

Assignment 3

Harigovind Raghunath 22B0057

Vm setup

I used Virtual Box to set up a VM running Ubuntu-Server (Ubuntu 24.04.2 LTS)

Tor setup

```
sudo apt update
sudo apt install -y build-essential libevent-dev libssl-dev
zlib1g-dev libzstd-dev liblzma-dev \ pkg-config libssystemd-dev
libseccomp-dev git automake autoconf libtool
git clone https://git.torproject.org/tor.git
cd tor
./autogen.sh
./configure
make -j$(nproc)
sudo make install
tor --version
sudo apt upgrade tor (in retrospect directly installing tor using apt would have been
more convenient)
tor (to make sure tor bootstraps till 100%)
```

Change the torrc file located in `/etc/tor/torrc` and uncomment the following

```
ControlPort 9051
CookieAuthentication 1
```

```
Sudo service tor restart (restart tor after changing torrc)
Sudo apt install nix (if you want to use nix, which I have)
```

Screenshots

Tor 4 hop circuit creation using the script -

```
Classified relays - Guards: 5495, Middles: 2388, Exits: 2557
Hop 1: CebolaServer (FF3D4B174CE81927E3424C665F761CB6A3C54FBD) - 92.222.79.186:443
Hop 2: dotsrcExit6 (43C9F5C28EA90A1858727E2AB380612EA9CD9F42) - 185.129.61.6:443
Hop 3: F3Netze (8E38B11E849336D62AB6264FBAE9B03C70F07863) - 185.220.100.240:9100
Hop 4: NTH4R8 (5AE330C85957952B1D4A742AFC1D0FD0107B6165) - 192.42.116.194:9007

Circuit 53469 built successfully!
Connecting to check.torproject.org...
Attached stream 49000 to our circuit 53469
Connection and data test successful!
```

Nyx view of the 4 hop circuit(note that this has the same circuit ID) -

```
torr [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Relaying Disabled, Control Port (cookie): 9051 press 'n' for a new identity
page 2 / 5 - m: menu, p: pause, h: page help, q: quit
connections (2 outbound, 13 circuit, 3 directory, 1 control)
127.0.0.1:15:33116 -> 5.22.222.168:443 (pl) 98B864B7CB387B5D061EE1ACF9AC62CC889464AD Unnamed +48.1s (OUTBOUND)
10.0.2.15:52366 -> 92.222.79.186:443 (fr) FF3D4B174CEB1927E3424C665F761CB6A3C54FBD CebolaServer +48.1s (OUTBOUND)
127.0.0.1: -> Building... Purpose: Measure_timeout, Circuit ID: 53465 2.9m (CIRCUIT)
  95.217.202.113:9001 (fi) 2AB739D65B02ECA4544BC2A3C605BCF203E8A55B LaunchYT 1 / Guard
  193.190.168.53:9001 (be) ACCB74AD6D4D3AC308CB6C044620A159A1123196 kulcosictor 2 / Middle
  185.220.101.79:9100 (de) 4DECD5614F54AA3022A060074EC6BB43102E1D33 CCCStuttgartBer 3 / Extending
127.0.0.1: -> Building... Purpose: Measure_timeout, Circuit ID: 53474 2.7m (CIRCUIT)
  95.217.202.113:9001 (fi) 2AB739D65B02ECA4544BC2A3C605BCF203E8A55B LaunchYT 1 / Guard
  146.19.143.166:8080 (uz) 145C1A48FA9D246080535BC24CA4BCC9E9FFBA5F setupRelayPrivate 2 / Middle
  185.220.101.79:9100 (de) 4DECD5614F54AA3022A060074EC6BB43102E1D33 CCCStuttgartBer 3 / Extending
127.0.0.1: -> Building... Purpose: Measure_timeout, Circuit ID: 53477 2.5m (CIRCUIT)
  95.217.202.113:9001 (fi) 2AB739D65B02ECA4544BC2A3C605BCF203E8A55B LaunchYT 1 / Guard
  87.236.195.198:443 (cz) 8BC58633C9537A2E0F93A5EC09B0F40FC3247715 Determination 2 / Middle
  185.220.101.79:9100 (de) 4DECD5614F54AA3022A060074EC6BB43102E1D33 CCCStuttgartBer 3 / Extending
127.0.0.1: -> 51.91.48.151:9001 (fr) Purpose: General, Circuit ID: 53471 2.8m (CIRCUIT)
  5.22.222.168:443 (pl) 98B864B7CB387B5D061EE1ACF9AC62CC889464AD Unnamed 1 / Guard
  51.91.48.151:9001 (fr) 12D978C2A4CB4AC17940FE88F899B678A0FF9BAAD shorinax 2 / Middle
  51.91.48.151:9001 (fr) 94A1C04DDB810A7F387B862A8643CB4D9BDC9E7F2 ExitstintEZ 3 / End
127.0.0.1: -> 185.220.101.19:9003 (de) Purpose: General, Circuit ID: 53470 2.8m (CIRCUIT)
  5.22.222.168:443 (pl) 98B864B7CB387B5D061EE1ACF9AC62CC889464AD Unnamed 1 / Guard
  37.120.186.229:443 (de) FDE948EA89D927DFCE7FEF741B1707C2C5F67DBA mytorrelayinDE 2 / Middle
  185.220.101.19:9003 (de) 854778D26E70FCAD85C16EFD9C94915563B0AE678 artikel10ber75 3 / End
127.0.0.1: -> 185.220.101.64:9100 (de) Purpose: Measure_timeout, Circuit ID: 53472 2.8m (CIRCUIT)
  78.46.123.26:8443 (de) BFC4044119080D8BEF70218978EE83C3FC16AE7A antifaang 1 / Guard
  157.180.27.170:443 (de) E0D08DD134D5F2E2E40238B2D125D3B949CB7F radiance 2 / Middle
  185.220.101.64:9100 (de) 9785BD5AC04E6112071EA9172591275465FD758D CCCStuttgartBer 3 / End
127.0.0.1: -> 185.220.101.64:9100 (de) Purpose: Measure_timeout, Circuit ID: 53475 2.6m (CIRCUIT)
  78.46.123.26:8443 (de) BFC4044119080D8BEF70218978EE83C3FC16AE7A antifaang 1 / Guard
  185.242.225.19:39974 (nl) B9CC0848C297834E7974A5A85C865B8D6F554C85 hyberion 2 / Middle
  185.220.101.64:9100 (de) 9785BD5AC04E6112071EA9172591275465FD758D CCCStuttgartBer 3 / End
127.0.0.1: -> 185.220.101.64:9100 (de) Purpose: Conflux_unlinked, Circuit ID: 53480 2.4m (CIRCUIT)
  5.22.222.168:443 (pl) 98B864B7CB387B5D061EE1ACF9AC62CC889464AD Unnamed 1 / Guard
  193.218.118.202:443 (ua) FB4D059F0015FDBFE2270A9E6AB38BDF6ACFF8F0 TORtellino 2 / Middle
  185.220.101.64:9100 (de) 9785BD5AC04E6112071EA9172591275465FD758D CCCStuttgartBer 3 / End
127.0.0.1: -> 185.220.101.79:9100 (de) Purpose: Conflux_unlinked, Circuit ID: 53478 2.4m (CIRCUIT)
  5.22.222.168:443 (pl) 98B864B7CB387B5D061EE1ACF9AC62CC889464AD Unnamed 1 / Guard
  159.69.153.203:4587 (de) CB40C6277FC05D971F583AB325D126324361A065 secharo 2 / Middle
  185.220.101.79:9100 (de) 4DECD5614F54AA3022A060074EC6BB43102E1D33 CCCStuttgartBer 3 / End
127.0.0.1: -> 192.42.116.194:9007 (nl) Purpose: General, Circuit ID: 53469 2.9m (CIRCUIT)
  92.222.79.186:443 (fr) FF3D4B174CEB1927E3424C665F761CB6A3C54FBD CebolaServer 1 / Guard
  185.129.61.6:443 (dk) 43C9F5C28E990A1858727E2AB380612EA9CD9F42 dotsrcExit6 2 / Middle
  185.220.100.240:9100 (de) 8E38B11E849336D62AB6264FBAE9B83C70F07863 F3Netze 3 / Middle
  192.42.116.194:9007 (nl) 5AE330C85957952B1D4A742AFC1D0FD0107B6165 NTH4R8 4 / End
127.0.0.1: -> 192.42.116.219:9003 (nl) Purpose: Measure_timeout, Circuit ID: 53473 2.7m (CIRCUIT)
  78.46.123.26:8443 (de) BFC4044119080D8BEF70218978EE83C3FC16AE7A antifaang 1 / Guard
```

