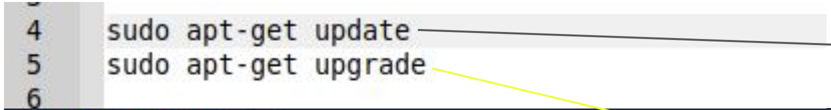
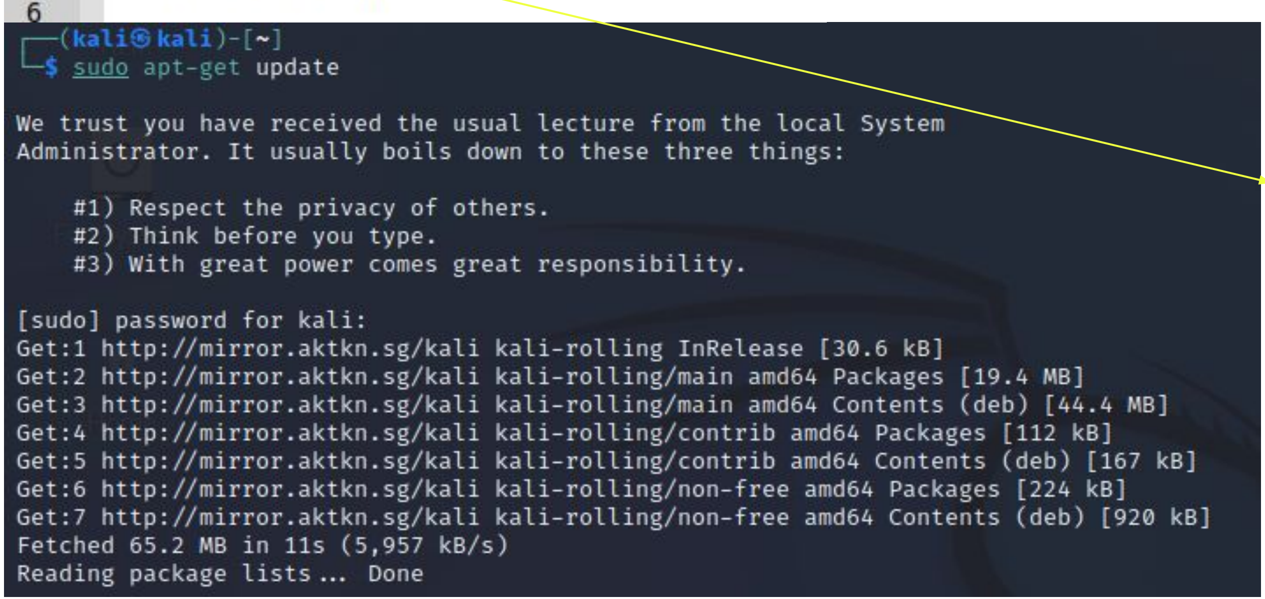
Remote Control
Ahmad Shafie S11
CFC3110



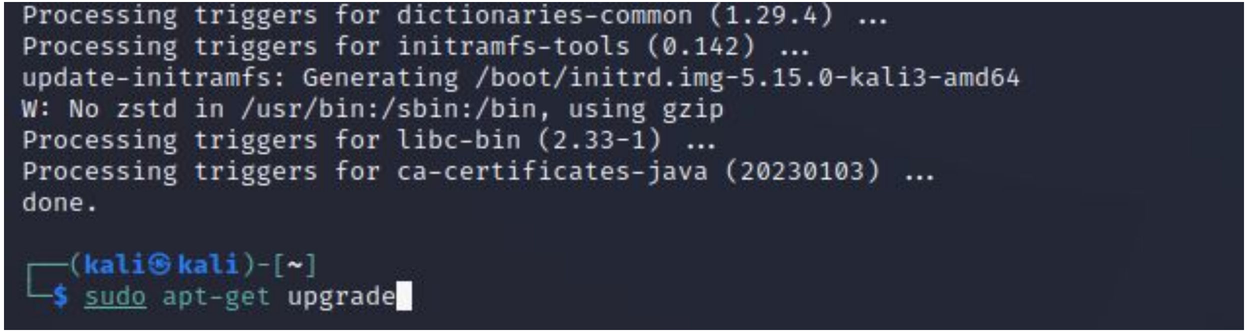
```
sudo apt-get update
sudo apt-get upgrade
```

The sudo apt-get update command is used to download package information from all configured sources.

The sudo apt-get upgrade command downloads and installs the updates for each outdated package and dependency on your system.

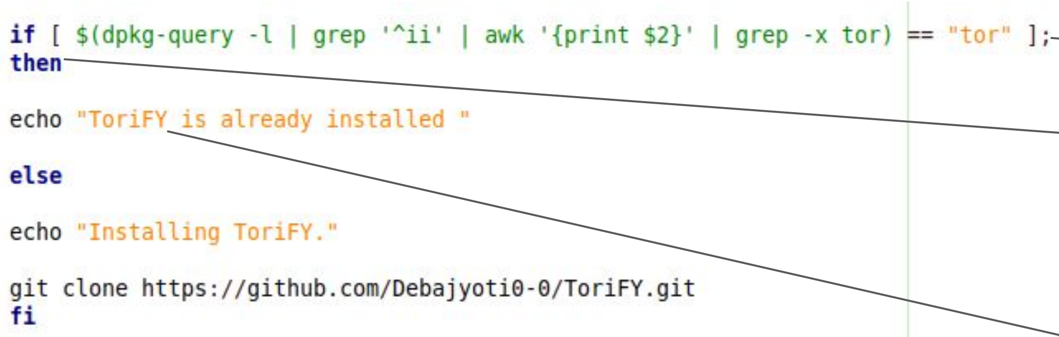


```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get update

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for kali:
Get:1 http://mirror.aktkn.sg/kali kali-rolling InRelease [30.6 kB]
Get:2 http://mirror.aktkn.sg/kali kali-rolling/main amd64 Packages [19.4 MB]
Get:3 http://mirror.aktkn.sg/kali kali-rolling/main amd64 Contents (deb) [44.4 MB]
Get:4 http://mirror.aktkn.sg/kali kali-rolling/contrib amd64 Packages [112 kB]
Get:5 http://mirror.aktkn.sg/kali kali-rolling/contrib amd64 Contents (deb) [167 kB]
Get:6 http://mirror.aktkn.sg/kali kali-rolling/non-free amd64 Packages [224 kB]
Get:7 http://mirror.aktkn.sg/kali kali-rolling/non-free amd64 Contents (deb) [920 kB]
Fetched 65.2 MB in 11s (5,957 kB/s)
Reading package lists... Done
```

