TOR ONION SERVICES

Or how I learned to stop worrying about my IP address and learned to love the tor

Andrew Denner,

Central Iowa Linux Users Group (CIALUG)

- Have you signed up for our mailing list yet?
- Website: http://cialug.org
- Slack/IRC

WELCOME TO CIALUG

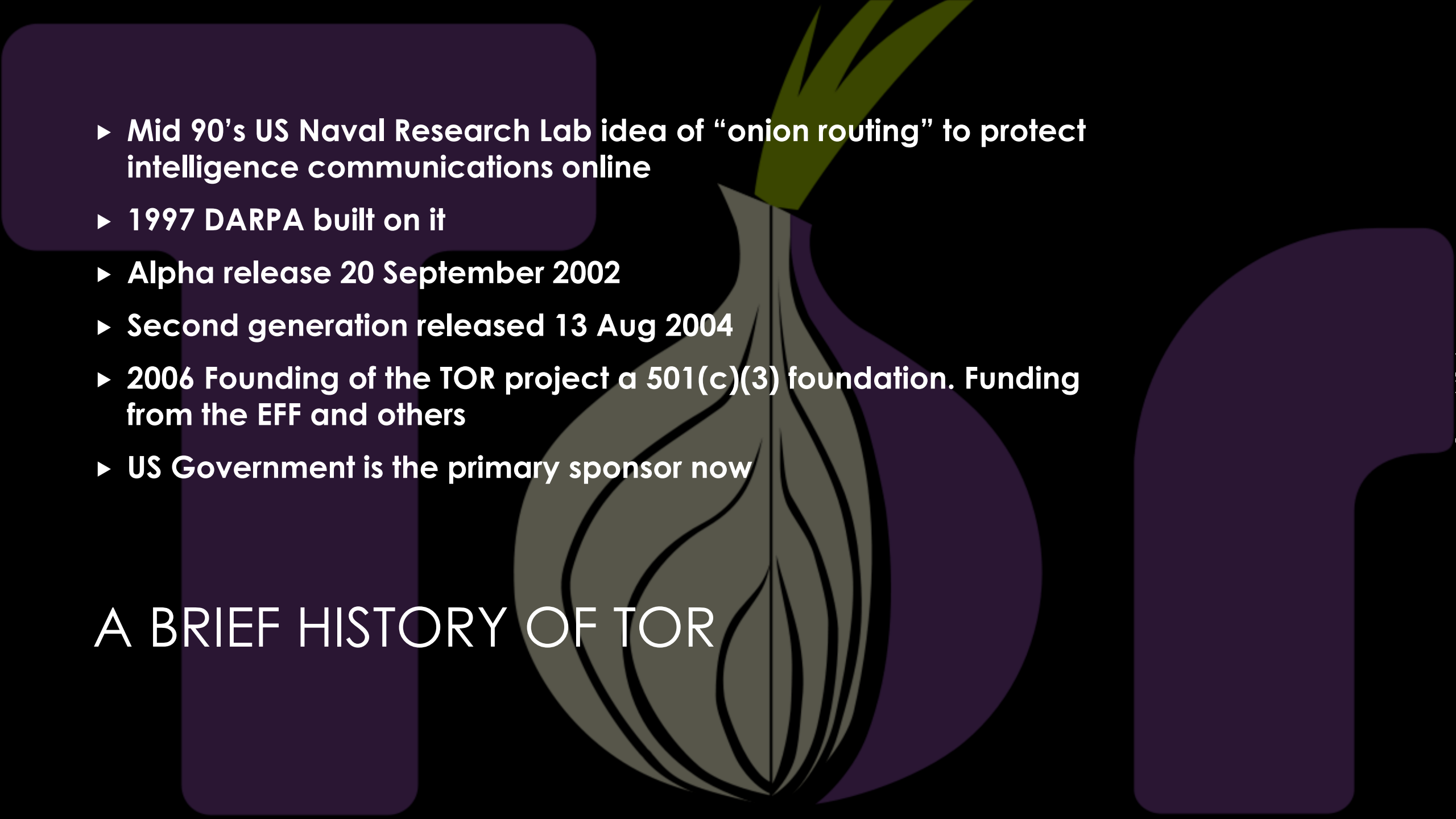
A LITTLE ABOUT ME:

- Slides will be posted at: https://denner.co
- Twitter: @adenner

ON TO OUR FEATURED PRESENTATION

A BRIEF HISTORY OF TOR

- Mid 90's US Naval Research Lab idea of "onion routing" to protect intelligence communications online
- 1997 DARPA built on it
- Alpha release 20 September 2002
- Second generation released 13 Aug 2004
- 2006 Founding of the TOR project a 501(c)(3) foundation. Funding from the EFF and others
- US Government is the primary sponsor now

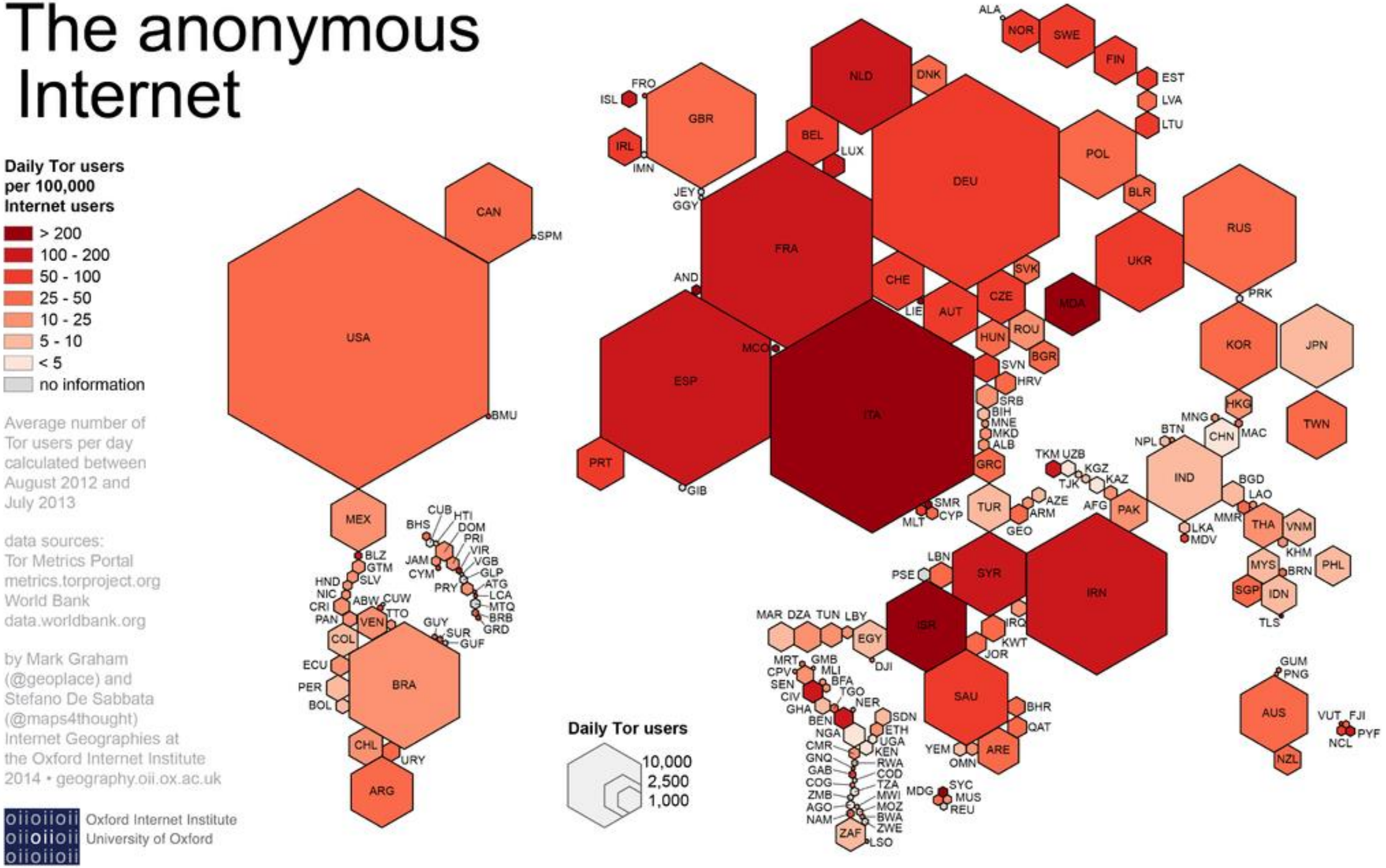


WHY?

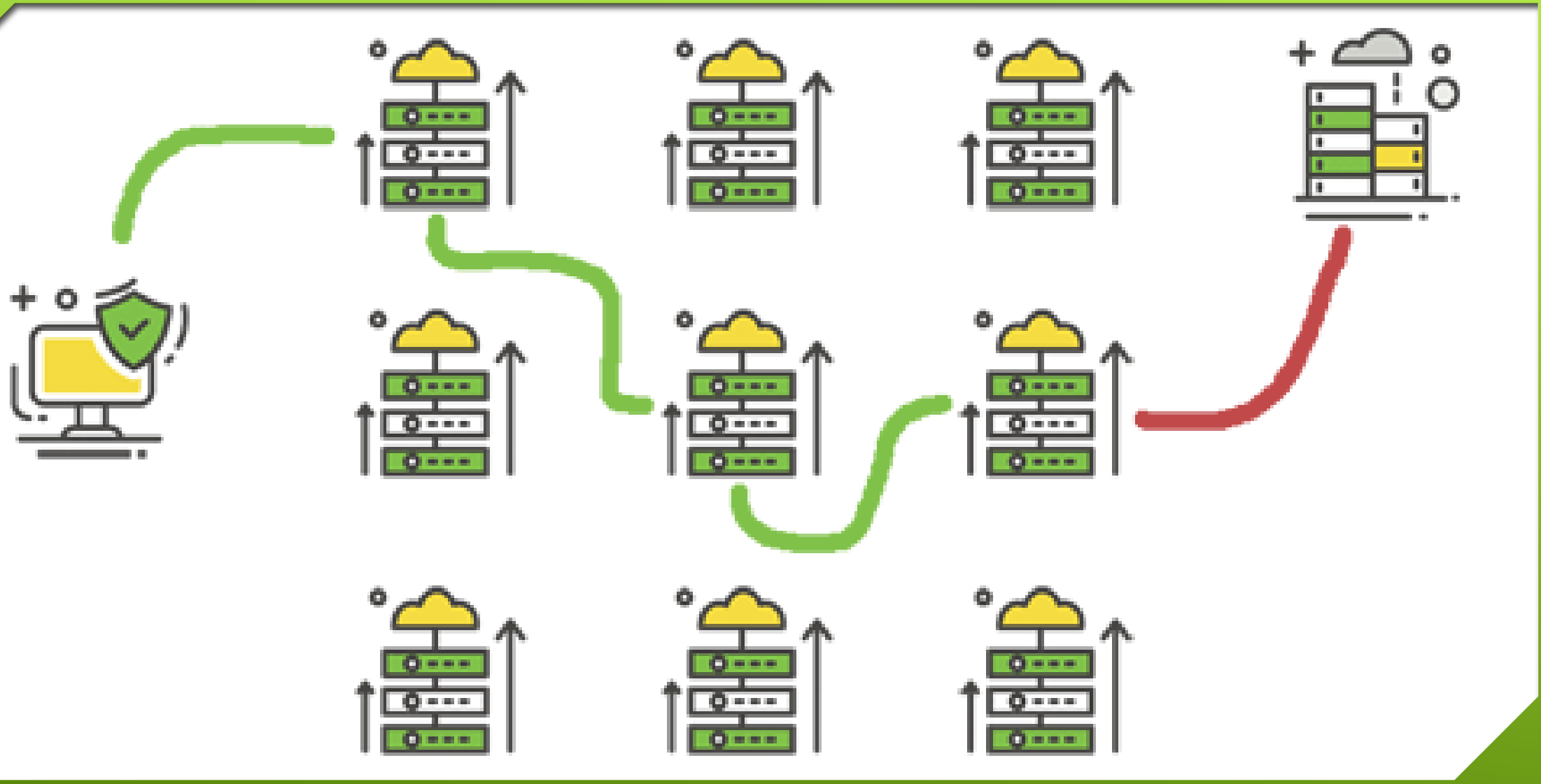
- https://www.whoishostingthis.com/blog/2014/11/17/who-funded-tor/
- “The Tor network is used by all kinds of people around the world; anyone with a need or desire to protect their online privacy. Regular Internet users who want to keep their emails private or protect their children from online predators use Tor to retain their anonymity. Citizens of countries who censor the Internet use Tor to access blocked news or social media sites, or research sensitive information on topics like AIDs or birth control that may not be available elsewhere. Journalists, bloggers, and human rights activists use Tor to protect themselves from retaliation from governments or employers. And whistleblowers use Tor to keep safe when reporting corruption.”

