# Data Exfiltration

## Technical Details

Technique: Exfiltration over Alternate Protocol

Sub-technique: Exfiltration Over Unencrypted Non-C2 Protocol

Steps (Pre-Requisites):

1. apt-get install steghide
2. apt-get install servefile
3. Install Wireshark on windows 10
4. Install winRAR on windows 10

### Technique 1: MITRE ATT&CK TECHNIQUE NUMBER AND NAME

MITRE ATT&CK TECHNIQUE NAME: Exfiltration Over Unencrypted Non-C2 Protocol

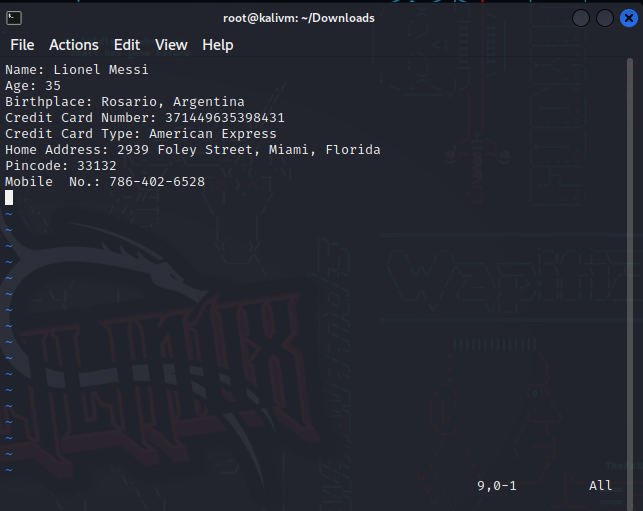
MITRE ATT&CK TECHNIQUE NUMBER : T1048.003

Implemented by: Aniket Kumar

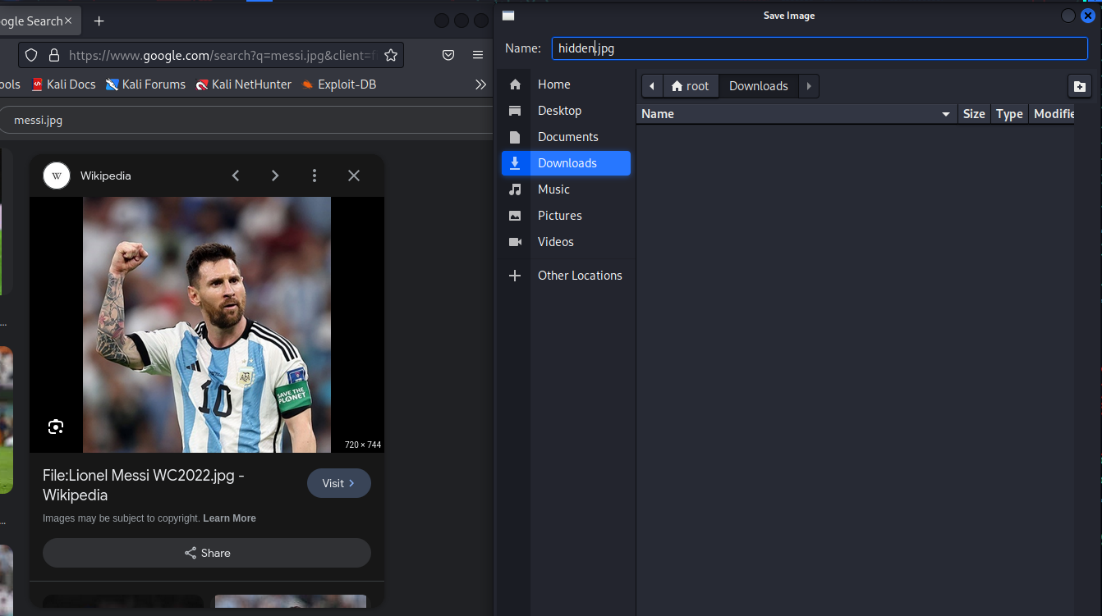
#### Demonstration

Steps that need to be done by Attacker to conduct the attack:

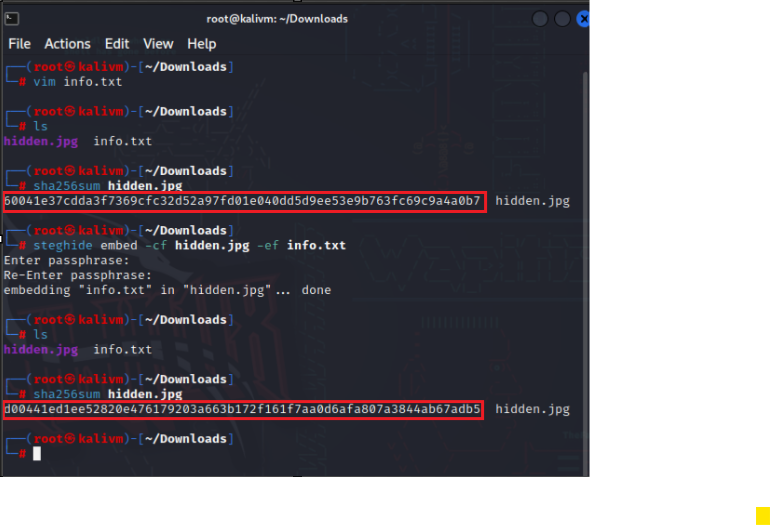
1. Open root terminal and go to any folder they wish to store the exfiltrated data in a text file. (In this scenario we will use the Downloads folder)
2. Create the said text file. (Saved as info.txt)



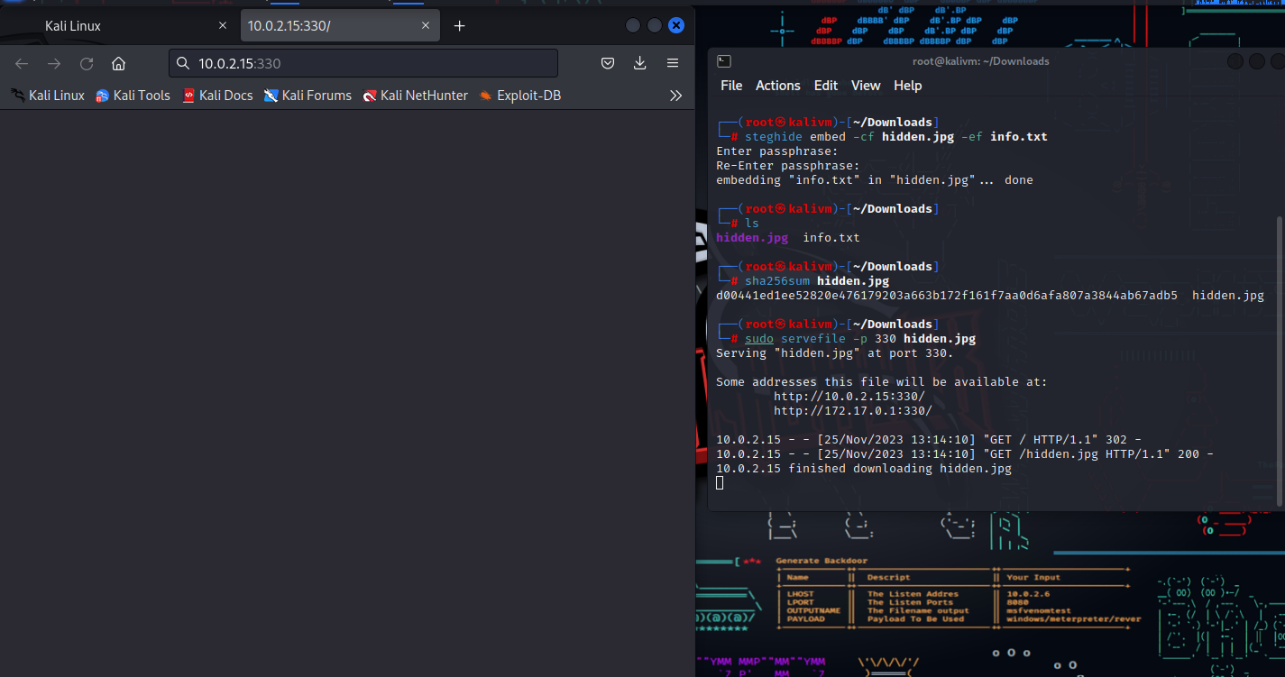
1. Go on the internet and find any jpeg image to obfuscate/hide the data.



