

# DNS TUNNELING DETECTOR

Running Simulation Presentation

Topics in Network Security 1/10

Omer Bornstein, Alex Degtiarov

# Running Simulation Presentation

Programs showed in this running example:

- DNS server - dnsmasq
- DNS Tunnel:
  - ❖ Client - dnscat client
  - ❖ Server- dnscat server
- DNS detector- Designed by us

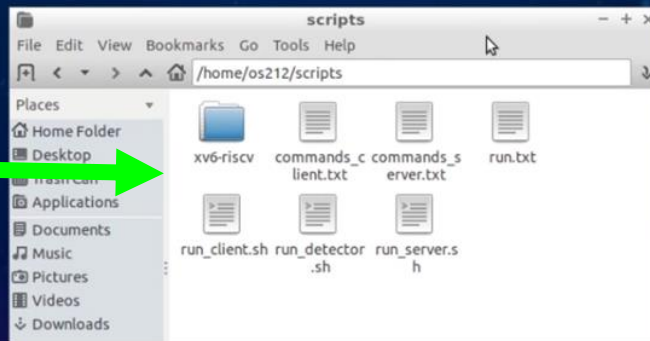
# Running Simulation Presentation

- Goals of the running simulation:
  - ❑ Explain the program's GUI
  - ❑ Explain how to run the simulation
  - ❑ Detect DNS tunnel in real time
  - ❑ Block the DNS tunnel

```
os212@os212-lubuntu: ~/scripts  
File Edit Tabs Help
```

```
...  
...  
...  
...  
...  
...  
...  
...  
...  
...  
...  
...  
...  
...  
...  
...  
...  
...  
going to save  
saved  
saved blocked  
Thread Exiting  
os212@os212-lubuntu:~/scripts$ ./run_detector.sh
```

Script are in the folder called "scripts "

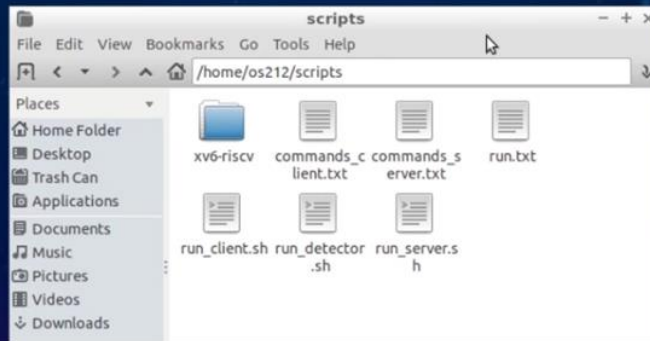


```
os212@os212-lubuntu: ~/scripts
File Edit Tabs Help
command (os212-lubuntu) l> ping
Ping!
command (os212-lubuntu) l> ping
Ping!
command (os212-lubuntu) l> ping
Ping!
command (os212-lubuntu) l> ping
Ping!
command (os212-lubuntu) l>
command (os212-lubuntu) l> Wrote 1048576 bytes from /home/os212/dnscat2/client/s
ecretFile to /home/os212/dnscat2/server/secretFile!
Pong!
Pong!
Pong!
Pong!
Pong!
Pong!
Pong!
Pong!
Pong!
Pong!
command (os212-lubuntu) l>
command (os212-lubuntu) l> Input thread is over
os212@os212-lubuntu: ~/scripts
```

Run our detector program with:

```
./run_detector.sh
```

```
going to save
saved
saved blocked
Thread Exiting
os212@os212-lubuntu:~/scripts$ ./run_detector.sh
```

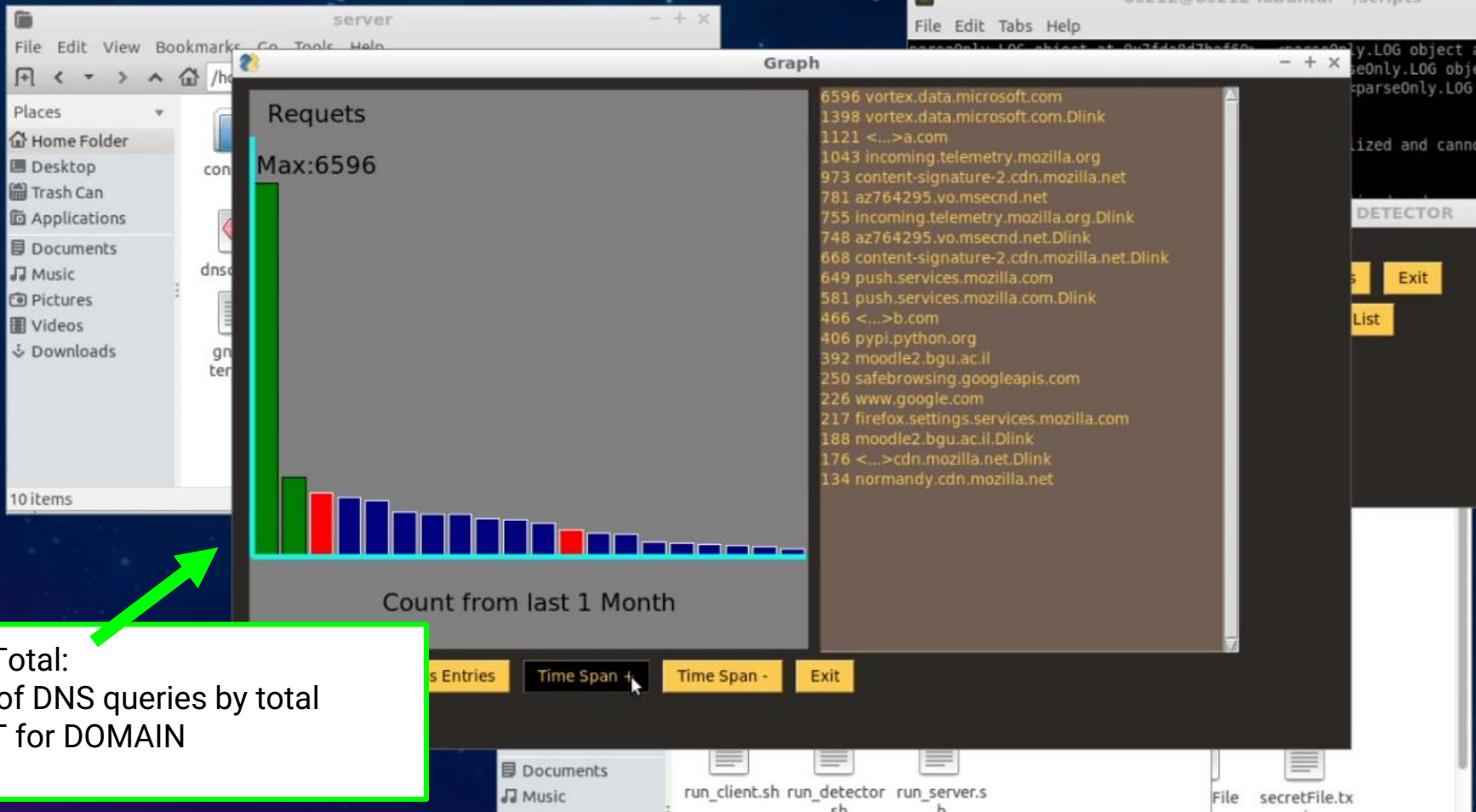













Show Total:  
Graph of DNS queries by total  
COUNT for DOMAIN

[illegible]

DNS Tunnel Detector

Buttons: Show Total, Show Peaks, Exit, Approved List, Blocked List



Bookmarks Go Tools Help

/home/os212/scripts

- xv6-riscv
- commands\_c
- commands\_s
- run.txt
- run\_client.sh
- run\_detector.sh
- run\_server.sh

```

os212@os212-lubuntu: ~/scripts
File Edit Tabs Help

command (os212-lubuntu) 1> ping
Ping!
command (os212-lubuntu) 1> ping
Ping!
command (os212-lubuntu) 1> ping
Ping!
command (os212-lubuntu) 1> ping
Ping!
command (os212-lubuntu) 1>
command (os212-lubuntu) 1> Wrote 1048576 bytes from /home/os212/dnscat
secretFile to /home/os212/dnscat2/server/secretFile!
Pong!
Pong!
Pong!
Pong!
Pong!
Pong!
Pong!
Pong!
Pong!
Pong!

command (os212-lubuntu) 1>
command (os212-lubuntu) 1> Input thread is over
os212@os212-lubuntu: ~/scripts$

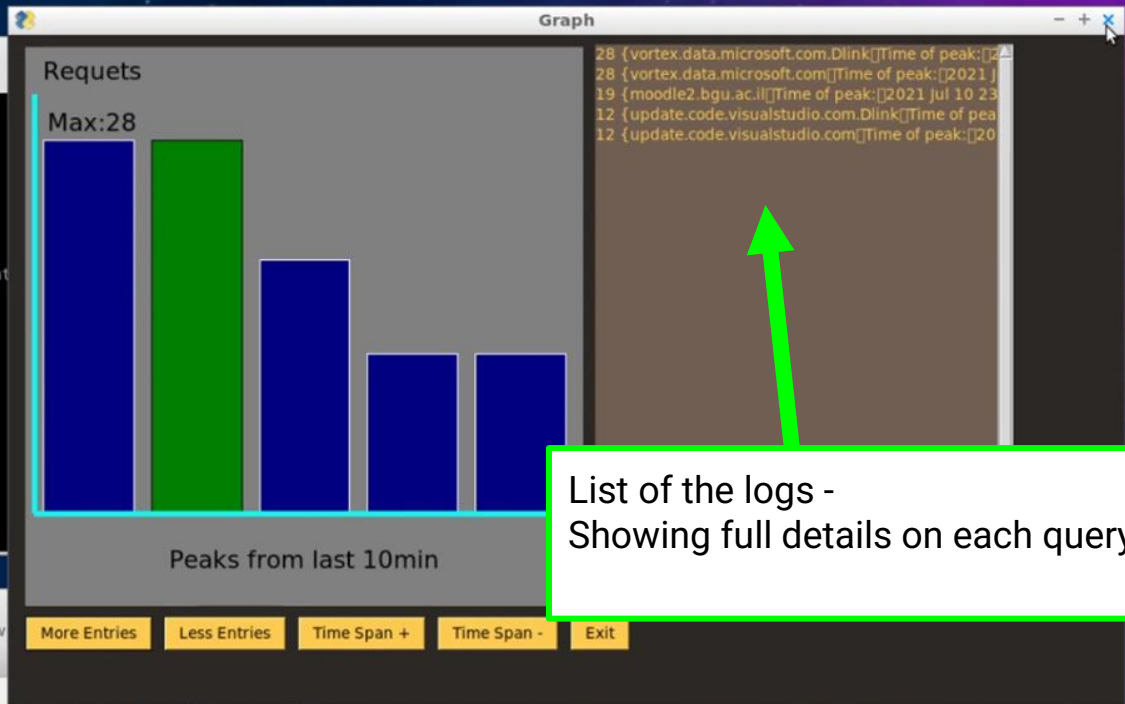
```



TOP (N) peaks from last (T) time,  
Control N and T with the buttons.

```
os212@os212-lubuntu: ~/scripts
```

	File	Edit	Tabs	Help
command (os212-lubuntu) 1>	ping			
Ping!				
command (os212-lubuntu) 1>	ping			
Ping!				
command (os212-lubuntu) 1>	ping			
Ping!				
command (os212-lubuntu) 1>	ping			
Ping!				
command (os212-lubuntu) 1>				
command (os212-lubuntu) 1>	Wrote 1048576 bytes from /home/os212/dnscat2/secretFile to /home/os212/dnscat2/server/secretFile!			
Pong!				
Pong!				
Pong!				
Pong!				
Pong!				
Pong!				
Pong!				
Pong!				
command (os212-lubuntu) 1>				
command (os212-lubuntu) 1>	Input thread is over			
os212@os212-lubuntu:~/scripts\$				