WHO IS USING TOR?

The anonymous Internet

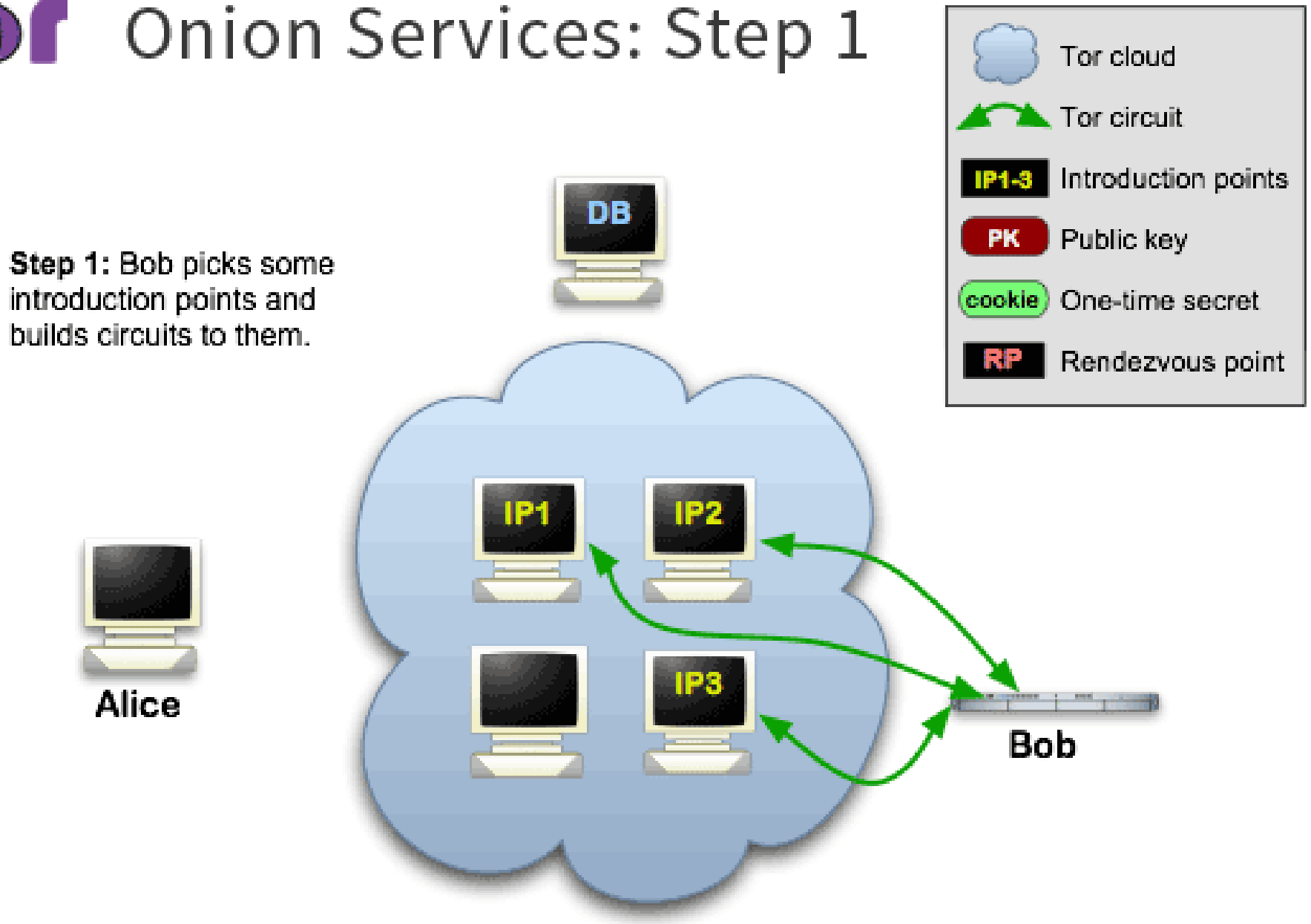


HOW DOES TOR WORK?



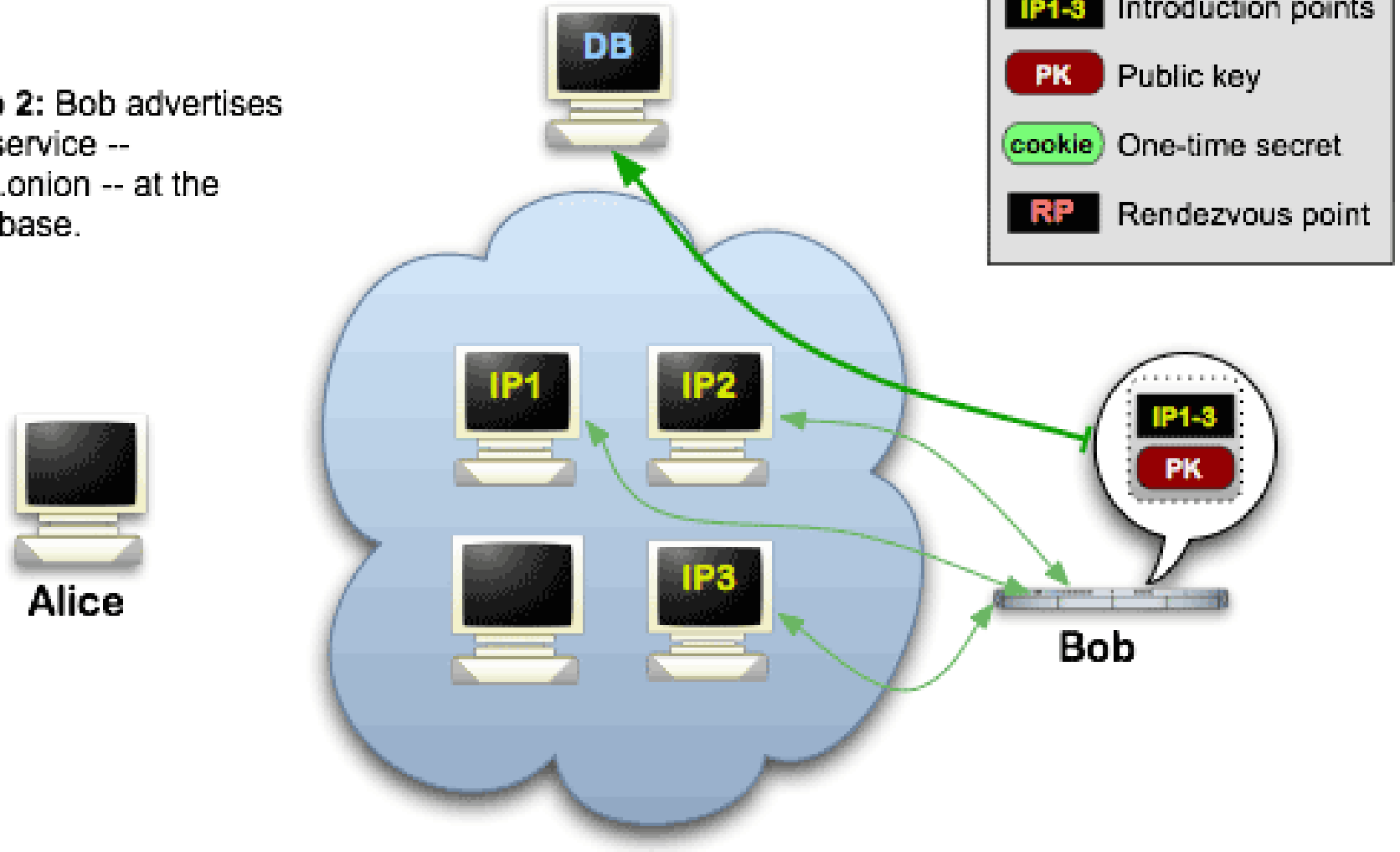
WHAT IF WE NEVER HAD TO LEAVE TOR?

Onion Services: Step 1



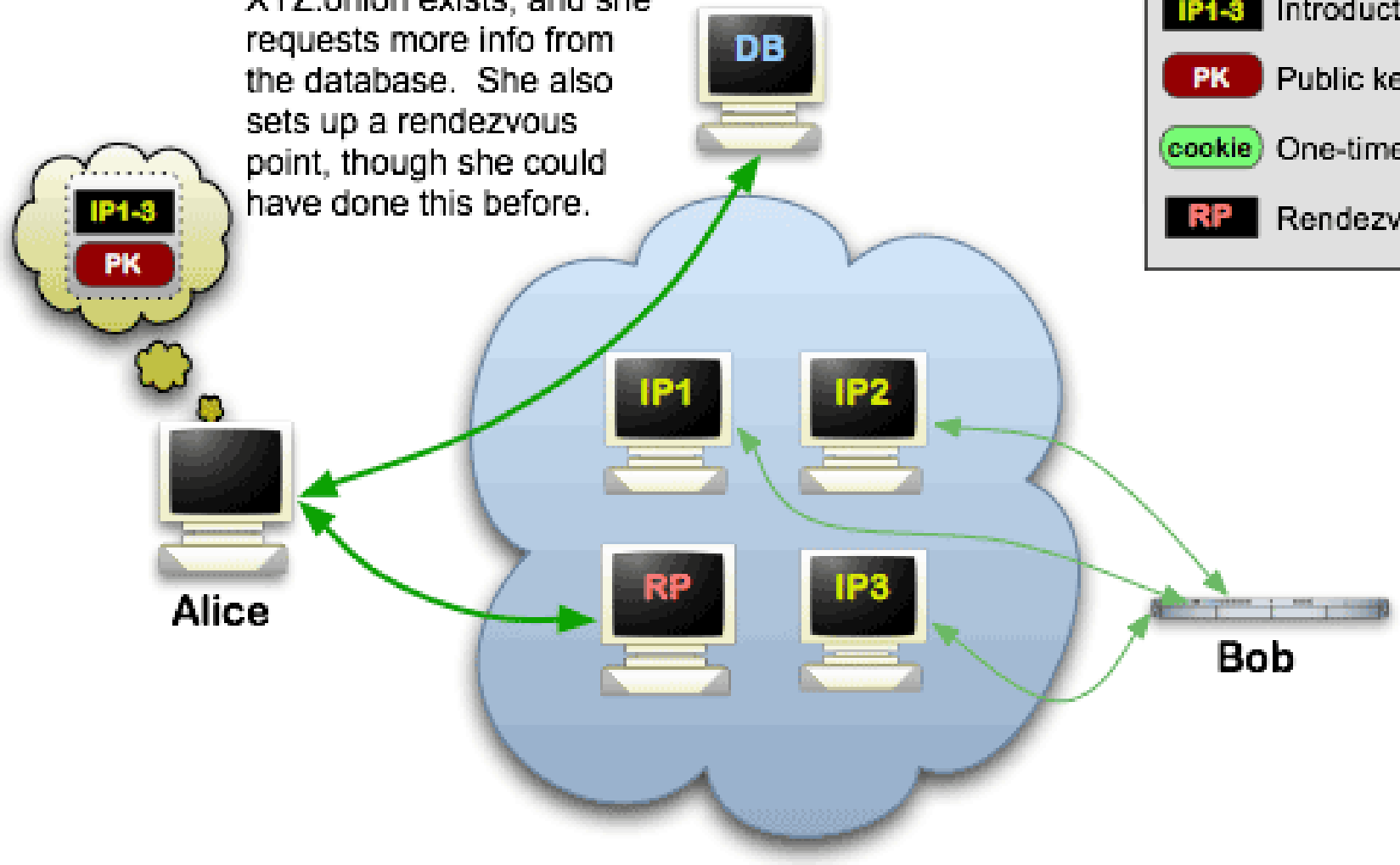
Onion Services: Step 2

Step 2: Bob advertises his service -- XYZ.onion -- at the database.



