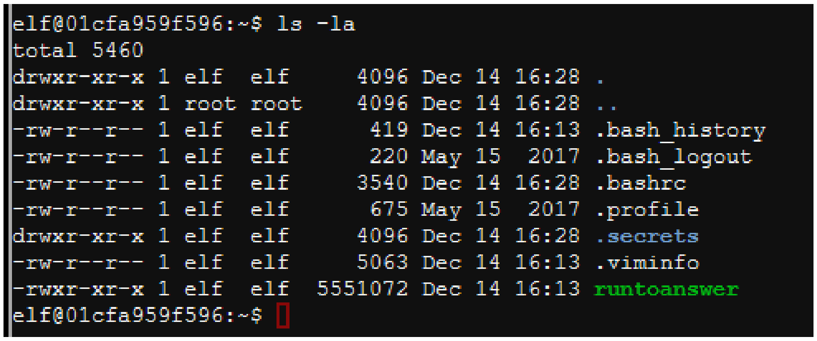
Terminal Challenge--LethalForensics (part 2)

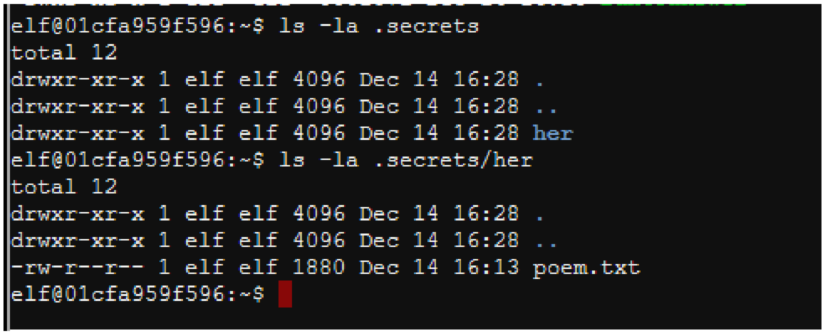
Finding vim artifacts

The article in the hints mentioned a hidden file, `.viminfo`. Let's use `ls -la` to see what else is there.



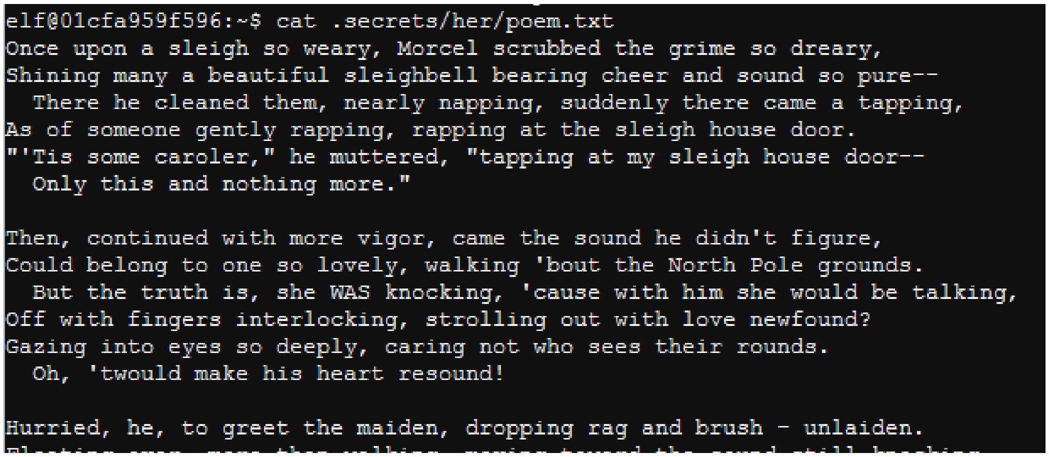
```
elf@01cfa959f596:~$ ls -la
total 5460
drwxr-xr-x 1 elf  elf     4096 Dec 14 16:28 .
drwxr-xr-x 1 root root    4096 Dec 14 16:28 ..
-rw-r--r-- 1 elf  elf      419 Dec 14 16:13 .bash_history
-rw-r--r-- 1 elf  elf      220 May 15  2017 .bash_logout
-rw-r--r-- 1 elf  elf     3540 Dec 14 16:28 .bashrc
-rw-r--r-- 1 elf  elf      675 May 15  2017 .profile
drwxr-xr-x 1 elf  elf     4096 Dec 14 16:28 .secrets
-rw-r--r-- 1 elf  elf     5063 Dec 14 16:13 .viminfo
-rwxr-xr-x 1 elf  elf  5551072 Dec 14 16:13 runtoanswer
elf@01cfa959f596:~$
```