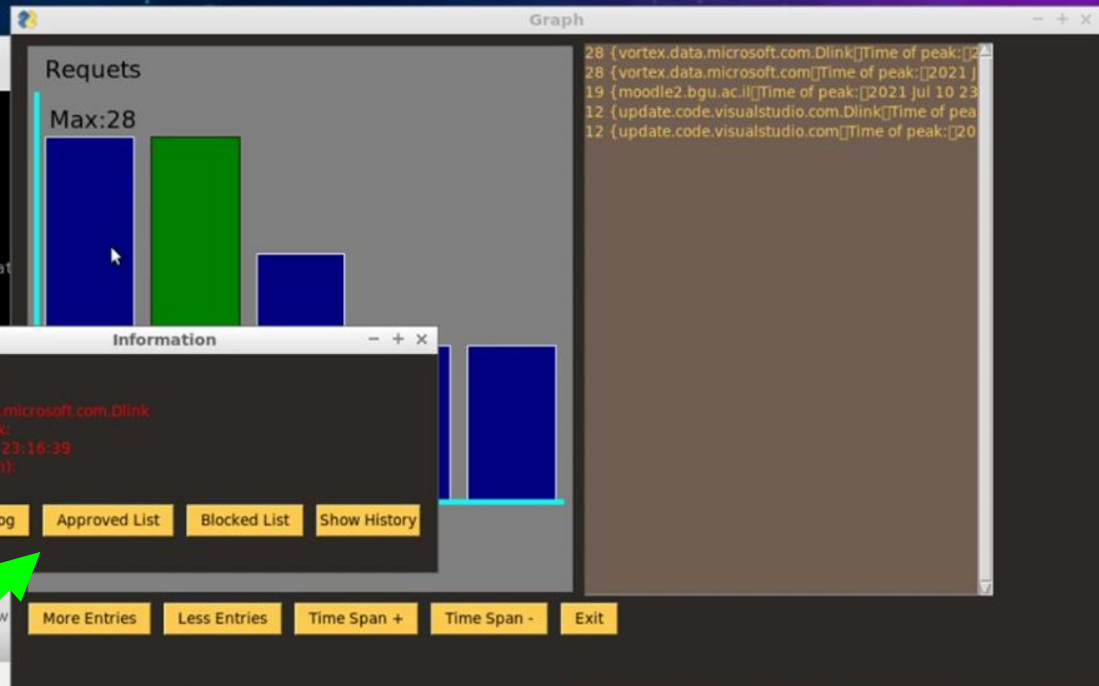
```
os212@os212-lubuntu: ~/scripts
File Edit Tabs Help
command (os212-lubuntu) 1> ping
Ping!
command (os212-lubuntu) 1> ping
Ping!
command (os212-lubuntu) 1> ping
Ping!
command (os212-lubuntu) 1> ping
Ping!
command (os212-lubuntu) 1>
command (os212-lubuntu) 1> Wrote 1048576 bytes from /home/os212/dnscat
secretFile to /home/os212/dnscat2/server/secretFile!
```

Domains who are colored Green are approved by the user.  
Red domains are blocked by the program or by the user.  
Blue domains are neither .





```
os212@os212-lubuntu: ~/scripts
File Edit Tabs Help
command (os212-lubuntu) l> ping
Ping!
command (os212-lubuntu) l> ping
Ping!
command (os212-lubuntu) l> ping
Ping!
command (os212-lubuntu) l> ping
Ping!
command (os212-lubuntu) l> ping
Ping!
command (os212-lubuntu) l> Wrote 1048576 bytes from /home/os212/dnscat
secretFile to /home/os212/dnscat2/server/secretFile!
Ping!
Ping!
Ping!
Ping!
Ping!
Ping!
Ping!
Ping!
Ping!
Ping!
command (os212-lubuntu) l>
command (os212-lubuntu) l> Input thread is over
os212@os212-lubuntu:~/scripts$
```

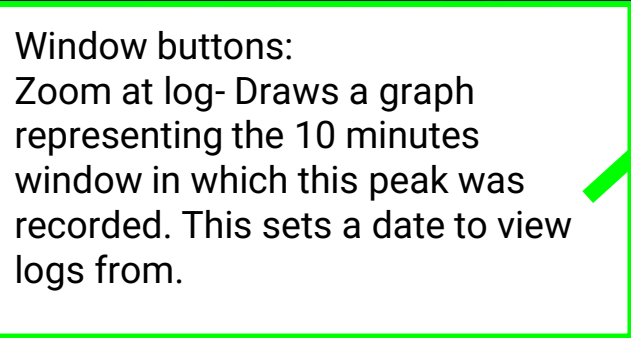


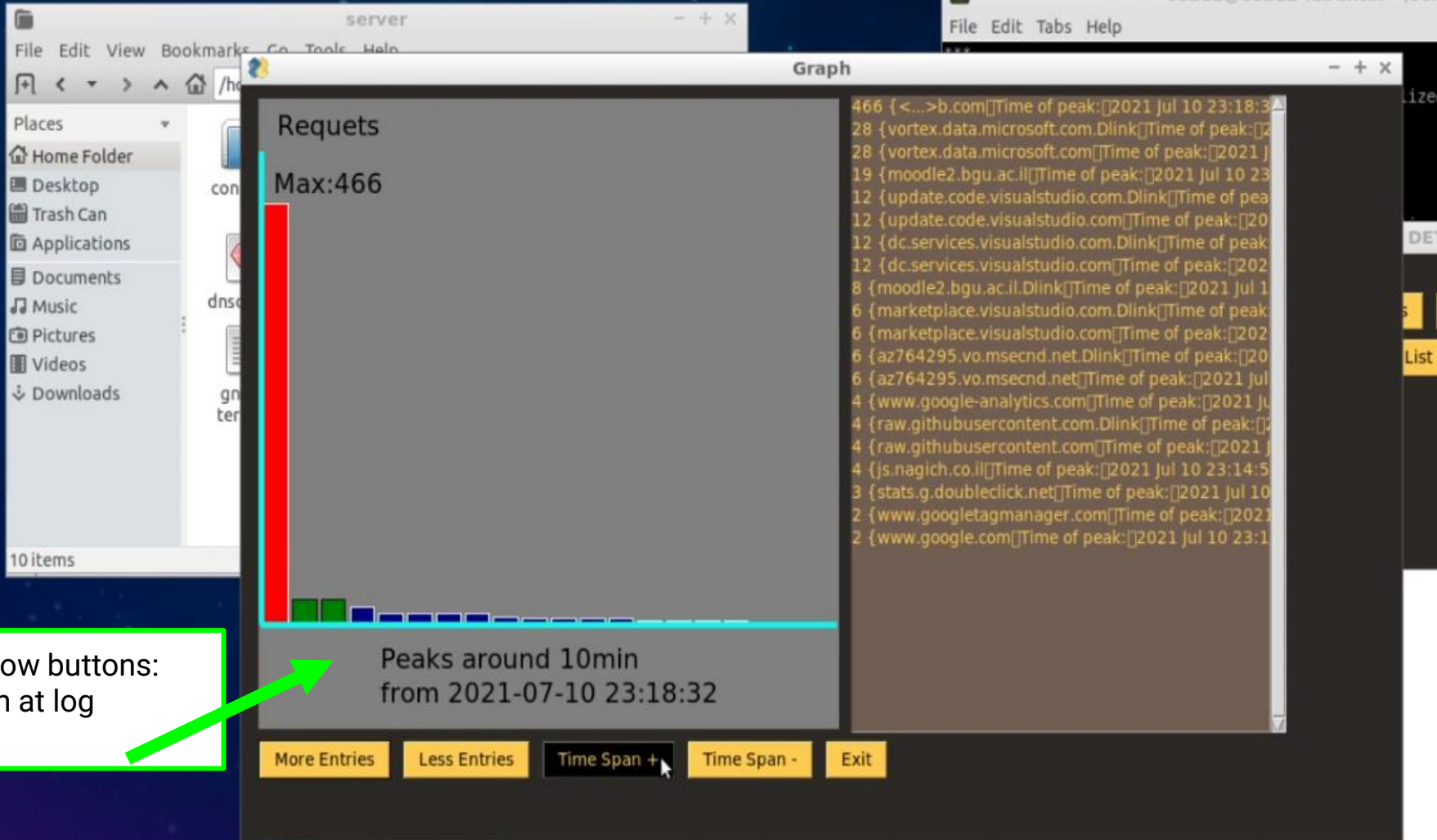
information window includes full  
log information for the specific  
peak: Domain, Date , Count.



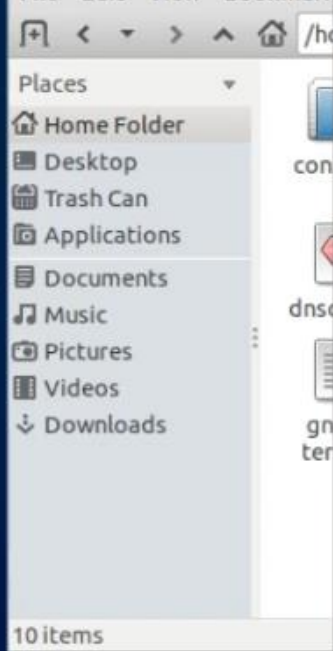






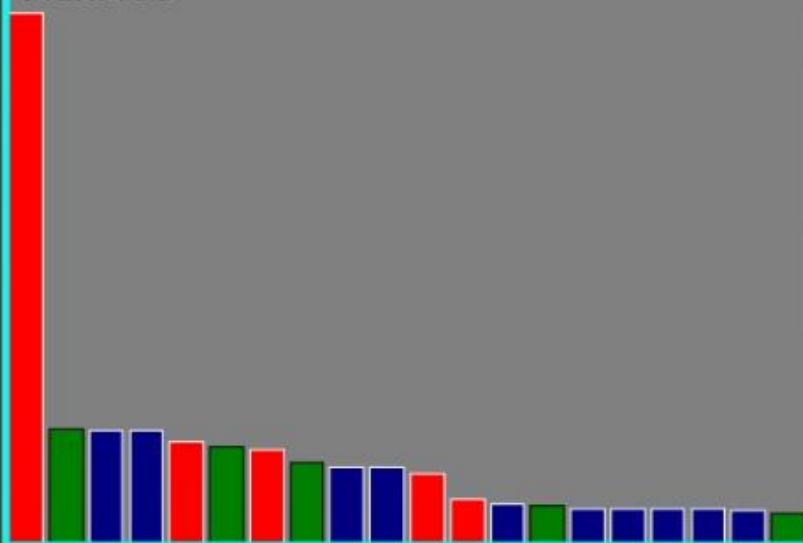


Window buttons:  
Zoom at log



## Requets

Max:466



Peaks around 1 Day  
from 2021-07-10 23:18:32

More Entries

Less Entries

Time Span +

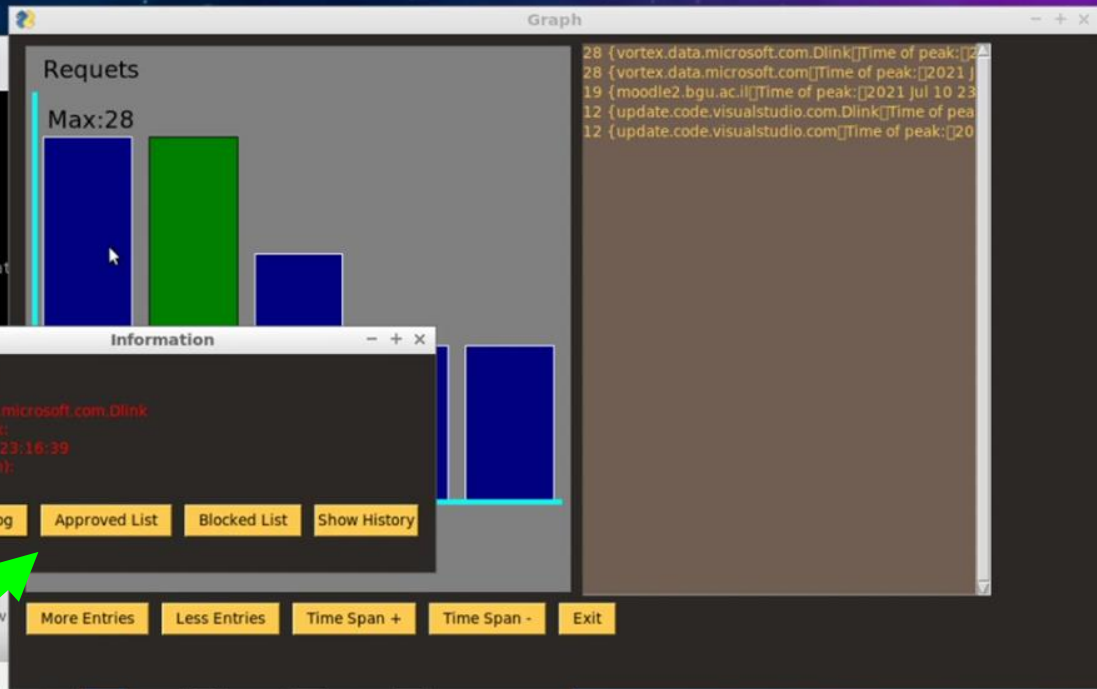
Time Span -

Exit

```
466 {<...>b.com[]Time of peak:[]2021 Jul 10 23:18:32}
102 {vortex.data.microsoft.com[]Time of peak:[]2021
100 {push.services.mozilla.com.Dlink[]Time of peak:[]
100 {push.services.mozilla.com[]Time of peak:[]2021
91 {<...>a.com[]Time of peak:[]2021 Jul 10 13:20:25
86 {vortex.data.microsoft.com.Dlink[]Time of peak:[]2
83 {<...>a.com[]Time of peak:[]2021 Jul 10 15:33:08
72 {vortex.data.microsoft.com[]Time of peak:[]2021 J
68 {incoming.telemetry.mozilla.org.Dlink[]Time of pe
68 {incoming.telemetry.mozilla.org[]Time of peak:[]2
63 {<...>a.com[]Time of peak:[]2021 Jul 10 15:43:20
40 {<...>a.com[]Time of peak:[]2021 Jul 10 15:04:18
36 {incoming.telemetry.mozilla.org[]Time of peak:[]2
34 {vortex.data.microsoft.com[]Time of peak:[]2021 J
32 {moodle2.bgu.ac.il.Dlink[]Time of peak:[]2021 Jul
32 {moodle2.bgu.ac.il[]Time of peak:[]2021 Jul 10 14
32 {incoming.telemetry.mozilla.org.Dlink[]Time of pe
32 {incoming.telemetry.mozilla.org[]Time of peak:[]2
30 {detectportal.firefox.com[]Time of peak:[]2021 Jul
28 {vortex.data.microsoft.com.Dlink[]Time of peak:[]2
```