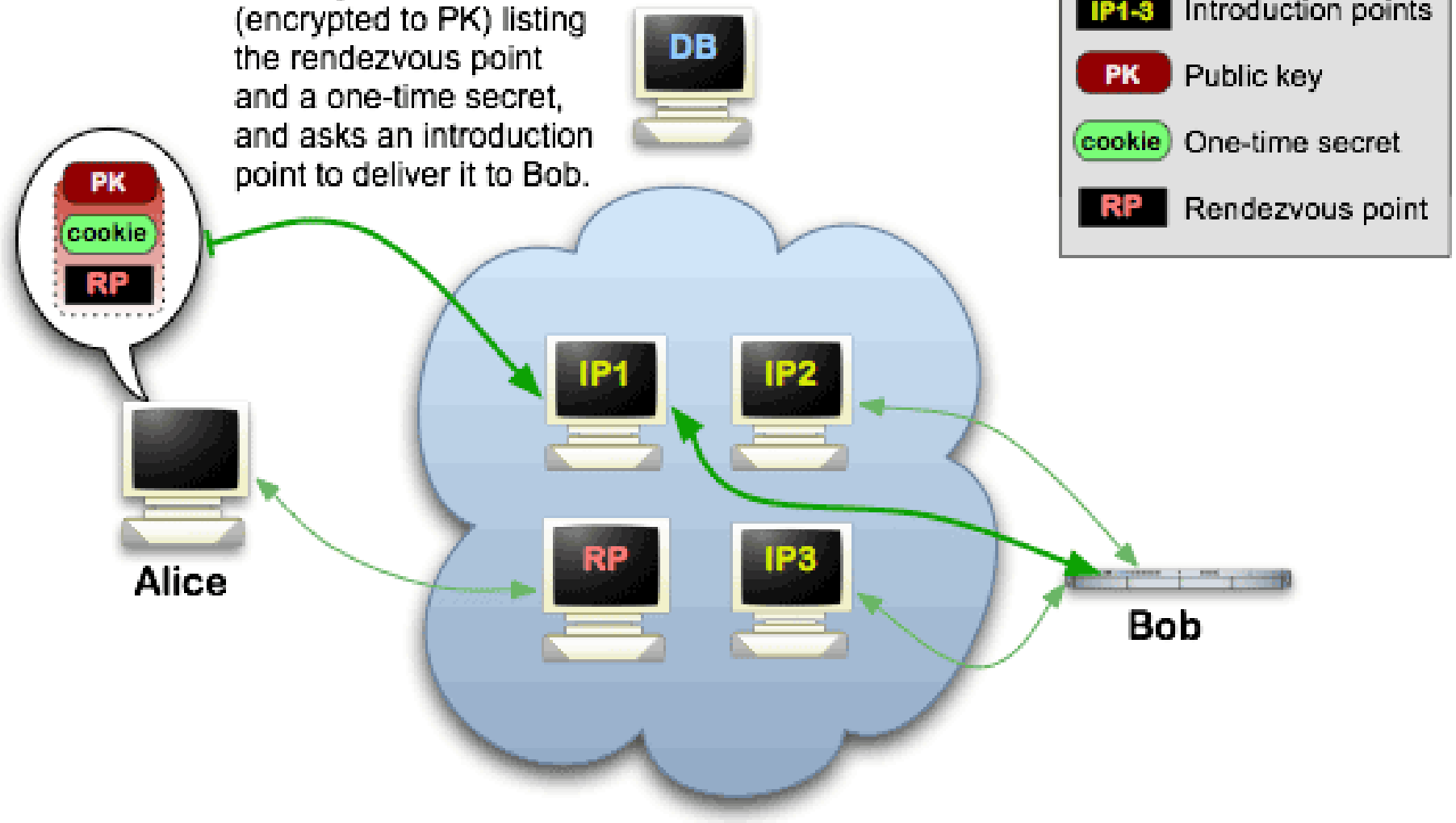
Onion Services: Step 3

Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.

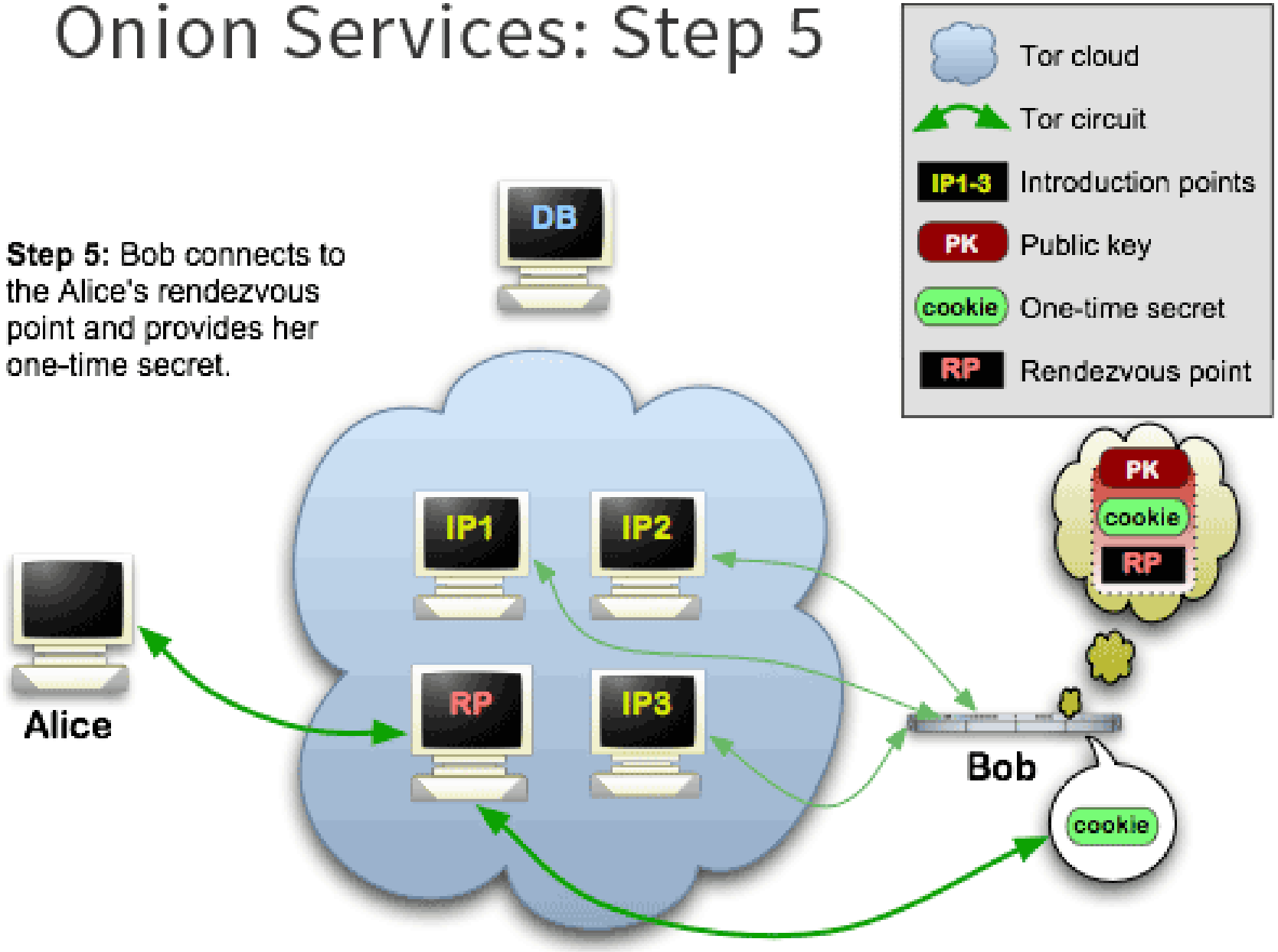


Onion Services: Step 4

Step 4: Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.

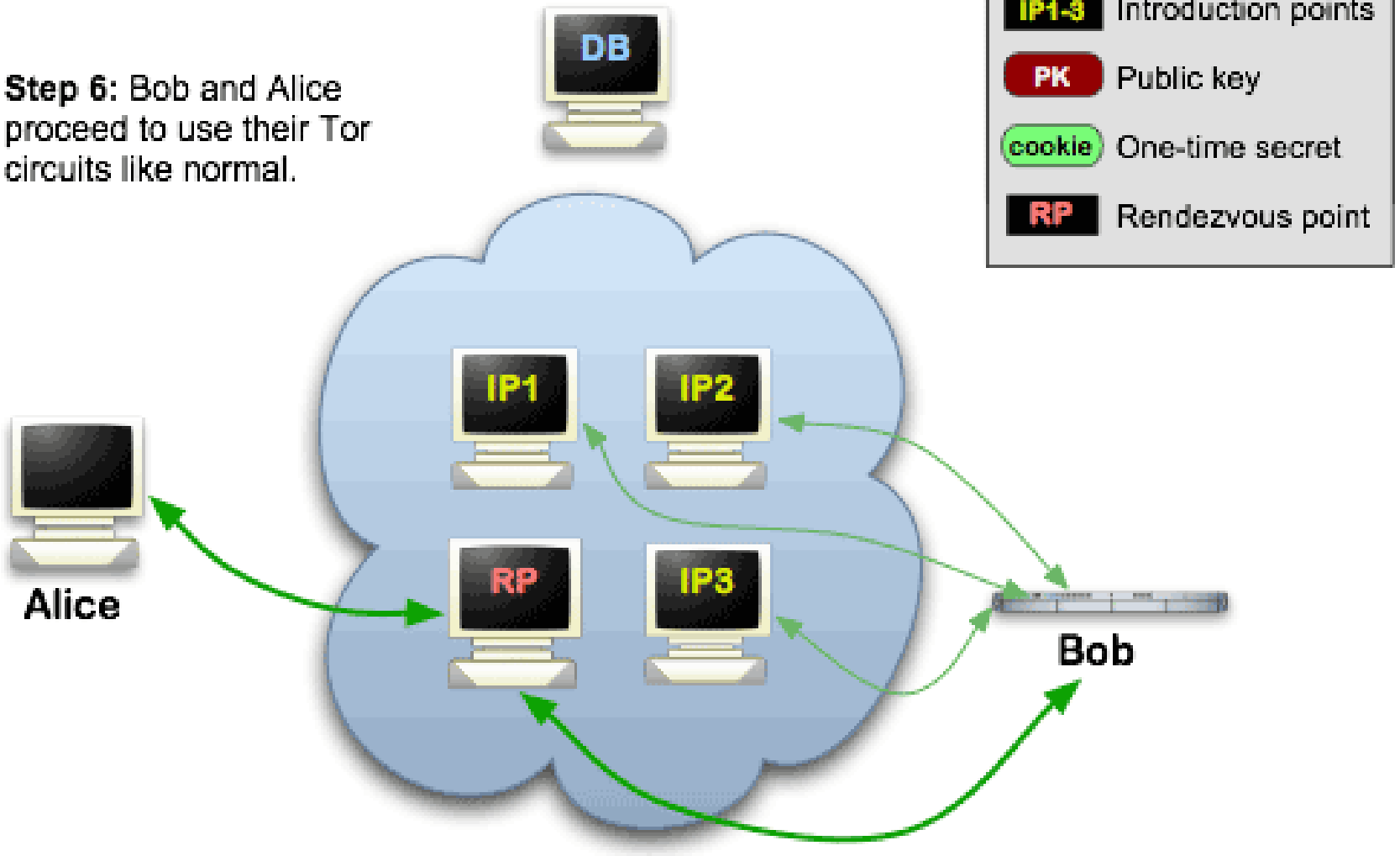


Onion Services: Step 5



Onion Services: Step 6

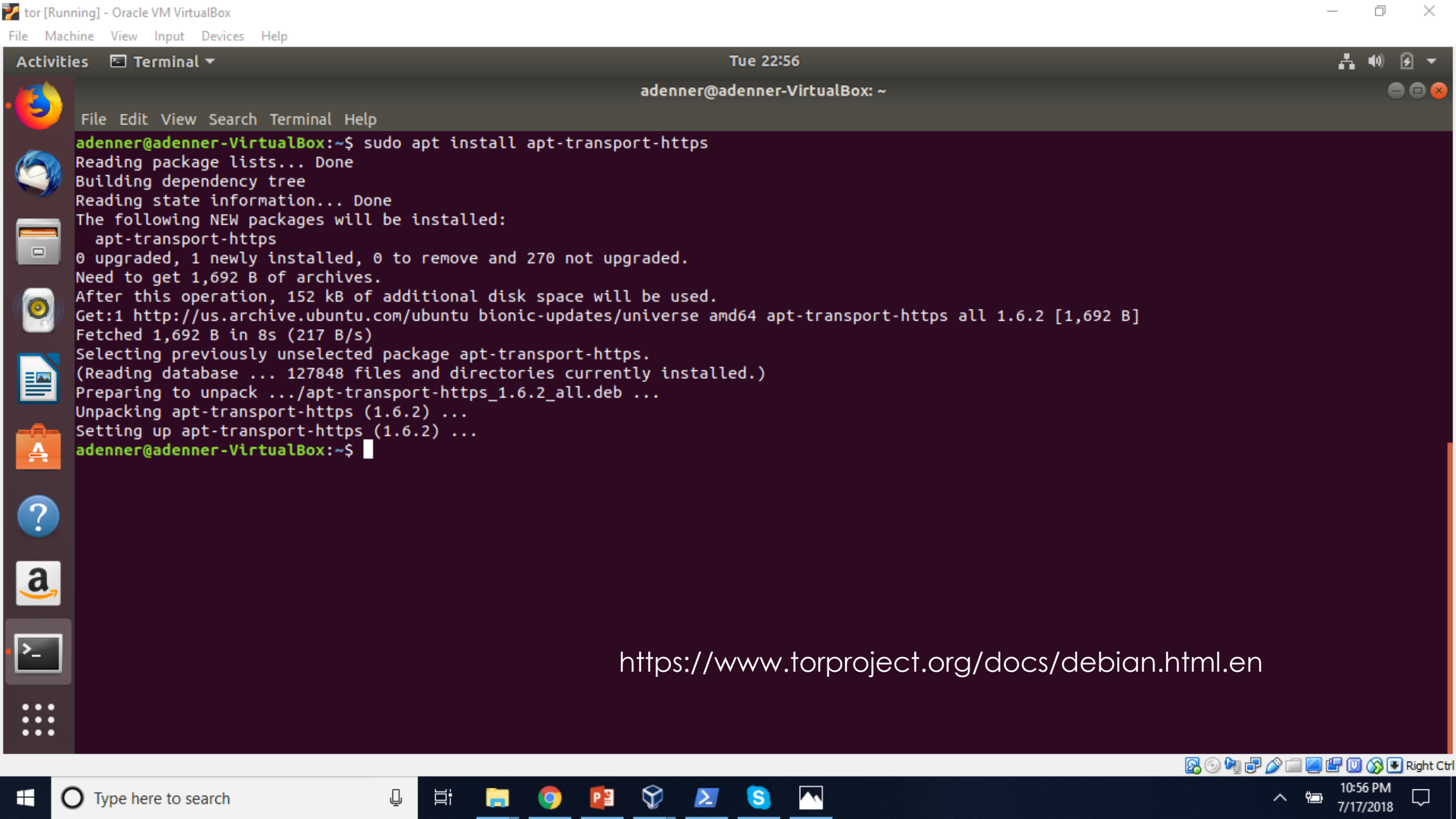
Step 6: Bob and Alice proceed to use their Tor circuits like normal.