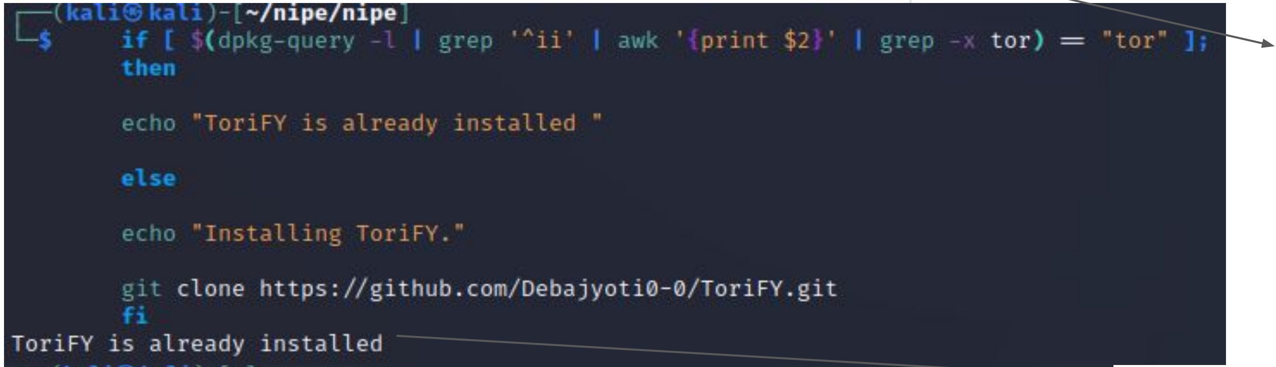


```
Processing triggers for dictionaries-common (1.29.4) ...
Processing triggers for initramfs-tools (0.142) ...
update-initramfs: Generating /boot/initrd.img-5.15.0-kali3-amd64
W: No zstd in /usr/bin:/sbin:/bin, using gzip
Processing triggers for libc-bin (2.33-1) ...
Processing triggers for ca-certificates-java (20230103) ...
done.

┌──(kali㉿kali)-[~]
└─$ sudo apt-get upgrade
```

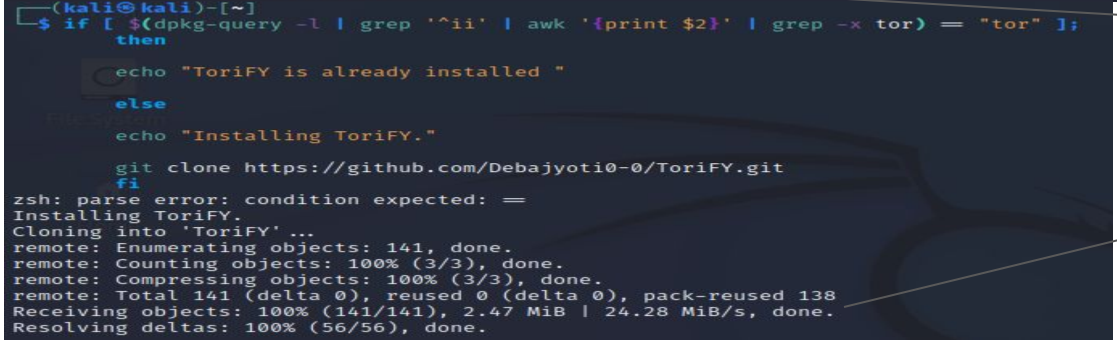
Shown here are both the outputs for sudo apt-get update/upgrade respectively. Please note that upgrade takes a significantly longer processing time



```
if [ $(dpkg-query -l | grep '^ii' | awk '{print $2}' | grep -x tor) == "tor" ];
then

echo "ToriFY is already installed "

else

echo "Installing ToriFY."

git clone https://github.com/Debajyoti0-0/ToriFY.git
fi
```



```
┌──(kali㉿kali)-[~/nipe/nipe]
└─$     if [ $(dpkg-query -l | grep '^ii' | awk '{print $2}' | grep -x tor) == "tor" ];
        then

        echo "ToriFY is already installed "

        else

        echo "Installing ToriFY."

        git clone https://github.com/Debajyoti0-0/ToriFY.git
        fi
ToriFY is already installed
```



```
┌──(kali㉿kali)-[~]
└─$ if [ $(dpkg-query -l | grep '^ii' | awk '{print $2}' | grep -x tor) == "tor" ];
        then

        echo "ToriFY is already installed "

        else

        echo "Installing ToriFY."

        git clone https://github.com/Debajyoti0-0/ToriFY.git
        fi
zsh: parse error: condition expected: ==
Installing ToriFY.
Cloning into 'ToriFY'...
remote: Enumerating objects: 141, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 141 (delta 0), reused 0 (delta 0), pack-reused 138
Receiving objects: 100% (141/141), 2.47 MiB | 24.28 MiB/s, done.
Resolving deltas: 100% (56/56), done.
```

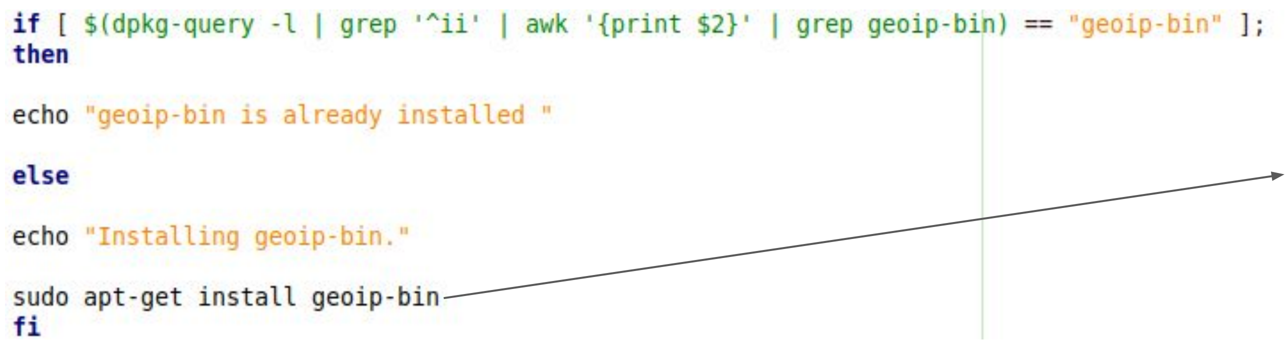
dpkg-query is a tool to show information about packages listed in the dpkg database.

