# Assignment 3

**Kaleb Alstott**

For this assignment, you will gain hands-on experience using TruffleHog to search through filesystems for secrets.

Note: Once you’ve unzipped the zip file that this word document came in, do NOT move any of the files already in it or else the commands you have in this lab may produce unintended results.

First, download Trufflehog from its github releases page <https://github.com/trufflesecurity/trufflehog/releases> into the same folder you have this word document in. Please look through the possible assets to see which one is appropriate for your computer. Whichever asset you choose, it is recommended you use version 3.63.8 since that is what was used in the lectures. There is nothing to install.

Next, open your command prompt or terminal and navigate to the folder this word document is in. Inspect the test\_code folder using the command `.\trufflehog.exe filesystem test\_code` if on Windows or `.\trufflehog filesystem test\_code` on Mac/Linux. Paste a screenshot of your command window (you should not have found any secrets, verified or not).

A screenshot of a computer screen

Description automatically generated



Next, run trufflehog with the detector.yml file using the command `.\trufflehog filesystem --config=detector.yml test\_code` if on Windows or `.\trufflehog filesystem --config=detector.yml test\_code` on Mac/Linux. Paste screenshots of your command and its entire output (you should have detected the ES\_PASSWORD, DB\_PASS, and NVD\_API\_KEY variables in “.env” file)

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Knowledge check:** suppose that instead of a subdirectory of code with no source control, test\_code was actually a git repository on your laptop that you needed to inspect using trufflehog. What command would you use to do this? (hint: run `.\trufflehog git --help` on Windows or `.\trufflehog git --help` on Mac/Linux and read through the output).

I believe the command you would use in our case of a git repository on your laptop rather than a subdirectory of code with no source control would be trufflehog git <file://local-repo/> or trufflehog git <file://folder/> (source: <https://trufflesecurity.com/blog/trufflehog-commands-git-vs-filesystem/> ). I also believe that if you use this command below that our return will also be a little better due to a limited amount of false positives that the entropy might pick up if it wasn’t set to false or no.

Trufflehog git --entropy=NO --regex {git\_repo\_path\_or\_url}

Source: <https://materials.rangeforce.com/tutorial/2020/03/16/TruffleHog/>