Window buttons:  
Zoom at log

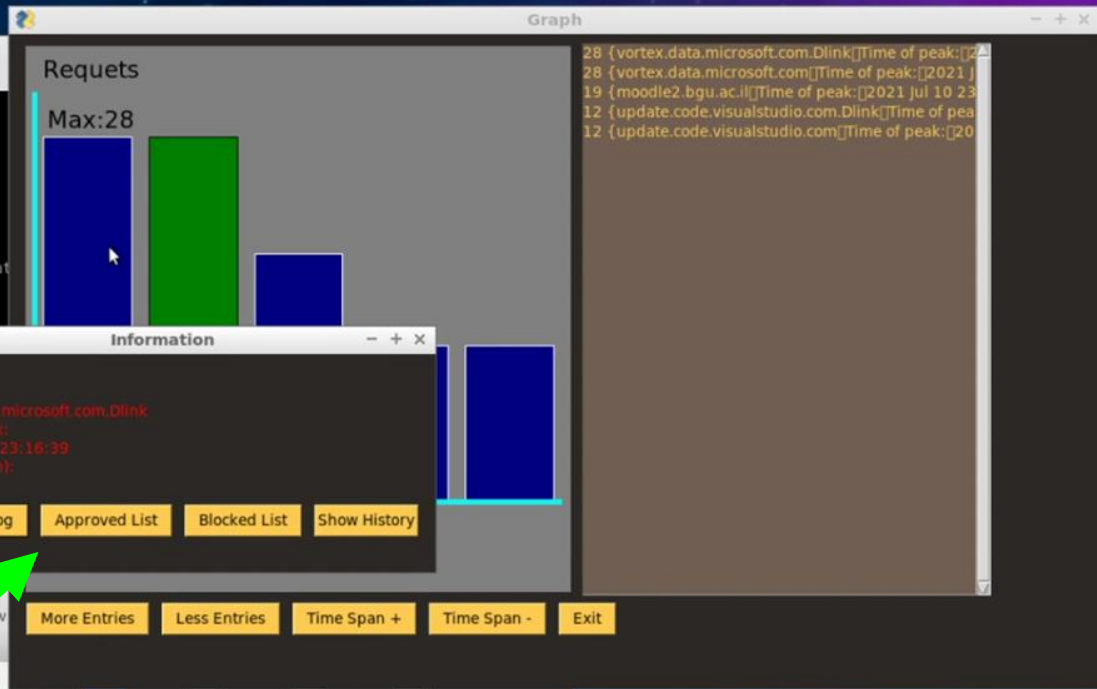
```
os212@os212-lubuntu: ~/scripts
File Edit Tabs Help
command (os212-lubuntu) 1> ping
Ping!
command (os212-lubuntu) 1> ping
Ping!
command (os212-lubuntu) 1> ping
Ping!
command (os212-lubuntu) 1> ping
Ping!
command (os212-lubuntu) 1> ping
Ping!
command (os212-lubuntu) 1>
command (os212-lubuntu) 1> Wrote 1048576 bytes from /home/os212/dnscat
secretFile to /home/os212/dnscat2/server/secretFile!
Pong!
Pong!
Pong!
Pong!
Pong!
Pong!
Pong!
Pong!
Pong!
Pong!
Pong!
command (os212-lubuntu) 1>
command (os212-lubuntu) 1> Input thread is over
os212@os212-lubuntu:~/scripts$
```



Window buttons:

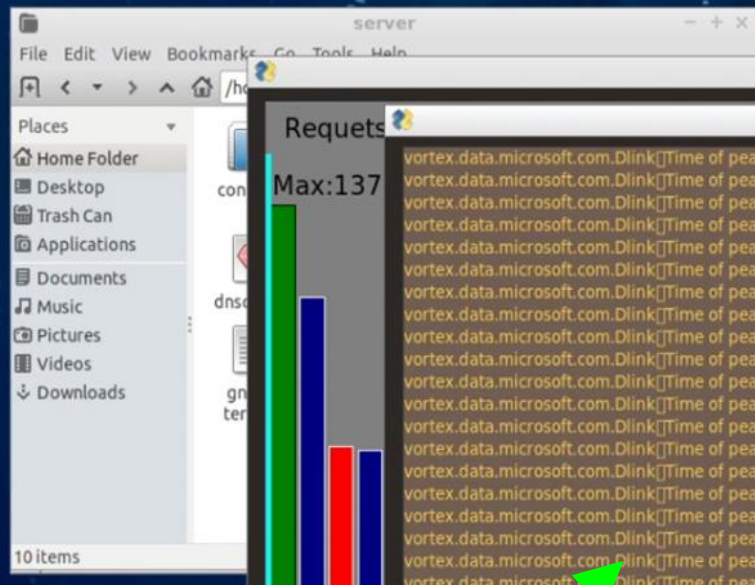
Approved list / Blocked list -  
inserts the domain to the selected  
list

```
os212@os212-lubuntu: ~/scripts
File Edit Tabs Help
command (os212-lubuntu) 1> ping
Ping!
command (os212-lubuntu) 1> ping
Ping!
command (os212-lubuntu) 1> ping
Ping!
command (os212-lubuntu) 1> ping
Ping!
command (os212-lubuntu) 1> ping
Ping!
command (os212-lubuntu) 1>
command (os212-lubuntu) 1> Wrote 1048576 bytes from /home/os212/dnscat
secretFile to /home/os212/dnscat2/server/secretFile!
Pong!
Pong!
Pong!
Pong!
Pong!
Pong!
Pong!
Pong!
Pong!
Pong!
Pong!
Pong!
command (os212-lubuntu) 1>
command (os212-lubuntu) 1> Input thread is over
os212@os212-lubuntu:~/scripts$
```



Window buttons:  
Show history- show a full list of  
logs for the specific domain





Requests

Max:137



Window buttons:  
Show history- show a full list of  
logs for the specific domain



Graph

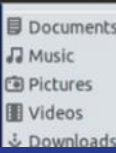
Window Title

```
vortex.data.microsoft.com.Dlink[]Time of peak:[2021 Jul 10 23:16:39[]count(10min):[]28
vortex.data.microsoft.com.Dlink[]Time of peak:[2021 Jul 10 15:02:48[]count(10min):[]2
vortex.data.microsoft.com.Dlink[]Time of peak:[2021 Jul 10 14:08:54[]count(10min):[]22
vortex.data.microsoft.com.Dlink[]Time of peak:[2021 Jul 10 13:07:59[]count(10min):[]86
vortex.data.microsoft.com.Dlink[]Time of peak:[2021 Jul 09 19:31:00[]count(10min):[]1
vortex.data.microsoft.com.Dlink[]Time of peak:[2021 Jul 09 19:20:35[]count(10min):[]16
vortex.data.microsoft.com.Dlink[]Time of peak:[2021 Jul 09 19:10:16[]count(10min):[]87
vortex.data.microsoft.com.Dlink[]Time of peak:[2021 Jul 09 19:00:16[]count(10min):[]101
vortex.data.microsoft.com.Dlink[]Time of peak:[2021 Jul 09 18:50:12[]count(10min):[]68
vortex.data.microsoft.com.Dlink[]Time of peak:[2021 Jul 09 18:40:03[]count(10min):[]55
vortex.data.microsoft.com.Dlink[]Time of peak:[2021 Jul 09 18:28:57[]count(10min):[]66
vortex.data.microsoft.com.Dlink[]Time of peak:[2021 Jul 09 18:13:35[]count(10min):[]120
vortex.data.microsoft.com.Dlink[]Time of peak:[2021 Jul 09 18:03:00[]count(10min):[]150
vortex.data.microsoft.com.Dlink[]Time of peak:[2021 Jul 09 17:53:00[]count(10min):[]128
vortex.data.microsoft.com.Dlink[]Time of peak:[2021 Jul 09 17:42:59[]count(10min):[]136
vortex.data.microsoft.com.Dlink[]Time of peak:[2021 Jul 09 17:32:45[]count(10min):[]4
vortex.data.microsoft.com.Dlink[]Time of peak:[2021 Jul 03 10:38:35[]count(10min):[]2
vortex.data.microsoft.com.Dlink[]Time of peak:[2021 Jul 03 10:23:43[]count(10min):[]65
vortex.data.microsoft.com.Dlink[]Time of peak:[2021 Jul 02 23:07:28[]count(10min):[]7
vortex.data.microsoft.com.Dlink[]Time of peak:[2021 Jul 02 22:57:10[]count(10min):[]36
vortex.data.microsoft.com.Dlink[]Time of peak:[2021 Jul 02 22:42:42[]count(10min):[]42
vortex.data.microsoft.com.Dlink[]Time of peak:[2021 Jul 02 22:32:41[]count(10min):[]98
vortex.data.microsoft.com.Dlink[]Time of peak:[2021 Jul 02 22:17:48[]count(10min):[]4
vortex.data.microsoft.com.Dlink[]Time of peak:[2021 Jul 02 22:07:32[]count(10min):[]62
vortex.data.microsoft.com.Dlink[]Time of peak:[2021 Jul 02 15:54:47[]count(10min):[]12
```

DETECTOR

Exit

List



run\_client.sh run\_detector run\_server.s  
.sh h

File secretFile.tx  
t

Free space: 8.8 GiB (Total: 19.6 GiB)

[illegible]

