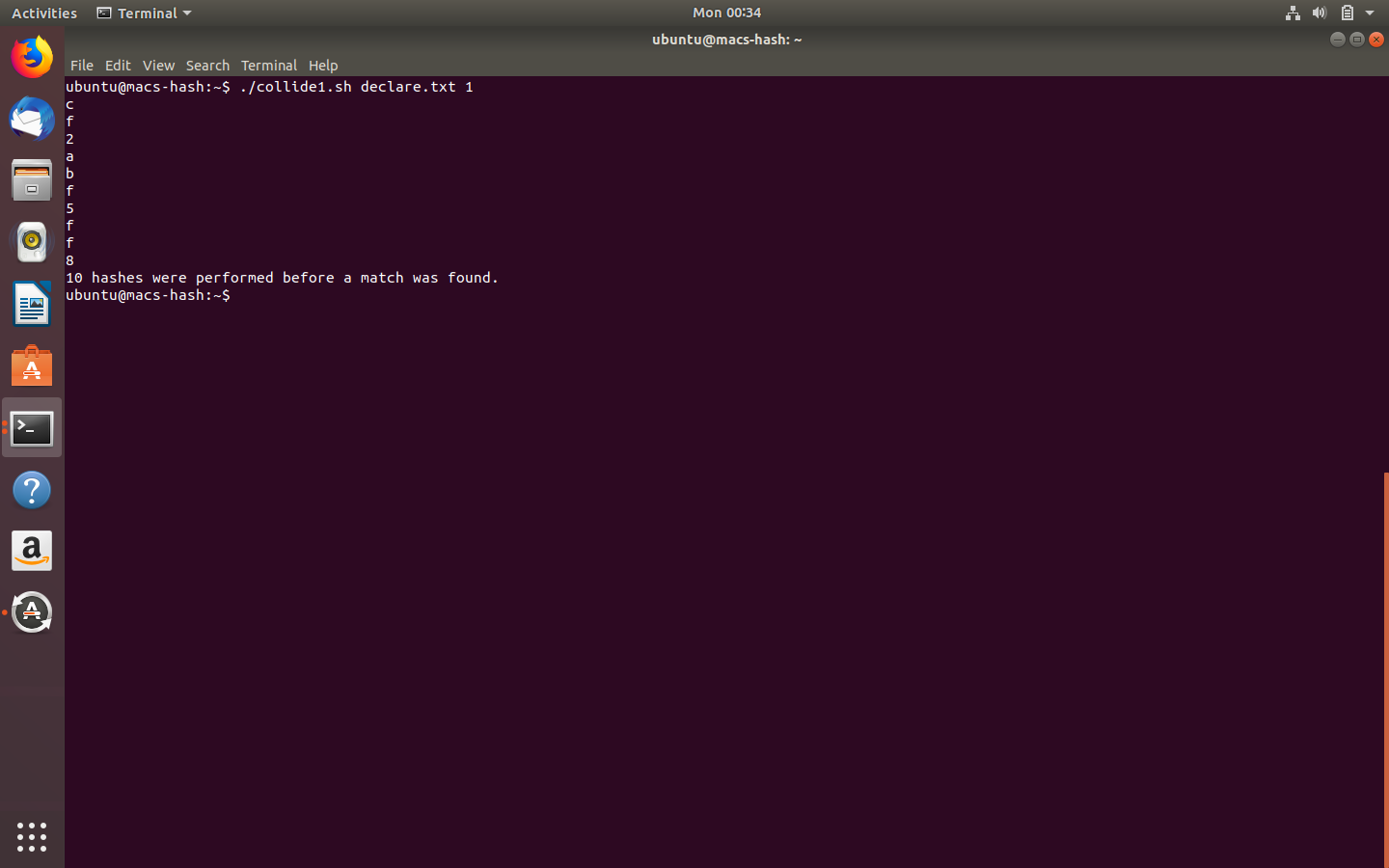
**Please include your commands, screenshots, and explanation for task 4 here:**

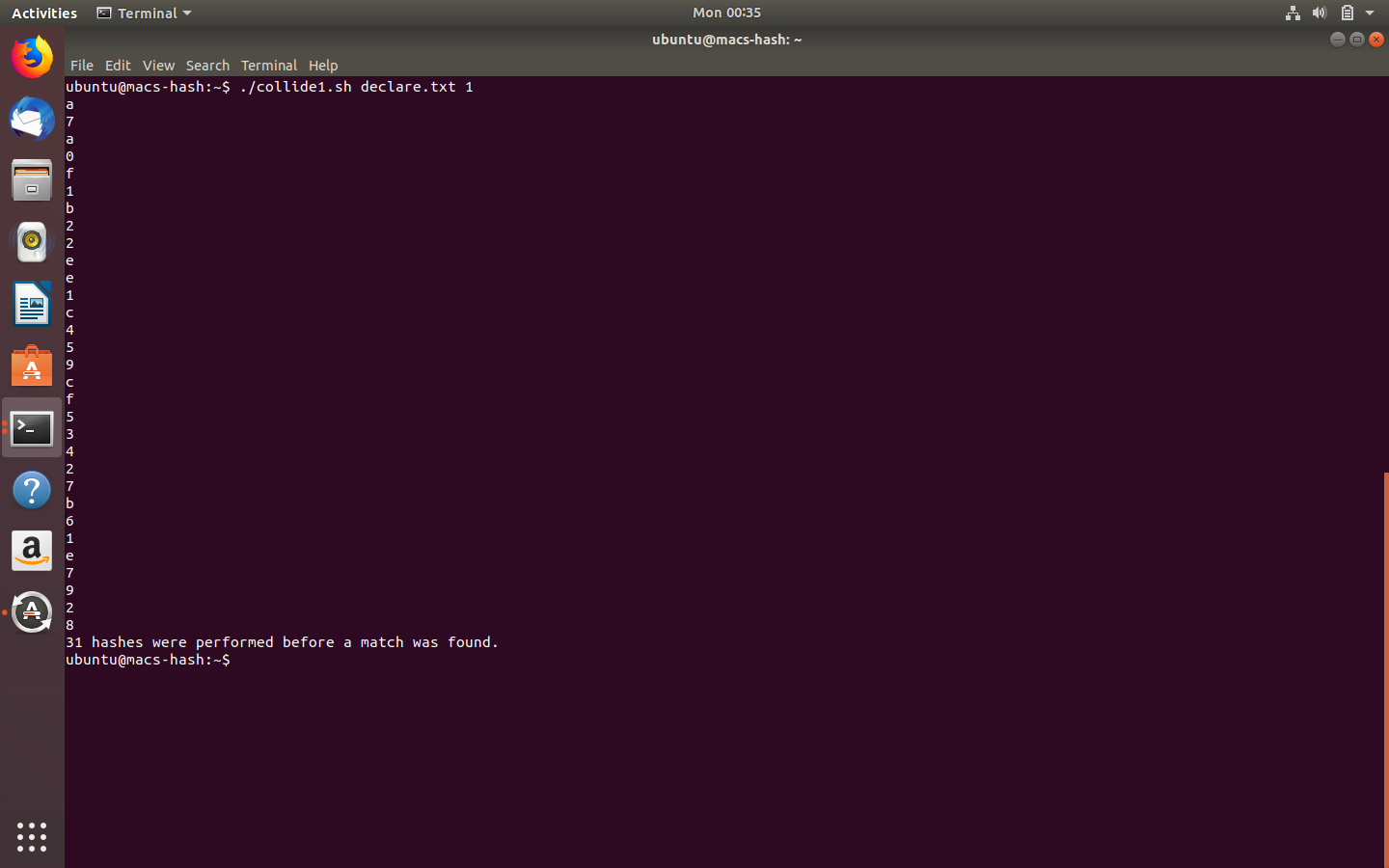
Screenshots: The number of attempts to match on the last hex digit of the digest for declare.txt.