The IF THEN ELSE function tests a condition, then returns a value based on the result of that condition. The IF THEN ELSE expression can be defined in two ways: IF (boolean condition) THEN (true value) ELSE (false value).

ToriFY is a tool to Automate and to redirect all the traffic in your device to TOR and spoof your mac address within a one click. And it also can change your IP in a certain amount for an example every 1 or 10s.

Following are output if the condition value are true which also means that ToriFY are installed.

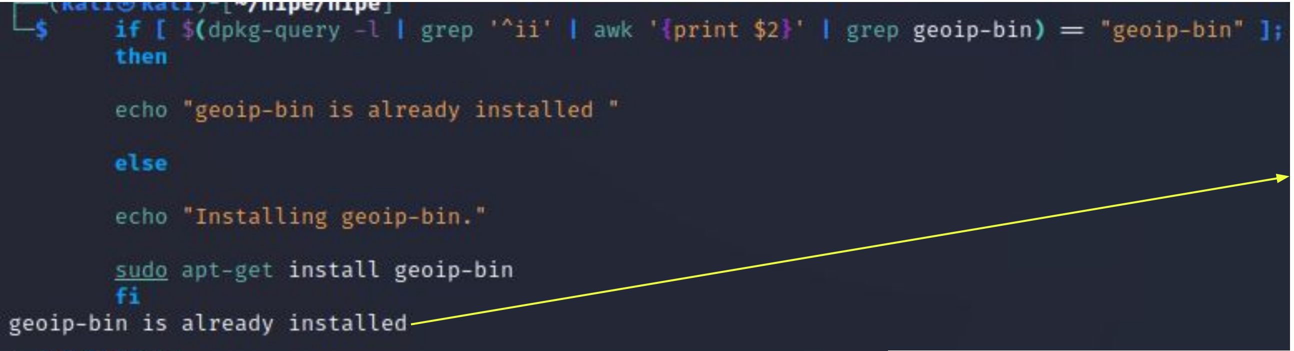
And if the conditions are not met, ToriFY will be installed as shown.



```
if [ $(dpkg-query -l | grep '^ii' | awk '{print $2}' | grep geoip-bin) == "geoip-bin" ];
then

echo "geoip-bin is already installed "

else

echo "Installing geoip-bin."

sudo apt-get install geoip-bin
fi
```

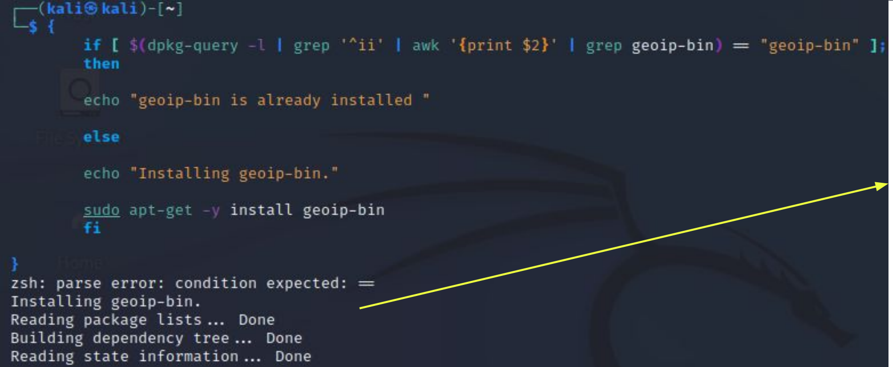
GeoIP is a C library that enables the user to find the country that any IP address or hostname originates from. It uses a file based database.

This database simply contains IP blocks as keys, and countries as values and it should be more complete and accurate than using reverse DNS lookups.



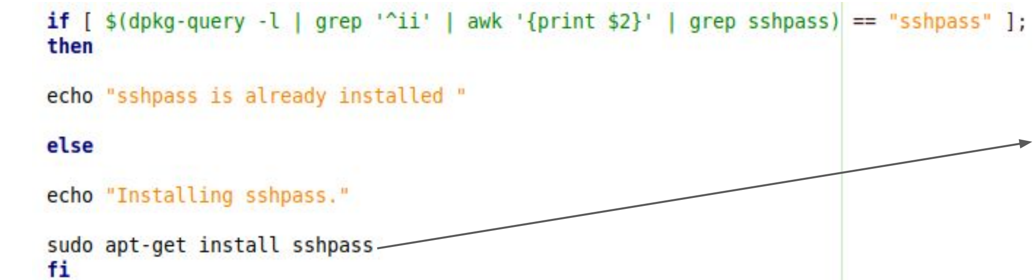
```
┌──(kali㉿kali)-[~/nipe/nipe]
└─$     if [ $(dpkg-query -l | grep '^ii' | awk '{print $2}' | grep geoip-bin) == "geoip-bin" ];
        then

        echo "geoip-bin is already installed "

        else

        echo "Installing geoip-bin."

        sudo apt-get install geoip-bin
        fi
geoip-bin is already installed
```

The output shown here is the result if the conditions are met, so if geoip-bin was already installed, it will echo out “geoip-bin is already installed” and proceed to the next command



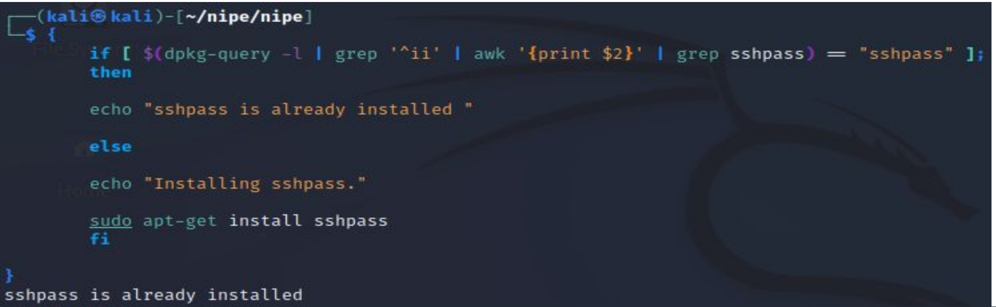
```
┌──(kali㉿kali)-[~]
└─$ {
        if [ $(dpkg-query -l | grep '^ii' | awk '{print $2}' | grep geoip-bin) == "geoip-bin" ];
        then

        echo "geoip-bin is already installed "

        else

        echo "Installing geoip-bin."

        sudo apt-get -y install geoip-bin
        fi

}
zsh: parse error: condition expected: ==
Installing geoip-bin.
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
```