DNS Tunnel Detector

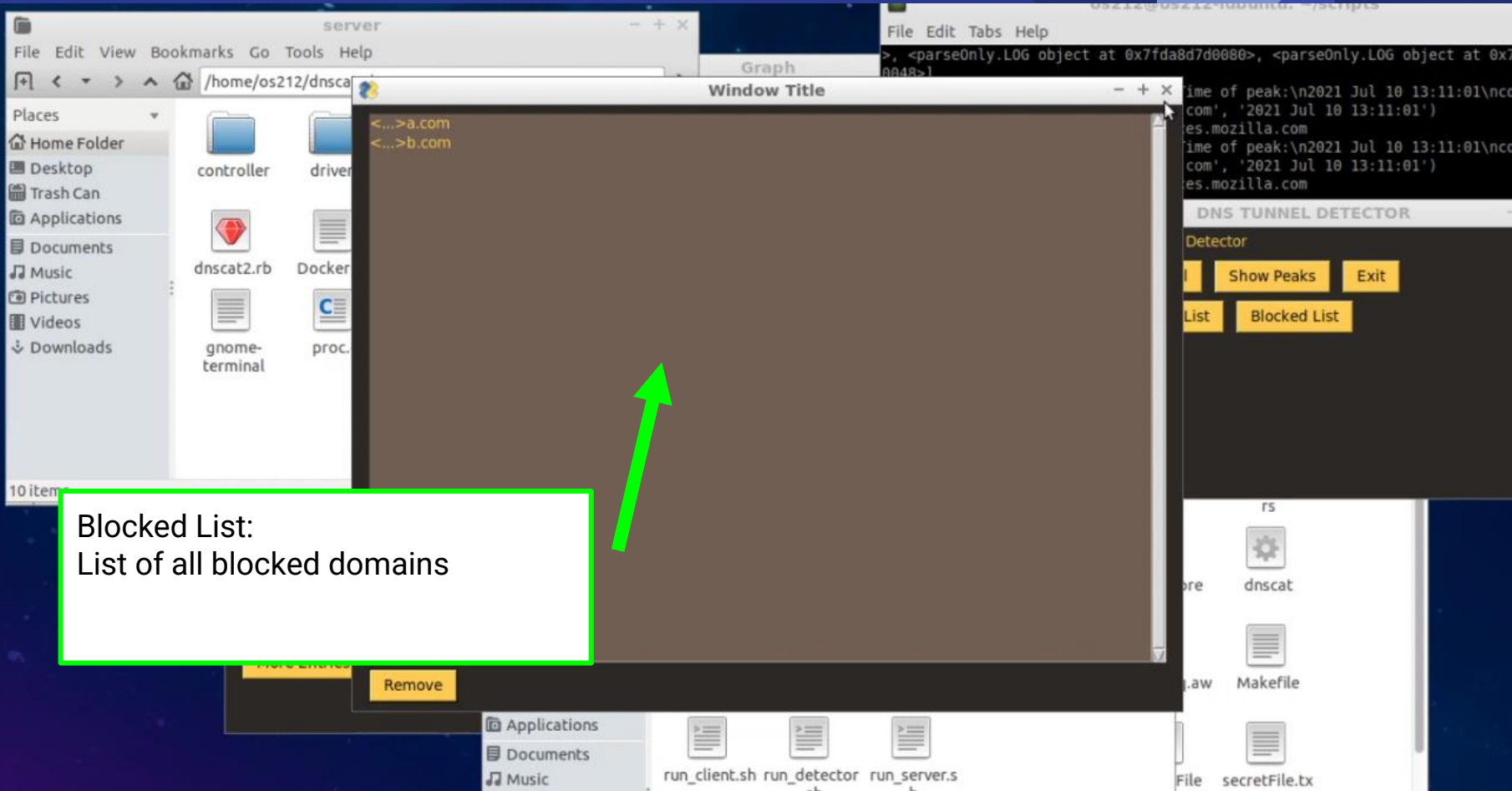
Show Total Show Peaks Exit

Approved List Blocked List

home/os212/scripts

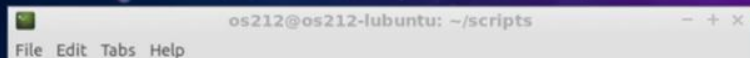
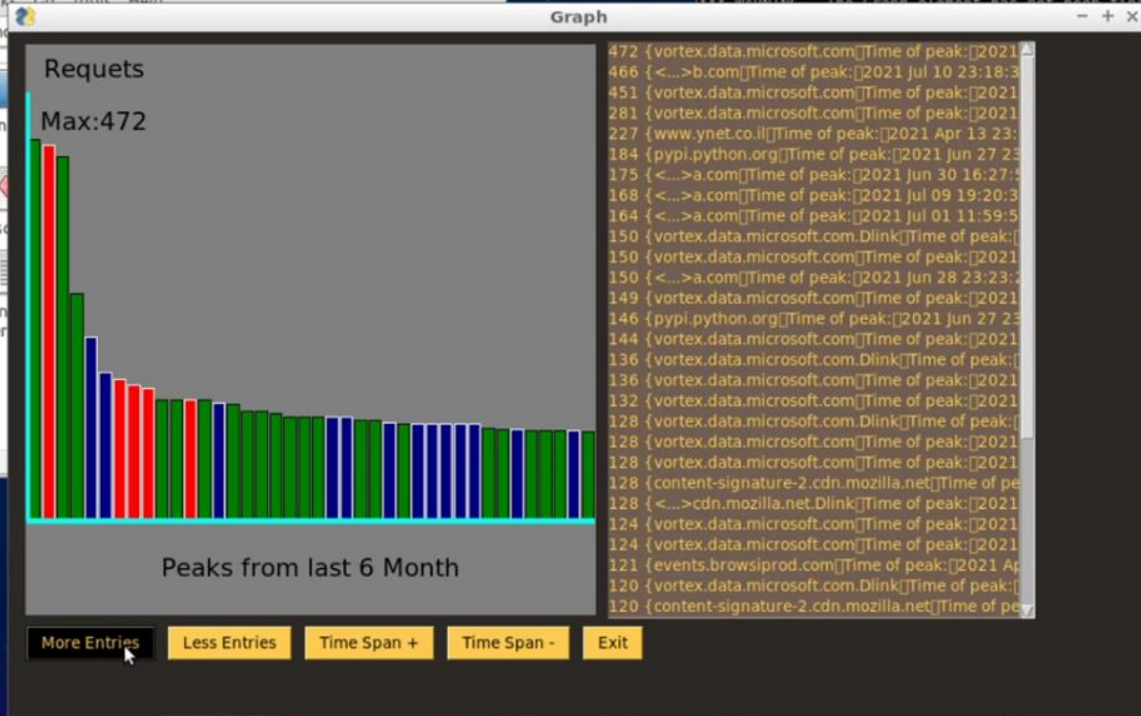
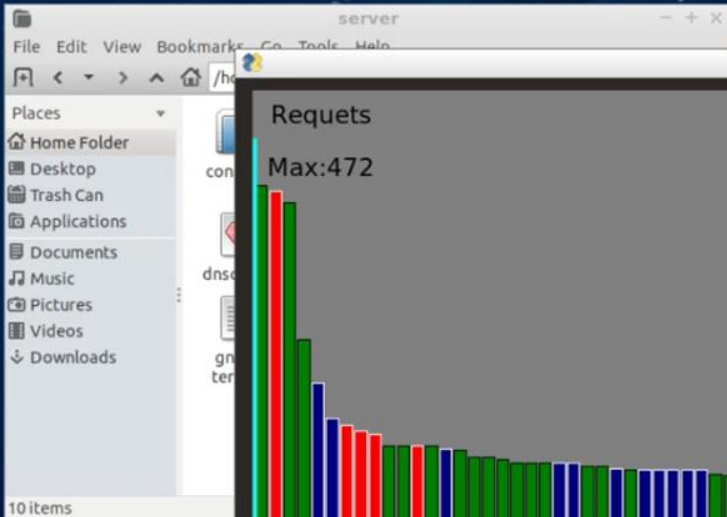
xv6-riscv commands\_client.txt commands\_server.txt run.txt

run\_client.sh run\_detector.sh run\_server.sh

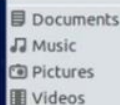








```
File Edit Tabs Help
The Graph element has not been finalized and cannot be drawn upon
472 {vortex.data.microsoft.com}Time of peak:[2021
466 {<...>b.com}Time of peak:[2021 Jul 10 23:18:3
451 {vortex.data.microsoft.com}Time of peak:[2021
281 {vortex.data.microsoft.com}Time of peak:[2021
227 {www.ynet.co.il}Time of peak:[2021 Apr 13 23:
184 {pypi.python.org}Time of peak:[2021 Jun 27 23
175 {<...>a.com}Time of peak:[2021 Jun 30 16:27:5
168 {<...>a.com}Time of peak:[2021 Jul 09 19:20:3
164 {<...>a.com}Time of peak:[2021 Jul 01 11:59:5
150 {vortex.data.microsoft.com}Dlink}Time of peak:[
150 {vortex.data.microsoft.com}Time of peak:[2021
150 {<...>a.com}Time of peak:[2021 Jun 28 23:23:2
149 {vortex.data.microsoft.com}Time of peak:[2021
146 {pypi.python.org}Time of peak:[2021 Jun 27 23
144 {vortex.data.microsoft.com}Time of peak:[2021
136 {vortex.data.microsoft.com}Dlink}Time of peak:[
136 {vortex.data.microsoft.com}Time of peak:[2021
132 {vortex.data.microsoft.com}Time of peak:[2021
128 {vortex.data.microsoft.com}Dlink}Time of peak:[
128 {vortex.data.microsoft.com}Time of peak:[2021
128 {vortex.data.microsoft.com}Time of peak:[2021
128 {content-signature-2.cdn.mozilla.net}Time of pe
128 {<...>cdn.mozilla.net}Dlink}Time of peak:[2021
124 {vortex.data.microsoft.com}Time of peak:[2021
124 {vortex.data.microsoft.com}Time of peak:[2021
121 {events.browsiprod.com}Time of peak:[2021 Ap
120 {vortex.data.microsoft.com}Dlink}Time of peak:[
120 {content-signature-2.cdn.mozilla.net}Time of pe
```



run\_client.sh run\_detector run\_server.s



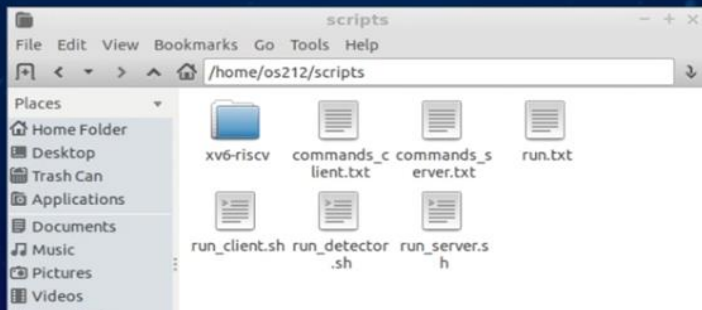
# Running Simulation Presentation

- Goals of the running simulation:
  - ❑ Explain the program's GUI
  - ❑ Explain how to run the simulation
  - ❑ Detect DNS tunnel in real time
  - ❑ Block the DNS tunnel

```
os212@os212-lubuntu: ~/scripts
File Edit Tabs Help
command (os212-lubuntu) 1> ping
Ping!
command (os212-lubuntu) 1> ping
Ping!
command (os212-lubuntu) 1> ping
Ping!
command (os212-lubuntu) 1> ping
Ping!
command (os212-lubuntu) 1> Wrote 1048576 bytes from /home/os212/dn
secretFile to /home/os212/dnscat2/server/secretFile!
Ping!
Ping!
Ping!
Ping!
Ping!
Ping!
Ping!
Ping!
Ping!
Ping!
command (os212-lubuntu) 1>
command (os212-lubuntu) 1> Input thread is over
os212@os212-lubuntu:~/scripts$ ./run_server.sh
```

Our DNS server was pre-configured to support this simulation, We read the logs acquired from the server

```
os212@os212-lubuntu: ~/scripts
File Edit Tabs Help
Jul 10 23:17:57 dnsmasq[28142]: using nameserver 8.8.8.8#53
Jul 10 23:17:57 dnsmasq[28142]: using nameserver 127.0.0.1#53531 for domain b.co
using nameserver 127.0.0.1#53531 for default
using namese
read /etc/ho
read /home/o
.Dlink\nTime
crosoft.com.D
data.microsof
graph+UP
graph+UP
graph+UP
*** WARNING - The Graph element has not been
***
Call Window.Finalize() prior to this operati
```







# Running Simulation Presentation

- Goals of the running simulation:
  - ❑ Explain the program's GUI
  - ❑ Explain how to run the simulation
  - ❑ Detect DNS tunnel in real time
  - ❑ Block the DNS tunnel



Server is running

Client is running



```
os212@os212-lubuntu: ~/scripts
File Edit Tabs Help
New window created: 1
history size (session) => 1000
(not set) l> Session 1 security: ENCRYPTED BUT *NOT* VALIDATED
For added security, please ensure the client displays the same string:

>> Deepen Sippy Roving Surfs Exotic Pony
This is a command session!

That means you can enter a dnscat2 command such as
'ping'. For a full list of clients, try 'help'.

ping
Ping!
command (os212-lubuntu) l> Pong!
ping
Ping!
command (os212-lubuntu) l> Pong!
ping
Ping!
command (os212-lubuntu) l> Pong!
ping
Ping!
command (os212-lubuntu) l> Pong!
```

Server and Client are connected through the DNS

```
os212@os212-lubuntu: ~/scripts
File Edit Tabs Help
59a654fba8c5f2118f.887902cc2bf7cbdede9b5d817e9a5387fdd2abb481f277630b17915f30cb.
1365683dc020fcb5e4435d8131c0ee727b7642831485e62df90d43564197.ea86d2c516499cee631
7bba7e57bb85def14e48dd3f665502f32.b.com is ee750189bd29ca8f2ddc65ffff8a26e348

Jul 10 23:18:43 dnsmasq[28142]: query[TXT] ab730189bda9165b118b10001f5a5fea00dff
9cb515c9b7a98b471323335.d33cf16ba68945ebd408b1029ef08cde7a42754c48fdbfe0667dbad6
93c6.410aff59c3d57e90eb31b7440467bd5d3f5420e9eff2fb87.b.com from 127.0.0.1

Jul 10 23:18:43 dnsmasq[28142]: forwarded ab730189bda9165b118b10001f5a5fea00dff
323335.d33cf16ba68945ebd408b1029ef08cde7a42754c48fdbfe0667dbad6
7e90eb31b7440467bd5d3f5420e9eff2fb87.b.com to 127.0.0.1

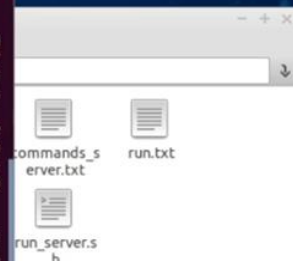
dnsmasq[28142]: reply ab730189bda9165b118b10001f5a5fea00dff
35.d33cf16ba68945ebd408b1029ef08cde7a42754c48fdbfe0667dbad6
eb31b7440467bd5d3f5420e9eff2fb87.b.com

Jul 10 23:18:43 dnsmasq[28142]: query[MX] a9cb515c9b7a98b471323335.d33cf16ba68945ebd408b1029ef08cde7a42754c48fdbfe0667dbad6
om from 127.0.0.1

Jul 10 23:18:43 dnsmasq[28142]: forwarded a9cb515c9b7a98b471323335.d33cf16ba68945ebd408b1029ef08cde7a42754c48fdbfe0667dbad6
om to 127.0.0.1
```



```
File Edit View Search terminal Help
H
Got a command: COMMAND_PING [request] :: request id: 0x0003 :: data: YSGEMDNSQXR
WJQNUPLQVJPONGMNDJOFENDHRTJQAWPASCVCNNXNZTHLLSUAWYALCREQCBEERMXLAVQCQYFGKZWPCMPW
PTBVNQZVZQWCCEDTMEYMAHARNUPHVRURGAEDTRXEIVNLLHFMFSGLEBASJTZFNCTELLVOFINXIWIZYFZXC
FZXCNAZVDLTHYKWTISIABYLLEOQHSLUAHQGLQVMFIZDTANXTWNSVMHDOCVJROMXGLOPKVYVNBABNMGT
SDWSK
[[ WARNING ]] :: Got a ping request! Responding!
Response: COMMAND_PING [response] :: request id: 0x0003 :: data: YSGEMDNSQXRWJQNU
UPLQVJPONGMNDJOFENDHRTJQAWPASCVCNNXNZTHLLSUAWYALCREQCBEERMXLAVQCQYFGKZWPCMPWPTBV
NQZVZQWCCEDTMEYMAHARNUPHVRURGAEDTRXEIVNLLHFMFSGLEBASJTZFNCTELLVOFINXIWIZYFZXC
NAZVDLTHYKWTISIABYLLEOQHSLUAHQGLQVMFIZDTANXTWNSVMHDOCVJROMXGLOPKVYVNBABNMGTSDWS
K
Got a command: COMMAND_PING [request] :: request id: 0x0004 :: data: KXXNUTUHLFP
AENCGAEPJEKRSNTIYSEJEPLMPUEKBZEUOKLQIGVQIYABSDQPEECRKXSFTJUXCMCTOZQHXZFSDHMMDBQ
TANAXGIZMOYRSYBIMCHOFKNGUFLQDAXPSRPQKXDUJVEDGWYAVANMFCIUHZRWRMGSCIVVDQXJFWJXFI
PMUBVPXNAOKRJWIAVCMCPDRIZNTNSUKBITNFWCDXIUJFHEQOEXDHSYIDXESKRHOIXQPOPCCAUCAWAO
CSDXO
[[ WARNING ]] :: Got a ping request! Responding!
Response: COMMAND_PING [response] :: request id: 0x0004 :: data: KXXNUTUHLFPAENC
GAEPJEKRSNTIYSEJEPLMPUEKBZEUOKLQIGVQIYABSDQPEECRKXSFTJUXCMCTOZQHXZFSDHMMDBQ
TANAXGIZMOYRSYBIMCHOFKNGUFLQDAXPSRPQKXDUJVEDGWYAVANMFCIUHZRWRMGSCIVVDQXJFWJXFI
PMUBVPXNAOKRJWIAVCMCPDRIZNTNSUKBITNFWCDXIUJFHEQOEXDHSYIDXESKRHOIXQPOPCCAUCAWAO
CSDXO
```