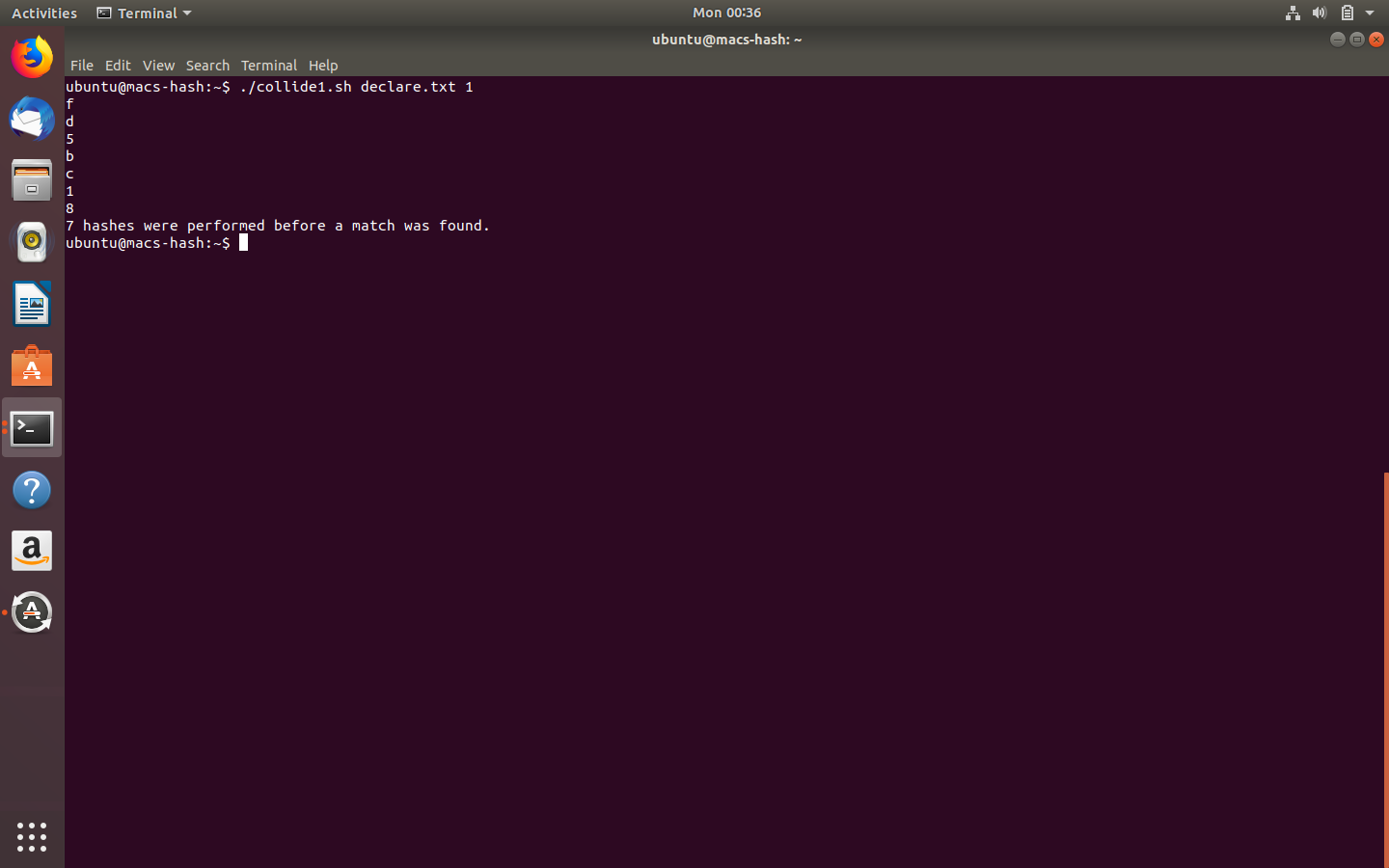
****

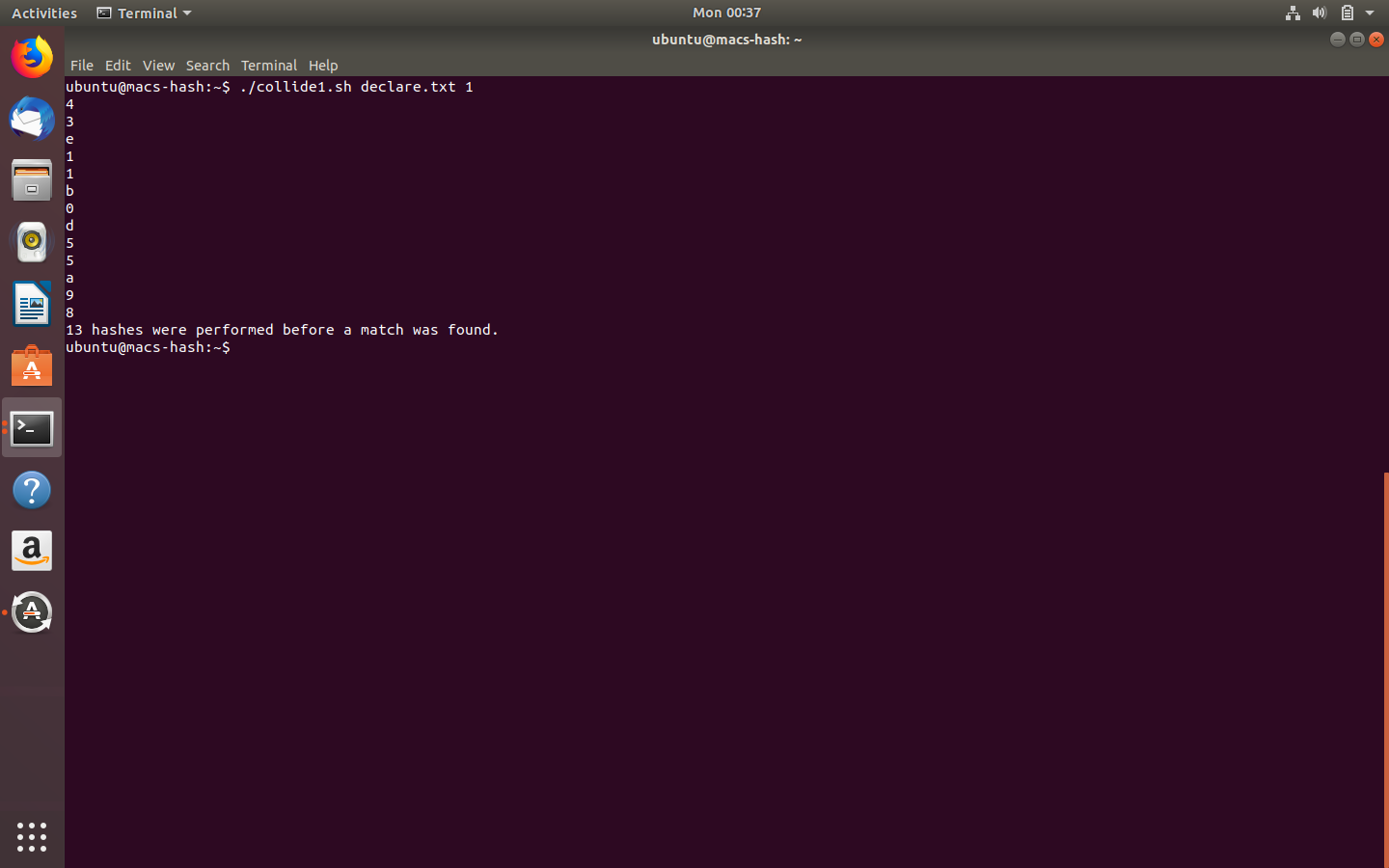
****

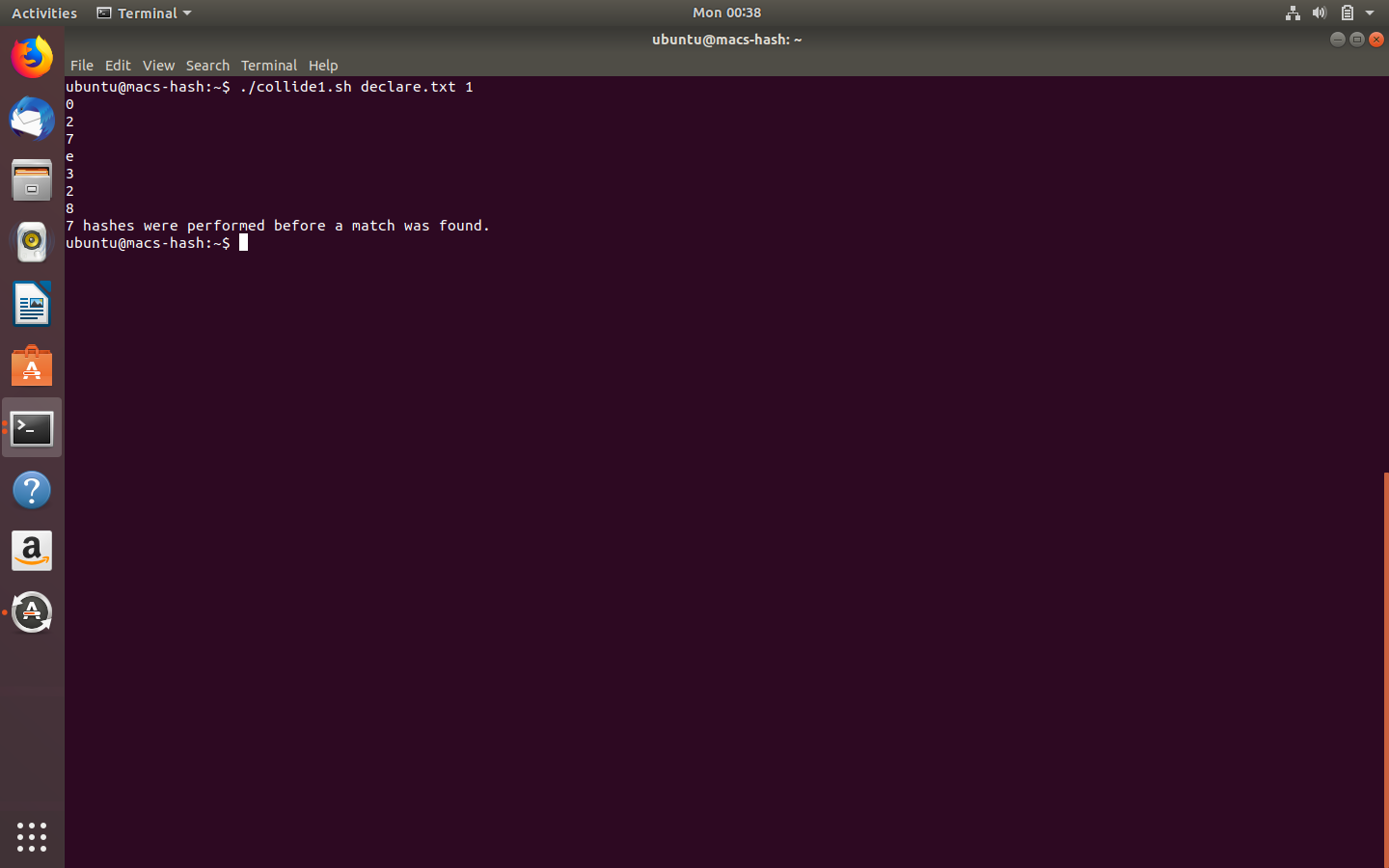
****

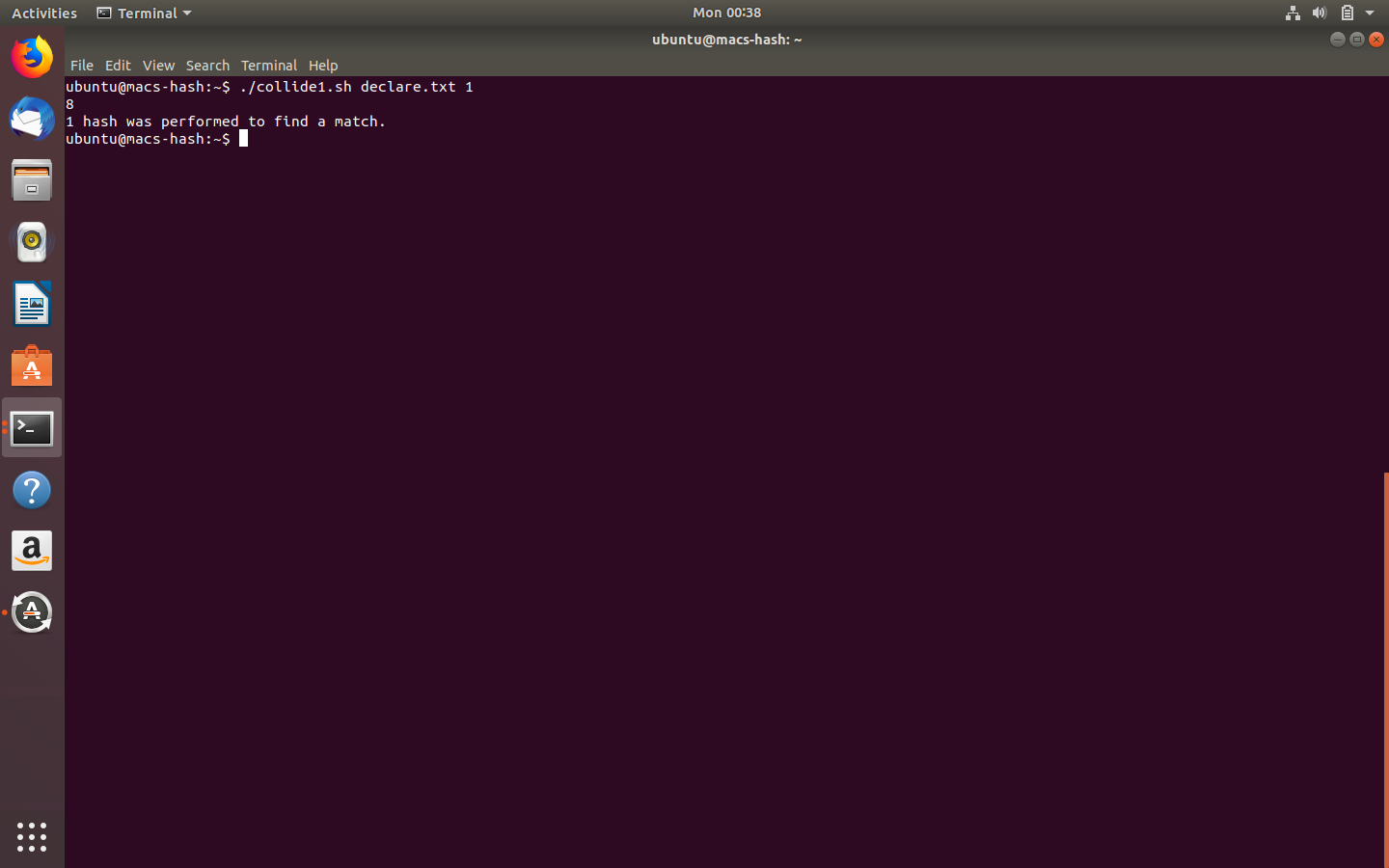
****

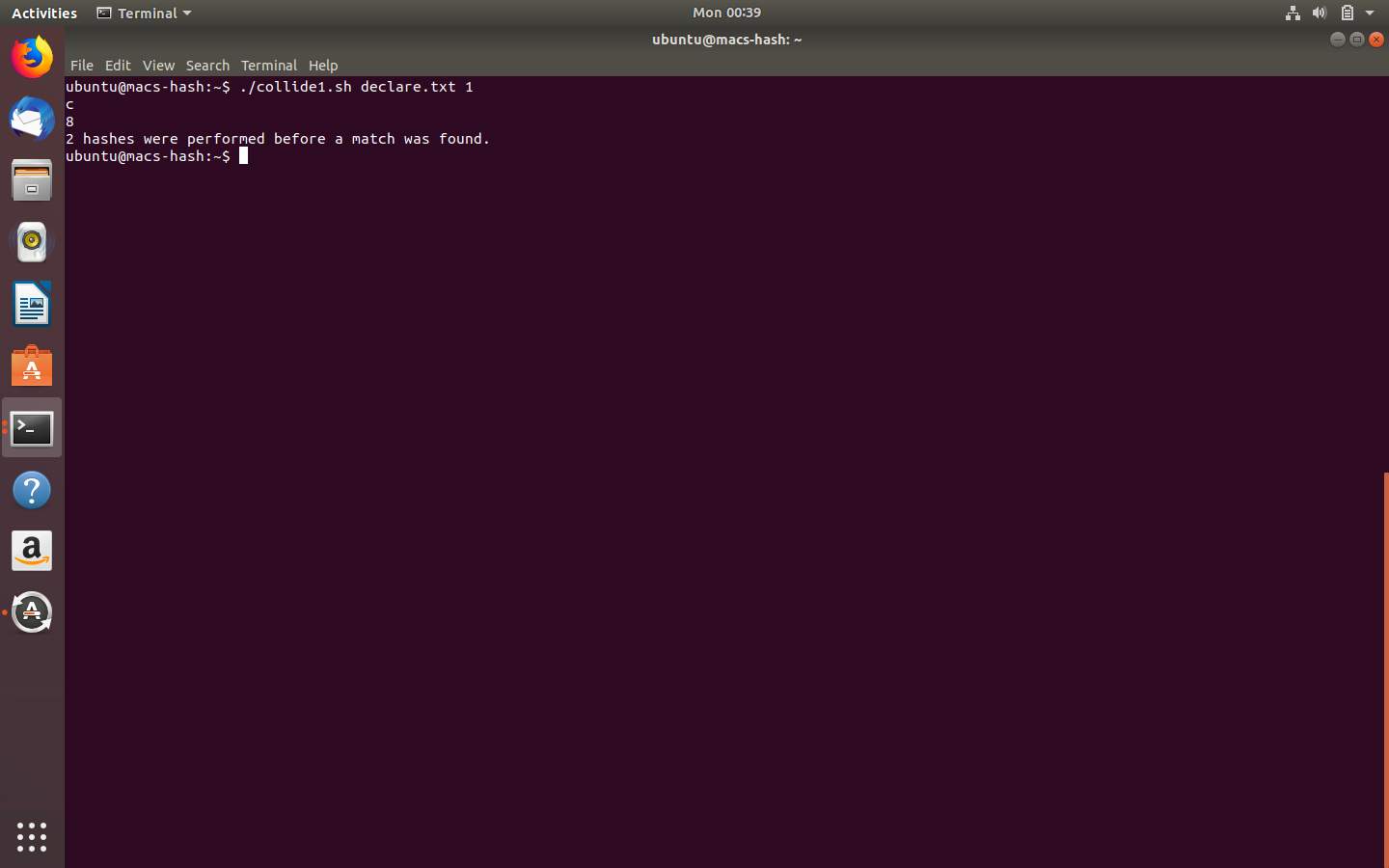
****

****

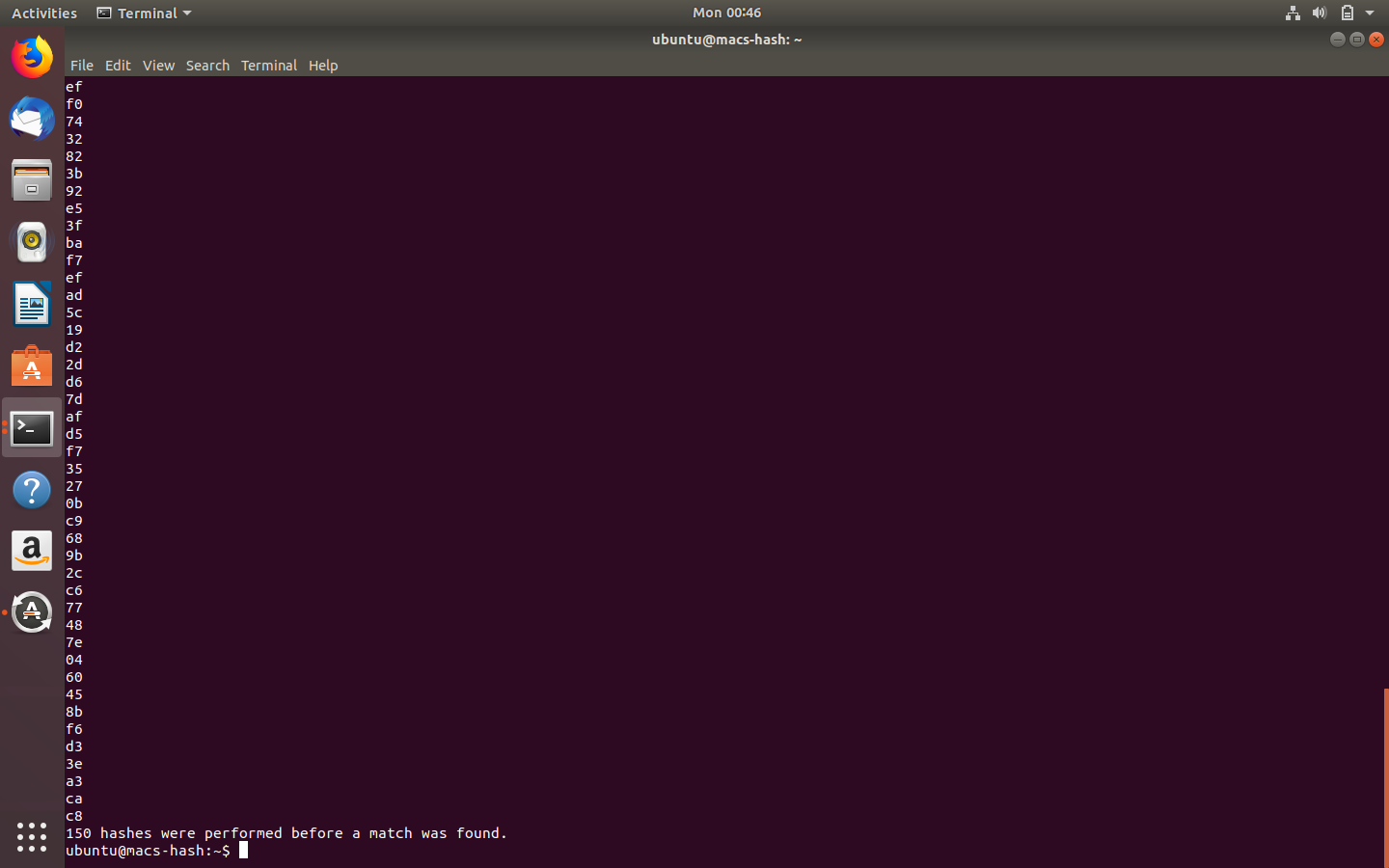