Otherwise if it’s not installed, it is programmed to automatically download the required service before moving on to the next task

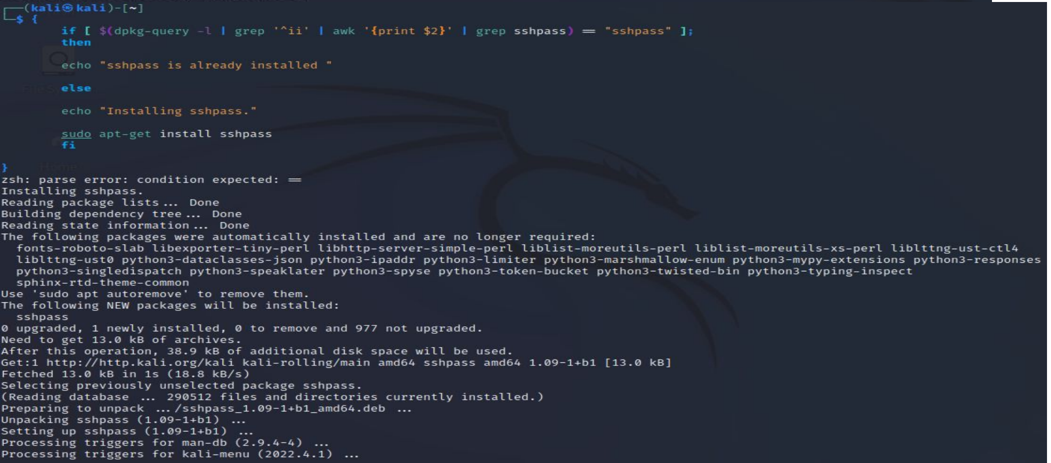


```
if [ $(dpkg-query -l | grep '^ii' | awk '{print $2}' | grep sshpass) == "sshpass" ];
then

echo "sshpass is already installed "

else

echo "Installing sshpass."

sudo apt-get install sshpass
fi
```

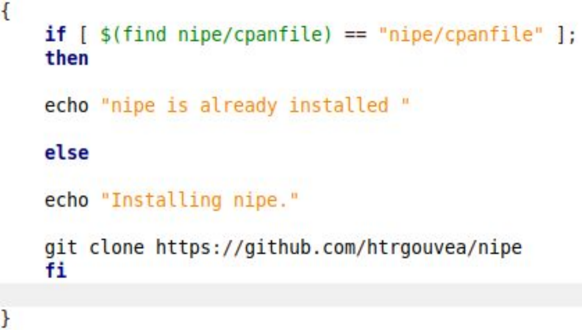
The sshpass utility is designed to run SSH using the keyboard-interactive password authentication mode, but in a non-interactive way. SSH uses direct TTY access to ensure that the password is indeed issued by an interactive keyboard user.



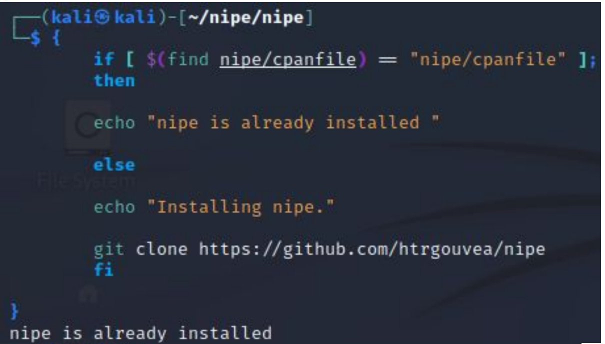
```
┌──(kali㉿kali)-[~/nipe/nipe]
└─$ {
        if [ $(dpkg-query -l | grep '^ii' | awk '{print $2}' | grep sshpass) == "sshpass" ];
        then

        echo "sshpass is already installed "

        else

        echo "Installing sshpass."

        sudo apt-get install sshpass
        fi

}
sshpass is already installed
```



```
┌──(kali㉿kali)-[~]
└─$ {
        if [ $(dpkg-query -l | grep '^ii' | awk '{print $2}' | grep sshpass) == "sshpass" ];
        then

        echo "sshpass is already installed "

        else

        echo "Installing sshpass."

        sudo apt-get install sshpass
        fi

}
zsh: parse error: condition expected: ==
Installing sshpass.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  fonts-roboto-slab libexporter-tiny-perl libhttp-server-simple-perl liblist-moreutils-perl liblist-moreutils-xs-perl liblttng-ust-ctl4
  liblttng-ust0 python3-dataclasses-json python3-ipaddr python3-limiter python3-marshmallow-enum python3-mypy-extensions python3-responses
  python3-singledispatch python3-speaklater python3-spyse python3-token-bucket python3-twisted-bin python3-typing-inspect
  sphinx-rtd-theme-common
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  sshpass
0 upgraded, 1 newly installed, 0 to remove and 977 not upgraded.
Need to get 13.0 kB of archives.
After this operation, 38.9 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 sshpass amd64 1.09-1+b1 [13.0 kB]
Fetched 13.0 kB in 1s (18.8 kB/s)
Selecting previously unselected package sshpass.
(Reading database ... 290512 files and directories currently installed.)
Preparing to unpack .../sshpass_1.09-1+b1_amd64.deb ...
Unpacking sshpass (1.09-1+b1) ...
Setting up sshpass (1.09-1+b1) ...
Processing triggers for man-db (2.9.4-4) ...
Processing triggers for kali-menu (2022.4.1) ...
```