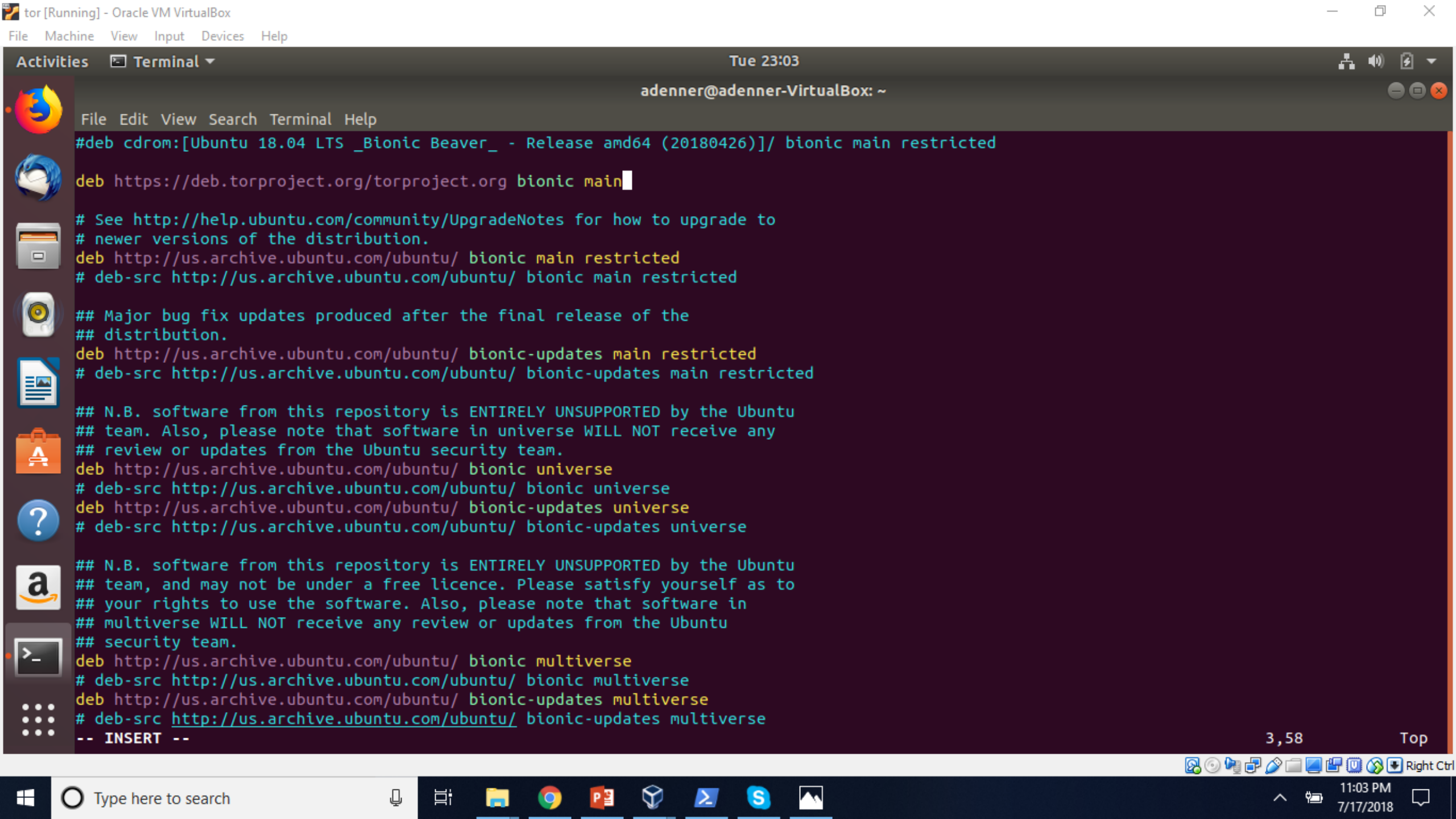


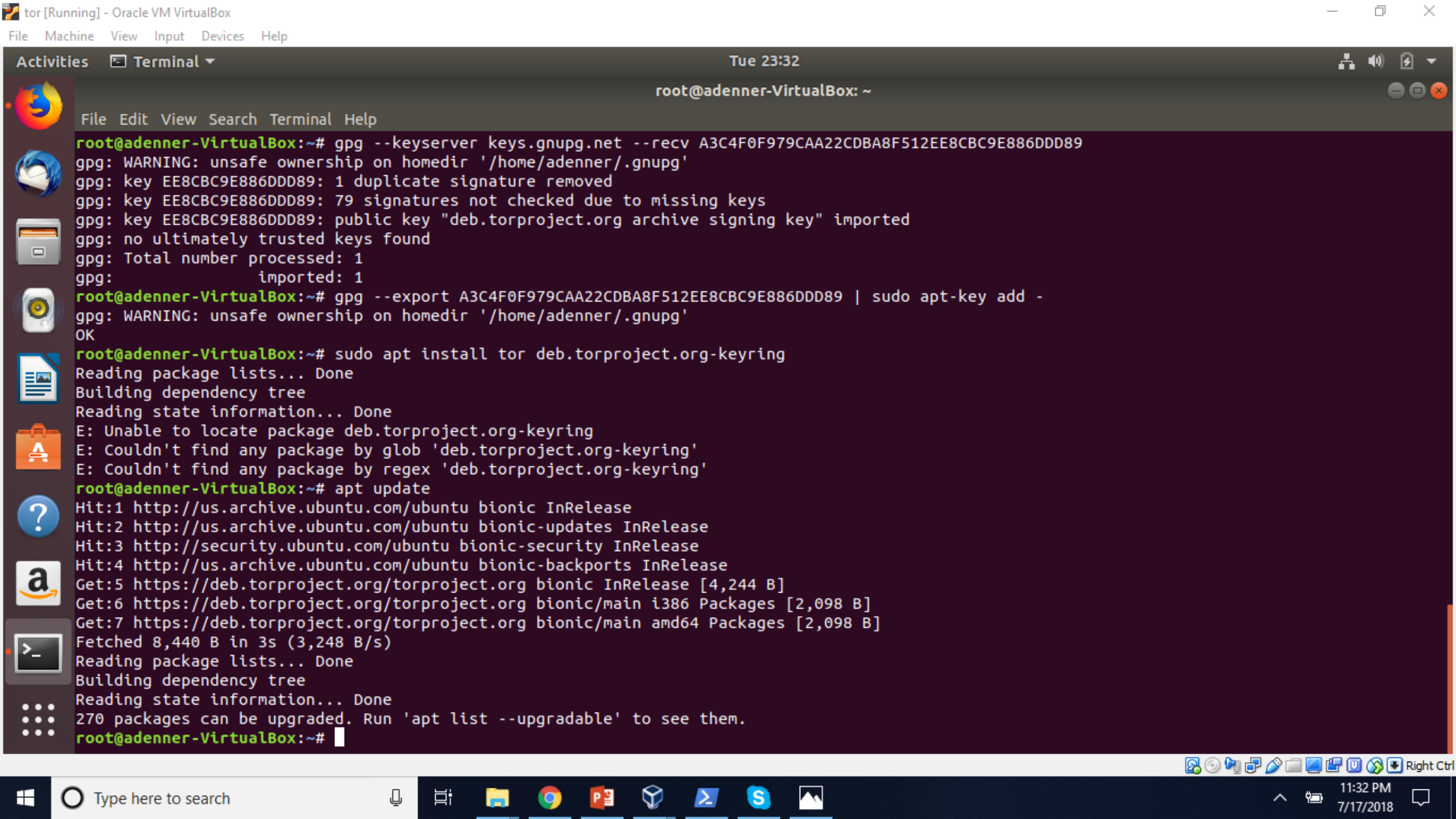
WHO USES ONION SERVICES?

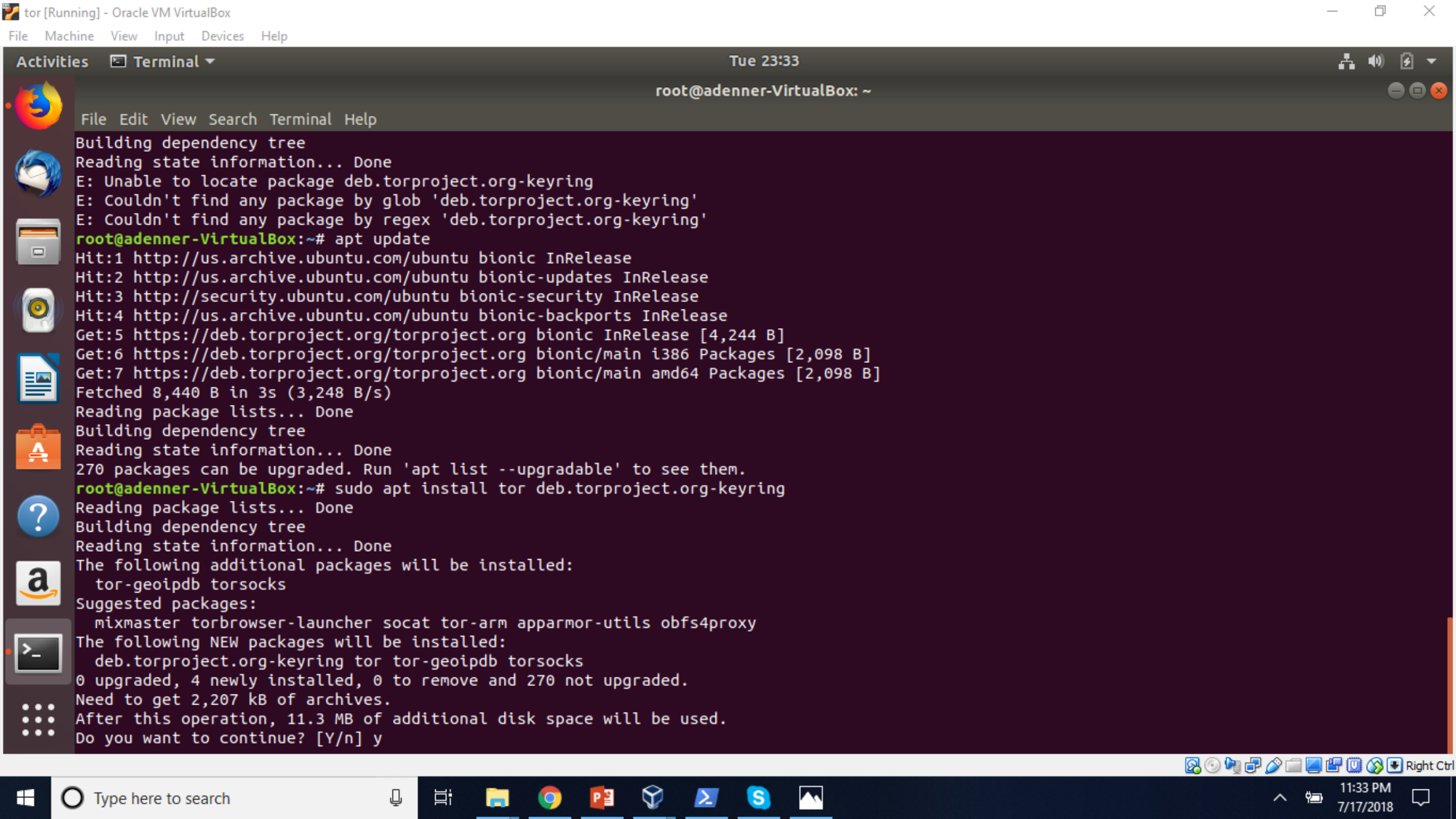
- The New York Times https://www.nytimes3xbfgragh.onion/
- The Guardian's secure drop: **33y6fjyhs3phzfjj.onion**
- **Propublica: http://propub3r6espa33w.onion/**
- **Facebook:** https://facebookcorewwwi.onion/
- Protonmail: https://protonirockerxow.onion/
- Riseup: vww6ybal4bd7szmgncyruucpgfkqahzddi37ktceo3ah7ngmcopnpyyd.onion
-