****

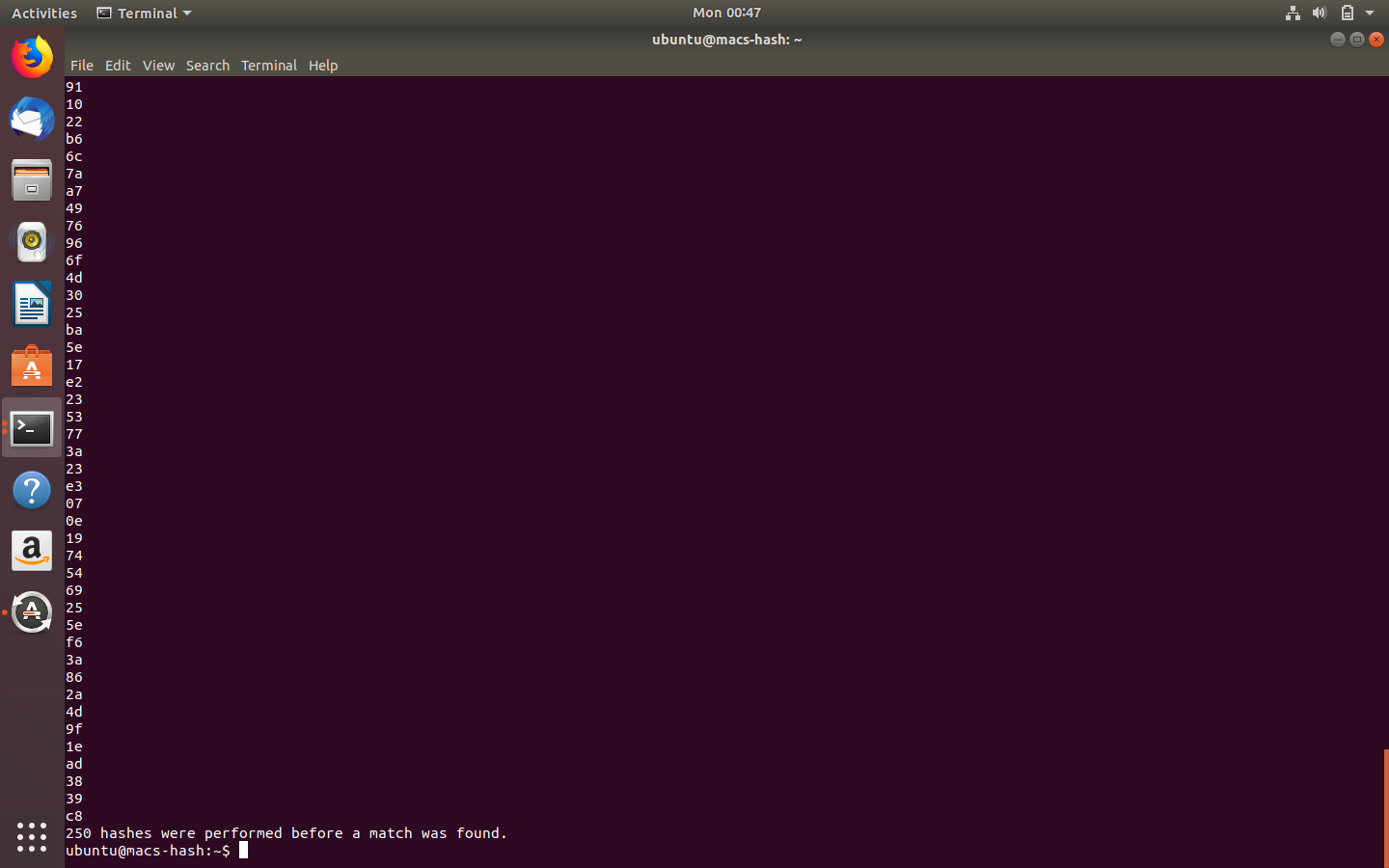
****

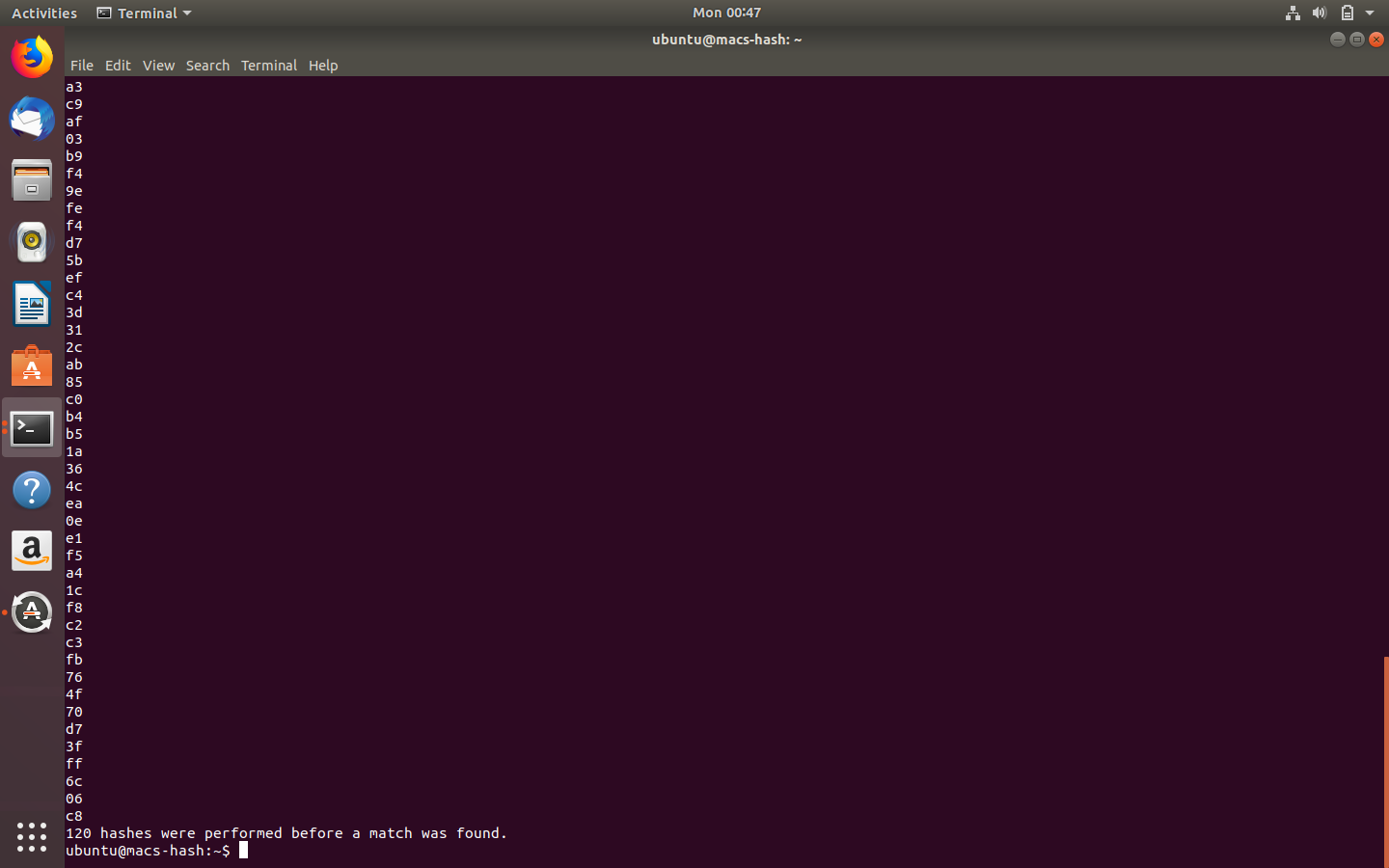
****

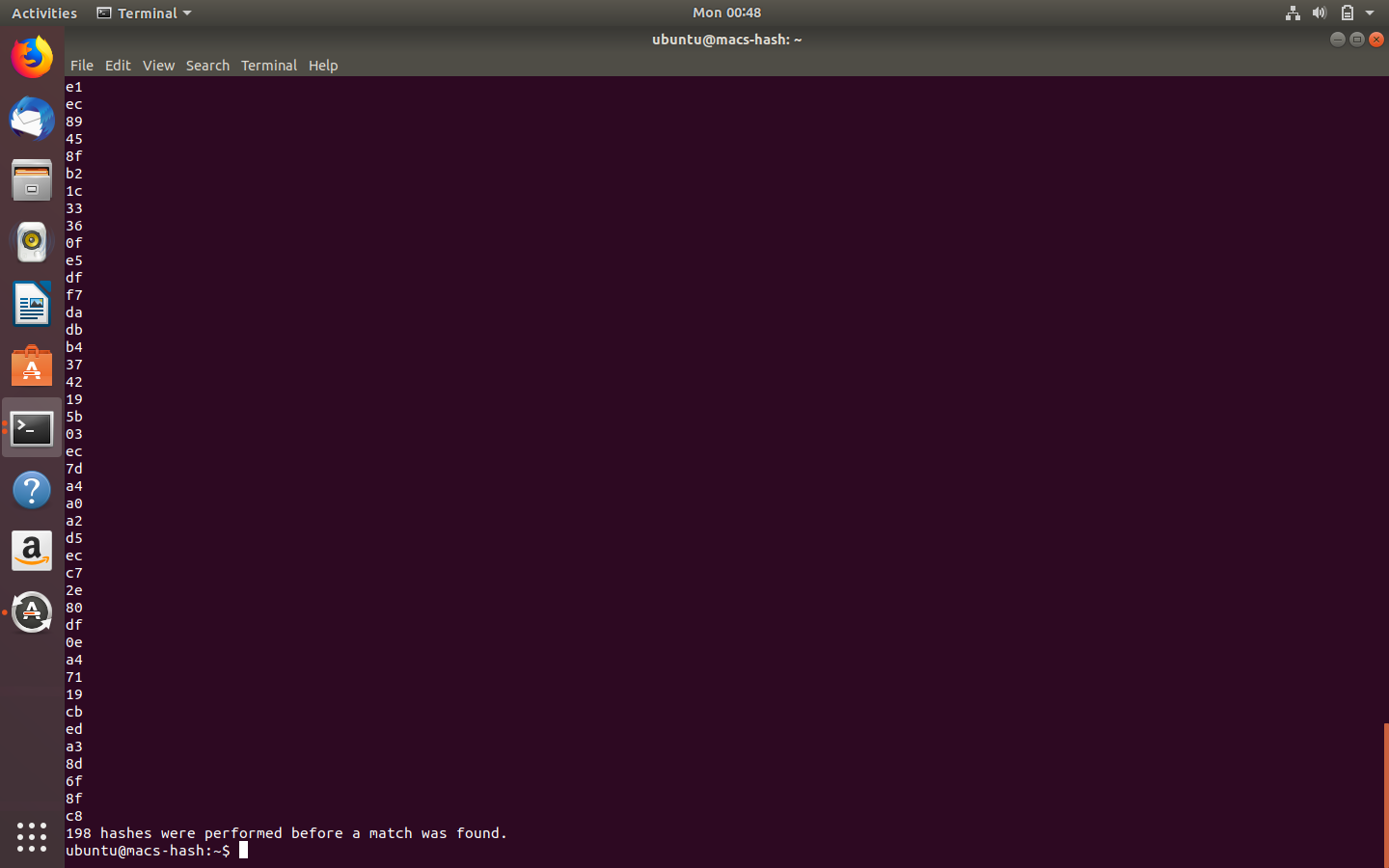
****

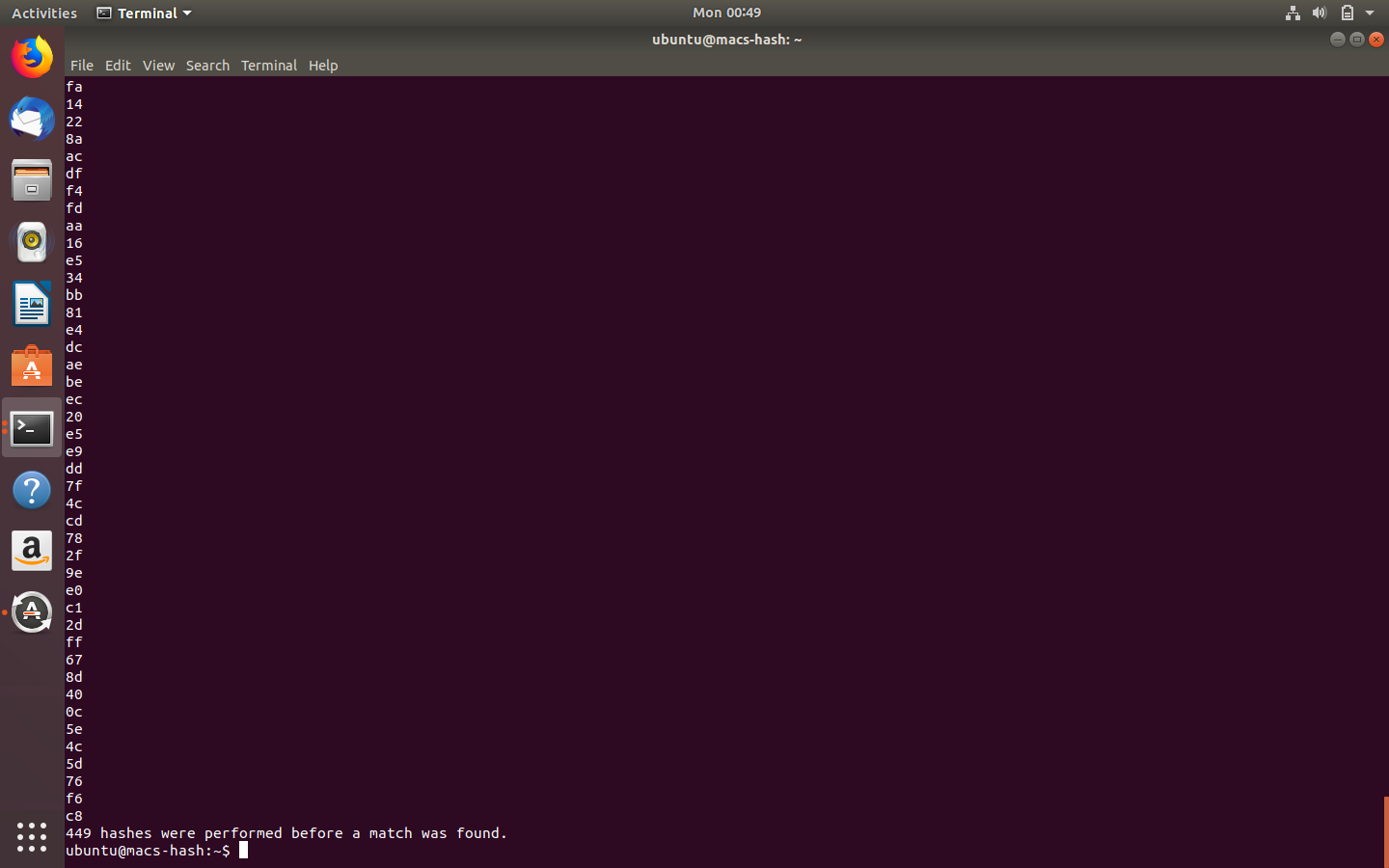
Screenshots: The number of attempts to match on the last two hex digit of the digest for declare.txt.