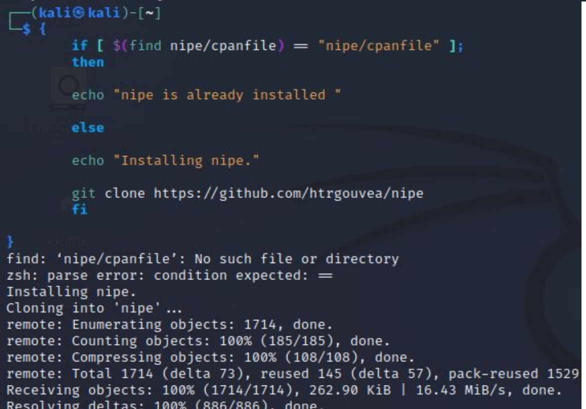


```
{
    if [ $(find nipe/cpanfile) == "nipe/cpanfile" ];
    then

    echo "nipe is already installed "

    else

    echo "Installing nipe."

    git clone https://github.com/htrgouvea/nipe
    fi

}
```

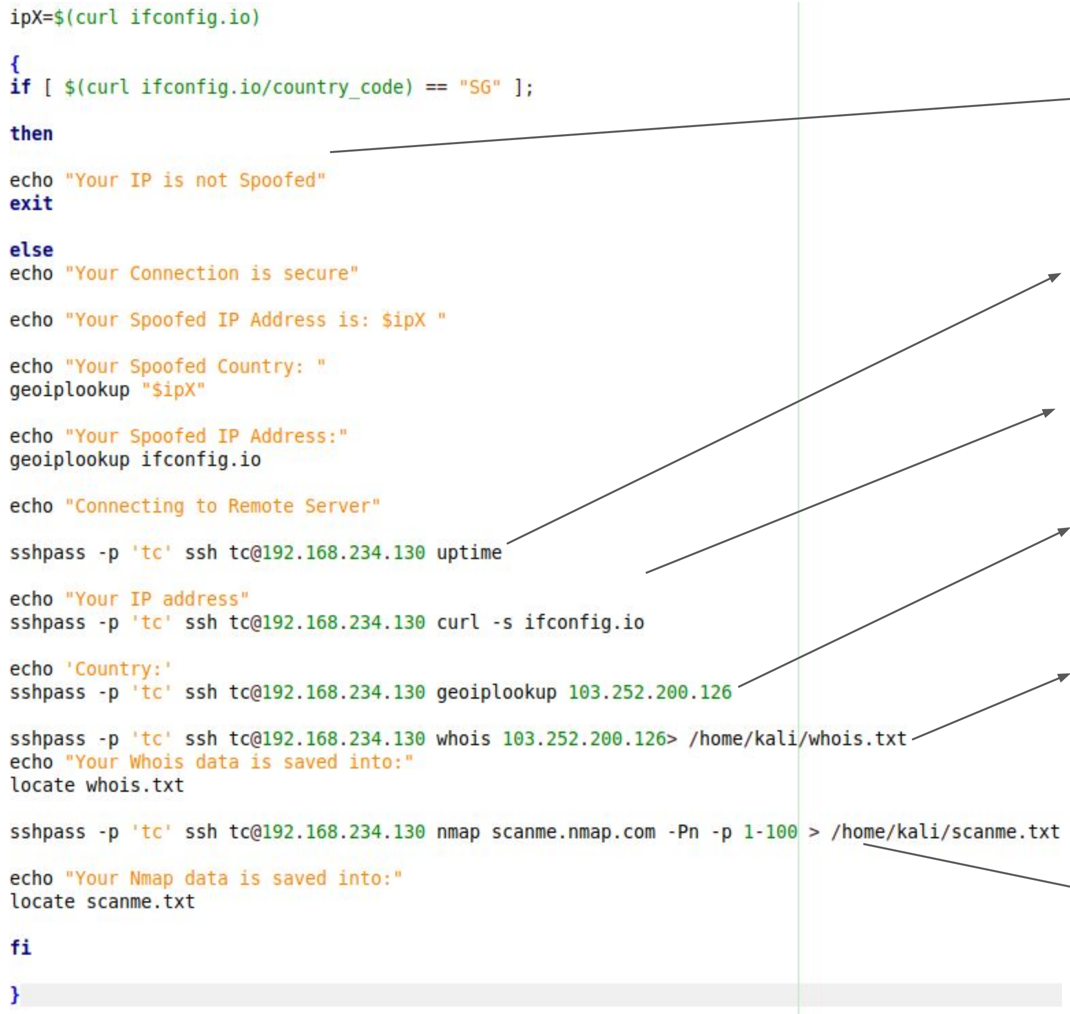


```
┌──(kali㉿kali)-[~/nipe/nipe]
└─$ {
        if [ $(find nipe/cpanfile) == "nipe/cpanfile" ];
        then

        echo "nipe is already installed "

        else

        echo "Installing nipe."

        git clone https://github.com/htrgouvea/nipe
        fi

}
nipe is already installed
```

Nipe is an engine, developed in Perl, that aims on making the Tor network your default network gateway. Nipe can route the traffic from your machine to the Internet through Tor network, so you can surf the Internet having a more formidable stance on privacy and anonymity in cyberspace.



```
┌──(kali㉿kali)-[~]
└─$ {
        if [ $(find nipe/cpanfile) == "nipe/cpanfile" ];
        then

        echo "nipe is already installed "

        else

        echo "Installing nipe."

        git clone https://github.com/htrgouvea/nipe
        fi

}
find: ‘nipe/cpanfile’: No such file or directory
zsh: parse error: condition expected: ==
Installing nipe.
Cloning into 'nipe'...
remote: Enumerating objects: 1714, done.
remote: Counting objects: 100% (185/185), done.
remote: Compressing objects: 100% (108/108), done.
remote: Total 1714 (delta 73), reused 145 (delta 57), pack-reused 1529
Receiving objects: 100% (1714/1714), 262.90 KiB | 16.43 MiB/s, done.
Resolving deltas: 100% (886/886), done.
```



```
ipX=$(curl ifconfig.io)

{
if [ $(curl ifconfig.io/country_code) == "SG" ];

then

echo "Your IP is not Spoofed"
exit

else
echo "Your Connection is secure"

echo "Your Spoofed IP Address is: $ipX "

echo "Your Spoofed Country: "
geoiplookup "$ipX"

echo "Your Spoofed IP Address:"
geoiplookup ifconfig.io

echo "Connecting to Remote Server"

sshpass -p 'tc' ssh tc@192.168.234.130 uptime

echo "Your IP address"
sshpass -p 'tc' ssh tc@192.168.234.130 curl -s ifconfig.io

echo 'Country:'
sshpass -p 'tc' ssh tc@192.168.234.130 geoiplookup 103.252.200.126

sshpass -p 'tc' ssh tc@192.168.234.130 whois 103.252.200.126> /home/kali/whois.txt
echo "Your Whois data is saved into:"
locate whois.txt

sshpass -p 'tc' ssh tc@192.168.234.130 nmap scanme.nmap.com -Pn -p 1-100 > /home/kali/scanme.txt

echo "Your Nmap data is saved into:"
locate scanme.txt

fi

}
```