I always like to spy on secrets, especially when they are hidden files. Remember that in Linux, adding a period to the front of a file name makes it "hidden" so it won't appear in normal directory listings. `The -a` option in `ls` shows those hidden files.



```
elf@01cfa959f596:~$ ls -la .secrets
total 12
drwxr-xr-x 1 elf elf 4096 Dec 14 16:28 .
drwxr-xr-x 1 elf elf 4096 Dec 14 16:28 ..
drwxr-xr-x 1 elf elf 4096 Dec 14 16:28 her
elf@01cfa959f596:~$ ls -la .secrets/her
total 12
drwxr-xr-x 1 elf elf 4096 Dec 14 16:28 .
drwxr-xr-x 1 elf elf 4096 Dec 14 16:28 ..
-rw-r--r-- 1 elf elf 1880 Dec 14 16:13 poem.txt
elf@01cfa959f596:~$
```

Let's examine poem.txt just for fun.



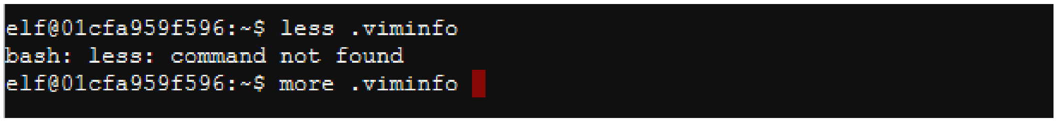
```
elf@01cfa959f596:~$ cat .secrets/her/poem.txt
Once upon a sleigh so weary, Morcel scrubbed the grime so dreary,
Shining many a beautiful sleighbell bearing cheer and sound so pure--
  There he cleaned them, nearly napping, suddenly there came a tapping,
As of someone gently rapping, rapping at the sleigh house door.
"'Tis some caroler," he muttered, "tapping at my sleigh house door--
  Only this and nothing more."

Then, continued with more vigor, came the sound he didn't figure,
Could belong to one so lovely, walking 'bout the North Pole grounds.
  But the truth is, she WAS knocking, 'cause with him she would be talking,
Off with fingers interlocking, strolling out with love newfound?
Gazing into eyes so deeply, caring not who sees their rounds.
  Oh, 'twould make his heart resound!

Hurried, he, to greet the maiden, dropping rag and brush - unlaiden.
```

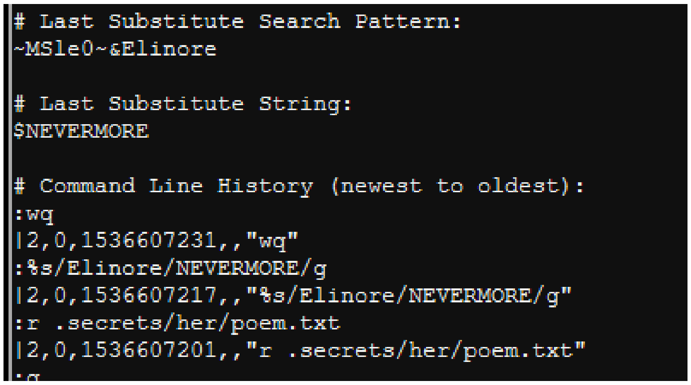
Hmm, it's not very original, just stolen from a famous poem. You don't see the name of the lady he's writing about, but there is one place where "NEVERMORE" is in a place that could hold a name.

Let’s get back to forensics. The article said we should look at `.viminfo`. It appears someone has removed the `less` command, which is not surprising since it is powerful. It’s older brother `more` will work for our purposes.



```
elf@01cfa959f596:~$ less .viminfo
bash: less: command not found
elf@01cfa959f596:~$ more .viminfo
```

There is some interesting information in `.viminfo`. It appears that the “author” of the poem, Marcel Nougat removed all instances of Elinore, replaced them with NEVERMORE, and saved the file (:wq).

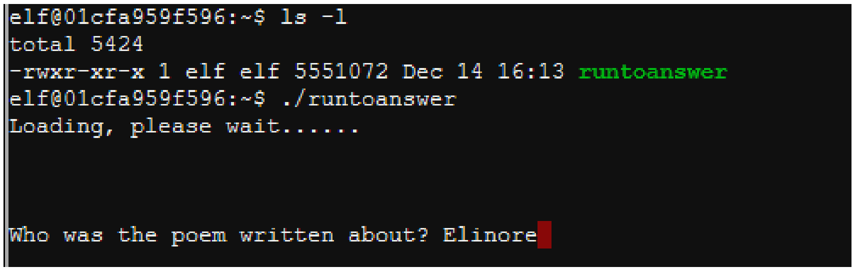


```
# Last Substitute Search Pattern:
~MSle0~&Elinore

# Last Substitute String:
$NEVERMORE

# Command Line History (newest to oldest):
:wq
|2,0,1536607231,,"wq"
:%s/Elinore/NEVERMORE/g
|2,0,1536607217,,"%s/Elinore/NEVERMORE/g"
:r .secrets/her/poem.txt
|2,0,1536607201,,"r .secrets/her/poem.txt"
:g
```