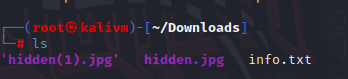
1. Use steghide command to hide the data in the image, you will be prompted for password you can choose any password you wish to use. (Can verify by checking the sha256 hash value)



1. Use the servefile command to download the hidden data across the network in the environment.



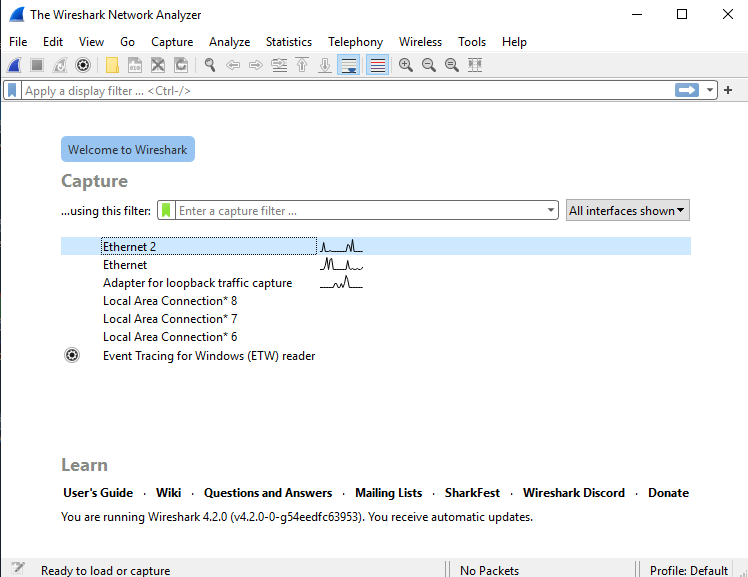
1. Check if the copy of the file was made then you can delete the files after extracting the picture out of the machine.