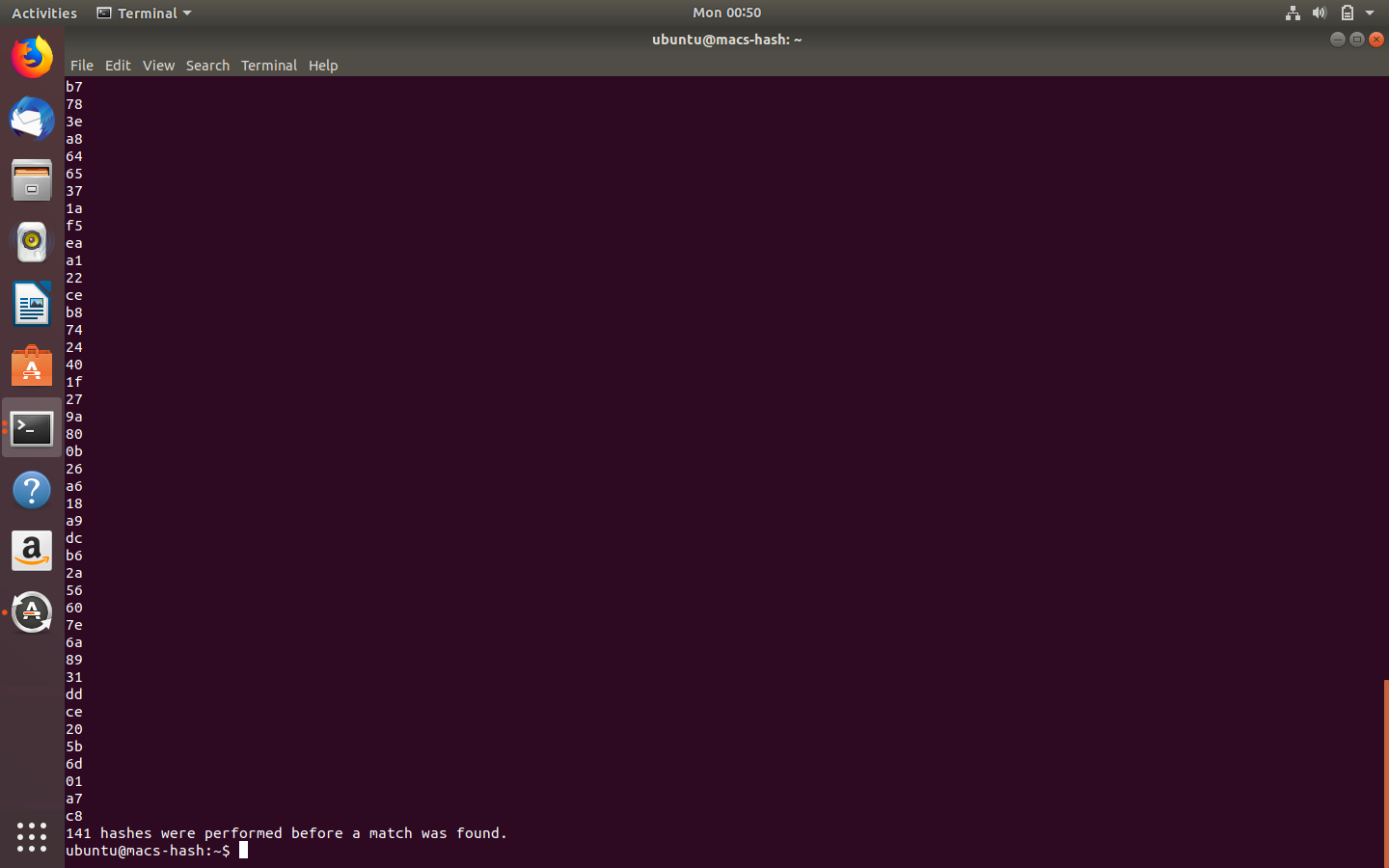
****

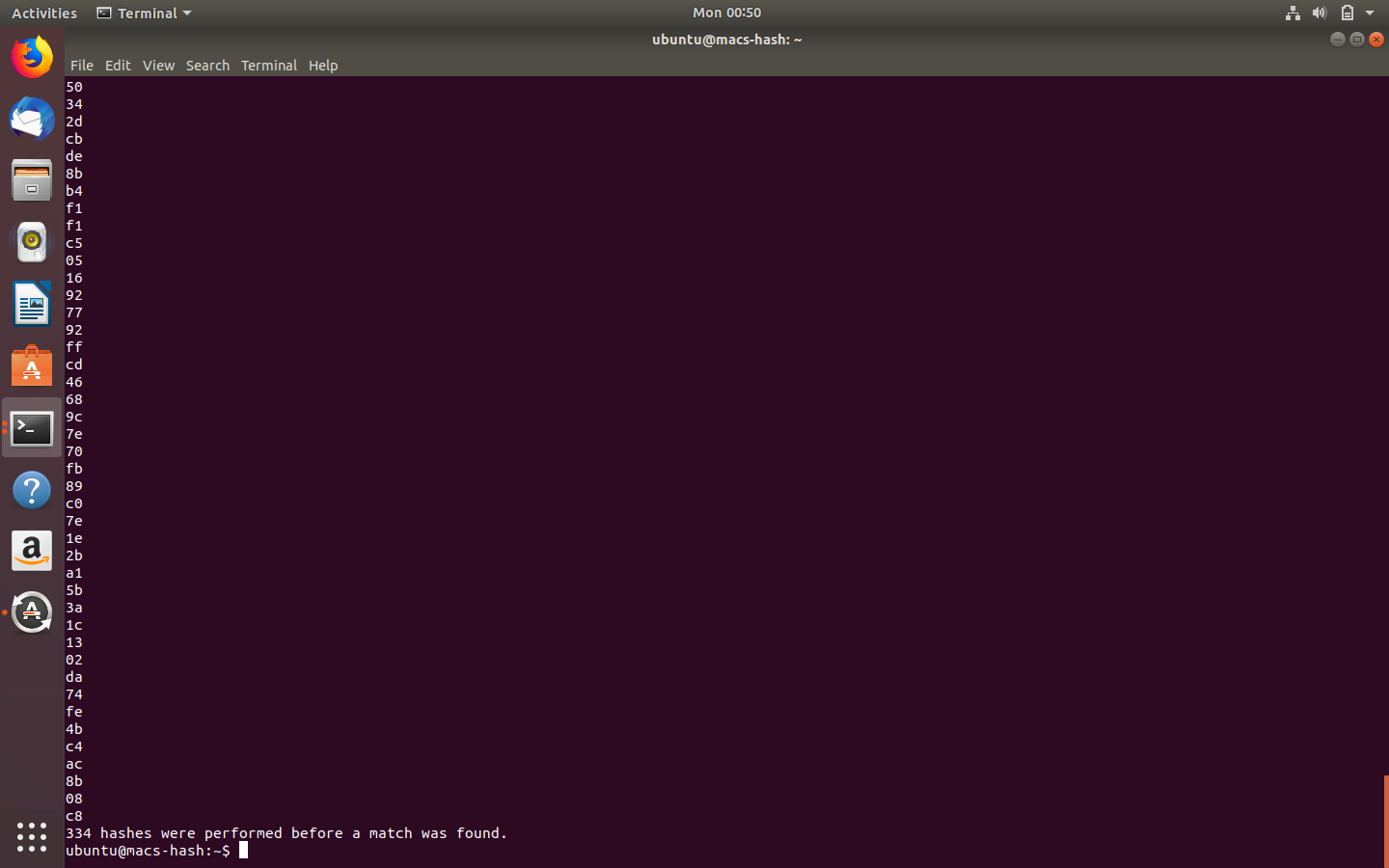
****

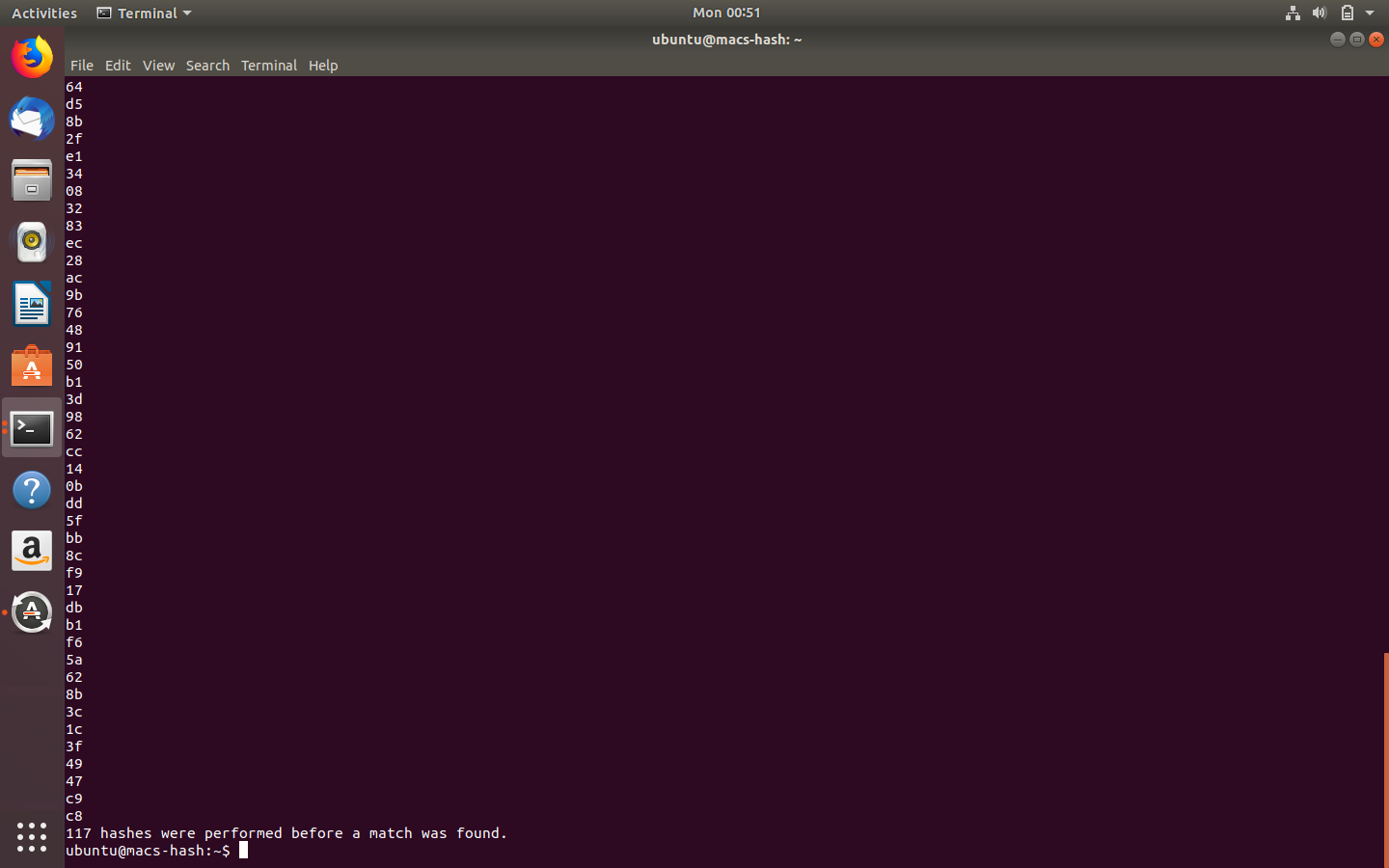
****

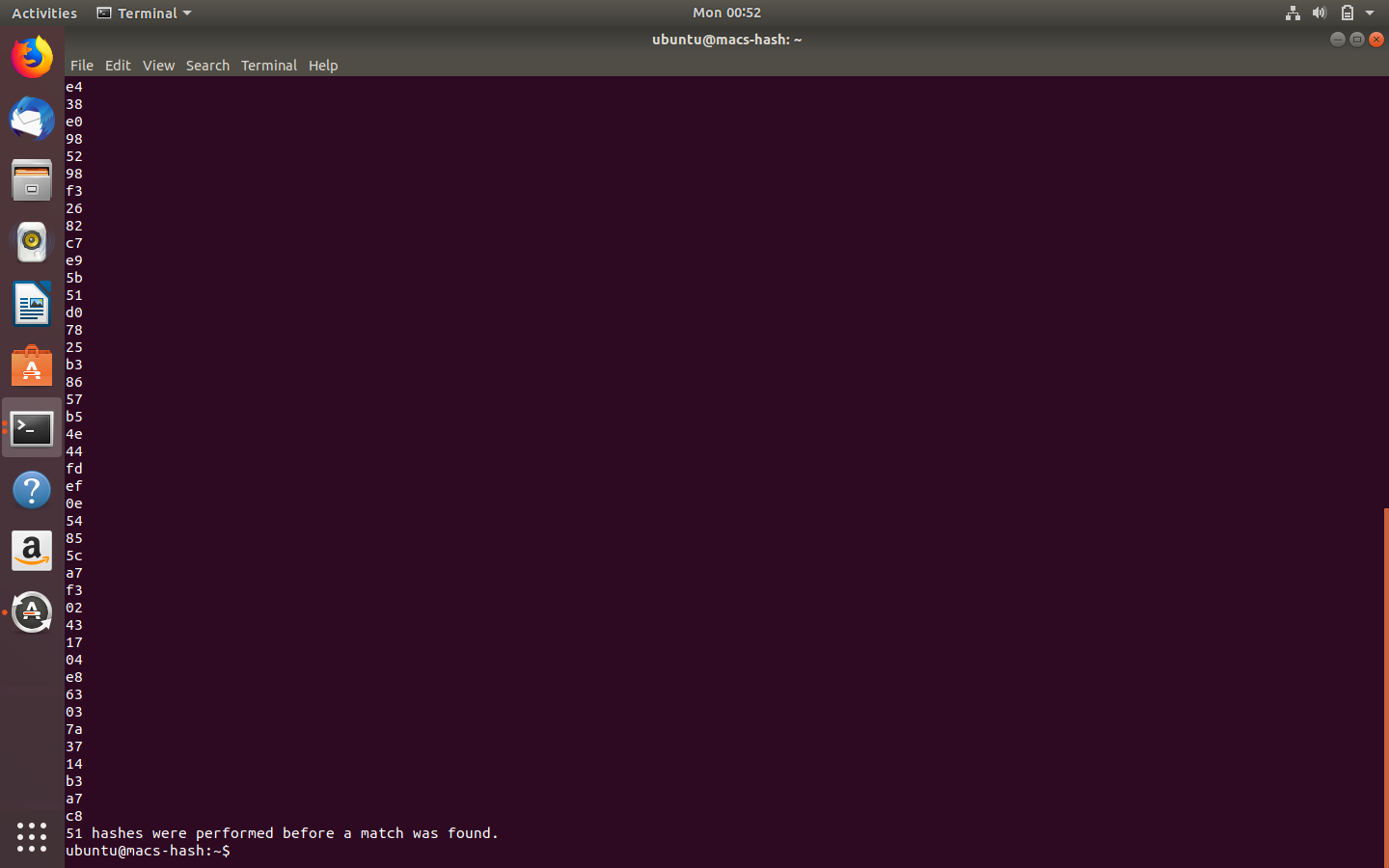
****

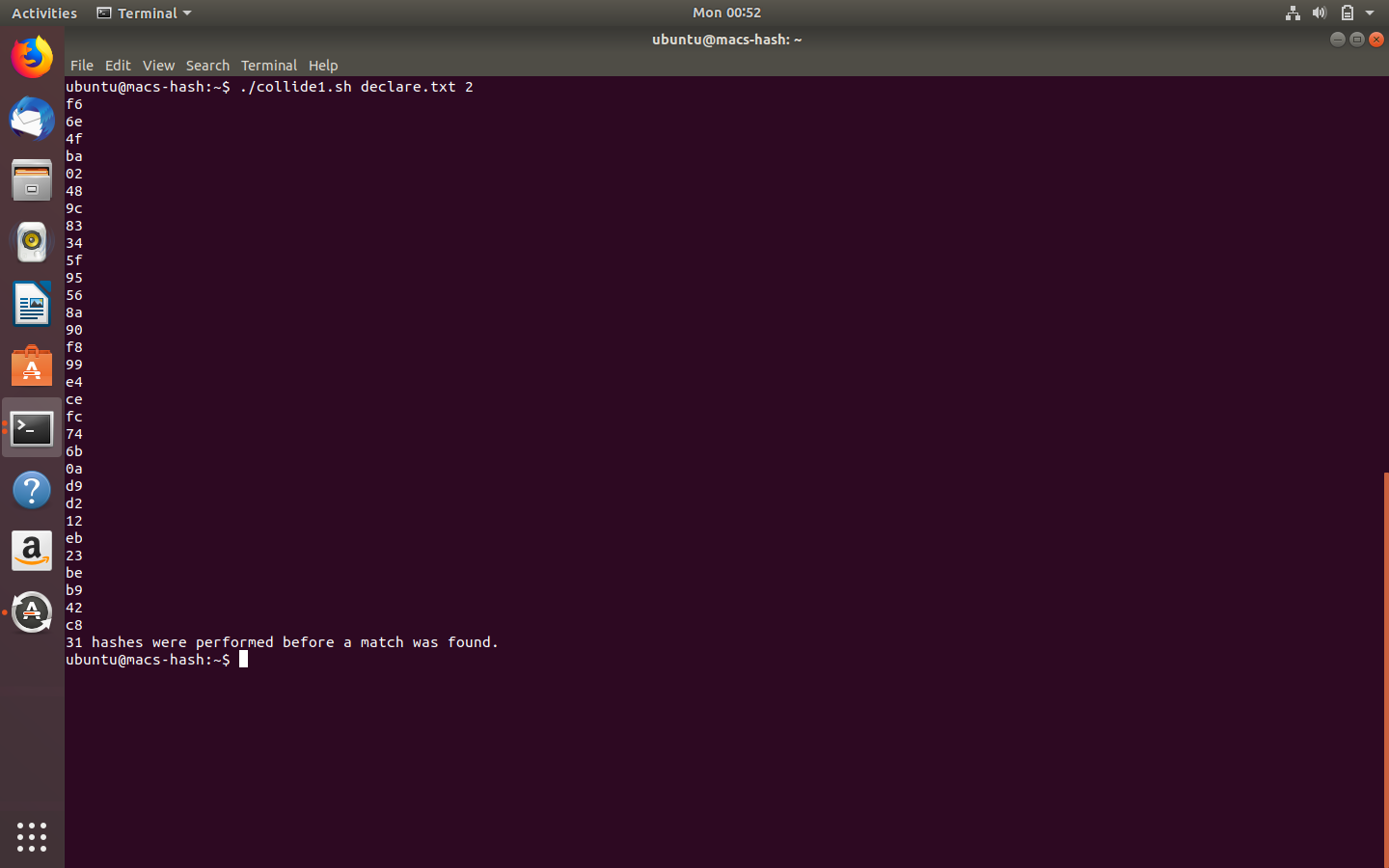
****

****

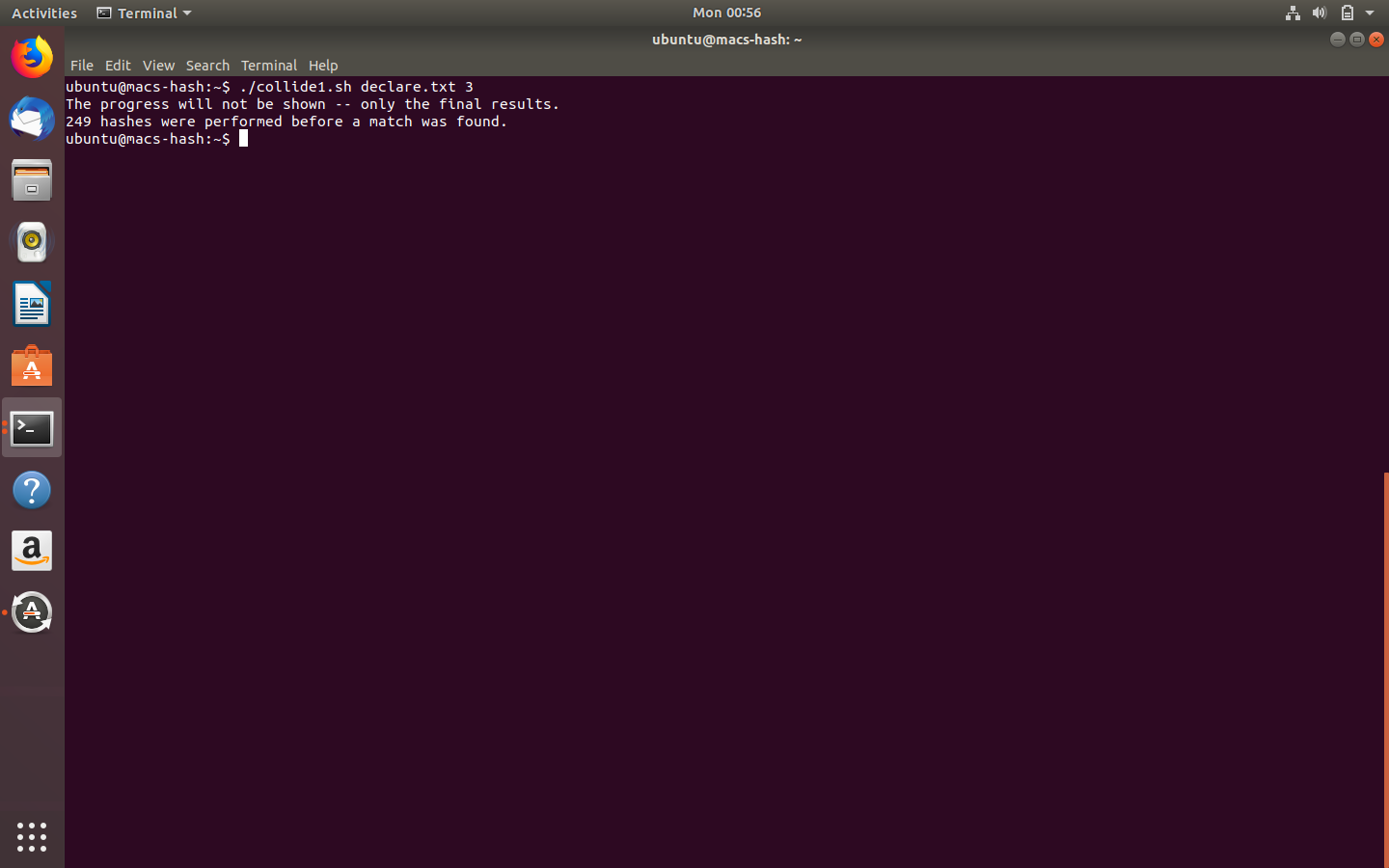