Performing curl on check.torproject to confirm that the circuit works for browsing and that we are using tor

```
ubuntu@torr:~$ curl --socks5 127.0.0.1:9050 https://check.torproject.org | grep "Congratulations"
% Total % Received % Xferd Average Speed Time Time Time Current
          Dload Upload Total Spent Left Speed
100 8299 0 8 Congratulations. This browser is configured to use Tor.
2 Congratulations. This browser is configured to use Tor.
99 0 0 7295 0 --:--:-- 0:00:01 --:--:-- 7299
```

Attachment of new stream to the circuit when curl command is used, demonstrating the use of the circuit by curl -

```
Classified relays - Guards: 5497, Middles: 2398, Exits: 2579
Hop 1: whocares (C56E98E934EDB5EEFA9322D5D4818E09325F7A80) - 92.205.17.93:443
Hop 2: relayon1145 (C746FE39C3592C470ADD8965A0FCBF5DC7E7FF091) - 185.220.101.145:11145
Hop 3: Bluejaybrd (727EDD6ED7E462532417034475C16E552F14E7E3) - 94.130.70.185:4443
Hop 4: bauruine (3A5134824DA7B1F490FD9853BFBF7E0AE50E3871) - 185.40.4.101:11443

Circuit 58583 built successfully!
Connecting to check.torproject.org...
Attached stream 50920 to our circuit 58583
Connection added data test successful!

Circuit is now ready for use
Attached stream 50921 to our custom circuit 58583
Attached stream 50922 to our custom circuit 58583
Attached stream 50923 to our custom circuit 58583
Attached stream 50924 to our custom circuit 58583
```

To run the script

sudo make install

```
Sudo make run
```

To use the circuit in curl

```
curl --socks5 127.0.0.1:9050 <domain>
```

Script explanation, methodology and assumptions are in the README