Server is sending Ping requests

Client answers

os212@os212-lubuntu: ~/scripts

```
File Edit Tabs Help
New window created: 1
history size (session) => 1000
(not set) l> Session 1 security: ENCRYPTED BUT *NOT* VALIDATED
For added security, please ensure the client displays the same string:
```

```
>> Deepen Sippy Roving Surfs Exotic Pony
This is a command session!
```

```
That means you can enter a dnscat2 command such as
'ping'. For a full list of clients, try 'help'.
```

```
ping
Ping!
command (os212-lubuntu) l> Pong!
ping
Ping!
command (os212-lubuntu) l> Pong!
ping
Ping!
command (os212-lubuntu) l> Pong!
ping
Ping!
command (os212-lubuntu) l> Pong!
```

File Edit View Search terminal Help

```
H
Got a command: COMMAND PING [request] :: request id: 0x0003 :: data: YSGEMDNSQXR
WJQNUPLQVJPONGMNDJOFENDHRTJQAWPASCVCNNXNZTHLLSUAWYALCREQCBEERMXLAVQCQYFGKZWPCMPW
PTBVNQZVQWCCEDTMEYMAHARNUPHVRURGAEDTRXEIVNLLHFMFSGLEBASJTZFNCTELLVOFINXIWIZY
FZXCNAZVDLTHYKWTISIABYLLEOQHSUAGLQVMFIZDTANXTWNSVMHDOCVJROMXGLOYPKVYVNBUBNMGTS
SDWSK
[[ WARNING ]] :: Got a ping request! Responding!
Response: COMMAND PING [response] :: request id: 0x0003 :: data: YSGEMDNSQXRWJQNU
UPLQVJPONGMNDJOFENDHRTJQAWPASCVCNNXNZTHLLSUAWYALCREQCBEERMXLAVQCQYFGKZWPCMPWPTBV
NQZVQWCCEDTMEYMAHARNUPHVRURGAEDTRXEIVNLLHFMFSGLEBASJTZFNCTELLVOFINXIWIZYFZXC
NAZVDLTHYKWTISIABYLLEOQHSUAGLQVMFIZDTANXTWNSVMHDOCVJROMXGLOYPKVYVNBUBNMGTS
SDWSK
Got a command: COMMAND PING [request] :: request id: 0x0004 :: data: KXXNUTUHLFP
AENCGAEPJEKQSNITIESEJPLMPUEKBZEUOKLQIGVQIYABSDQPEECRKXSFTJUXCMCTOZQHXZFSDHMMDBQ
TANAXGIZMOYRSYBJMCHOFLKNGUFLQDAXPSRPQKXDUJVEDGWYAVANMFCIUHZRWRMGSCIVVDQXJFWJXFI
PMUBVPXNAOKRJWIAVCMCEPDRIZNTNSUKBITNFWCDXIUJFHEQOEXDHSYIDXESKRHOIXQPCCCAUCAWAO
CSDXO
[[ WARNING ]] :: Got a ping request! Responding!
Response: COMMAND PING [response] :: request id: 0x0004 :: data: KXXNUTUHLFPAENC
GAEPJEKQSNITIESEJPLMPUEKBZEUOKLQIGVQIYABSDQPEECRKXSFTJUXCMCTOZQHXZFSDHMMDBQ
TANAXGIZMOYRSYBJMCHOFLKNGUFLQDAXPSRPQKXDUJVEDGWYAVANMFCIUHZRWRMGSCIVVDQXJFWJXFI
PMUBVPXNAOKRJWIAVCMCEPDRIZNTNSUKBITNFWCDXIUJFHEQOEXDHSYIDXESKRHOIXQPCCCAUCAWAO
CSDXO
0
```

os212@os212-lubuntu: ~/scripts

```
File Edit Tabs Help
59a654fba8c5f2118f.887962cc2bf7cbdede9b5d817e9a5387fdd2abb481f277630b17915f30cb.
1365683dc026fcb5e4435d8131c0ee727b7642831485e62df90d43564197.ea86d2c516499cee631
7bba7e57bb85def14e48dd3f665502f32.b.com is ee750189bd29ca8f2ddc65ffff8a26e348
```

```
Jul 10 23:18:43 dnsmasq[28142]: query[TXT] ab730189bda9165b118b10001f5a5fea00dff
9cb515c9b7a98b471323335.d33cf16ba68945ebd408b1029ef08cde7a42754c48fdbfe0667dbad6
93c6.410aff59c3d57e90eb31b7440467bd5d3f5420e9eff2fb87.b.com from 127.0.0.1
```

```
dnsmasq[28142]: forwarded ab730189bda9165b118b10001f5a5fea00dff
3335.d33cf16ba68945ebd408b1029ef08cde7a42754c48fdbfe0667dbad6
90eb31b7440467bd5d3f5420e9eff2fb87.b.com from 127.0.0.1
```

```
dnsmasq[28142]: reply ab730189bda9165b118b10001f5a5fea00dff
3335.d33cf16ba68945ebd408b1029ef08cde7a42754c48fdbfe0667dbad6
31b7440467bd5d3f5420e9eff2fb87.b.com from 127.0.0.1
```

```
dnsmasq[28142]: query[MX] a9
3335.d33cf16ba68945ebd408b1029ef08cde7a42754c48fdbfe0667dbad6
31b7440467bd5d3f5420e9eff2fb87.b.com from 127.0.0.1
```

```
Jul 10 23:18:43 dnsmasq[28142]: forwarded a9
3335.d33cf16ba68945ebd408b1029ef08cde7a42754c48fdbfe0667dbad6
31b7440467bd5d3f5420e9eff2fb87.b.com from 127.0.0.1
```

DNS TUNNEL DETECTOR

DNS Tunnel Detector

Show Total Show Peaks Exit

Approved List Blocked List

commands\_s

server.txt

run.txt

run\_servers

h

All of the communication is over DNS queries sent through our DNS server

```
os212@os212-lubuntu: ~/scripts
File Edit Tabs Help
New window created: 1
history size (session) => 1000
(not set) l> Session 1 security: ENCRYPTED BUT *NOT* VALIDATED
For added security, please ensure the client displays the same string:
```

```
>> Deepen Sippy Roving Surfs Exotic Pony
This is a command session!

That means you can enter a dnscat2 command such as
'ping'. For a full list of clients, try 'help'.
```

```
ping
Ping!
command (os212-lubuntu) l> Pong!
ping
Ping!
command (os212-lubuntu) l> Pong!
ping
Ping!
command (os212-lubuntu) l> Pong!
ping
Ping!
command (os212-lubuntu) l> Pong!
```

```
File Edit View Search terminal Help
H
Got a command: COMMAND PING [request] :: request id: 0x0003 :: data: YSGEMDNSQXR
WJQNUPLOQVJPQNGMNDJOFENDHRTJQAWPASCVCNNXNZTHLLSUAWYALCREQCBEERMXLAVQCQYFGKZWPCMPW
PTBVNQZVQWCCEDTMEYMAHARNUPHVRURGAEDTRXEIVNLLHFMFSGLPBASJTZFNCTELLVOFINXIWIZYFZXC
NAZVDLTHYKWTSIABYLLEOQHSUAHQGLQVMFIZDTANXTWNSVMHDOCVJROMXGLOYPKVYVNBABNMGTSDWS
K
[[ WARNING ]] :: Got a ping request! Responding!
Response: COMMAND PING [response] :: request id: 0x0003 :: data: YSGEMDNSQXRWJQN
UPLQVJPQNGMNDJOFENDHRTJQAWPASCVCNNXNZTHLLSUAWYALCREQCBEERMXLAVQCQYFGKZWPCMPWPTBV
NQZVQWCCEDTMEYMAHARNUPHVRURGAEDTRXEIVNLLHFMFSGLPBASJTZFNCTELLVOFINXIWIZYFZXC
NAZVDLTHYKWTSIABYLLEOQHSUAHQGLQVMFIZDTANXTWNSVMHDOCVJROMXGLOYPKVYVNBABNMGTSDWS
K
Got a command: COMMAND PING [request] :: request id: 0x0004 :: data: KXXNUTUHLFP
AENCGAEPJEKRSNTIYSEJEPLMPUEKBZEUOKLQIGVQIYABSDQPEECRKXSFTJUXCMCTOZQHXZFSDHMMDBQ
TANAXGIZMOYRSYBJMCHOFLKNGUFLQDAXPSRPQKXDUJVEDGWYAVANMFCIUHZRWRMGSCIVVDQXJFWJXFI
PMHUBVPXNAOKRJWIAVCMCPDRIZNTNSUKBITNFWCDXIUJFHEQOEXDHSYIDXESKRHOIXQPCCCAUCAWAO
CSDXO
[[ WARNING ]] :: Got a ping request! Responding!
Response: COMMAND PING [response] :: request id: 0x0004 :: data: KXXNUTUHLFPAENC
GAEPJEKRSNTIYSEJEPLMPUEKBZEUOKLQIGVQIYABSDQPEECRKXSFTJUXCMCTOZQHXZFSDHMMDBQ
TANAXGIZMOYRSYBJMCHOFLKNGUFLQDAXPSRPQKXDUJVEDGWYAVANMFCIUHZRWRMGSCIVVDQXJFWJXFI
PMHUBVPXNAOKRJWIAVCMCPDRIZNTNSUKBITNFWCDXIUJFHEQOEXDHSYIDXESKRHOIXQPCCCAUCAWAO
CSDXO
```

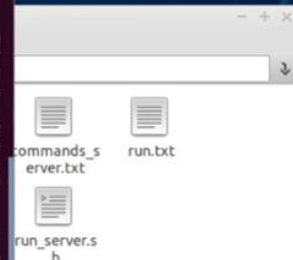
```
os212@os212-lubuntu: ~/scripts
File Edit Tabs Help
59a654fba8c5f2118f.887962cc2bf7cbdede9b5d817e9a5387fdd2abb481f277630b17915f30cb.
1365683dc020fcb5e4435d0131c0ee727b7642831485e62df90d43564197.ea86d2c516499cee631
7bba7e57bb85def14e48dd3f665502f32.b.com is ee750189bd29ca8f2ddc65ffff8a26e348

Jul 10 23:18:43 dnsmasq[28142]: query[TXT] ab730189bda9165b118b10001f5a5fea00dff
9cb515c9b7a98b471323335.d33cf16ba68945ebd408b1029ef08cde7a42754c48fdbfe0667dbad6
93c6.410aff59c3d57e90eb31b7440467bd5d3f5420e9eff2fb87.b.com from 127.0.0.1
```

```
dnsmasq[28142]: forwarded ab730189bda9165b118b10001f5a5fea00dff
3335.d33cf16ba68945ebd408b1029ef08cde7a42754c48fdbfe0667dbad6
90eb31b7440467bd5d3f5420e9eff2fb87.b.com to 127.0.0.1

dnsmasq[28142]: query[MX] a93335.d33cf16ba68945ebd408b1029ef08cde7a42754c48fdbfe0667dbad6
31b7440467bd5d3f5420e9eff2fb87.b.com from 127.0.0.1

dnsmasq[28142]: forwarded a93335.d33cf16ba68945ebd408b1029ef08cde7a42754c48fdbfe0667dbad6
31b7440467bd5d3f5420e9eff2fb87.b.com to 127.0.0.1
```





ox

ext

dio

nal

```

os212@os212-lubuntu: ~/scripts
File Edit Tabs Help
New window created: 1
history size (session) => 1000
(not set) l> Session 1 security: ENCRYPTED BUT *NOT* VALIDATED
For added security, please ensure the client displays the same string:

>> Deepen Sippy Roving Surfs Exotic Pony
This is a command session!

That means you can enter a dnscat2 command such as
'ping'. For a full list of clients, try 'help'.

ping
Ping!
command (os212-lubuntu) l> Ping!
ping
Ping!
command (os212-lubuntu) l> Ping!
ping
Ping!
command (os212-lubuntu) l> Ping!
ping
Ping!
command (os212-lubuntu) l> Ping!