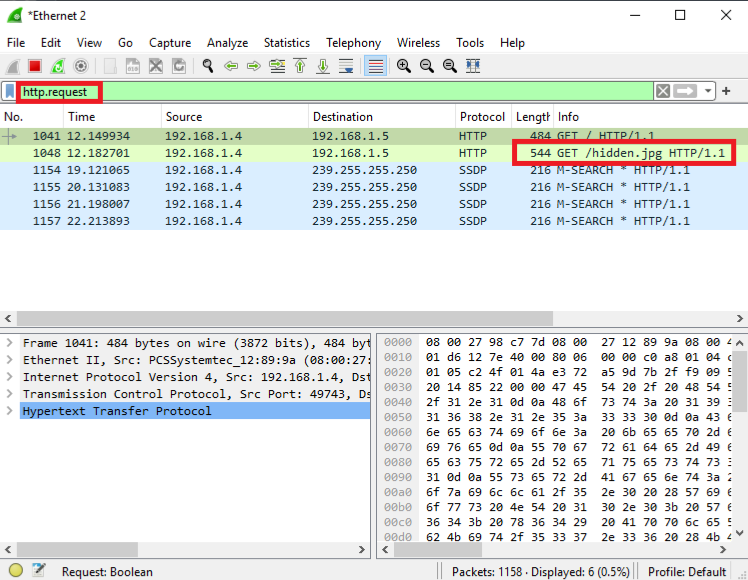


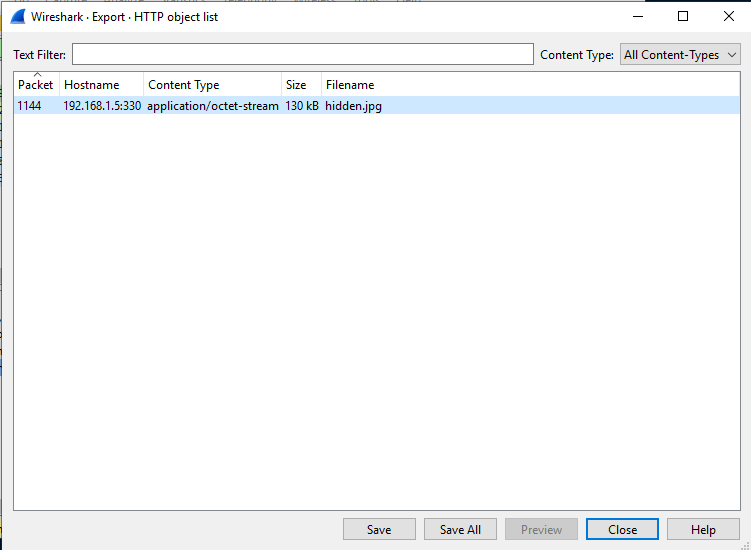
#### Detection

Write down how can this technique be detected (Be specific, provide evidence of log files / artifacts to look out for).

This technique can be detected by multiple methods, but one main method is surveying network traffic, most notably using the tool Wireshark. Open Wireshark and click on **Ethernet 2** **traffic option (**img 1) and then filter out the request to be http specific and you should be able to see this:

 img 1





This should raise alarm bells instantly for anyone who is detecting traffic flow.

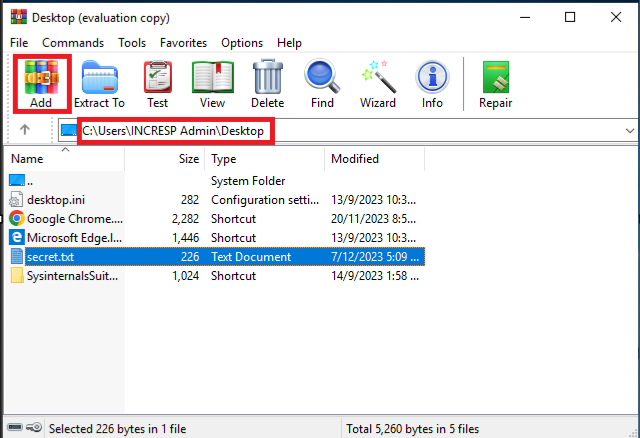
#### Rectification / Eradication

Write down the steps to take when stopping this technique (e.g security controls, remediation steps).

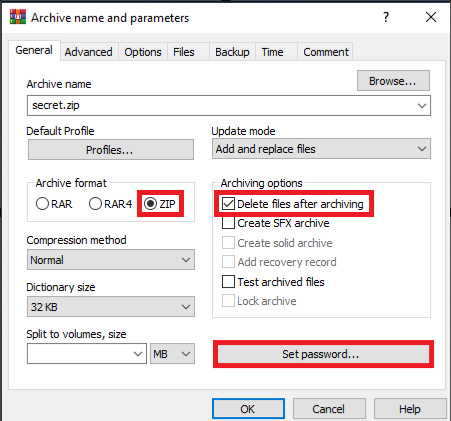
Some steps that can be taken to stop this technique is:

1. **Data Loss Prevention**: Data Loss Prevention (DLP) is the practice of detecting and preventing data breaches, exfiltration, or unwanted destruction of sensitive data. Organizations use DLP to protect and secure their data and comply with regulations. Often used by big companies and is provided by various vendors.

