**Gathering Evidence**

* The first step is to navigate into the /03-student/day2/Gathering\_Evidence/ folder on your VM. To do this, run the following command:
  + cd /03-student/day2/Gathering\_Evidence/
* In the Gathering\_Evidence Folder, make a directory called Slugworth\_evidence by running:
  + mkdir Slugworth\_evidence
* Next, move into the email directory:
  + cd email
* List the emails referencing Slugworth, and place the results in a file called Slugworth\_email\_evidence:
  + grep -il slugworth \* > slugworth\_email\_evidence
* Next, add to the same file the number of emails that contain Slugworth:

grep -il slugworth \* | wc -l >> slugworth\_email\_evidence

* The next step is to place into a new file called slugworth\_web\_evidence the following data:
  + Which web log file contains Slugworth's IP address.
  + The number of Slugworth IPs addresses found in this file.
* Access the web\_logs directory by going back a directory (cd ..), then:
  + cd web\_logs
* To find the log files that have the IP address of 13.16.23.234 and place them in a new file called slugworth\_web\_evidence, run:
  + grep -il 13.16.23.234 \* > slugworth\_web\_evidence
* Next, to append to this file the number of records that contain the IP address, run:
  + grep -i 13.16.23.234 \* | wc -l >> slugworth\_web\_evidence
* Now we will move both of the evidence files over to the Slugworth\_evidence directory that we created:
  + cd ../../
  + mv ./Gathering\_Evidence/email/slugworth\_email\_evidence ./Gathering\_Evidence/Slugworth\_evidence/
  + mv ./Gathering\_Evidence/web\_logs/slugworth\_web\_evidence ./Gathering\_Evidence/Slugworth\_evidence/
* Next, navigate to the Slugworth\_evidence directory, and concatenate the files into a single file called Slugworth\_evidence\_for\_authorities:
  + cd Gathering\_Evidence/Slugworth\_evidence/
  + cat slugworth\_email\_evidence slugworth\_web\_evidence > Slugworth\_evidence\_for\_authorities
* The last step is to confirm the file has the correct data for the authorities. Run:
  + cat Slugworth\_evidence\_for\_authorities
* The results should be:
* email5
* email7
* email8
* 3
* 0518weblog

22

While this file contains all the data the authorities need, this is not obvious. In tomorrow's lesson we'll learn how to edit the contents of a file to further describe the evidence.