```

Here we see the requests being read by our detector

```

os212@os212-lubuntu: ~/scripts
File Edit Tabs Help
59a654fba8c5f2118f.887902cc2bf7cbdede9b5d817e9a5387fdd2abb481f277630b17915f30cb.
1365683dc020fcb5e4435d8131c0ee727b7642831485e62df90d43564197.ea86d2c516499cee631
7bba7e57bb85def14e48dd3f665502f32.b.com is ee750189bd29ca8f2ddc65ffff8a26e348

Jul 10 23:18:43 dnsmasq[28142]: query[TXT] ab730189bda9165b118b10001f5a5fea00dfff
bb7a98b471323335.d33cf16ba68945ebd408b1029ef08cde7a42754c48fdbfe0667dbad6
baff59c3d57e90eb31b7440467bd5d3f5420e9efff7b87.b.com from 127.0.0.1

Jul 10 23:18:43 dnsmasq[28142]: forwarded ab730189bda9165b118b10001f5a5fea00dfff
bb7a98b471323335.d33cf16ba68945ebd408b1029ef08cde7a42754c48fdbfe0667dbad6
baff59c3d57e90eb31b7440467bd5d3f5420e9efff7b87.b.com from 127.0.0.1

Jul 10 23:18:43 dnsmasq[28142]: reply ab730189bda9165b118b10001f5a5fea00dfff
bb7a98b471323335.d33cf16ba68945ebd408b1029ef08cde7a42754c48fdbfe0667dbad6
baff59c3d57e90eb31b7440467bd5d3f5420e9efff7b87.b.com to 127.0.0.1

Jul 10 23:18:43 dnsmasq[28142]: query[MX] a90189bda9165b118b10001f5a5fea00dfff
om from 127.0.0.1

Jul 10 23:18:43 dnsmasq[28142]: forwarded a90189bda9165b118b10001f5a5fea00dfff
om to 127.0.0.1

```

DNS TUNNEL DETECTOR

DNS Tunnel Detector

Show Total

Show Peaks

Exit

Approved List

Blocked List

```

File Edit View Search Terminal Help
H
Got a command: COMMAND_PING [request] :: request_id: 0x0003 :: data: YSGEMDNSQXR
WJONUPLQVJPQNGMNDJOFENDHRTJQAWPASCVCNNXNZTHLLSUAUWYALCREQCBEERMXLAVQCQYFGKZWPCMPW
PTBVNQZVZQWNCEDTMEYMAHARNUPHVRURGAEDTRXEVNVLHFMFSGLPBASJTZFNCTELLVOFINXIWIZYFZXC
NAZVDLTHYKWTISIABYLLQOQSLUAHQGLQVMFIZDTANXTWNSVMHDOCVJROMXGLOYPKVYVNBABUNMGTSOWS
K
[[ WARNING ]] :: Got a ping request! Responding!
Response: COMMAND_PING [response] :: request_id: 0x0003 :: data: YSGEMDNSQXRWJON
UPLQVJPQNGMNDJOFENDHRTJQAWPASCVCNNXNZTHLLSUAUWYALCREQCBEERMXLAVQCQYFGKZWPCMPWPTBV
NQZVZQWNCEDTMEYMAHARNUPHVRURGAEDTRXEVNVLHFMFSGLPBASJTZFNCTELLVOFINXIWIZYFZXC
NAZVDLTHYKWTISIABYLLQOQSLUAHQGLQVMFIZDTANXTWNSVMHDOCVJROMXGLOYPKVYVNBABUNMGTSOWS
K
Got a command: COMMAND_PING [request] :: request_id: 0x0004 :: data: KXXNUTUHLFP
AENCGAEPJEKRQSNITIESEJEPLMPUEKBZEUOKLQIGVQIYABSDQPEECRKXSFTJUXCMCTOZQHXZFSDHMMDBQ
TANAXGIZMOYRSYBJMCHOFKNGUFHLQDAXPSRPQKXDUJVEDGWYAVANMFCIUHZRWRMGSCIVVDOXJFWJXFI
PMUBVPXNAOKRJWIAVCMCPDRIZNTNSUKBITNFWCDXIUIJFHEQOEXDHSYIDXESKRHIQXQPOPCCAUAWAO
CSDXO
[[ WARNING ]] :: Got a ping request! Responding!
Response: COMMAND_PING [response] :: request_id: 0x0004 :: data: KXXNUTUHLFPAENC
GAEPJEKRQSNITIESEJEPLMPUEKBZEUOKLQIGVQIYABSDQPEECRKXSFTJUXCMCTOZQHXZFSDHMMDBQ
TANAXGIZMOYRSYBJMCHOFKNGUFHLQDAXPSRPQKXDUJVEDGWYAVANMFCIUHZRWRMGSCIVVDOXJFWJXFI
PMUBVPXNAOKRJWIAVCMCPDRIZNTNSUKBITNFWCDXIUIJFHEQOEXDHSYIDXESKRHIQXQPOPCCAUAWAO
CSDXO

```

commands\_s

server.txt

run.txt

run\_server.s

h

ox

ext

dio

nal

```

os212@os212-lubuntu: ~/scripts
File Edit Tabs Help
New window created: 1
history size (session) => 1000
(not set) l> Session 1 security: ENCRYPTED BUT *NOT* VALIDATED
For added security, please ensure the client displays the same string:

>> Deepen Sippy Roving Surfs Exotic Pony
This is a command session!

That means you can enter a dnscat2 command such as
'ping'! For a full list of clients, try 'help'.

ping
Ping!
command (os212-lubuntu) l> Ping!
ping
Ping!
command (os212-lubuntu) l> Ping!
ping
Ping!
command (os212-lubuntu) l> Ping!
ping
Ping!
command (os212-lubuntu) l> Ping!

```

Here we see the requests being read by our detector

```

os212@os212-lubuntu: ~/scripts
File Edit Tabs Help
59a654fba8c5f2118f.887902cc2bf7cbdede9b5d817e9a5387fdd2abb481f277630b17915f30cb.
1365683dc020fcb5e4435d8131c0ee727b7642831485e62df90d43564197.ea86d2c516499cee631
7bba7e57bb85def14e48dd3f665502f32.b.com is ee750189bd29ca8f2ddc65ffff8a26e348

Jul 10 23:18:43 dnsmasq[28142]: query[TXT] ab730189bda9165b118b10001f5a5fea00dff
bb7a98b471323335.d33cf16ba68945ebd408b1029ef08cde7a42754c48fdbfe0667dbad6
baff59c3d57e90eb31b7440467bd5d3f5420e9efff7fb87.b.com from 127.0.0.1

Jul 10 23:18:43 dnsmasq[28142]: forwarded ab730189bda9165b118b10001f5a5fea00dff
bb7a98b471323335.d33cf16ba68945ebd408b1029ef08cde7a42754c48fdbfe0667dbad6
baff59c3d57e90eb31b7440467bd5d3f5420e9efff7fb87.b.com from 127.0.0.1

Jul 10 23:18:43 dnsmasq[28142]: reply ab730189bda9165b118b10001f5a5fea00dff
bb7a98b471323335.d33cf16ba68945ebd408b1029ef08cde7a42754c48fdbfe0667dbad6
baff59c3d57e90eb31b7440467bd5d3f5420e9efff7fb87.b.com to 127.0.0.1

Jul 10 23:18:43 dnsmasq[28142]: query[MX] a9b0c3d57e90eb31b7440467bd5d3f5420e9efff7fb87.b.com from 127.0.0.1

```

DNS TUNNEL DETECTOR

DNS Tunnel Detector

Show Total

Show Peaks

Exit

Approved List

Blocked List

```

File Edit View Search Terminal Help
H
Got a command: COMMAND_PING [request] :: request_id: 0x0003 :: data: YSGEMDNSQXR
WJONUPLQVJPQNGMNDJOFENDHRTJQAWPASCVCNNXNZTHLLSUAWYALCREQCBEERMXLAVQCQYFGKZWPCMPW
PTBVNQZVZQWNCEDTMEYMAHARNUPHVRURGAEDTRXEIVNLLHFMFSGLPBASJTZFNCTELLVOFINXIWIZYFZXC
NAZVDLTHYKWTISIABYLLEOQHSUAHQGLQVMFIZDTANXTWNSVMHDOCVJROMXGLOYPKVYVNBABUNMGTSOWS
K
[[ WARNING ]] :: Got a ping request! Responding!
Response: COMMAND_PING [response] :: request_id: 0x0003 :: data: YSGEMDNSQXRWJON
UPLQVJPQNGMNDJOFENDHRTJQAWPASCVCNNXNZTHLLSUAWYALCREQCBEERMXLAVQCQYFGKZWPCMPWPTBV
NQZVZQWNCEDTMEYMAHARNUPHVRURGAEDTRXEIVNLLHFMFSGLPBASJTZFNCTELLVOFINXIWIZYFZXC
NAZVDLTHYKWTISIABYLLEOQHSUAHQGLQVMFIZDTANXTWNSVMHDOCVJROMXGLOYPKVYVNBABUNMGTSOWS
K
Got a command: COMMAND_PING [request] :: request_id: 0x0004 :: data: KXXNUTUHLFP
AENCGAEPJEKRQSNITIESEJEPLMPUEKBZEUOKLQIGVQIYABSDQPEECRKXSFTJUXCMCTOZQHXZFSDHMMDBQ
TANAXGIZMOYRSYBIMCHOFKNGUFHLQDAXPSRPQKXDUJVEDGWYAVANMFCIUHZRWRMGSCIVVDOXJFWJXFI
PMUBVPXNAOKRJWIAVCMCPDRIZNTNSUKBITNFWCXDIUJFHEQOEXDHSYIDXESKRHIQXQPOPCCAUAWAOCSDX
O
[[ WARNING ]] :: Got a ping request! Responding!
Response: COMMAND_PING [response] :: request_id: 0x0004 :: data: KXXNUTUHLFPAENC
GAEPJEKRQSNITIESEJEPLMPUEKBZEUOKLQIGVQIYABSDQPEECRKXSFTJUXCMCTOZQHXZFSDHMMDBQ
TANAXGIZMOYRSYBIMCHOFKNGUFHLQDAXPSRPQKXDUJVEDGWYAVANMFCIUHZRWRMGSCIVVDOXJFWJXFI
PMUBVPXNAOKRJWIAVCMCPDRIZNTNSUKBITNFWCXDIUJFHEQOEXDHSYIDXESKRHIQXQPOPCCAUAWAOCSDX
O

```

commands\_s

server.txt

run.txt

run\_server.s

h

```
os212@os212-lubuntu: ~/scripts
File Edit Tabs Help

ping
Ping!
command (os212-lubuntu) 1> Pong!
ping
Ping!
command (os212-lubuntu) 1> Pong!
ping
Ping!
command (os212-lubuntu) 1> Pong!
ping
Ping!
command (os212-lubuntu) 1> Pong!
os212/dnscat2/server/secretFile /home/o
Attempting to download /home/os212/dnscat2/client/secretFile to /home/os212/dnscat2/server/secretFile
command (os212-lubuntu) 1> ping
Ping!
command (os212-lubuntu) 1> ping
Ping!
command (os212-lubuntu) 1> ping
Ping!
command (os212-lubuntu) 1> ping
Ping!
command (os212-lubuntu) 1> 
```

