Objective--Data Repo Analysis (part 1)

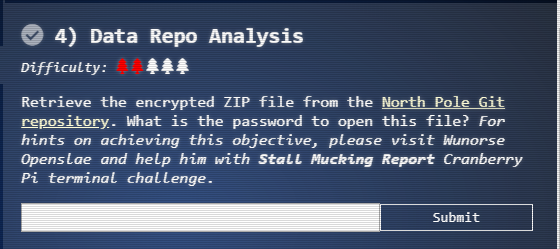
# What you can learn from this

More and more, developers are using web-based version control tools to help them collaborate on software. However, these tools pose a risk if sensitive information like passwords and cryptographic keys are inadvertently made public. Brian Hostetler lists several of the recent breaches this has caused in [his talk](https://www.youtube.com/watch?v=myKrWVaq3Cw). Repositories keep running logs of all changes made to software, so just removing a password in the current version will not help you. Previous version, and the change logs themselves, will still store that password.

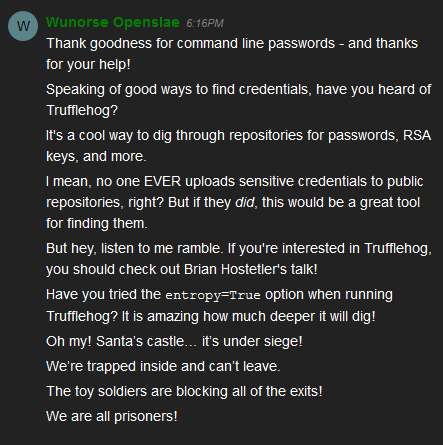
This challenge will demonstrate how publicly available tools make it easy to find credentials buried in public repositories. It will also demonstrate how to clone a Git repository so that you can install software on your local computer.

# Objective and hints

Since you have solved Wunorse’s problem with uploading his report, he has given you hints in his dialog and your badge (assuming you remembered to click on him after solving his problem.)



Although Wunorse mentions the entropy=True option in Trufflehog, he is a little out of date. Apparently, the option is so helpful it has been made the default, so you don’t need to use it. Do be sure not to use its opposite and set entropy to false; that will cause you to miss what you are looking for.



Again, the [link to Brian’s talk is here](https://www.youtube.com/watch?v=myKrWVaq3Cw). Please watch it.

# Installing Trufflehog.

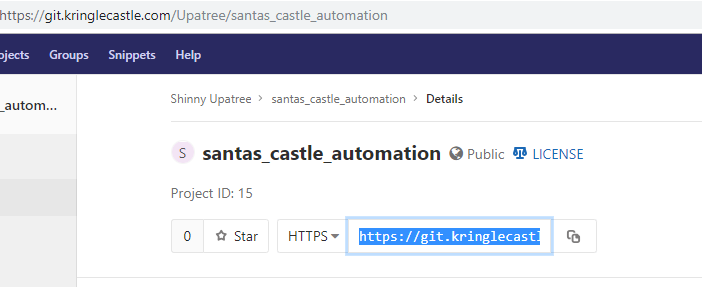
We will install Trufflehog on a Linux virtual machine (VM) because, well, it’s cool and it works well. Trufflehog is written in Python, and Python has its own repository called PIP. That makes the installation of Trufflehog very easy, except that you may need to install PIP first. (Trufflehog installation instructions are on the [Trufflehog Git repository](https://github.com/dxa4481/truffleHog).

Before installing software, it is a good idea to update your Linux OS, as older versions may have libraries that are incompatible with new installations. In Ubuntu or other Debian-based systems, update with:  
sudo apt-get update  
sudo apt-get upgrade  
In CentOS or other RedHat-based systems, use  
sudo yum update

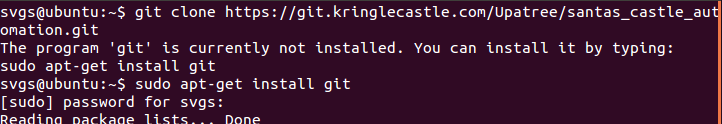
To install PIP in Ubuntu or other Debian-based systems use:  
sudo apt-get install python-pip  
In CentOS or other RedHat-based systems[, use](https://www.liquidweb.com/kb/how-to-install-pip-on-centos-7/):  
sudo yum install epel-release  
sudo yum update  
sudo yum install python-pip

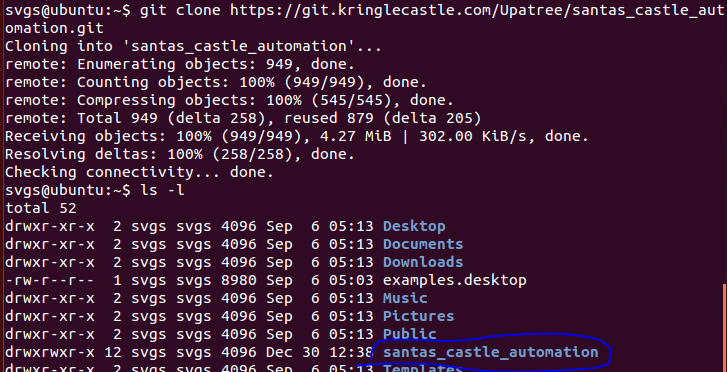
With that out of the way, installing Trufflehog is simple. Run PIP from your Linux terminal (BASH), not from inside Python.  
sudo pip install trufflehog

# Objective

We have been asked to find some encrypted zip files in the North Pole Git Repository, [which is available here](https://git.kringlecastle.com/Upatree/santas_castle_automation). The Git repository has search tools, but sometimes it is just as easy to create a local copy using the git clone command. Git repositories make it easy to copy the link to the repository.  


Just navigate to a directory where you would like to store a copy and execute: (one line)  
git clone <https://git.kringlecastle.com/Upatree/santas_castle_automation.git>

  
(oops)

  
Now just search the new directory for zip files using your usual tools.

To search for passwords, we might as well search the files we just cloned to our computer.  
 trufflehog santas\_castle\_automation/  


Note: The Trufflehog Read.Me file recommends using the --entropy=False option to cut down on noise. Don’t do that, as you will miss the passwords. Entropy is a measure of randomness. Cryptographic keys and good passwords should have a high degree of randomness. Trufflehog calculates the entropy for the strings it finds and displays any that rise above a preset threshold.

# Hand In

1. What is the name of the encrypted zip file?
2. What is the password?
3. What does the encrypted zip file contain?