This function here is to ensure that you successfully falsify the content in the Source IP header. If conditions are met and you have not spoofed your IP address, the programme will inform you and will not continue working

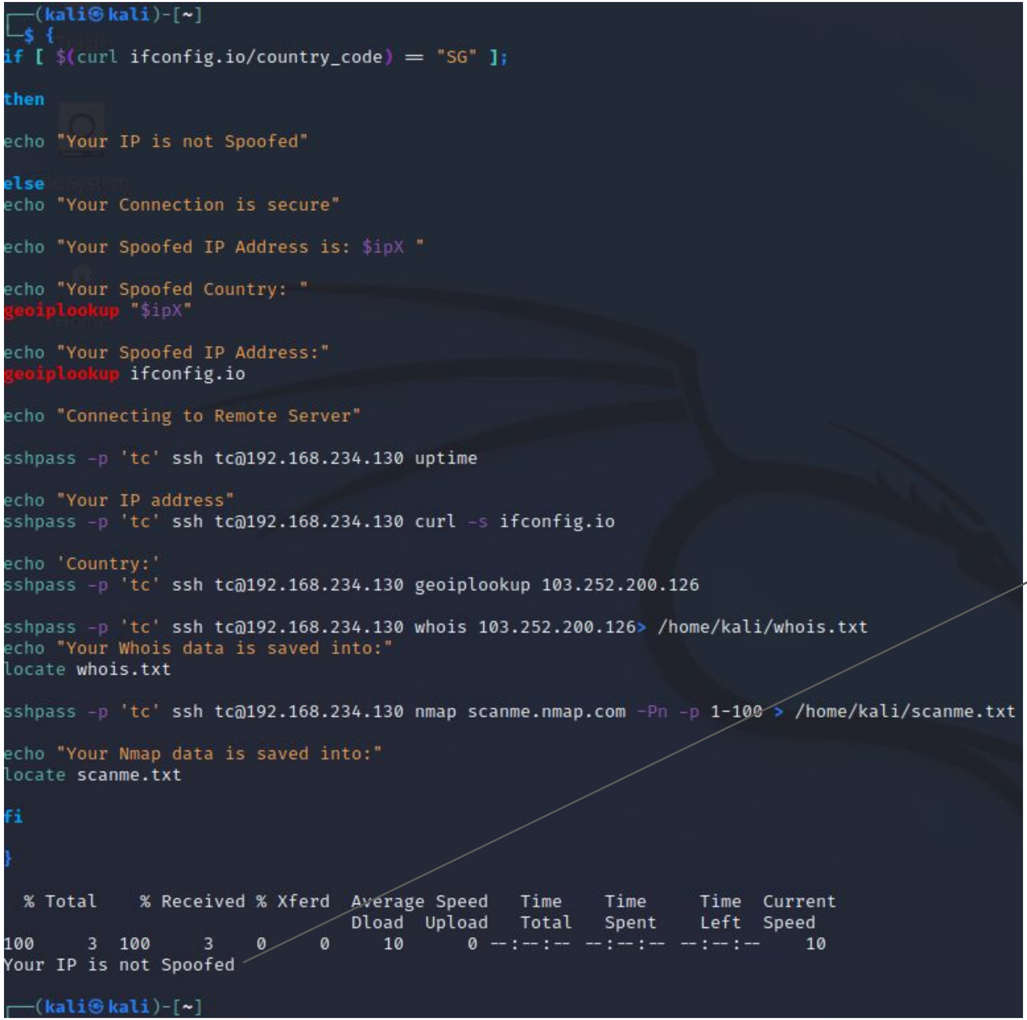
Uptime is a computer industry term for the time during which a computer or IT system is operational. Uptime can also be a metric that represents the percentage of time that hardware, a computer network, or a device is successfully operational.

curl command here is used to display data(IP address) of the remote server

geoiplookup uses the GeoIP library and database to find the Country that an IP address or hostname originates from.

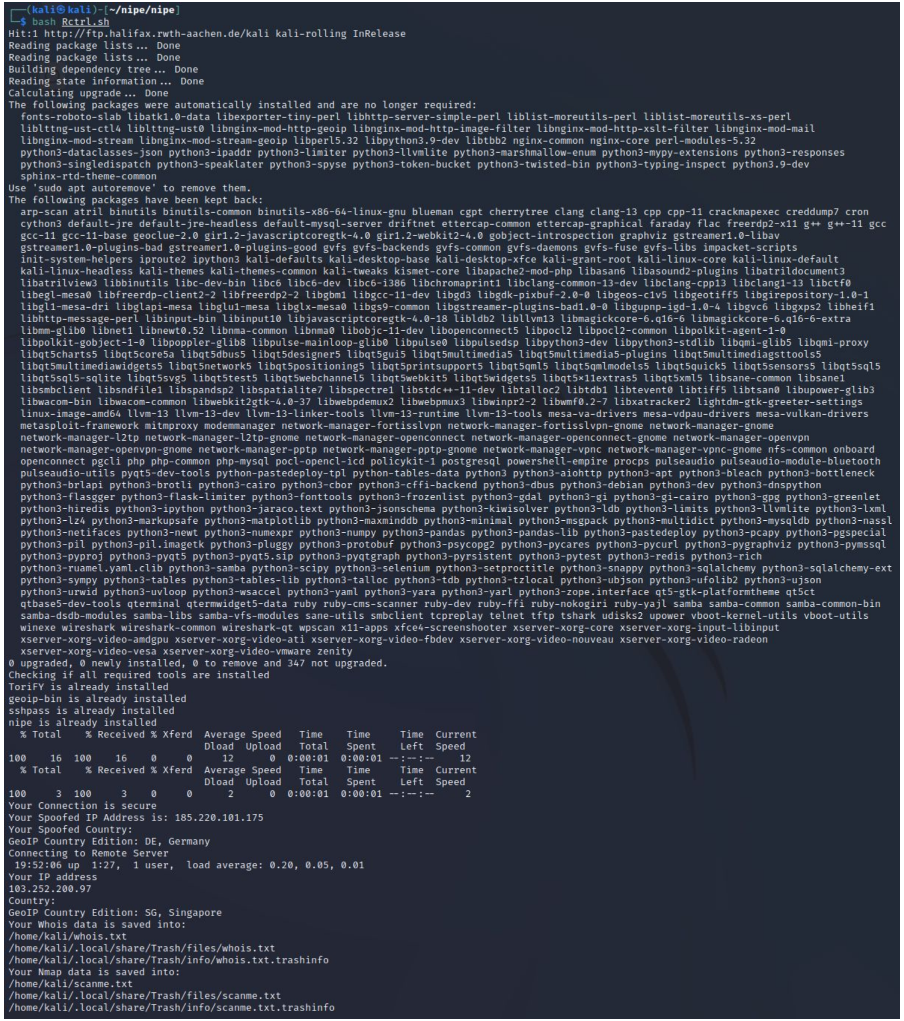
whois is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block or an autonomous system, but is also used for a wider range of other information. In this case, the output is saved into whois.txt