Here we see an attempt to send a file of 1MB over DNS from client to server

```
os212@os212-lubuntu: ~/scripts
File Edit Tabs Help

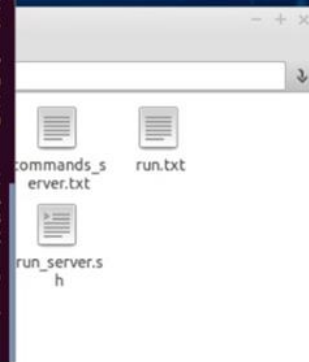
Jul 10 23:18:46 dnsmasq[28142]: forwarded fc450189bd5a541cbaed7d054f178495e5b2c
63cccd34b5323fc223f418.fefa38ecd8944f8ac1d01ee6f2bbfa4cf01a6c0661861ef7d6bc14de3
45a-6506f2b-05-58-60110632400b33031e2f0463c9abe714d3b451cfc8.5601c5552303316
b.com to 127.0.0.1
ping on receipt of SIGTERM
ed, version 2.79 cachesize 150
service limited to local subnets
le time options: IPv6 GNU-getopt DBus 118n
ipset auth nettlehash DNSSEC loop-detect 1

Jul 10 23:18:46 dnsmasq[28221]: using nameserver 8.8.8.8#53
Jul 10 23:18:46 dnsmasq[28221]: using nameserver 127.0.0.1#53531 for domain b.co
m
Jul 10 23:18:46 dnsmasq[28221]: using nameserver 127.0.0.1#53531 for default

```

```
File Edit View Search Terminal Help
FZXCNZVDLTHYKWSIABYLL00QHSUAHQGLQVMFIZDTANXTWNSHD0CVJROMXGLOYPKYVYNBAUBNMGTS
SDWSK
[[ WARNING ]] :: Got a ping request! Responding!
Response: COMMAND_PING [request] :: request_id: 0x0003 :: data: YSGEMDNSQXRWJQN
UPLQVJPQNGMNDJOFENDHRTJQAWPASCVCNNXNZTHLLSUAKALCREQCBEERMXLAVQCQYFGKZWPCMPWPTBV
NQVZQWCCEDTMEYMAHHARNUPHVRURGAEDTRXEIVNLLMFSGLPBASJTZFNCTELLVDFINXIWIYZFXC
NAZVDLTHYKWSIABYLL00QHSUAHQGLQVMFIZDTANXTWNSVMD0CVJROMXGLOYPKYVYNBAUBNMGTS
SDWSK
Got a command: COMMAND_PING [request] :: request_id: 0x0004 :: data: KXXNUTUHLFP
AENC GAEPJEKRQSNITIYSEJEPLMPUEKBZEUOKLQIYABSDQPEECRKXSFTJUXCMCTOZQHXZFSDDHMMDBQ
TANAXGIZMOYRSYBJMCHOFKNGUFLQDAXPSRFPQKXDUJVEDGWYAVANMFCIUHZRWRMGSCIVVD0XJFWJXFI
PMUBVPXNAOKRJWIAVCMCEPDRIZNTNSUKBITFWCDXIUJFHEQOEXDHSYIDXESKRHIQXQPOPCCCAUCAWA0
CSDX0
[[ WARNING ]] :: Got a ping request! Responding!
Response: COMMAND_PING [request] :: request_id: 0x0004 :: data: KXXNUTUHLFPAENC
GAEPJEKRQSNITIYSEJEPLMPUEKBZEUOKLQIYABSDQPEECRKXSFTJUXCMCTOZQHXZFSDDHMMDBQ
TANAXGIZMOYRSYBJMCHOFKNGUFLQDAXPSRFPQKXDUJVEDGWYAVANMFCIUHZRWRMGSCIVVD0XJFWJXFI
PMUBVPXNAOKRJWIAVCMCEPDRIZNTNSUKBITFWCDXIUJFHEQOEXDHSYIDXESKRHIQXQPOPCCCAUCAWA0
CSDX0
Got a command: COMMAND_DOWNLOAD [request] :: request_id: 0x0005 :: filename: /ho
me/os212/dnscat2/client/secretFile
Response: COMMAND_DOWNLOAD [response] :: request_id: 0x0005 :: data: 0x100000 by
tes

```





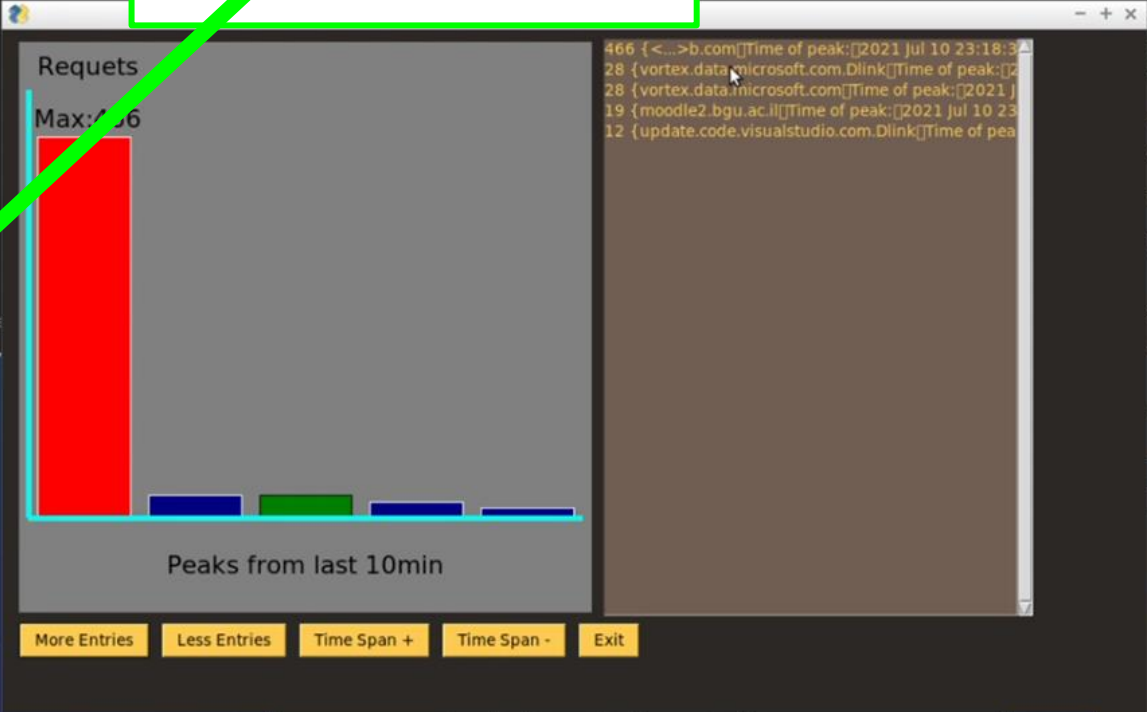


The program pops up a window of the blocked domain in red to inform the user


The program pops up a window of the blocked domain in red to inform the user



The server doesn't manage to download the file in time and closes (client closes too)



```
File Edit Tabs Help  
at2/server/secretFile  
command (os212-lubuntu) l> ping  
Ping!  
command (os212-lubuntu) l> ping  
Ping!  
command (os212-lubuntu) l> ping  
Ping!  
command (os212-lubuntu) l> ping  
Ping!  
command (os212-lubuntu) l> ping  
Ping!  
command (os212-lubuntu) l> ping  
Ping!  
command (os212-lubuntu) l> ping  
Ping!  
command (os212-lubuntu) l> ping  
Ping!  
command (os212-lubuntu) l>  
command (os212-lubuntu) l>  
command (os212-lubuntu) l>  
command (os212-lubuntu) l> Input thread is  
os212@os212-lubuntu:~/scripts$
```



os212@os212-lubuntu: ~/scripts

File Edit Tabs Help

- + x

b0bd5a541cbaed7d054f178495e5b42c  
bbf4cf01a6c0661861ef7d6bc14de3  
be714d3b451cfc8.5601c5552303316  
7.0.0.1  
c of SIGTERM  
2.79 cachesize 150  
ed to local subnets  
ons: IPv6 GNU-getopt DBus i18n  
nettlehash DNSSEC loop-detect i  
3.8.8.8#53  
127.0.0.1#53531 for domain b.co  
127.0.0.1#53531 for default

DNS TUNNEL DETECTOR

## DNS Tunnel Detector

Show Total Show Peaks Exit

Show Total Show Peaks Exit

Show Total Show Peaks Exit

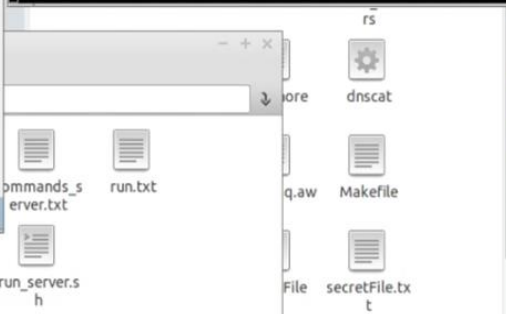
Approved List	Blocked List
<p>1. <b>Approved</b></p> <p>2. <b>Approved</b></p> <p>3. <b>Approved</b></p> <p>4. <b>Approved</b></p> <p>5. <b>Approved</b></p> <p>6. <b>Approved</b></p> <p>7. <b>Approved</b></p> <p>8. <b>Approved</b></p> <p>9. <b>Approved</b></p> <p>10. <b>Approved</b></p> <p>11. <b>Approved</b></p> <p>12. <b>Approved</b></p> <p>13. <b>Approved</b></p> <p>14. <b>Approved</b></p> <p>15. <b>Approved</b></p> <p>16. <b>Approved</b></p> <p>17. <b>Approved</b></p> <p>18. <b>Approved</b></p> <p>19. <b>Approved</b></p> <p>20. <b>Approved</b></p> <p>21. <b>Approved</b></p> <p>22. <b>Approved</b></p> <p>23. <b>Approved</b></p> <p>24. <b>Approved</b></p> <p>25. <b>Approved</b></p> <p>26. <b>Approved</b></p> <p>27. <b>Approved</b></p> <p>28. <b>Approved</b></p> <p>29. <b>Approved</b></p> <p>30. <b>Approved</b></p> <p>31. <b>Approved</b></p> <p>32. <b>Approved</b></p> <p>33. <b>Approved</b></p> <p>34. <b>Approved</b></p> <p>35. <b>Approved</b></p> <p>36. <b>Approved</b></p> <p>37. <b>Approved</b></p> <p>38. <b>Approved</b></p> <p>39. <b>Approved</b></p> <p>40. <b>Approved</b></p> <p>41. <b>Approved</b></p> <p>42. <b>Approved</b></p> <p>43. <b>Approved</b></p> <p>44. <b>Approved</b></p> <p>45. <b>Approved</b></p> <p>46. <b>Approved</b></p> <p>47. <b>Approved</b></p> <p>48. <b>Approved</b></p> <p>49. <b>Approved</b></p> <p>50. <b>Approved</b></p> <p>51. <b>Approved</b></p> <p>52. <b>Approved</b></p> <p>53. <b>Approved</b></p> <p>54. <b>Approved</b></p> <p>55. <b>Approved</b></p> <p>56. <b>Approved</b></p> <p>57. <b>Approved</b></p> <p>58. <b>Approved</b></p> <p>59. <b>Approved</b></p> <p>60. <b>Approved</b></p> <p>61. <b>Approved</b></p> <p>62. <b>Approved</b></p> <p>63. <b>Approved</b></p> <p>64. <b>Approved</b></p> <p>65. <b>Approved</b></p> <p>66. <b>Approved</b></p> <p>67. <b>Approved</b></p> <p>68. <b>Approved</b></p> <p>69. <b>Approved</b></p> <p>70. <b>Approved</b></p> <p>71. <b>Approved</b></p> <p>72. <b>Approved</b></p> <p>73. <b>Approved</b></p> <p>74. <b>Approved</b></p> <p>75. <b>Approved</b></p> <p>76. <b>Approved</b></p> <p>77. <b>Approved</b></p> <p>78. <b>Approved</b></p> <p>79. <b>Approved</b></p> <p>80. <b>Approved</b></p> <p>81. <b>Approved</b></p> <p>82. <b>Approved</b></p> <p>83. <b>Approved</b></p> <p>84. <b>Approved</b></p> <p>85. <b>Approved</b></p> <p>86. <b>Approved</b></p> <p>87. <b>Approved</b></p> <p>88. <b>Approved</b></p> <p>89. <b>Approved</b></p> <p>90. <b>Approved</b></p> <p>91. <b>Approved</b></p> <p>92. <b>Approved</b></p> <p>93. <b>Approved</b></p> <p>94. <b>Approved</b></p> <p>95. <b>Approved</b></p> <p>96. <b>Approved</b></p> <p>97. <b>Approved</b></p> <p>98. <b>Approved</b></p> <p>99. <b>Approved</b></p> <p>100. <b>Approved</b></p>	<p>1. <b>Blocked</b></p> <p>2. <b>Blocked</b></p> <p>3. <b>Blocked</b></p> <p>4. <b>Blocked</b></p> <p>5. <b>Blocked</b></p> <p>6. <b>Blocked</b></p> <p>7. <b>Blocked</b></p> <p>8. <b>Blocked</b></p> <p>9. <b>Blocked</b></p> <p>10. <b>Blocked</b></p> <p>11. <b>Blocked</b></p> <p>12. <b>Blocked</b></p> <p>13. <b>Blocked</b></p> <p>14. <b>Blocked</b></p> <p>15. <b>Blocked</b></p> <p>16. <b>Blocked</b></p> <p>17. <b>Blocked</b></p> <p>18. <b>Blocked</b></p> <p>19. <b>Blocked</b></p> <p>20. <b>Blocked</b></p> <p>21. <b>Blocked</b></p> <p>22. <b>Blocked</b></p> <p>23. <b>Blocked</b></p> <p>24. <b>Blocked</b></p> <p>25. <b>Blocked</b></p> <p>26. <b>Blocked</b></p> <p>27. <b>Blocked</b></p> <p>28. <b>Blocked</b></p> <p>29. <b>Blocked</b></p> <p>30. <b>Blocked</b></p> <p>31. <b>Blocked</b></p> <p>32. <b>Blocked</b></p> <p>33. <b>Blocked</b></p> <p>34. <b>Blocked</b></p> <p>35. <b>Blocked</b></p> <p>36. <b>Blocked</b></p> <p>37. <b>Blocked</b></p> <p>38. <b>Blocked</b></p> <p>39. <b>Blocked</b></p> <p>40. <b>Blocked</b></p> <p>41. <b>Blocked</b></p> <p>42. <b>Blocked</b></p> <p>43. <b>Blocked</b></p> <p>44. <b>Blocked</b></p> <p>45. <b>Blocked</b></p> <p>46. <b>Blocked</b></p> <p>47. <b>Blocked</b></p> <p>48. <b>Blocked</b></p> <p>49. <b>Blocked</b></p> <p>50. <b>Blocked</b></p> <p>51. <b>Blocked</b></p> <p>52. <b>Blocked</b></p> <p>53. <b>Blocked</b></p> <p>54. <b>Blocked</b></p> <p>55. <b>Blocked</b></p> <p>56. <b>Blocked</b></p> <p>57. <b>Blocked</b></p> <p>58. <b>Blocked</b></p> <p>59. <b>Blocked</b></p> <p>60. <b>Blocked</b></p> <p>61. <b>Blocked</b></p> <p>62. <b>Blocked</b></p> <p>63. <b>Blocked</b></p> <p>64. <b>Blocked</b></p> <p>65. <b>Blocked</b></p> <p>66. <b>Blocked</b></p> <p>67. <b>Blocked</b></p> <p>68. <b>Blocked</b></p> <p>69. <b>Blocked</b></p> <p>70. <b>Blocked</b></p> <p>71. <b>Blocked</b></p> <p>72. <b>Blocked</b></p> <p>73. <b>Blocked</b></p> <p>74. <b>Blocked</b></p> <p>75. <b>Blocked</b></p> <p>76. <b>Blocked</b></p> <p>77. <b>Blocked</b></p> <p>78. <b>Blocked</b></p> <p>79. <b>Blocked</b></p> <p>80. <b>Blocked</b></p> <p>81. <b>Blocked</b></p> <p>82. <b>Blocked</b></p> <p>83. <b>Blocked</b></p> <p>84. <b>Blocked</b></p> <p>85. <b>Blocked</b></p> <p>86. <b>Blocked</b></p> <p>87. <b>Blocked</b></p> <p>88. <b>Blocked</b></p> <p>89. <b>Blocked</b></p> <p>90. <b>Blocked</b></p> <p>91. <b>Blocked</b></p> <p>92. <b>Blocked</b></p> <p>93. <b>Blocked</b></p> <p>94. <b>Blocked</b></p> <p>95. <b>Blocked</b></p> <p>96. <b>Blocked</b></p> <p>97. <b>Blocked</b></p> <p>98. <b>Blocked</b></p> <p>99. <b>Blocked</b></p> <p>100. <b>Blocked</b></p>