****

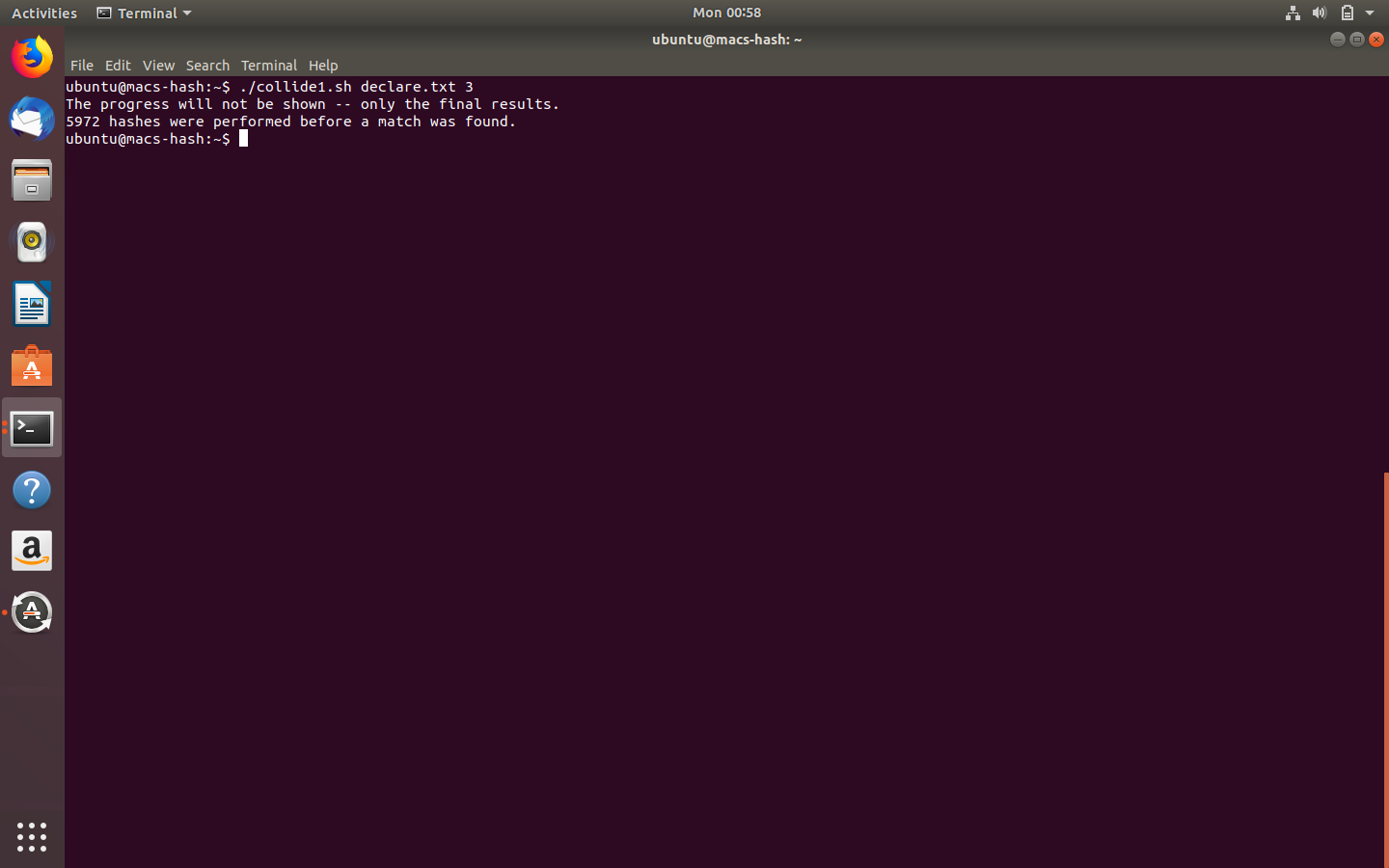
****

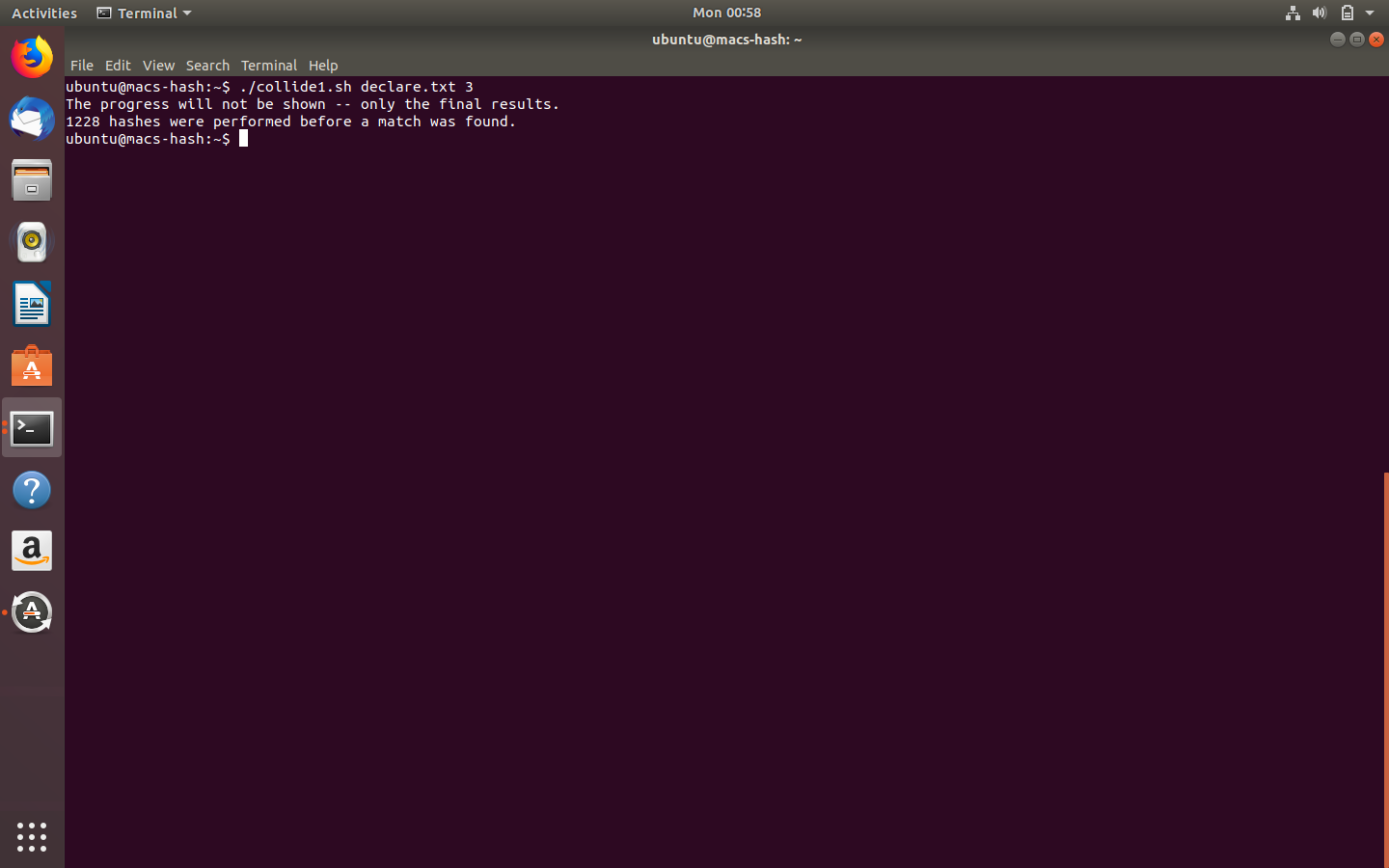
****

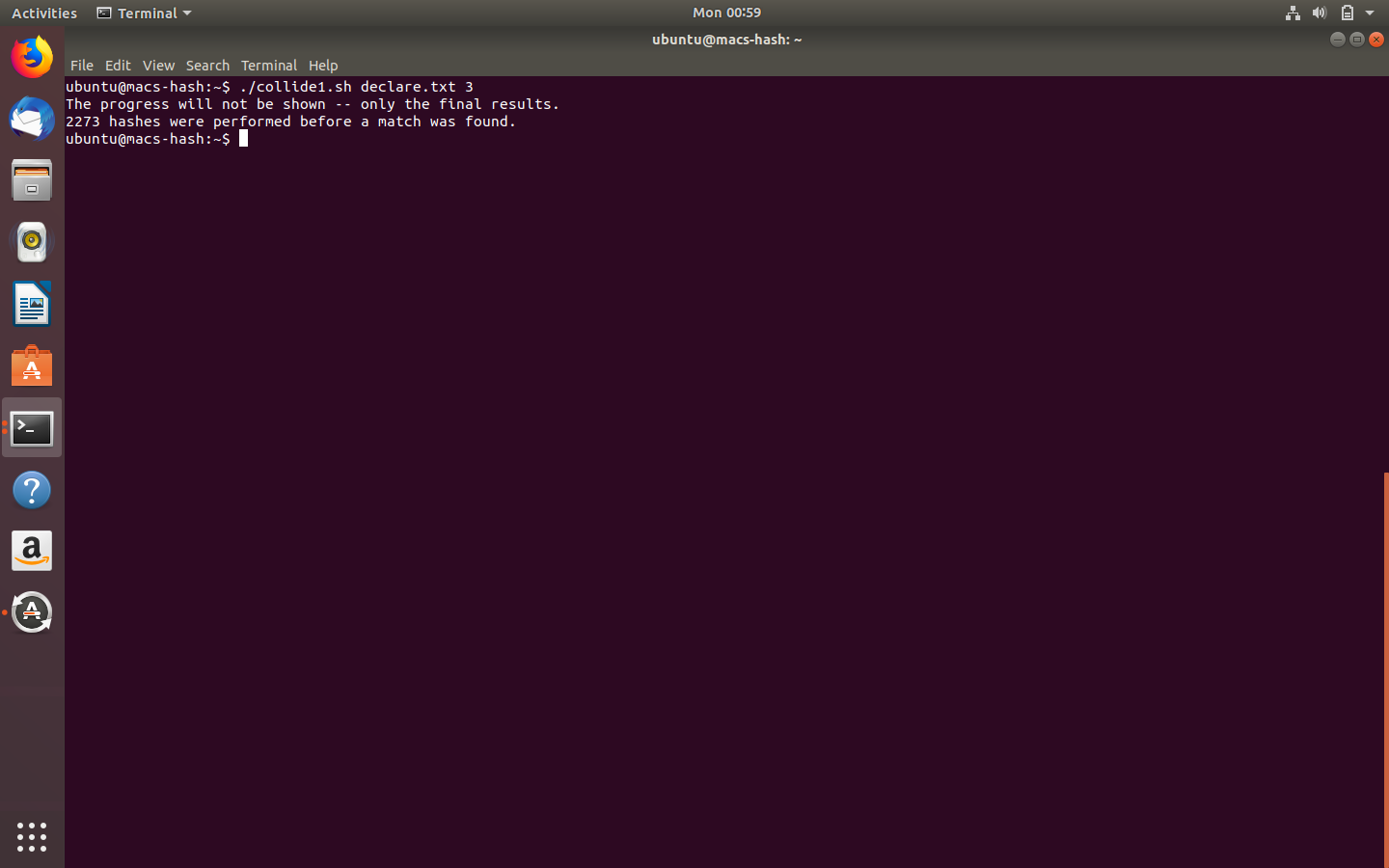
****

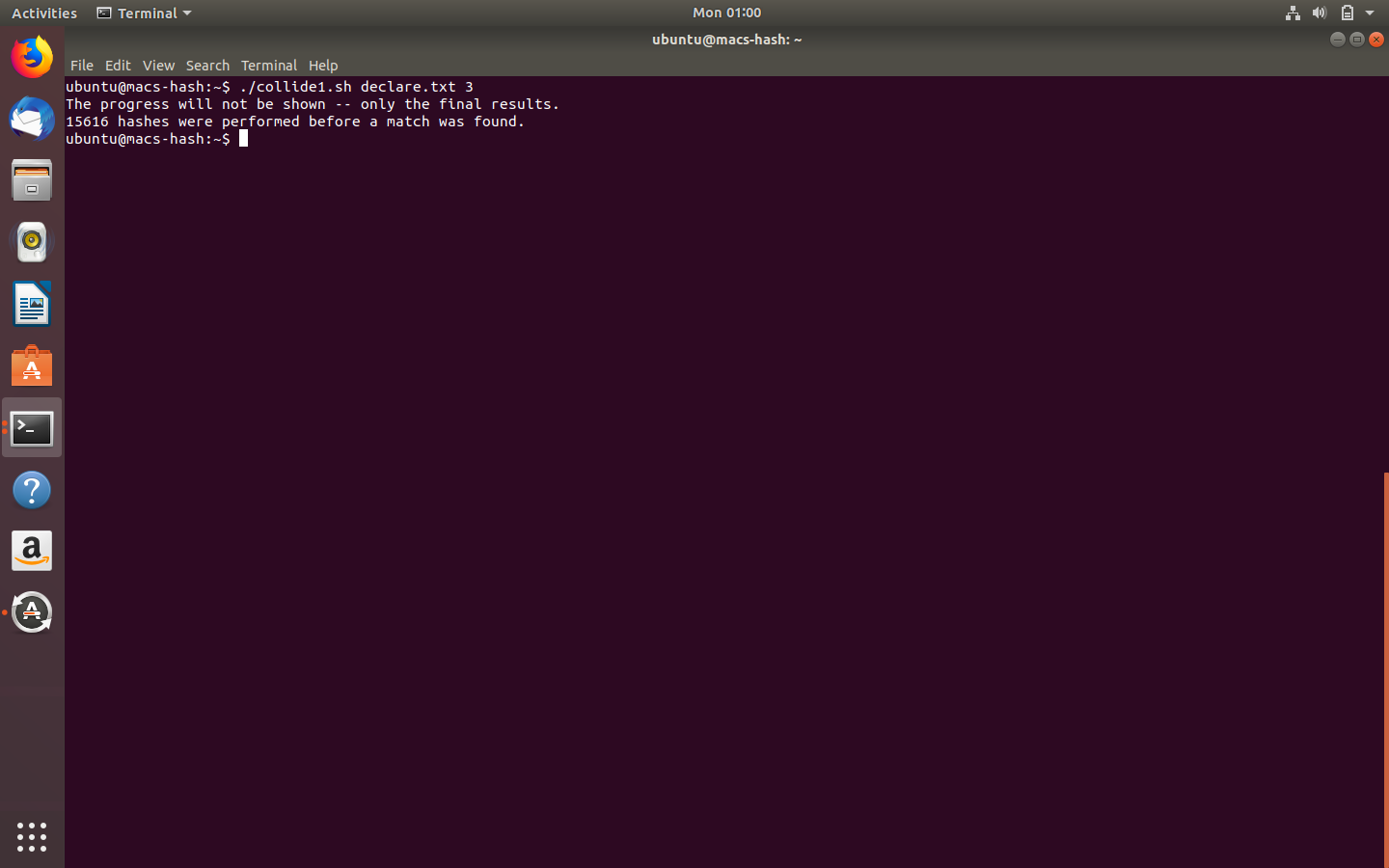
Screenshots: The number of attempts to match on the last three hex digit of the digest for declare.txt.