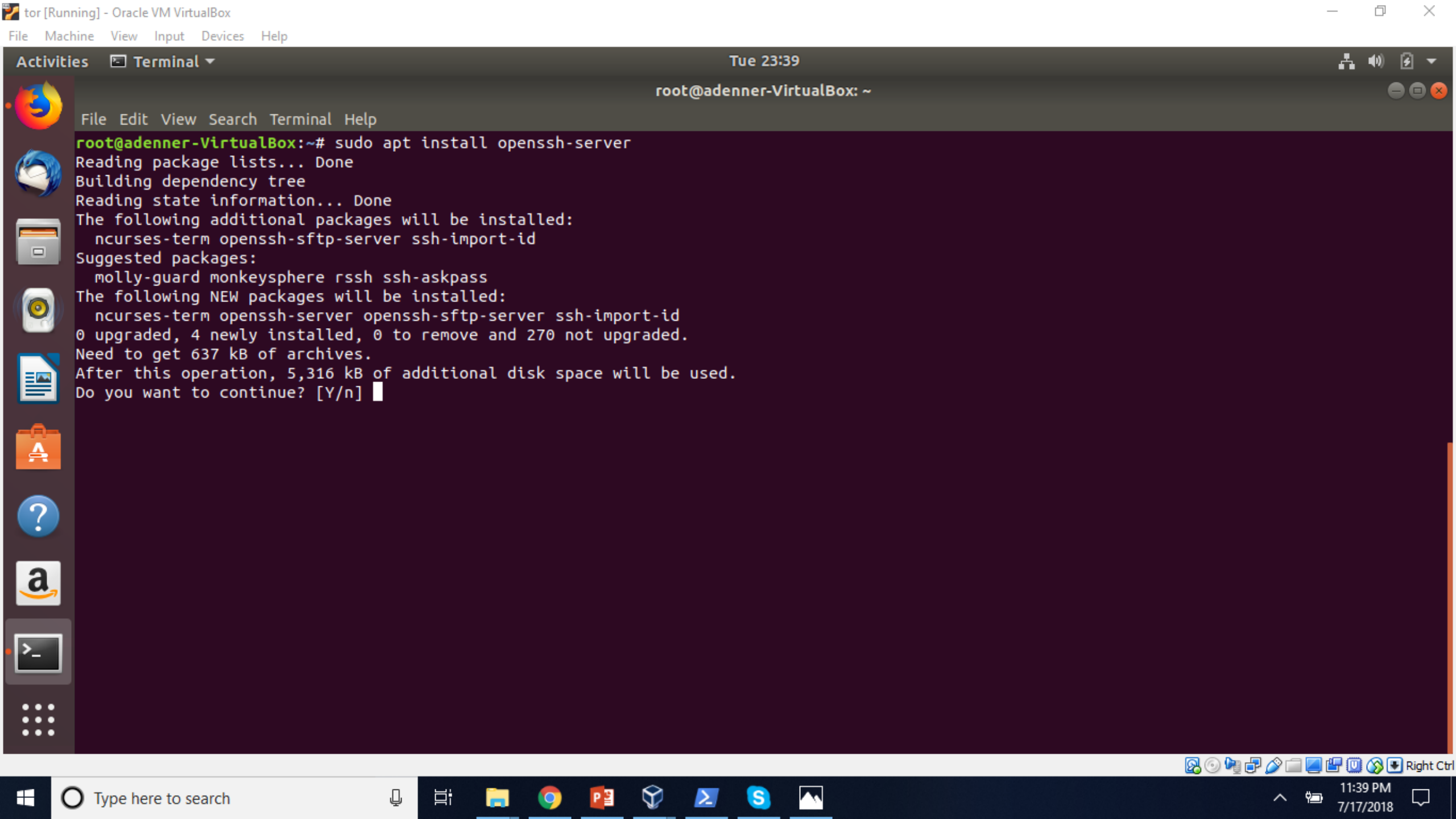
DEMO TIME!

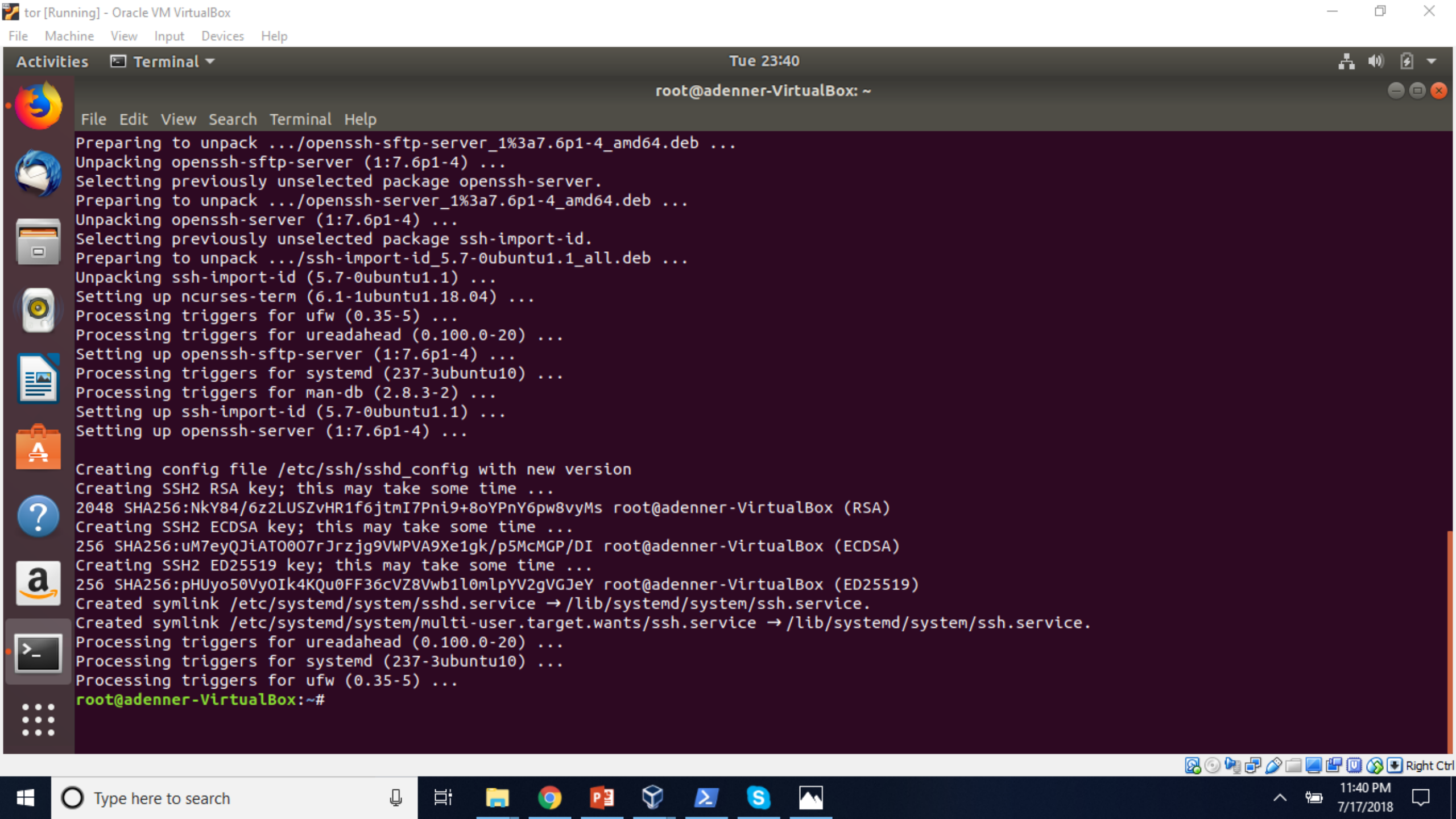

tor [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Tue 22:56
adenner@adenner-VirtualBox: ~
File Edit View Search Terminal Help
adenner@adenner-VirtualBox:~$ sudo apt install apt-transport-https
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
apt-transport-https
0 upgraded, 1 newly installed, 0 to remove and 270 not upgraded.
Need to get 1,692 B of archives.
After this operation, 152 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 apt-transport-https all 1.6.2 [1,692 B]
Fetched 1,692 B in 8s (217 B/s)
Selecting previously unselected package apt-transport-https.
(Reading database ... 127848 files and directories currently installed.)
Preparing to unpack .../apt-transport-https_1.6.2_all.deb ...
Unpacking apt-transport-https (1.6.2) ...
Setting up apt-transport-https (1.6.2) ...
adenner@adenner-VirtualBox:~$
https://www.torproject.org/docs/debian.html.en
Right Ctrl
Type here to search
10:56 PM
7/17/2018