nmap command-line tool for network exploration and security auditing. It is used here to scan for open ports between port number 1-100 and the data is saved into scanme.txt



```
┌──(kali㉿kali)-[~]
└─$ {
if [ $(curl ifconfig.io/country_code) == "SG" ];

then

echo "Your IP is not Spoofed"

else
echo "Your Connection is secure"

echo "Your Spoofed IP Address is: $ipX "

echo "Your Spoofed Country: "
geoiplookup "$ipX"

echo "Your Spoofed IP Address:"
geoiplookup ifconfig.io

echo "Connecting to Remote Server"

sshpass -p 'tc' ssh tc@192.168.234.130 uptime

echo "Your IP address"
sshpass -p 'tc' ssh tc@192.168.234.130 curl -s ifconfig.io

echo 'Country:'
sshpass -p 'tc' ssh tc@192.168.234.130 geoiplookup 103.252.200.126

sshpass -p 'tc' ssh tc@192.168.234.130 whois 103.252.200.126> /home/kali/whois.txt
echo "Your Whois data is saved into:"
locate whois.txt

sshpass -p 'tc' ssh tc@192.168.234.130 nmap scanme.nmap.com -Pn -p 1-100 > /home/kali/scanme.txt

echo "Your Nmap data is saved into:"
locate scanme.txt

fi

}

  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100     3  100     3    0     0     10      0 --:--:-- --:--:-- --:--:--    10
Your IP is not Spoofed

┌──(kali㉿kali)-[~]
```