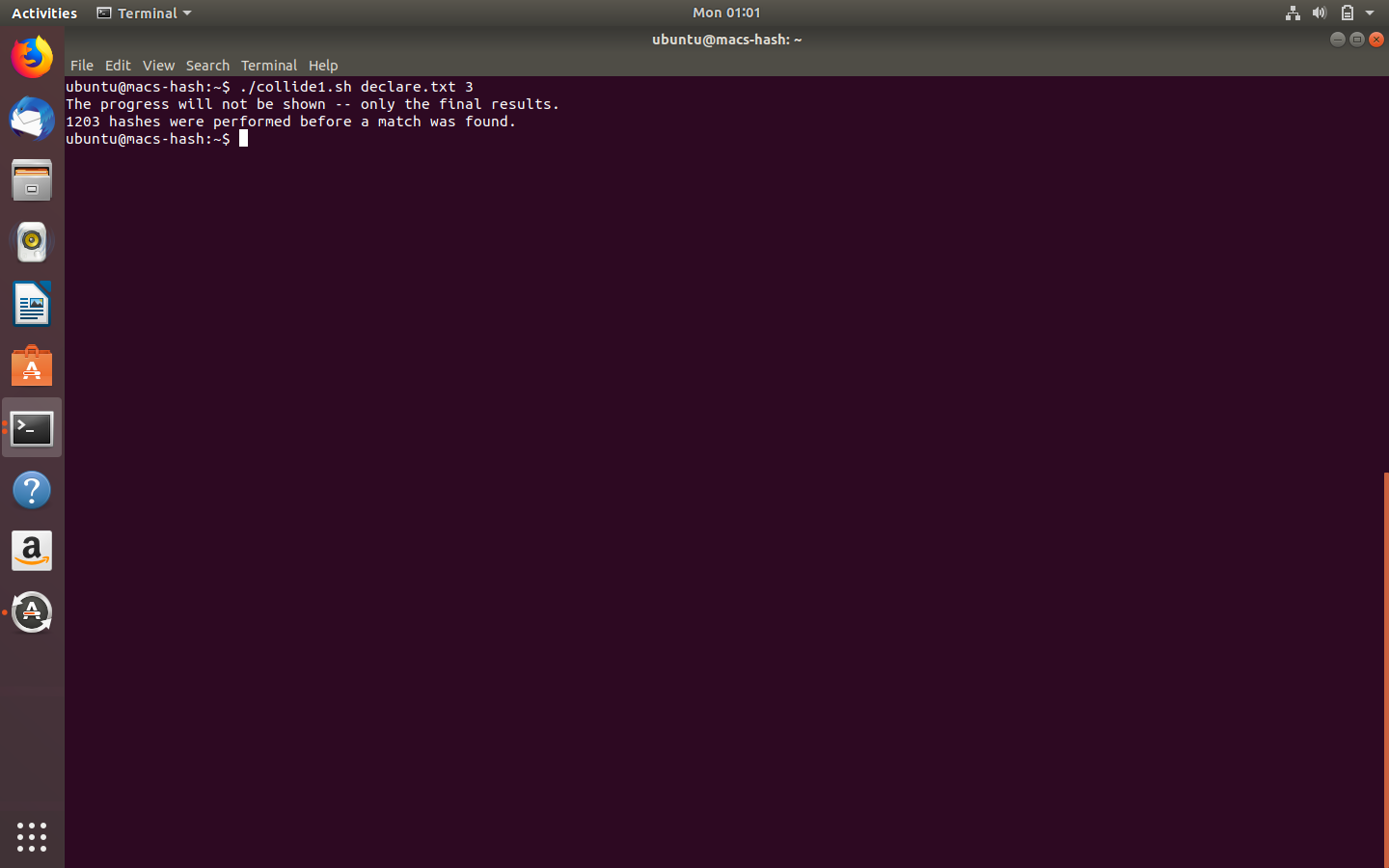
****

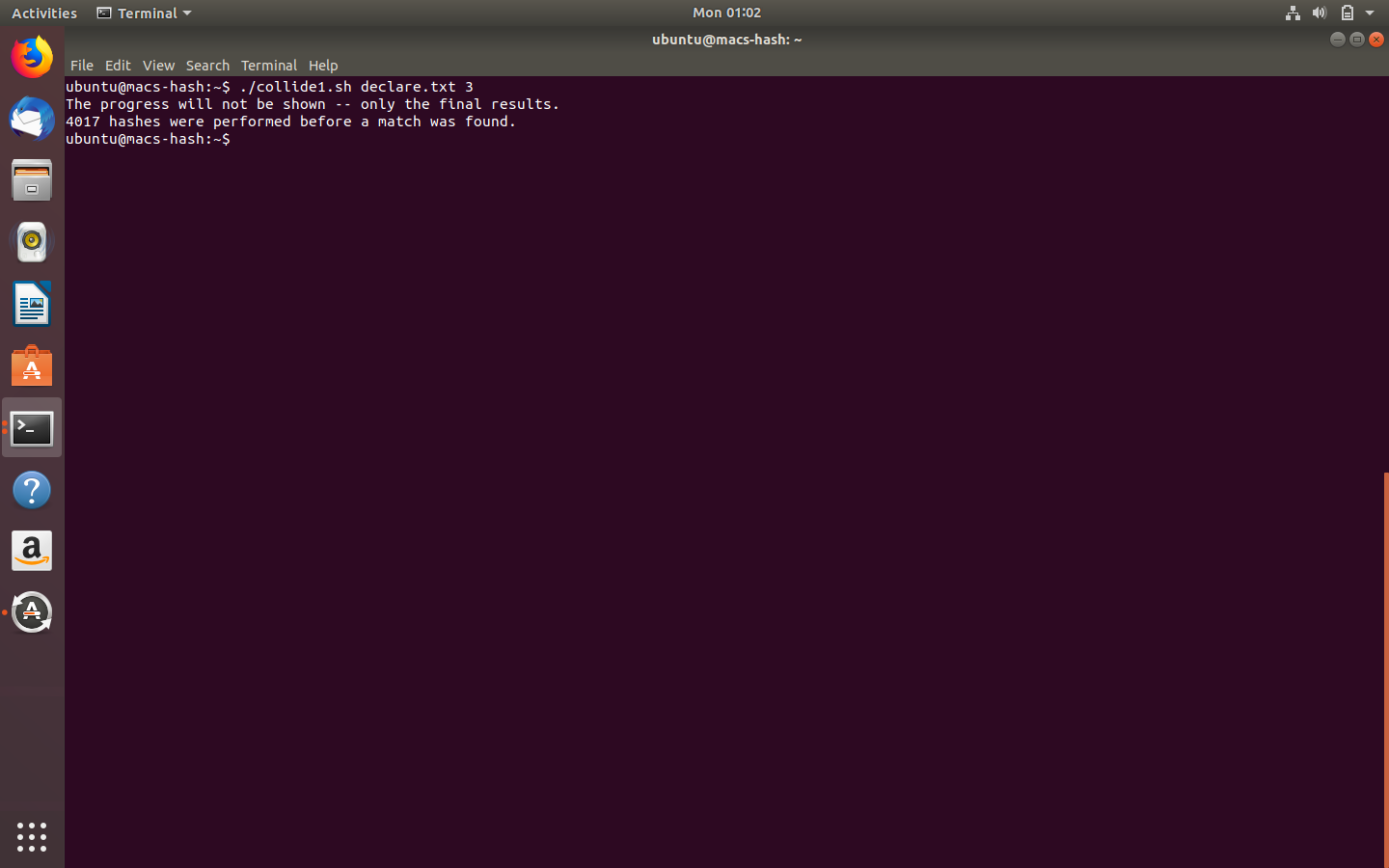
****

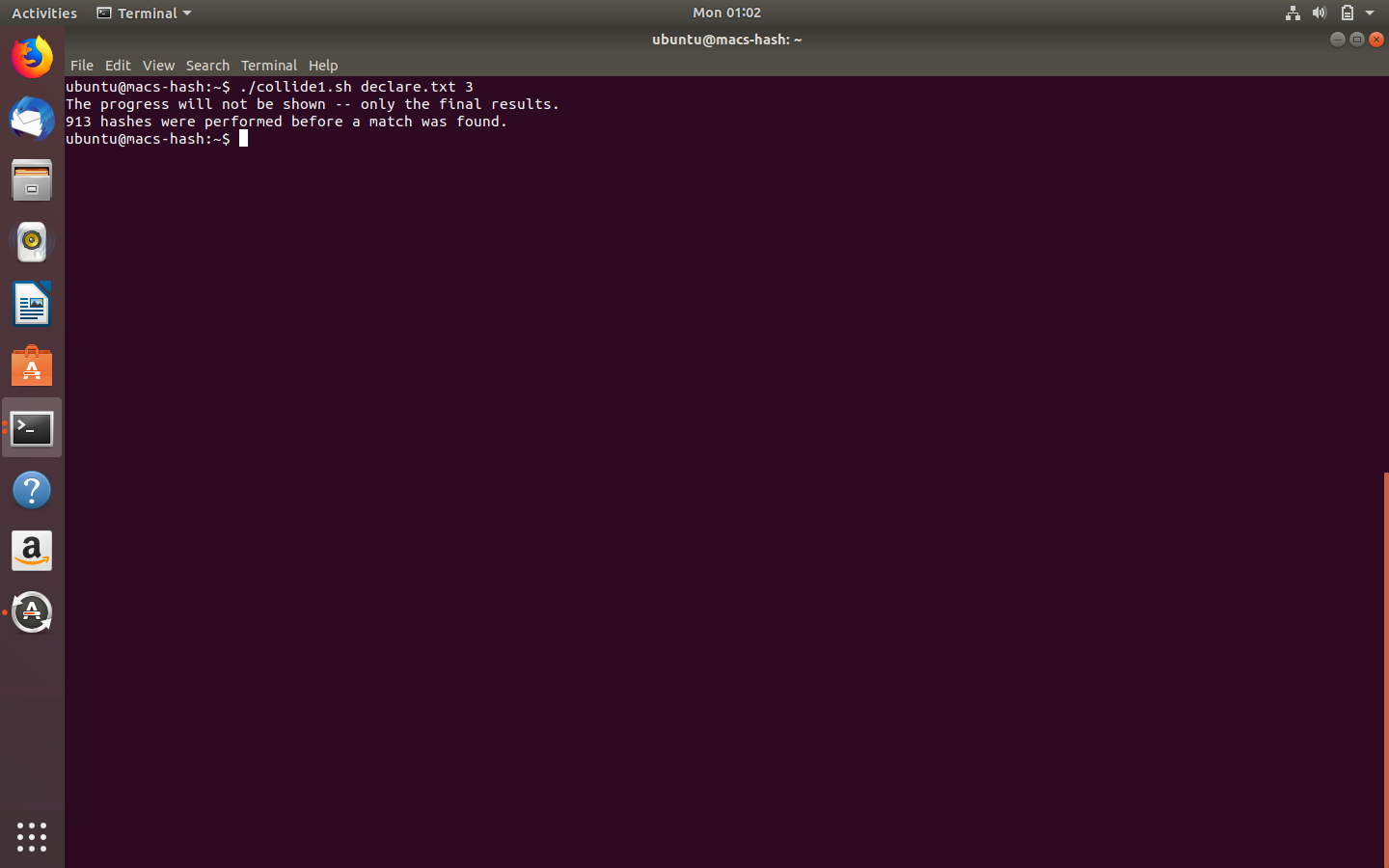
****

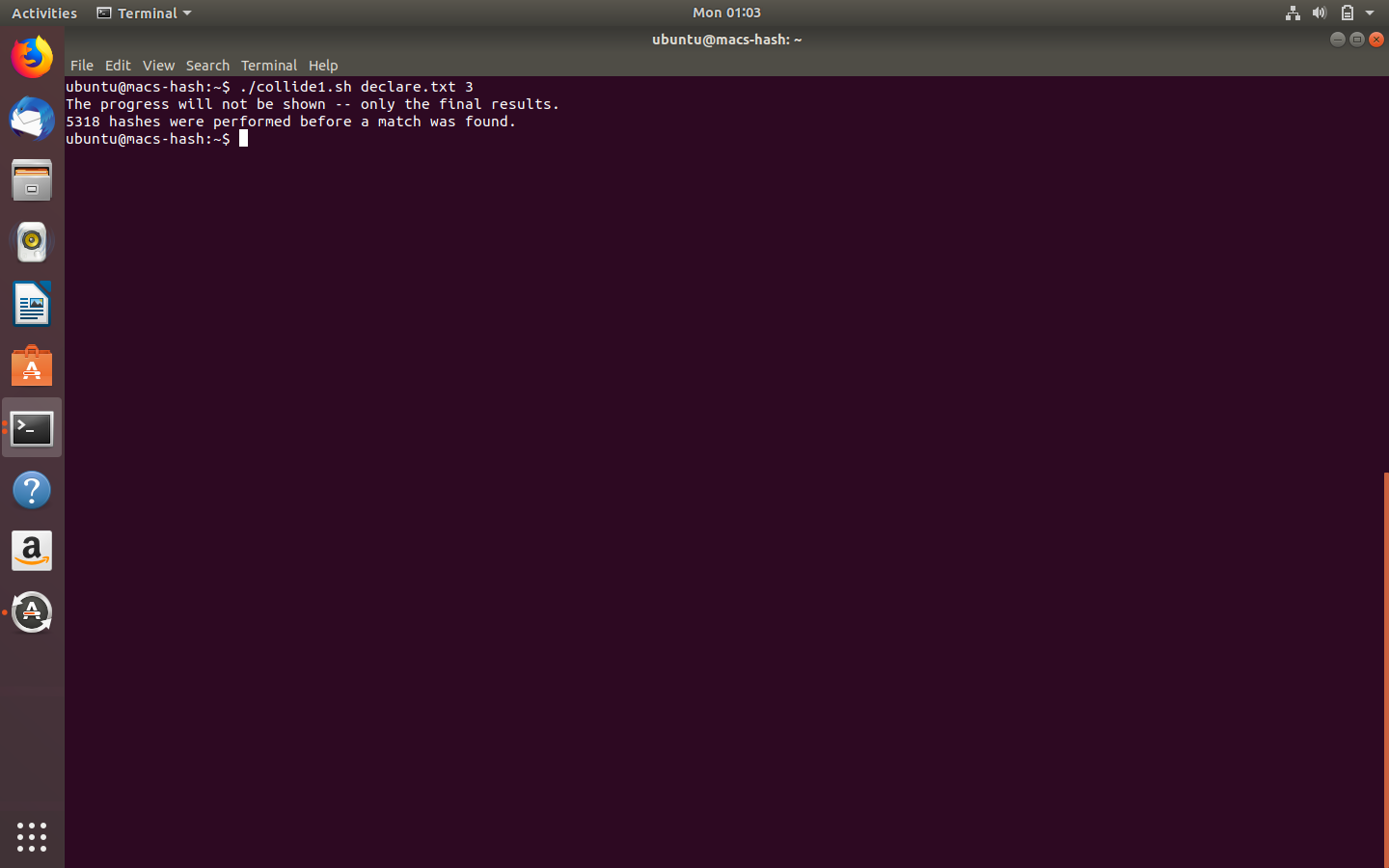
****

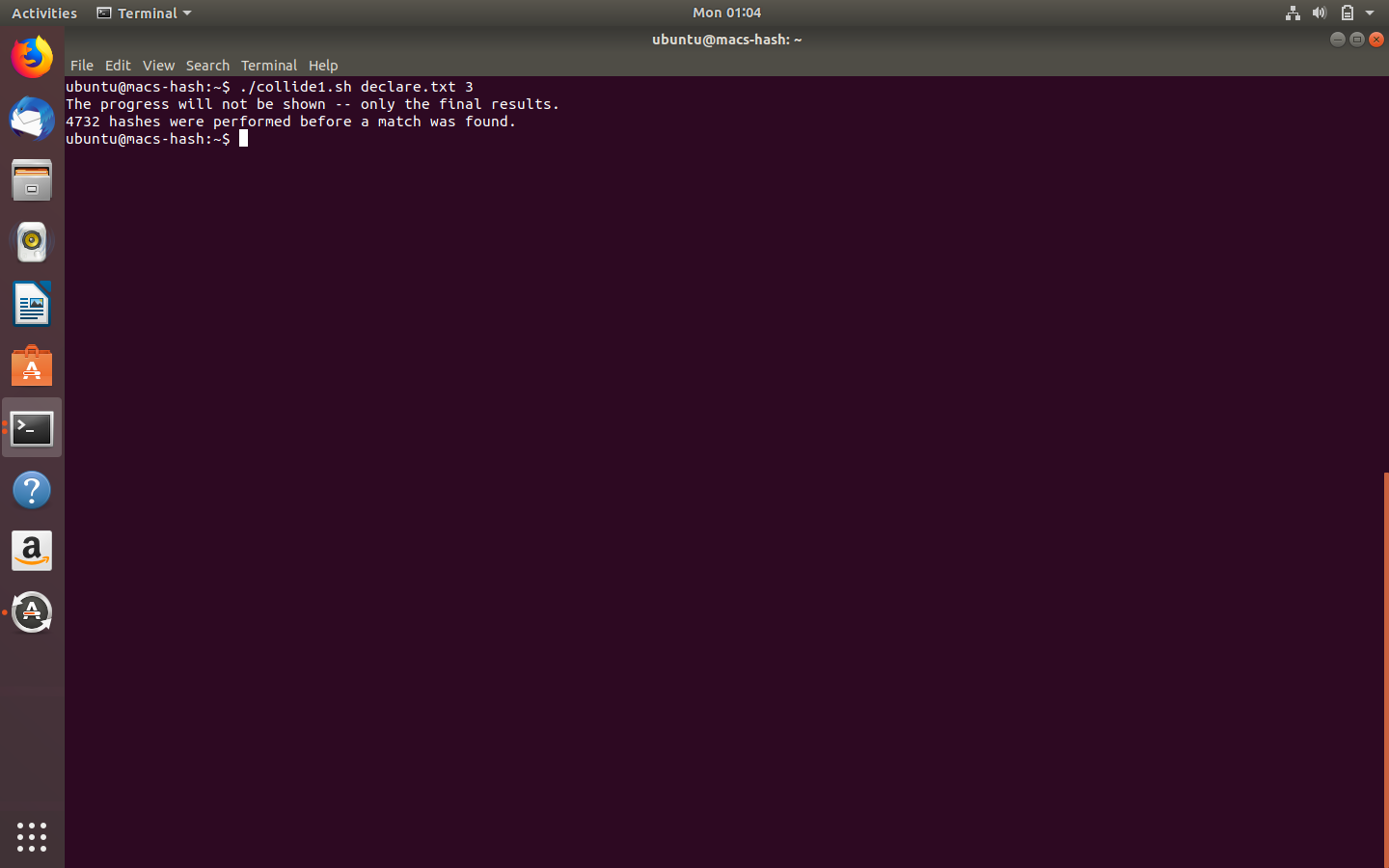
****

****

****

****

****

****

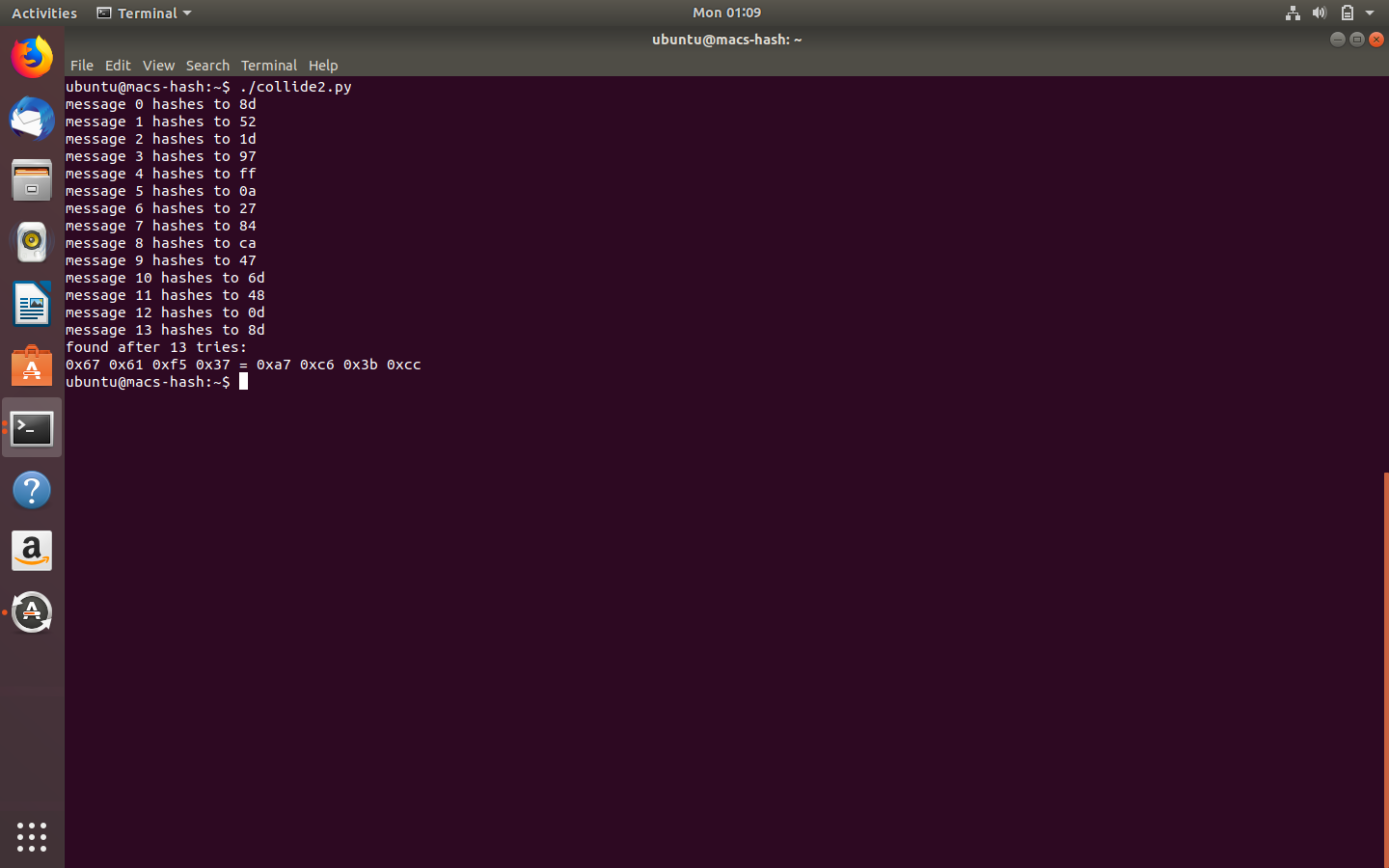
# **Exploring Collision Resistance**

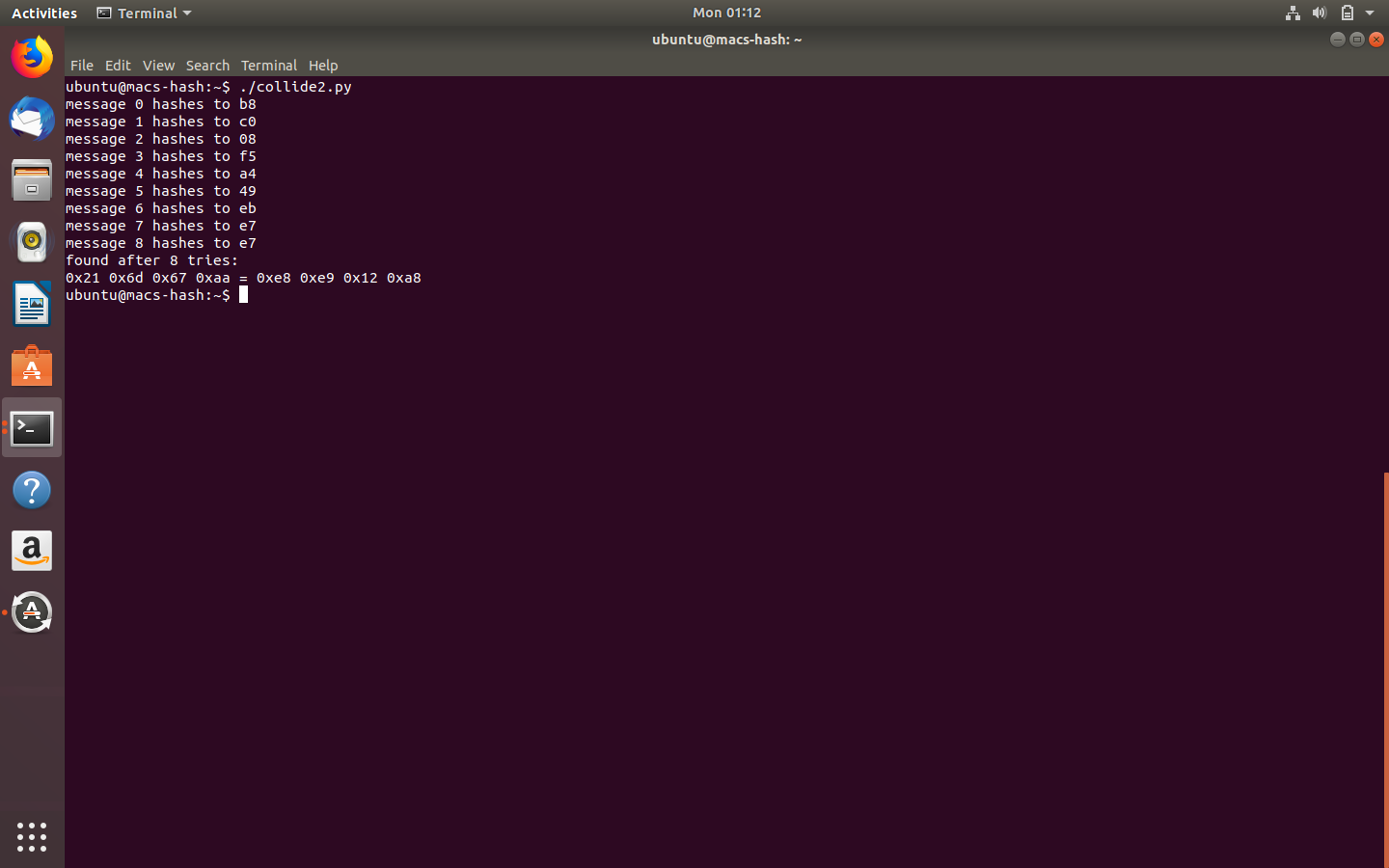
1. The number of attempts to find two random messages whose digests match on the last byte (i.e., the last **two** hex digits).