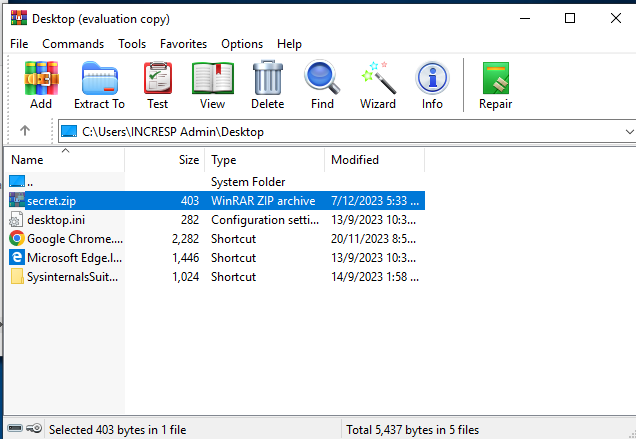
Step 1: Download winRAR

Step 2: Enter winRAR and navigate to file path of text file and click on “Add” for the selected text file 

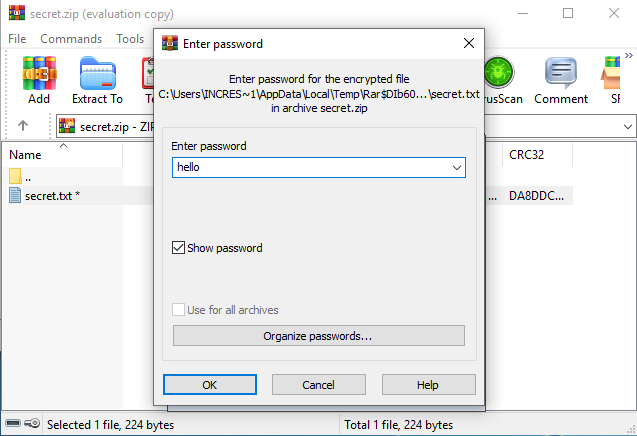
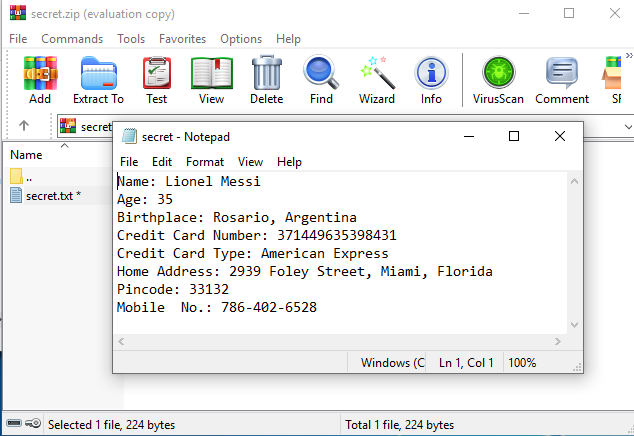
Step 3: Select the file type you want to hide your text file as (we’ll choose zip in this case). Select “delete files after archiving” what it does is that it deletes the original text file from the original file path and hides it inside the zip file.



Step 4: After clicking OK you can see that the original secret.txt file disappears and a new secret.zip is created.



Step 5: Click on secret.zip and you will be prompted for a password. Enter it and you will be able to access the text file. To check if the original text file is really deleted recheck the recycle bin and original file path it should not exist.

1. **Filter Network Traffic:** Use dedicated servers and enforce proxies for services like DNS. Only permit communication between those systems and other systems on the network via the appropriate ports and protocols.
2. **Network Segmentation:** To ensure that only essential ports and traffic are allowed to enter and exit the network, adhere to recommended procedures while configuring network firewalls.