The output shown “Your IP is not Spoofed” is the outcome if the conditions are met(your IP is not redirected).



```
┌──(kali㉿kali)-[~/nipe/nipe]
└─$ bash Rctrl.sh
Hit:1 http://ftp.halifax.rwth-aachen.de/kali kali-rolling InRelease
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  fonts-roboto-slab libatk1.0-data libexporter-tiny-perl libhttp-server-simple-perl liblist-moreutils-perl liblist-moreutils-xs-perl
  liblttng-ust-ctl4 liblttng-ust0 libnginx-mod-http-geoip libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter libnginx-mod-mail
  libnginx-mod-stream libnginx-mod-stream-geoip libperl5.32 libpython3.9-dev libtbb2 nginx-common nginx-core perl-modules-5.32
  python3-dataclasses-json python3-ipaddr python3-limiter python3-llvmlite python3-marshmallow-enum python3-mypy-extensions python3-responses
  python3-singledispatch python3-speaklater python3-spyse python3-token-bucket python3-twisted-bin python3-typing-inspect python3.9-dev
  sphinx-rtd-theme-common
Use 'sudo apt autoremove' to remove them.
The following packages have been kept back:
  arp-scan atril binutils binutils-common binutils-x86-64-linux-gnu blueman cgpt cherrytree clang clang-13 cpp cpp-11 crackmapexec creddump7 cron
  cython3 default-jre default-jre-headless default-mysql-server driftnet ettercap-common ettercap-graphical faraday flac freerdp2-x11 g++ g++-11 gcc
  gcc-11 gcc-11-base geoclue-2.0 gir1.2-javascriptcoregtk-4.0 gir1.2-webkit2-4.0 gobject-introspection graphviz gstreamer1.0-libav
  gstreamer1.0-plugins-bad gstreamer1.0-plugins-good gvfs gvfs-backends gvfs-common gvfs-daemons gvfs-fuse gvfs-libs impacket-scripts
  init-system-helpers iproute2 ipython3 kali-defaults kali-desktop-base kali-desktop-xfce kali-grant-root kali-linux-core kali-linux-default
  kali-linux-headless kali-themes kali-themes-common kali-tweaks kismet-core libapache2-mod-php libasan6 libasound2-plugins libatrildocument3
  libatrilview3 libbinutils libc-dev-bin libc6 libc6-dev libc6-i386 libchromaprint1 libclang-common-13-dev libclang-cpp13 libclang1-13 libctf0
  libegl-mesa0 libfreerdp-client2-2 libfreerdp2-2 libgbm1 libgcc-11-dev libgd3 libgdk-pixbuf-2.0-0 libgeos-c1v5 libgeotiff5 libgirepository-1.0-1
  libgl1-mesa-dri libglapi-mesa libglu1-mesa libglx-mesa0 libgs9-common libgstreamer-plugins-bad1.0-0 libgupnp-igd-1.0-4 libgvc6 libgxps2 libheif1
  libhttp-message-perl libinput-bin libinput10 libjavascriptcoregtk-4.0-18 libldb2 libllvm13 libmagickcore-6.q16-6 libmagickcore-6.q16-6-extra
  libmm-glib0 libnet1 libnewt0.52 libnma-common libnma0 libobjc-11-dev libopenconnect5 libpocl2 libpocl2-common libpolkit-agent-1-0
  libpolkit-gobject-1-0 libpoppler-glib8 libpulse-mainloop-glib0 libpulse0 libpulsedsp libpython3-dev libpython3-stdlib libqmi-glib5 libqmi-proxy
  libqt5charts5 libqt5core5a libqt5dbus5 libqt5designer5 libqt5gui5 libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediagsttools5
  libqt5multimediawidgets5 libqt5network5 libqt5positioning5 libqt5printsupport5 libqt5qml5 libqt5qmlmodels5 libqt5quick5 libqt5sensors5 libqt5sql5
  libqt5sql5-sqlite libqt5svg5 libqt5test5 libqt5webchannel5 libqt5webkit5 libqt5widgets5 libqt5x11extras5 libqt5xml5 libsane-common libsane1
  libsmbclient libsndfile1 libspandsp2 libspatialite7 libspectre1 libstdc++-11-dev libtalloc2 libtdb1 libtevent0 libtiff5 libtsan0 libupower-glib3
  libwacom-bin libwacom-common libwebkit2gtk-4.0-37 libwebpdemux2 libwebpmux3 libwinpr2-2 libwmf0.2-7 libxatracker2 lightdm-gtk-greeter-settings
  linux-image-amd64 llvm-13 llvm-13-dev llvm-13-linker-tools llvm-13-runtime llvm-13-tools mesa-va-drivers mesa-vdpau-drivers mesa-vulkan-drivers
  metasploit-framework mitmproxy modemmanager network-manager-fortisslvpn network-manager-fortisslvpn-gnome network-manager-gnome
  network-manager-l2tp network-manager-l2tp-gnome network-manager-openconnect network-manager-openconnect-gnome network-manager-openvpn
  network-manager-openvpn-gnome network-manager-pptp network-manager-pptp-gnome network-manager-vpnc network-manager-vpnc-gnome nfs-common onboard
  openconnect pgcli php php-common php-mysql pocl-opencl-icd policykit-1 postgresql powershell-empire procps pulseaudio pulseaudio-module-bluetooth
  pulseaudio-utils pyqt5-dev-tools python-pastedeploy-tpl python-tables-data python3 python3-aiohttp python3-apt python3-bleach python3-bottleneck
  python3-brlapi python3-brotli python3-cairo python3-cbor python3-cffi-backend python3-dbus python3-debian python3-dev python3-dnspython
  python3-flasgger python3-flask-limiter python3-fonttools python3-frozenlist python3-gdal python3-gi python3-gi-cairo python3-gpg python3-greenlet
  python3-hiredis python3-ipython python3-jaraco.text python3-jsonschema python3-kiwisolver python3-ldb python3-limits python3-llvmlite python3-lxml
  python3-lz4 python3-markupsafe python3-matplotlib python3-maxminddb python3-minimal python3-msgpack python3-multidict python3-mysqldb python3-nassl
  python3-netifaces python3-newt python3-numexpr python3-numpy python3-pandas python3-pandas-lib python3-pastedeploy python3-pcapy python3-pgspecial
  python3-pil python3-pil.imagetk python3-pluggy python3-protobuf python3-psycopg2 python3-pycares python3-pycurl python3-pygraphviz python3-pymssql
  python3-pyproj python3-pyqt5 python3-pyqt5.sip python3-pyqtgraph python3-pyrsistent python3-pytest python3-redis python3-rich
  python3-ruamel.yaml.clib python3-samba python3-scipy python3-selenium python3-setproctitle python3-snappy python3-sqlalchemy python3-sqlalchemy-ext
  python3-sympy python3-tables python3-tables-lib python3-talloc python3-tdb python3-tzlocal python3-ubjson python3-ufolib2 python3-ujson
  python3-urwid python3-uvloop python3-wsaccel python3-yaml python3-yara python3-yarl python3-zope.interface qt5-gtk-platformtheme qt5ct
  qtbase5-dev-tools qterminal qtermwidget5-data ruby ruby-cms-scanner ruby-dev ruby-ffi ruby-nokogiri ruby-yajl samba samba-common samba-common-bin
  samba-dsdb-modules samba-libs samba-vfs-modules sane-utils smbclient tcpreplay telnet tftp tshark udisks2 upower vboot-kernel-utils vboot-utils
  winexe wireshark wireshark-common wireshark-qt wpscan x11-apps xfce4-screenshooter xserver-xorg-core xserver-xorg-input-libinput
  xserver-xorg-video-amdgpu xserver-xorg-video-ati xserver-xorg-video-fbdev xserver-xorg-video-nouveau xserver-xorg-video-radeon
  xserver-xorg-video-vesa xserver-xorg-video-vmware zenity
0 upgraded, 0 newly installed, 0 to remove and 347 not upgraded.
Checking if all required tools are installed
ToriFY is already installed
geoip-bin is already installed
sshpass is already installed
nipe is already installed
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    16  100    16    0     0     12      0  0:00:01  0:00:01 --:--:--    12
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100     3  100     3    0     0      2      0  0:00:01  0:00:01 --:--:--     2
Your Connection is secure
Your Spoofed IP Address is: 185.220.101.175
Your Spoofed Country:
GeoIP Country Edition: DE, Germany
Connecting to Remote Server
 19:52:06 up  1:27,  1 user,  load average: 0.20, 0.05, 0.01
Your IP address
103.252.200.97
Country:
GeoIP Country Edition: SG, Singapore
Your Whois data is saved into:
/home/kali/whois.txt
/home/kali/.local/share/Trash/files/whois.txt
/home/kali/.local/share/Trash/info/whois.txt.trashinfo
Your Nmap data is saved into:
/home/kali/scanme.txt
/home/kali/.local/share/Trash/files/scanme.txt
/home/kali/.local/share/Trash/info/scanme.txt.trashinfo
```

Final Result: If you successfully anonymized yourself, program will proceed as shown by the example on the left.

Credits

Mr James Lim, Head Trainer, Centre for Cybersecurity

Mr Evans Amoany(Sudoer), https://www.redhat.com/sysadmin/users/evans-amoany

Mr Kris Koishigawa: https://www.freecodecamp.org/news/author/kris/

Reference

sudo apt-get update/upgrade: https://www.freecodecamp.org/news/sudo-apt-get-update-vs-upgrade-what-is-the-difference/#:~:text=The sudo apt-get upgrade,want to perform the upgrades

dpkg-query: https://man7.org/linux/man-pages/man1/dpkg-query.1.html

Geoip-bin: https://packages.debian.org/stretch/geoip-bin

sshpass: https://www.redhat.com/sysadmin/ssh-automation-sshpass

nipe: https://github.com/htrgouvea/nipe