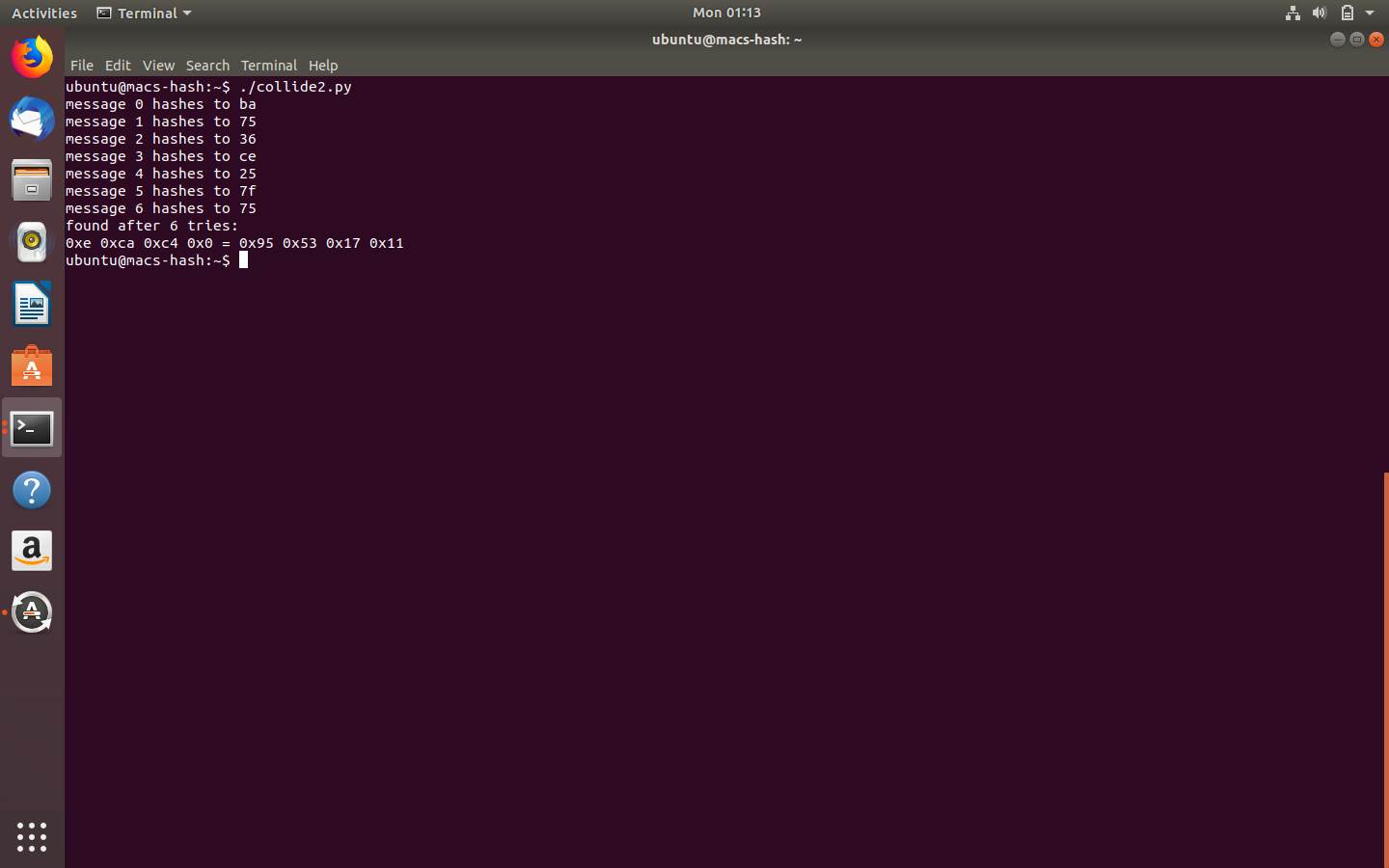
|  |  |
| --- | --- |
| Attempt | # Tries |
| 1 | 13 |
| 2 | 8 |
| 3 | 6 |
| 4 | 30 |
| 5 | 24 |
| 6 | 10 |
| 7 | 18 |
| 8 | 21 |
| 9 | 21 |
| 10 | 35 |

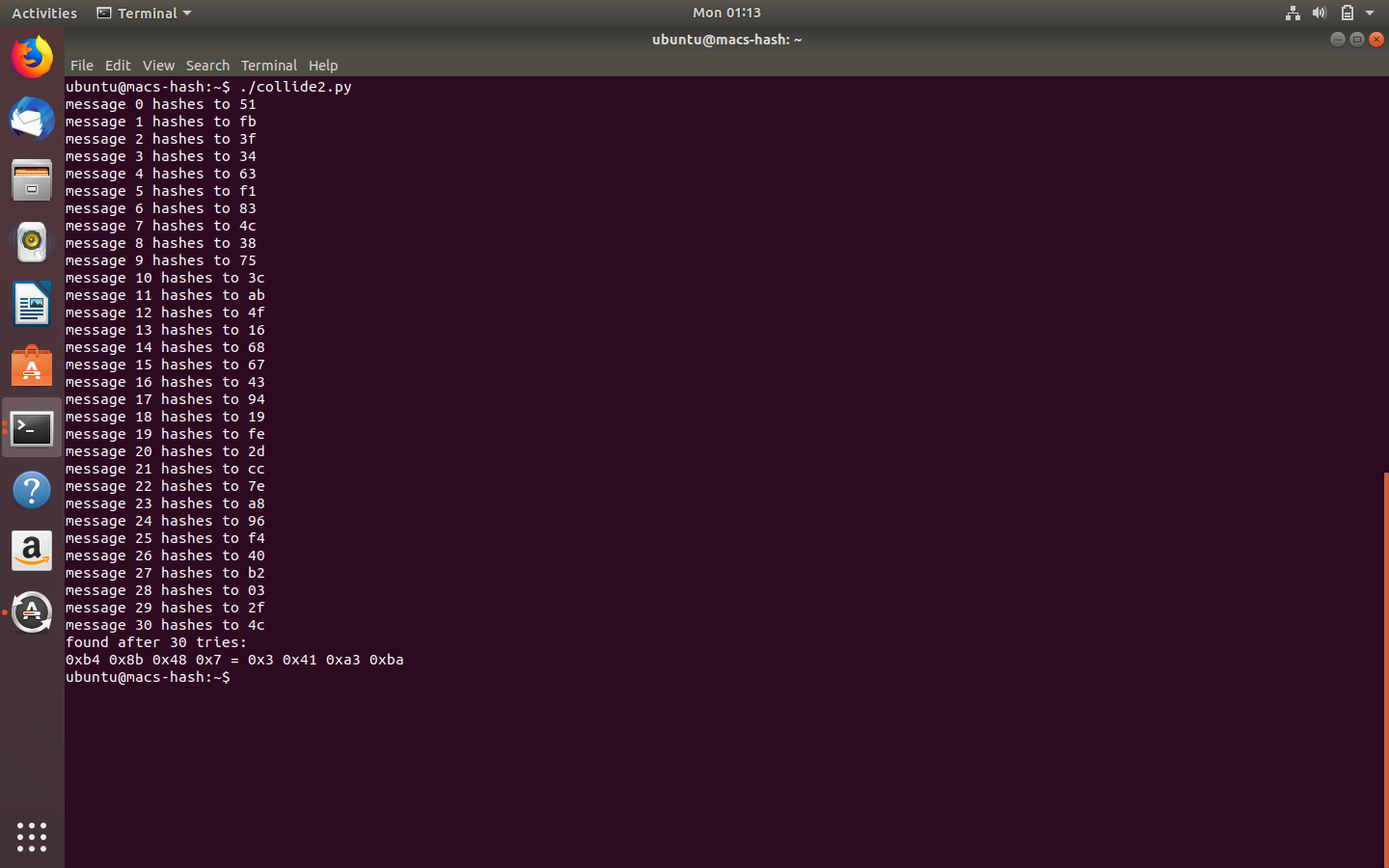
**Please include your commands, screenshots, and explanation for task 5 here:**

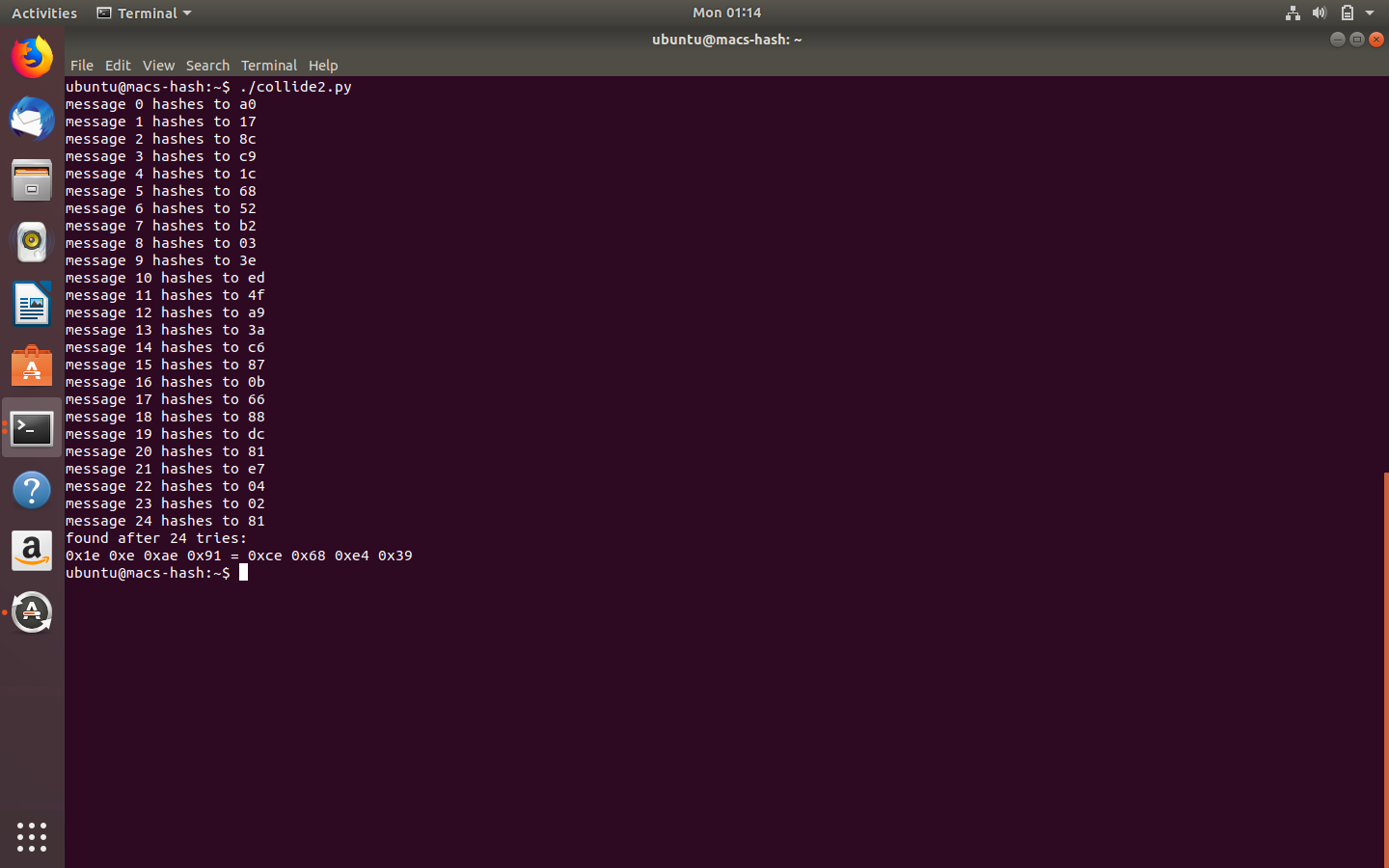
Screenshots: The number of attempts to find two random messages whose digests match on the last byte