We will submit Elinore as the answer. Again, remember the period before runtoanswer. The period is the abbreviation for “the current directory” and tells BASH we specifically want to run the file and not another with the same name that may be in our path. That way if someone puts an evil `ls` in our directory, we will not run the evil file by mistake when we type `ls`. Microsoft finally caught on after many years and incorporated the same feature into PowerShell.

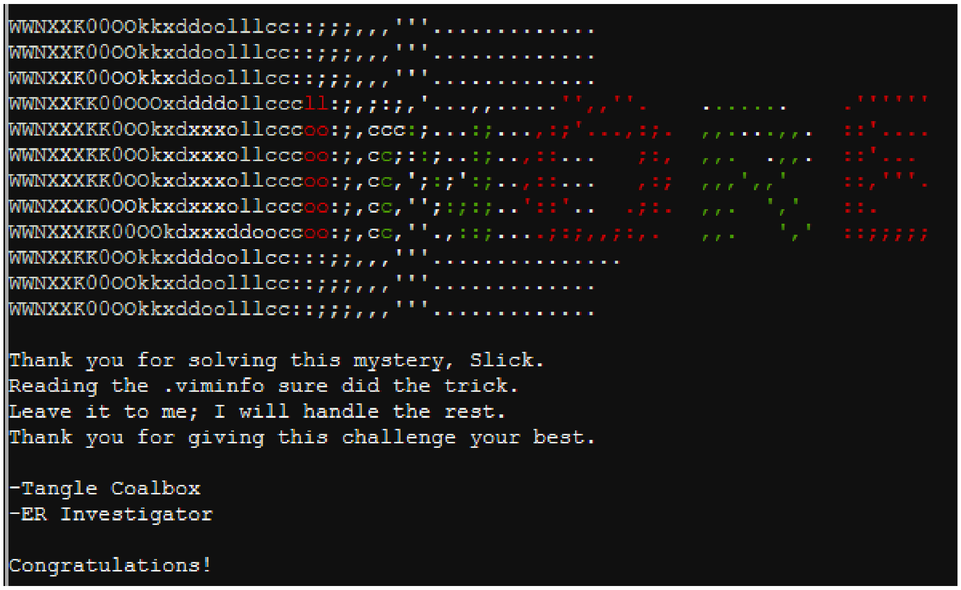


```
elf@01cfa959f596:~$ ls -l
total 5424
-rwxr-xr-x 1 elf elf 5551072 Dec 14 16:13 runtoanswer
elf@01cfa959f596:~$ ./runtoanswer
Loading, please wait......



Who was the poem written about? Elinore
```

Woot, woot! We were right!



```
WWNXXK00OOkkxddoolllcc::;;;,,,'''.............
WWNXXK00OOkkxddoolllcc::;;;,,,'''.............
WWNXXK00OOkkxddoolllcc::;;;,,,'''.............
WWNXXKK00OOOxddddollcccll:;,;:;,'...,,.....'',,''.    .......    .''''''
WWNXXXKK0OOkxdxxxollcccoo:;,ccc:;...:;...,:;'...,:;.  ,,.....,,.  ::'....
WWNXXXKK0OOkxdxxxollcccoo:;,cc;::;..:;..,::...    ;:,  ,,.  .,,.  ::'...
WWNXXXKK0OOkxdxxxollcccoo:;,cc,';:;':;..,::...    ,:;  ,,,',,'    ::,'''.
WWNXXXK0OOkkxdxxxollcccoo:;,cc,'';:;:;..'::'..  .;:.  ,,.   ','   ::.
WWNXXXKK00OOkdxxxddooccoo:;,cc,''.,::;....;:;,,;:,.   ,,.    ','  ::;;;;;
WWNXXKK0OOkkxdddoollcc:::;;,,,'''...............
WWNXXK00OOkkxddoolllcc::;;;,,,'''.............
WWNXXK00OOkkxddoolllcc::;;;,,,'''.............

Thank you for solving this mystery, Slick.
Reading the .viminfo sure did the trick.
Leave it to me; I will handle the rest.
Thank you for giving this challenge your best.

-Tangle Coalbox
-ER Investigator

Congratulations!
```

Now talk to Tangle to get hints (in his dialog and in your badge) about the next Objective.

Up Next

We will use the hints Tangle gave us to solve the de Bruijn sequence problem.