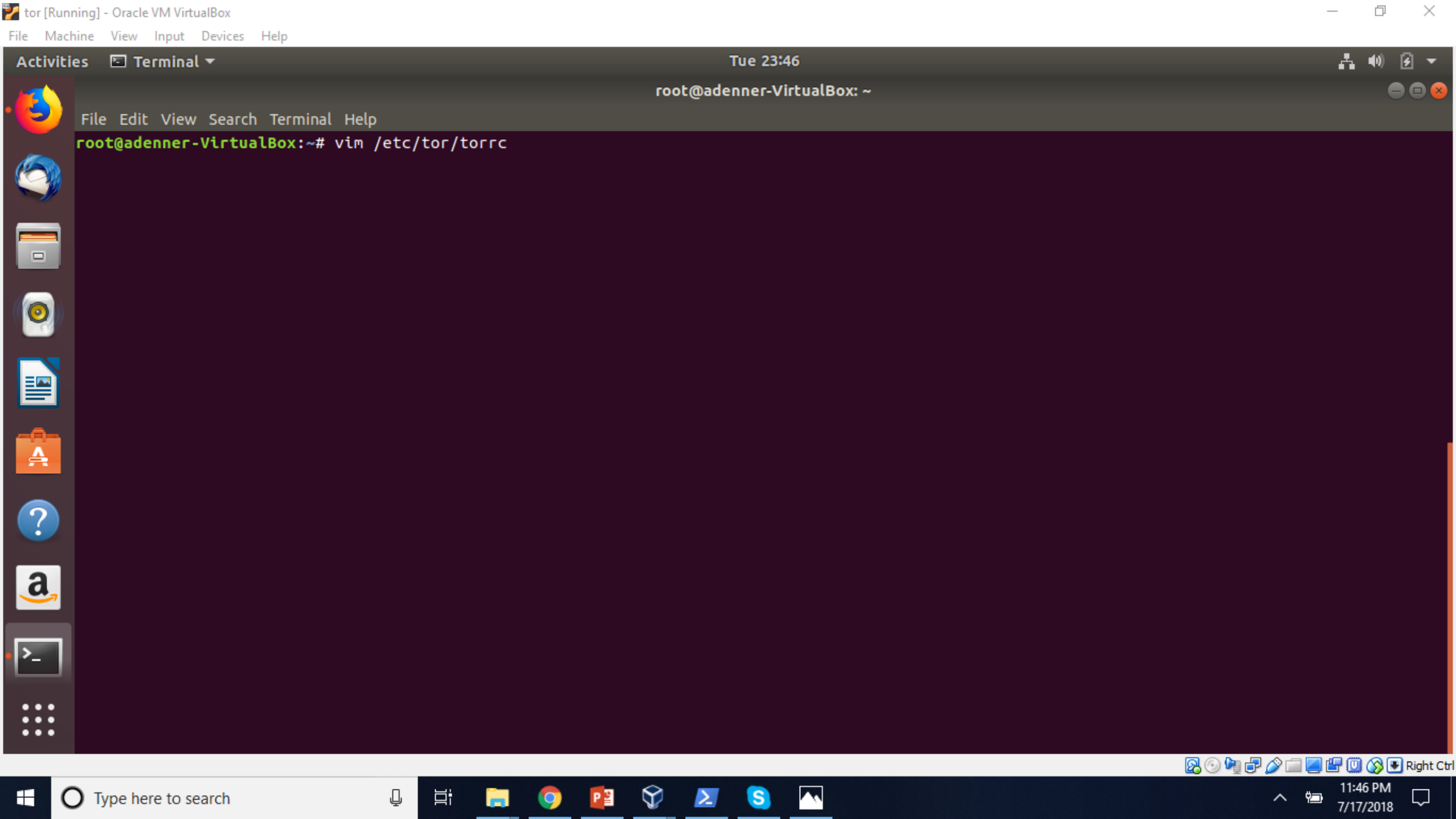

tor [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Tue 23:03
adenner@adenner-VirtualBox: ~
File Edit View Search Terminal Help
#deb cdrom:[Ubuntu 18.04 LTS _Bionic Beaver_ - Release amd64 (20180426)]/ bionic main restricted
deb https://deb.torproject.org/torproject.org bionic main
See http://help.ubuntu.com/community/UpgradeNotes for how to upgrade to
newer versions of the distribution.
deb http://us.archive.ubuntu.com/ubuntu/ bionic main restricted
deb-src http://us.archive.ubuntu.com/ubuntu/ bionic main restricted
Major bug fix updates produced after the final release of the
distribution.
deb http://us.archive.ubuntu.com/ubuntu/ bionic-updates main restricted
deb-src http://us.archive.ubuntu.com/ubuntu/ bionic-updates main restricted
N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
team. Also, please note that software in universe WILL NOT receive any
review or updates from the Ubuntu security team.
deb http://us.archive.ubuntu.com/ubuntu/ bionic universe
deb-src http://us.archive.ubuntu.com/ubuntu/ bionic universe
deb http://us.archive.ubuntu.com/ubuntu/ bionic-updates universe
deb-src http://us.archive.ubuntu.com/ubuntu/ bionic-updates universe
N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
team, and may not be under a free licence. Please satisfy yourself as to
your rights to use the software. Also, please note that software in
multiverse WILL NOT receive any review or updates from the Ubuntu
security team.
deb http://us.archive.ubuntu.com/ubuntu/ bionic multiverse
deb-src http://us.archive.ubuntu.com/ubuntu/ bionic multiverse
deb http://us.archive.ubuntu.com/ubuntu/ bionic-updates multiverse
deb-src http://us.archive.ubuntu.com/ubuntu/ bionic-updates multiverse
-- INSERT --
3,58
Top
Right Ctrl
Type here to search
11:03 PM
7/17/2018


tor [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Tue 23:32
root@adenner-VirtualBox: ~
File Edit View Search Terminal Help
root@adenner-VirtualBox:~# gpg --keyserver keys.gnupg.net --recv A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89
gpg: WARNING: unsafe ownership on homedir '/home/adenner/.gnupg'
gpg: key EE8CBC9E886DDD89: 1 duplicate signature removed
gpg: key EE8CBC9E886DDD89: 79 signatures not checked due to missing keys
gpg: key EE8CBC9E886DDD89: public key "deb.torproject.org archive signing key" imported
gpg: no ultimately trusted keys found
gpg: Total number processed: 1
gpg: imported: 1
root@adenner-VirtualBox:~# gpg --export A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89 | sudo apt-key add -
gpg: WARNING: unsafe ownership on homedir '/home/adenner/.gnupg'
OK
root@adenner-VirtualBox:~# sudo apt install tor deb.torproject.org-keyring
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package deb.torproject.org-keyring
E: Couldn't find any package by glob 'deb.torproject.org-keyring'
E: Couldn't find any package by regex 'deb.torproject.org-keyring'
root@adenner-VirtualBox:~# apt update
Hit:1 http://us.archive.ubuntu.com/ubuntu bionic InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:3 http://security.ubuntu.com/ubuntu bionic-security InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu bionic-backports InRelease
Get:5 https://deb.torproject.org/torproject.org bionic InRelease [4,244 B]
Get:6 https://deb.torproject.org/torproject.org bionic/main i386 Packages [2,098 B]
Get:7 https://deb.torproject.org/torproject.org bionic/main amd64 Packages [2,098 B]
Fetched 8,440 B in 3s (3,248 B/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
270 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@adenner-VirtualBox:~#
Right Ctrl
Type here to search
11:32 PM
7/17/2018

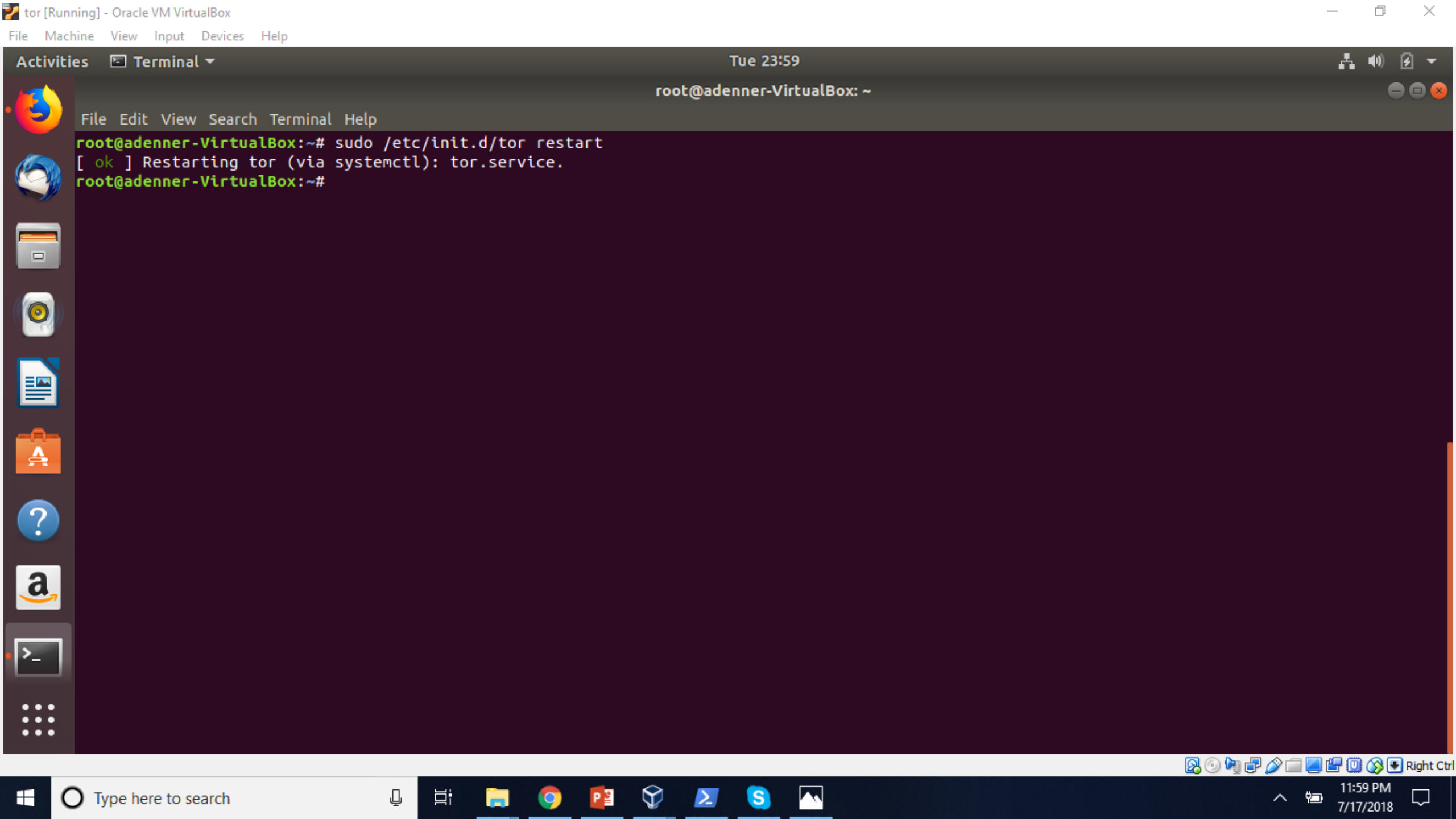

tor [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Tue 23:33
root@adenner-VirtualBox: ~
File Edit View Search Terminal Help
Building dependency tree
Reading state information... Done
E: Unable to locate package deb.torproject.org-keyring
E: Couldn't find any package by glob 'deb.torproject.org-keyring'
E: Couldn't find any package by regex 'deb.torproject.org-keyring'
root@adenner-VirtualBox:~# apt update
Hit:1 http://us.archive.ubuntu.com/ubuntu bionic InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:3 http://security.ubuntu.com/ubuntu bionic-security InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu bionic-backports InRelease
Get:5 https://deb.torproject.org/torproject.org bionic InRelease [4,244 B]
Get:6 https://deb.torproject.org/torproject.org bionic/main i386 Packages [2,098 B]
Get:7 https://deb.torproject.org/torproject.org bionic/main amd64 Packages [2,098 B]
Fetched 8,440 B in 3s (3,248 B/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
270 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@adenner-VirtualBox:~# sudo apt install tor deb.torproject.org-keyring
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
tor-geoipdb torsocks
Suggested packages:
mixmaster torbrowser-launcher socat tor-arm apparmor-utils obfs4proxy
The following NEW packages will be installed:
deb.torproject.org-keyring tor tor-geoipdb torsocks
0 upgraded, 4 newly installed, 0 to remove and 270 not upgraded.
Need to get 2,207 kB of archives.
After this operation, 11.3 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Right Ctrl
Type here to search
11:33 PM
7/17/2018

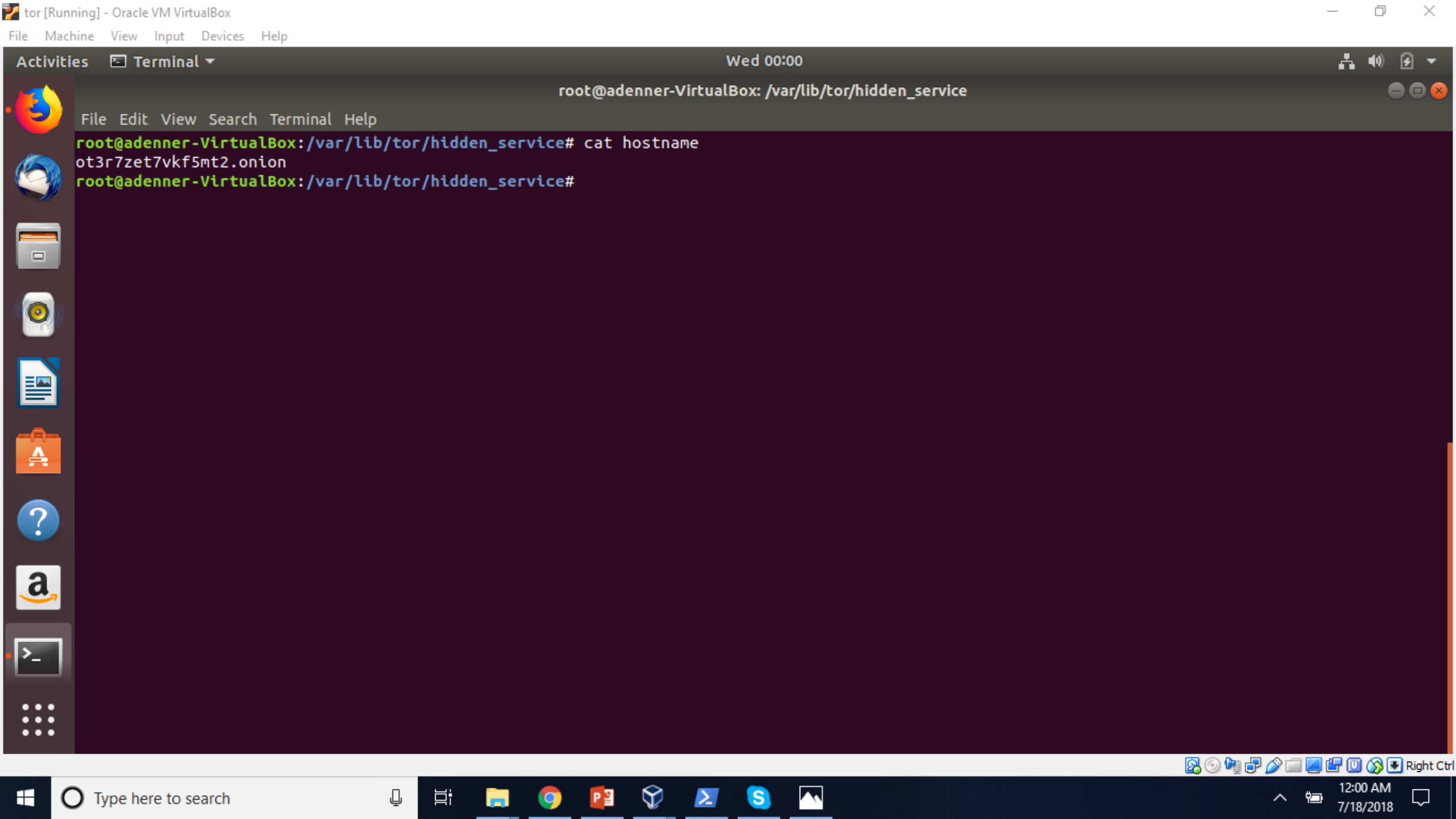

tor [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Tue 23:39
root@adenner-VirtualBox: ~
File Edit View Search Terminal Help
root@adenner-VirtualBox:~# sudo apt install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
molly-guard monkeysphere rssh ssh-askpass
The following NEW packages will be installed:
ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 270 not upgraded.
Need to get 637 kB of archives.
After this operation, 5,316 kB of additional disk space will be used.
Do you want to continue? [Y/n]
Right Ctrl
Type here to search
11:39 PM
7/17/2018