Approved List	Blocked List
<p>1. <b>Approved</b></p> <p>2. <b>Approved</b></p> <p>3. <b>Approved</b></p> <p>4. <b>Approved</b></p> <p>5. <b>Approved</b></p> <p>6. <b>Approved</b></p> <p>7. <b>Approved</b></p> <p>8. <b>Approved</b></p> <p>9. <b>Approved</b></p> <p>10. <b>Approved</b></p> <p>11. <b>Approved</b></p> <p>12. <b>Approved</b></p> <p>13. <b>Approved</b></p> <p>14. <b>Approved</b></p> <p>15. <b>Approved</b></p> <p>16. <b>Approved</b></p> <p>17. <b>Approved</b></p> <p>18. <b>Approved</b></p> <p>19. <b>Approved</b></p> <p>20. <b>Approved</b></p> <p>21. <b>Approved</b></p> <p>22. <b>Approved</b></p> <p>23. <b>Approved</b></p> <p>24. <b>Approved</b></p> <p>25. <b>Approved</b></p> <p>26. <b>Approved</b></p> <p>27. <b>Approved</b></p> <p>28. <b>Approved</b></p> <p>29. <b>Approved</b></p> <p>30. <b>Approved</b></p> <p>31. <b>Approved</b></p> <p>32. <b>Approved</b></p> <p>33. <b>Approved</b></p> <p>34. <b>Approved</b></p> <p>35. <b>Approved</b></p> <p>36. <b>Approved</b></p> <p>37. <b>Approved</b></p> <p>38. <b>Approved</b></p> <p>39. <b>Approved</b></p> <p>40. <b>Approved</b></p> <p>41. <b>Approved</b></p> <p>42. <b>Approved</b></p> <p>43. <b>Approved</b></p> <p>44. <b>Approved</b></p> <p>45. <b>Approved</b></p> <p>46. <b>Approved</b></p> <p>47. <b>Approved</b></p> <p>48. <b>Approved</b></p> <p>49. <b>Approved</b></p> <p>50. <b>Approved</b></p> <p>51. <b>Approved</b></p> <p>52. <b>Approved</b></p> <p>53. <b>Approved</b></p> <p>54. <b>Approved</b></p> <p>55. <b>Approved</b></p> <p>56. <b>Approved</b></p> <p>57. <b>Approved</b></p> <p>58. <b>Approved</b></p> <p>59. <b>Approved</b></p> <p>60. <b>Approved</b></p> <p>61. <b>Approved</b></p> <p>62. <b>Approved</b></p> <p>63. <b>Approved</b></p> <p>64. <b>Approved</b></p> <p>65. <b>Approved</b></p> <p>66. <b>Approved</b></p> <p>67. <b>Approved</b></p> <p>68. <b>Approved</b></p> <p>69. <b>Approved</b></p> <p>70. <b>Approved</b></p> <p>71. <b>Approved</b></p> <p>72. <b>Approved</b></p> <p>73. <b>Approved</b></p> <p>74. <b>Approved</b></p> <p>75. <b>Approved</b></p> <p>76. <b>Approved</b></p> <p>77. <b>Approved</b></p> <p>78. <b>Approved</b></p> <p>79. <b>Approved</b></p> <p>80. <b>Approved</b></p> <p>81. <b>Approved</b></p> <p>82. <b>Approved</b></p> <p>83. <b>Approved</b></p> <p>84. <b>Approved</b></p> <p>85. <b>Approved</b></p> <p>86. <b>Approved</b></p> <p>87. <b>Approved</b></p> <p>88. <b>Approved</b></p> <p>89. <b>Approved</b></p> <p>90. <b>Approved</b></p> <p>91. <b>Approved</b></p> <p>92. <b>Approved</b></p> <p>93. <b>Approved</b></p> <p>94. <b>Approved</b></p> <p>95. <b>Approved</b></p> <p>96. <b>Approved</b></p> <p>97. <b>Approved</b></p> <p>98. <b>Approved</b></p> <p>99. <b>Approved</b></p> <p>100. <b>Approved</b></p>	<p>1. <b>Blocked</b></p> <p>2. <b>Blocked</b></p> <p>3. <b>Blocked</b></p> <p>4. <b>Blocked</b></p> <p>5. <b>Blocked</b></p> <p>6. <b>Blocked</b></p> <p>7. <b>Blocked</b></p> <p>8. <b>Blocked</b></p> <p>9. <b>Blocked</b></p> <p>10. <b>Blocked</b></p> <p>11. <b>Blocked</b></p> <p>12. <b>Blocked</b></p> <p>13. <b>Blocked</b></p> <p>14. <b>Blocked</b></p> <p>15. <b>Blocked</b></p> <p>16. <b>Blocked</b></p> <p>17. <b>Blocked</b></p> <p>18. <b>Blocked</b></p> <p>19. <b>Blocked</b></p> <p>20. <b>Blocked</b></p> <p>21. <b>Blocked</b></p> <p>22. <b>Blocked</b></p> <p>23. <b>Blocked</b></p> <p>24. <b>Blocked</b></p> <p>25. <b>Blocked</b></p> <p>26. <b>Blocked</b></p> <p>27. <b>Blocked</b></p> <p>28. <b>Blocked</b></p> <p>29. <b>Blocked</b></p> <p>30. <b>Blocked</b></p> <p>31. <b>Blocked</b></p> <p>32. <b>Blocked</b></p> <p>33. <b>Blocked</b></p> <p>34. <b>Blocked</b></p> <p>35. <b>Blocked</b></p> <p>36. <b>Blocked</b></p> <p>37. <b>Blocked</b></p> <p>38. <b>Blocked</b></p> <p>39. <b>Blocked</b></p> <p>40. <b>Blocked</b></p> <p>41. <b>Blocked</b></p> <p>42. <b>Blocked</b></p> <p>43. <b>Blocked</b></p> <p>44. <b>Blocked</b></p> <p>45. <b>Blocked</b></p> <p>46. <b>Blocked</b></p> <p>47. <b>Blocked</b></p> <p>48. <b>Blocked</b></p> <p>49. <b>Blocked</b></p> <p>50. <b>Blocked</b></p> <p>51. <b>Blocked</b></p> <p>52. <b>Blocked</b></p> <p>53. <b>Blocked</b></p> <p>54. <b>Blocked</b></p> <p>55. <b>Blocked</b></p> <p>56. <b>Blocked</b></p> <p>57. <b>Blocked</b></p> <p>58. <b>Blocked</b></p> <p>59. <b>Blocked</b></p> <p>60. <b>Blocked</b></p> <p>61. <b>Blocked</b></p> <p>62. <b>Blocked</b></p> <p>63. <b>Blocked</b></p> <p>64. <b>Blocked</b></p> <p>65. <b>Blocked</b></p> <p>66. <b>Blocked</b></p> <p>67. <b>Blocked</b></p> <p>68. <b>Blocked</b></p> <p>69. <b>Blocked</b></p> <p>70. <b>Blocked</b></p> <p>71. <b>Blocked</b></p> <p>72. <b>Blocked</b></p> <p>73. <b>Blocked</b></p> <p>74. <b>Blocked</b></p> <p>75. <b>Blocked</b></p> <p>76. <b>Blocked</b></p> <p>77. <b>Blocked</b></p> <p>78. <b>Blocked</b></p> <p>79. <b>Blocked</b></p> <p>80. <b>Blocked</b></p> <p>81. <b>Blocked</b></p> <p>82. <b>Blocked</b></p> <p>83. <b>Blocked</b></p> <p>84. <b>Blocked</b></p> <p>85. <b>Blocked</b></p> <p>86. <b>Blocked</b></p> <p>87. <b>Blocked</b></p> <p>88. <b>Blocked</b></p> <p>89. <b>Blocked</b></p> <p>90. <b>Blocked</b></p> <p>91. <b>Blocked</b></p> <p>92. <b>Blocked</b></p> <p>93. <b>Blocked</b></p> <p>94. <b>Blocked</b></p> <p>95. <b>Blocked</b></p> <p>96. <b>Blocked</b></p> <p>97. <b>Blocked</b></p> <p>98. <b>Blocked</b></p> <p>99. <b>Blocked</b></p> <p>100. <b>Blocked</b></p>

[illegible]

The server doesn't manage to download the file in time and closed (client closes too)

```
File Edit Tabs Help
Jul 10 23:18:46 dnsmasq[28142]: exiting on receipt of SIGTERM
Jul 10 23:18:46 dnsmasq[28221]: started, version 2.79 cachesize 150
Jul 10 23:18:46 dnsmasq[28221]: DNS service limited to local subnets
Jul 10 23:18:46 dnsmasq[28221]: options: IPv6 GNU-getopt DBus 118n
with nettlehash DNSSEC loop-detect i
doesn't manage to
the file in time and
ent closes too)
ver 8.8.8.8#53
ver 127.0.0.1#53531 for domain b.co
ver 127.0.0.1#53531 for default
23:18:32\ncount(10min):\n466', '<
...>b.com', '2021 Jul 10 23:18:32')
up----- <...>b.com
graph+UP
<...>b.com
[<parseOnly.LOG object at 0x7fda8d5c9b0>]
```



## Detector

Show Peaks

Exit

Blocked List

Without our detector, running the same simulation results in the file being sent successfully to the server

# DNS TUNNELING DETECTOR

Running Simulation Presentation

Topics in Network Security 2021

Omer Bornstein, Alex Degtiariov