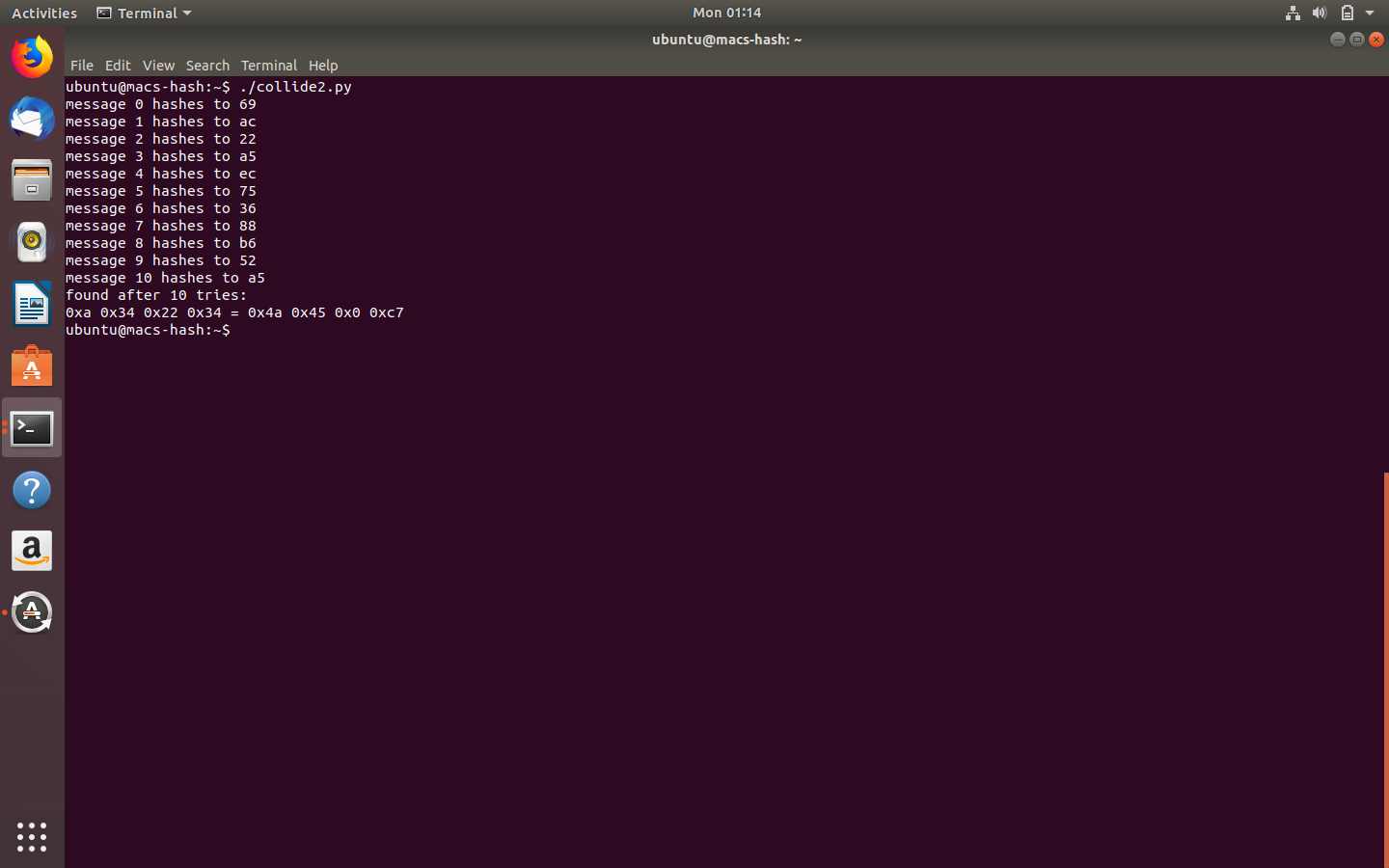


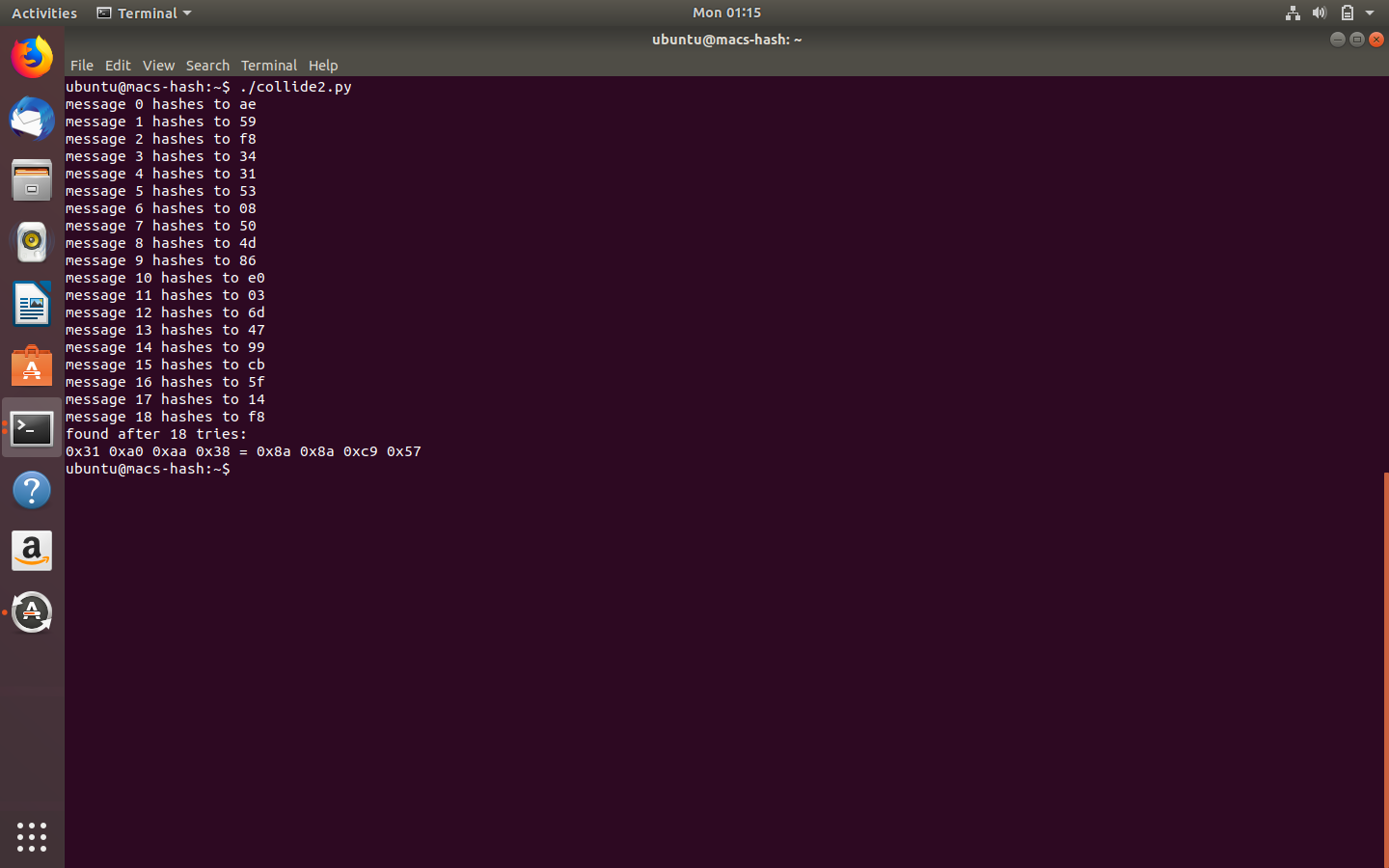


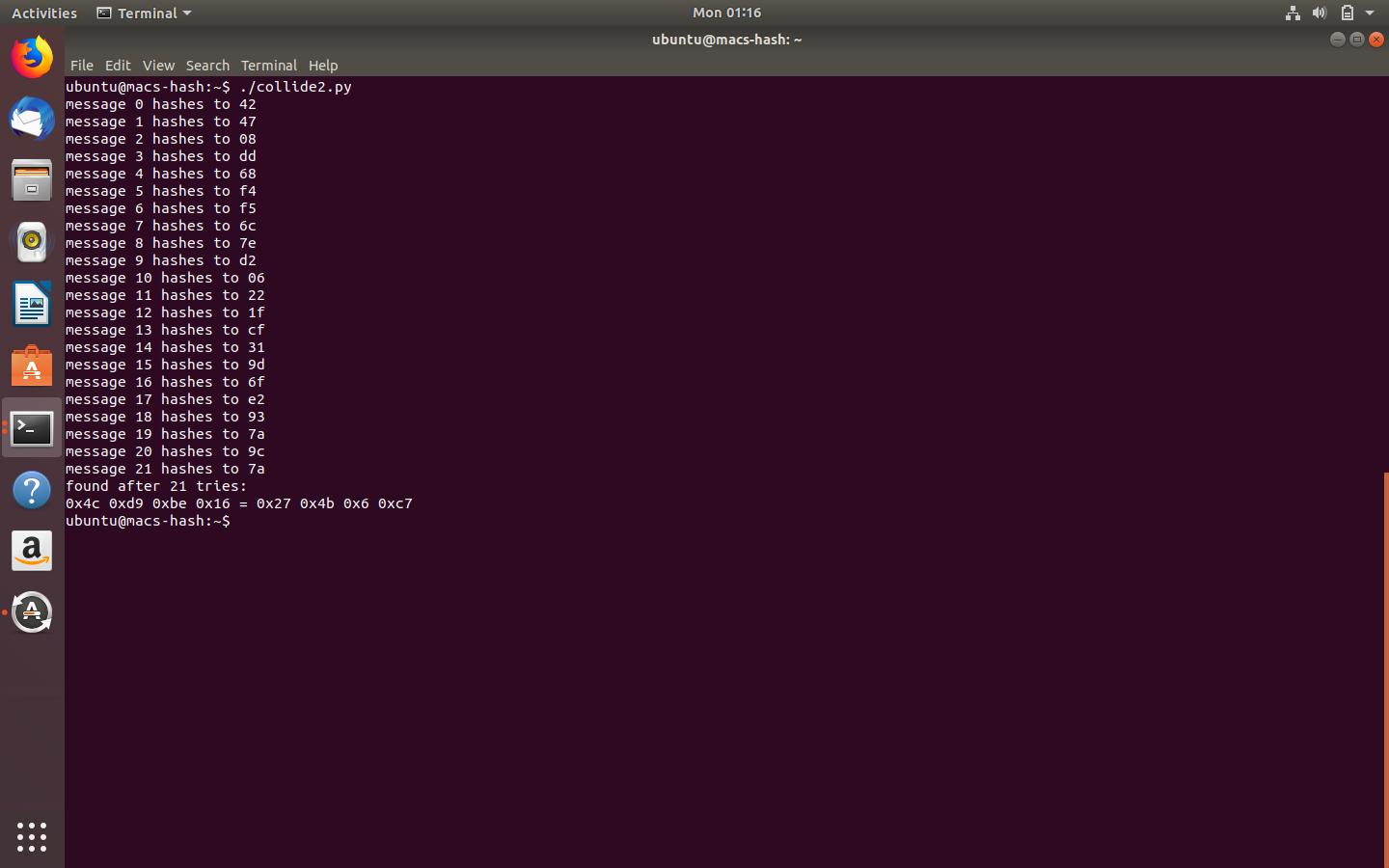


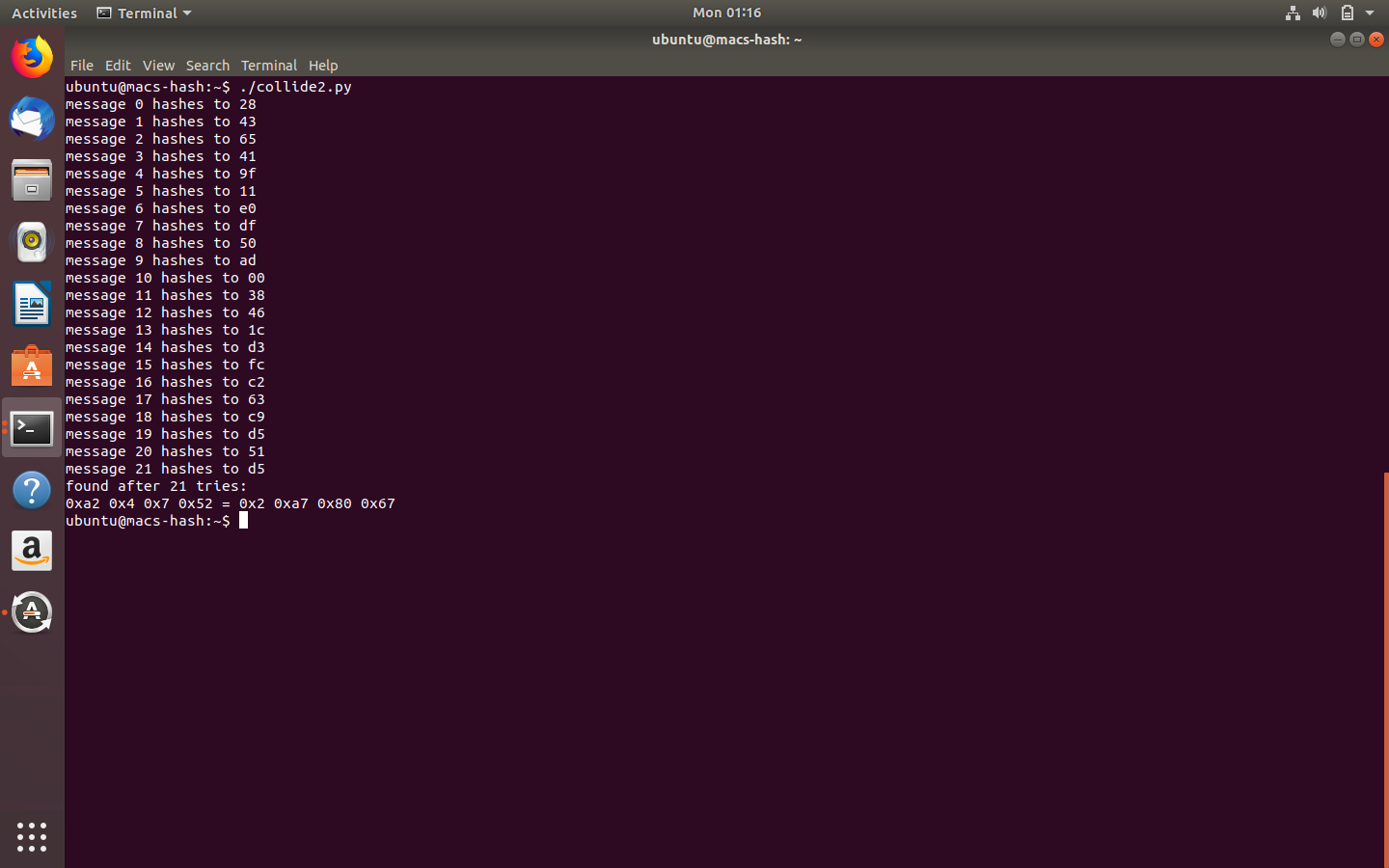


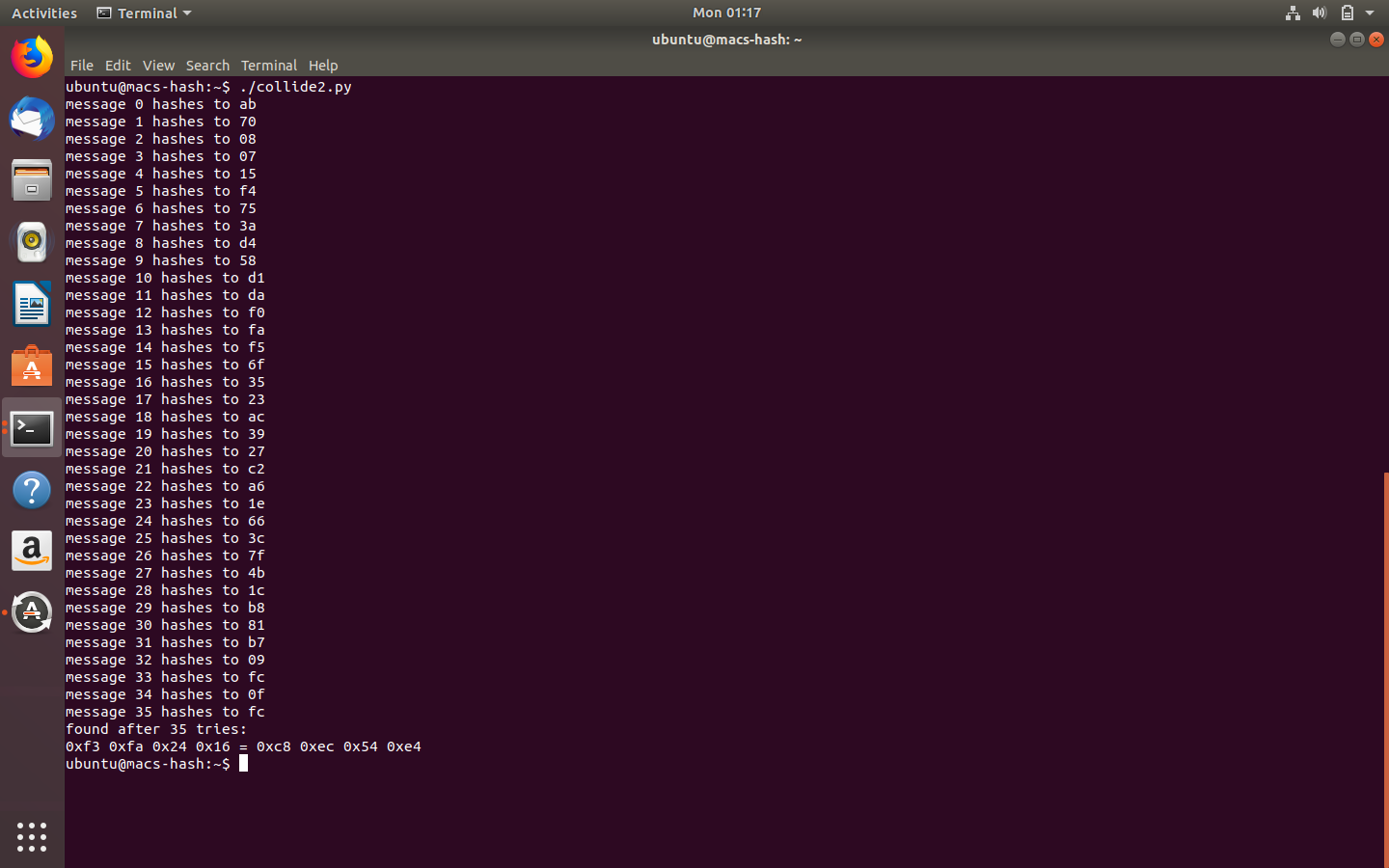












**Exploring Message Authentication Codes**

**Please include your commands, screenshots, and explanation for task 6 here:**