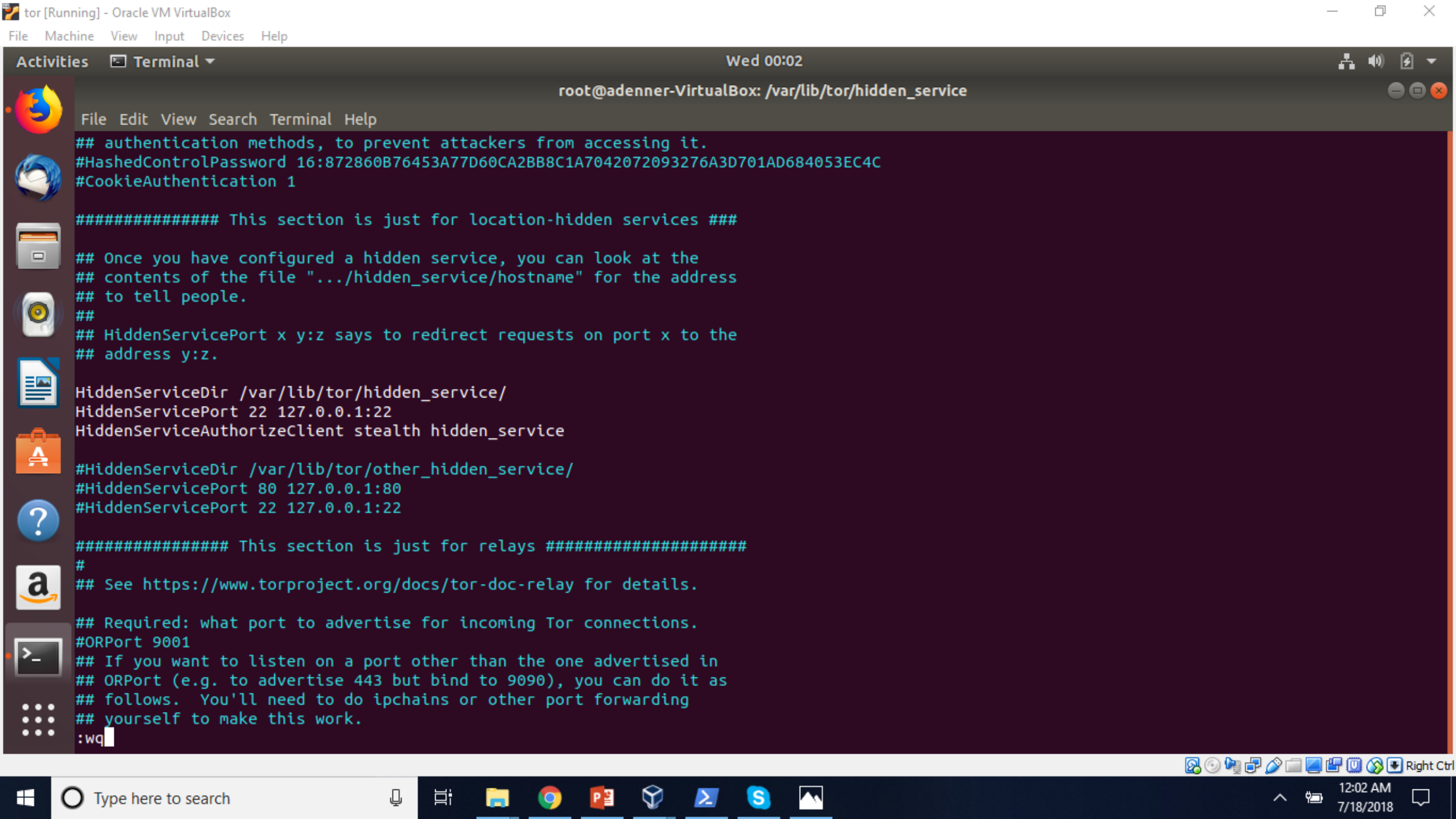

tor [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Tue 23:40
root@adenner-VirtualBox: ~
File Edit View Search Terminal Help
Preparing to unpack .../openssh-sftp-server_1%3a7.6p1-4_amd64.deb ...
Unpacking openssh-sftp-server (1:7.6p1-4) ...
Selecting previously unselected package openssh-server.
Preparing to unpack .../openssh-server_1%3a7.6p1-4_amd64.deb ...
Unpacking openssh-server (1:7.6p1-4) ...
Selecting previously unselected package ssh-import-id.
Preparing to unpack .../ssh-import-id_5.7-0ubuntu1.1_all.deb ...
Unpacking ssh-import-id (5.7-0ubuntu1.1) ...
Setting up ncurses-term (6.1-1ubuntu1.18.04) ...
Processing triggers for ufw (0.35-5) ...
Processing triggers for ureadahead (0.100.0-20) ...
Setting up openssh-sftp-server (1:7.6p1-4) ...
Processing triggers for systemd (237-3ubuntu10) ...
Processing triggers for man-db (2.8.3-2) ...
Setting up ssh-import-id (5.7-0ubuntu1.1) ...
Setting up openssh-server (1:7.6p1-4) ...
Creating config file /etc/ssh/sshd_config with new version
Creating SSH2 RSA key; this may take some time ...
2048 SHA256:NkY84/6z2LUSZvHR1f6jtmI7Pni9+8oYPnY6pw8vyMs root@adenner-VirtualBox (RSA)
Creating SSH2 ECDSA key; this may take some time ...
256 SHA256:uM7eyQJiATO0O7rJrzjg9VWPVA9Xe1gk/p5McMGP/DI root@adenner-VirtualBox (ECDSA)
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:pHUyo50VyOIk4KQu0FF36cVZ8Vwb1l0mlpYV2gVGJeY root@adenner-VirtualBox (ED25519)
Created symlink /etc/systemd/system/sshd.service → /lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/systemd/system/ssh.service.
Processing triggers for ureadahead (0.100.0-20) ...
Processing triggers for systemd (237-3ubuntu10) ...
Processing triggers for ufw (0.35-5) ...
root@adenner-VirtualBox:~#
Right Ctrl
Type here to search
11:40 PM
7/17/2018

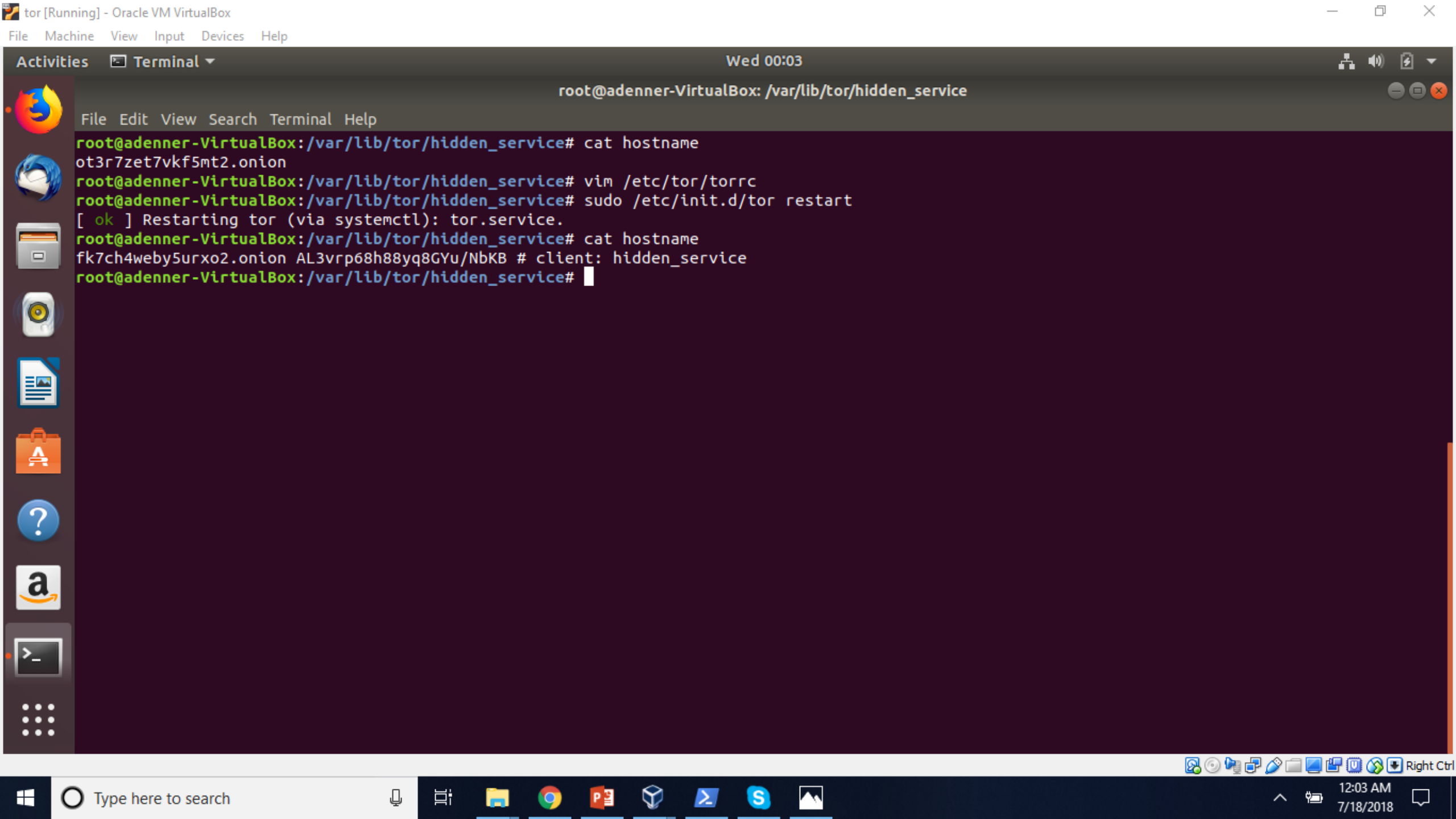

tor [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Tue 23:46
root@adenner-VirtualBox: ~
File Edit View Search Terminal Help
root@adenner-VirtualBox:~# vim /etc/tor/torrc
Right Ctrl
Type here to search
11:46 PM
7/17/2018

