Solution Guide: 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.