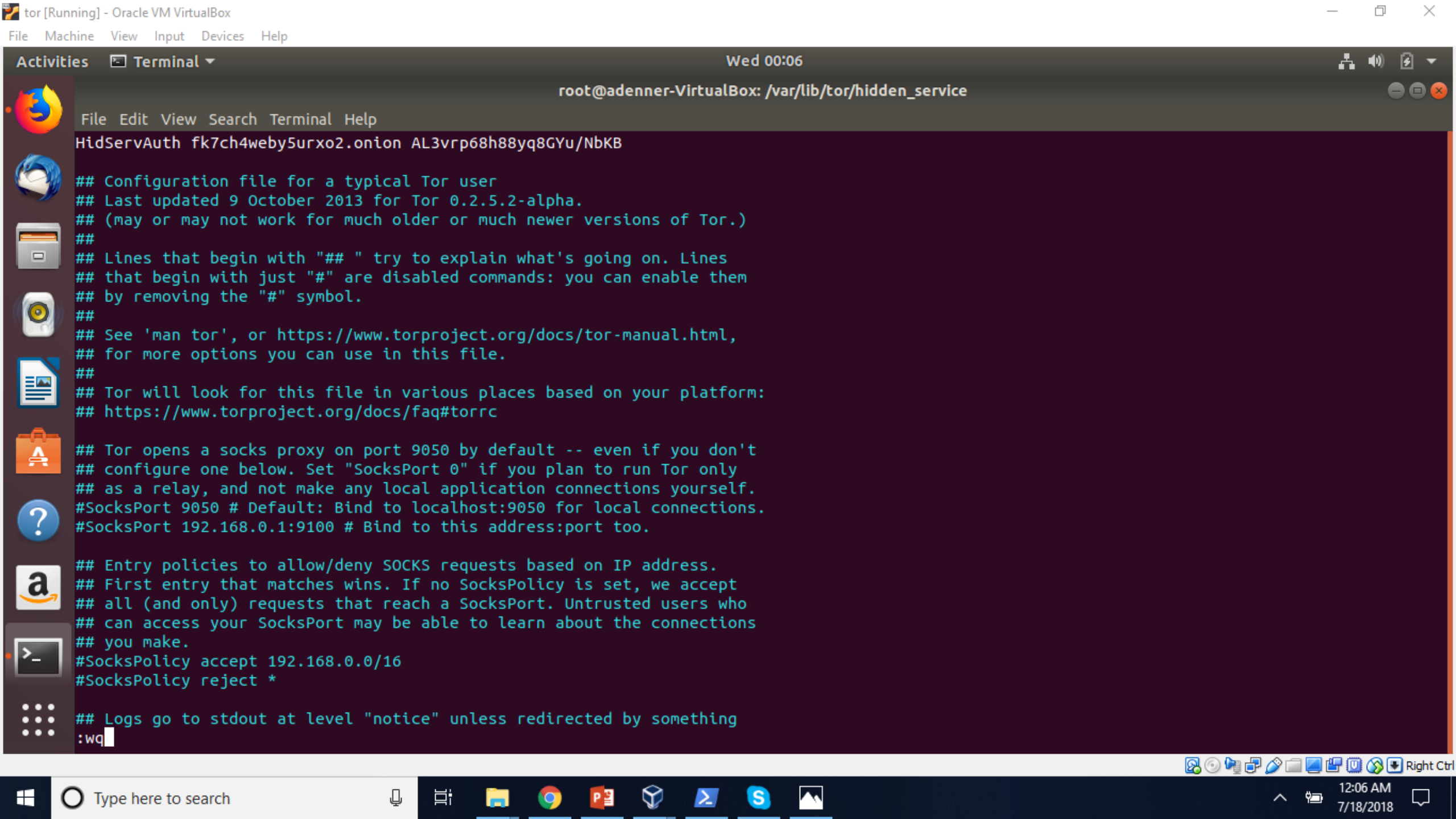
```
## see the FAQ entry if you want Tor to run as an NT service.
#RunAsDaemon 1

## The directory for keeping all the keys/etc. By default, we store
## things in $HOME/.tor on Unix, and in Application Data\tor on Windows.
#DataDirectory /var/lib/tor

## The port on which Tor will listen for local connections from Tor
## controller applications, as documented in control-spec.txt.
#ControlPort 9051
## If you enable the controlport, be sure to enable one of these
## authentication methods, to prevent attackers from accessing it.
#HashedControlPassword 16:872860B76453A77D60CA2BB8C1A7042072093276A3D701AD684053EC4C
#CookieAuthentication 1

############### This section is just for location-hidden services ###

## Once you have configured a hidden service, you can look at the
## contents of the file ".../hidden_service/hostname" for the address
## to tell people.
##
## HiddenServicePort x y:z says to redirect requests on port x to the
## address y:z.

HiddenServiceDir /var/lib/tor/hidden_service/
HiddenServicePort 22 127.0.0.1:22

#HiddenServiceDir /var/lib/tor/other_hidden_service/
#HiddenServicePort 80 127.0.0.1:80
#HiddenServicePort 22 127.0.0.1:22

-- INSERT --                                                    72,34         28%
```

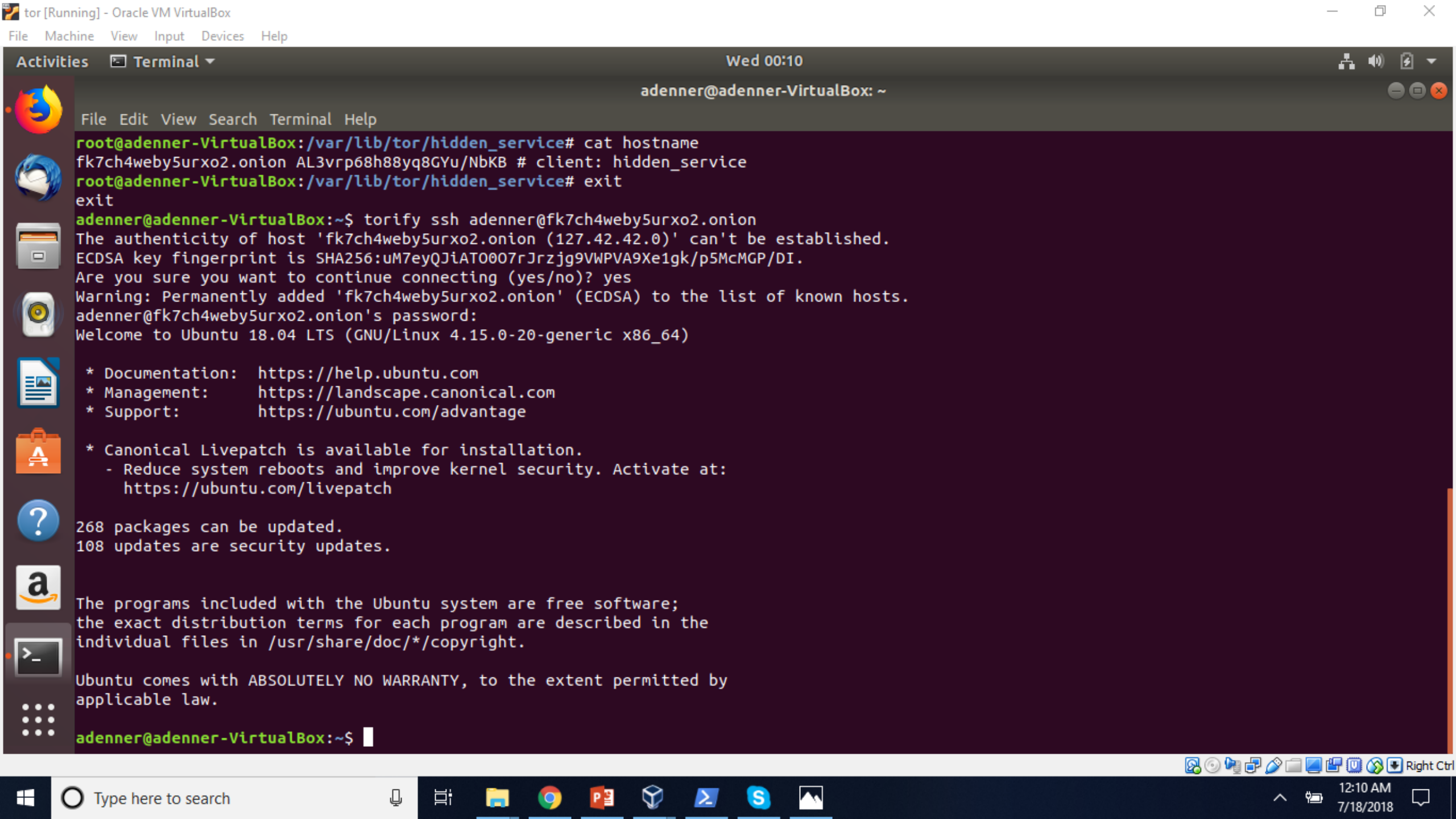

tor [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Tue 23:59
root@adenner-VirtualBox: ~
File Edit View Search Terminal Help
root@adenner-VirtualBox:~# sudo /etc/init.d/tor restart
[ok] Restarting tor (via systemctl): tor.service.
root@adenner-VirtualBox:~#
Right Ctrl
Type here to search
11:59 PM
7/17/2018


tor [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Wed 00:00
root@adenner-VirtualBox: /var/lib/tor/hidden_service
File Edit View Search Terminal Help
root@adenner-VirtualBox:/var/lib/tor/hidden_service# cat hostname
ot3r7zet7vkf5mt2.onion
root@adenner-VirtualBox:/var/lib/tor/hidden_service#
Right Ctrl
Type here to search
12:00 AM
7/18/2018


tor [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Wed 00:02
root@adenner-VirtualBox: /var/lib/tor/hidden_service
File Edit View Search Terminal Help
authentication methods, to prevent attackers from accessing it.
#HashedControlPassword 16:872860B76453A77D60CA2BB8C1A7042072093276A3D701AD684053EC4C
#CookieAuthentication 1
############### This section is just for location-hidden services ###
Once you have configured a hidden service, you can look at the
contents of the file ".../hidden_service/hostname" for the address
to tell people.
##
HiddenServicePort x y:z says to redirect requests on port x to the
address y:z.
HiddenServiceDir /var/lib/tor/hidden_service/
HiddenServicePort 22 127.0.0.1:22
HiddenServiceAuthorizeClient stealth hidden_service
#HiddenServiceDir /var/lib/tor/other_hidden_service/
#HiddenServicePort 80 127.0.0.1:80
#HiddenServicePort 22 127.0.0.1:22
################ This section is just for relays #####################
#
See https://www.torproject.org/docs/tor-doc-relay for details.
Required: what port to advertise for incoming Tor connections.
#ORPort 9001
If you want to listen on a port other than the one advertised in
ORPort (e.g. to advertise 443 but bind to 9090), you can do it as
follows. You'll need to do ipchains or other port forwarding
yourself to make this work.
:wq
Right Ctrl
Type here to search
12:02 AM
7/18/2018


tor [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Wed 00:03
root@adenner-VirtualBox: /var/lib/tor/hidden_service
File Edit View Search Terminal Help
root@adenner-VirtualBox:/var/lib/tor/hidden_service# cat hostname
ot3r7zet7vkf5mt2.onion
root@adenner-VirtualBox:/var/lib/tor/hidden_service# vim /etc/tor/torrc
root@adenner-VirtualBox:/var/lib/tor/hidden_service# sudo /etc/init.d/tor restart
[ok] Restarting tor (via systemctl): tor.service.
root@adenner-VirtualBox:/var/lib/tor/hidden_service# cat hostname
fk7ch4weby5urxo2.onion AL3vrp68h88yq8GYu/NbKB # client: hidden_service
root@adenner-VirtualBox:/var/lib/tor/hidden_service#
Right Ctrl
Type here to search
12:03 AM
7/18/2018


tor [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Wed 00:06
root@adenner-VirtualBox: /var/lib/tor/hidden_service
File Edit View Search Terminal Help
HidServAuth fk7ch4weby5urxo2.onion AL3vrp68h88yq8GYu/NbKB
Configuration file for a typical Tor user
Last updated 9 October 2013 for Tor 0.2.5.2-alpha.
(may or may not work for much older or much newer versions of Tor.)
##
Lines that begin with "## " try to explain what's going on. Lines
that begin with just "#" are disabled commands: you can enable them
by removing the "#" symbol.
##
See 'man tor', or https://www.torproject.org/docs/tor-manual.html,
for more options you can use in this file.
##
Tor will look for this file in various places based on your platform:
https://www.torproject.org/docs/faq#torrc
Tor opens a socks proxy on port 9050 by default -- even if you don't
configure one below. Set "SocksPort 0" if you plan to run Tor only
as a relay, and not make any local application connections yourself.
#SocksPort 9050 # Default: Bind to localhost:9050 for local connections.
#SocksPort 192.168.0.1:9100 # Bind to this address:port too.
Entry policies to allow/deny SOCKS requests based on IP address.
First entry that matches wins. If no SocksPolicy is set, we accept
all (and only) requests that reach a SocksPort. Untrusted users who
can access your SocksPort may be able to learn about the connections
you make.
#SocksPolicy accept 192.168.0.0/16
#SocksPolicy reject *
Logs go to stdout at level "notice" unless redirected by something
:wq
Right Ctrl
Type here to search
12:06 AM
7/18/2018


tor [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Wed 00:10
adenner@adenner-VirtualBox: ~
File Edit View Search Terminal Help
root@adenner-VirtualBox:/var/lib/tor/hidden_service# cat hostname
fk7ch4weby5urxo2.onion AL3vrp68h88yq8GYu/NbKB # client: hidden_service
root@adenner-VirtualBox:/var/lib/tor/hidden_service# exit
exit
adenner@adenner-VirtualBox:~$ torify ssh adenner@fk7ch4weby5urxo2.onion
The authenticity of host 'fk7ch4weby5urxo2.onion (127.42.42.0)' can't be established.
ECDSA key fingerprint is SHA256:uM7eyQJiATO0O7rJrzjg9VWPVA9Xe1gk/p5McMGP/DI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'fk7ch4weby5urxo2.onion' (ECDSA) to the list of known hosts.
adenner@fk7ch4weby5urxo2.onion's password:
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-20-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
* Canonical Livepatch is available for installation.
- Reduce system reboots and improve kernel security. Activate at:
https://ubuntu.com/livepatch
268 packages can be updated.
108 updates are security updates.
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
adenner@adenner-VirtualBox:~$
Right Ctrl
Type here to search
12:10 AM
7/18/2018

RESOURCES

- https://www.torproject.org/docs/onion-services.html.en
- https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf
- Tor onion services: more useful than you think https://www.youtube.com/watch?v=wHmxCeLpveA
- https://medium.com/@tzhenghao/how-to-ssh-over-tor-onion-service-c6d06194147