

LAB 11: *Using FOG for Cloning and Imaging Disks*

FOG is a free open-source cloning/imaging solution/rescue suite.

□ FOG can be used to image Windows XP, Vista, Windows 7 and Window 8 PCs using PXE, PartClone, and a Web GUI to tie it together. Includes features like memory and disk test, disk wipe, avscan & task scheduling.

Using FOG in Malware Analysis

If a computer is badly infected with a virus or malware, you can boot FOG in AV mode and have it remove the viruses.

- Set up Lab with physical machines
- Use Deep Freeze (restore), FOG (clone/restore), etc

Install FOG

1. Install the distribution you wish to install FOG on and fully update your system's software packages. Updating packages prior to the FOG setup is important, as updating post-install can break the install. So be sure to run **apt-get update** or **yum update**, as appropriate for your distribution.

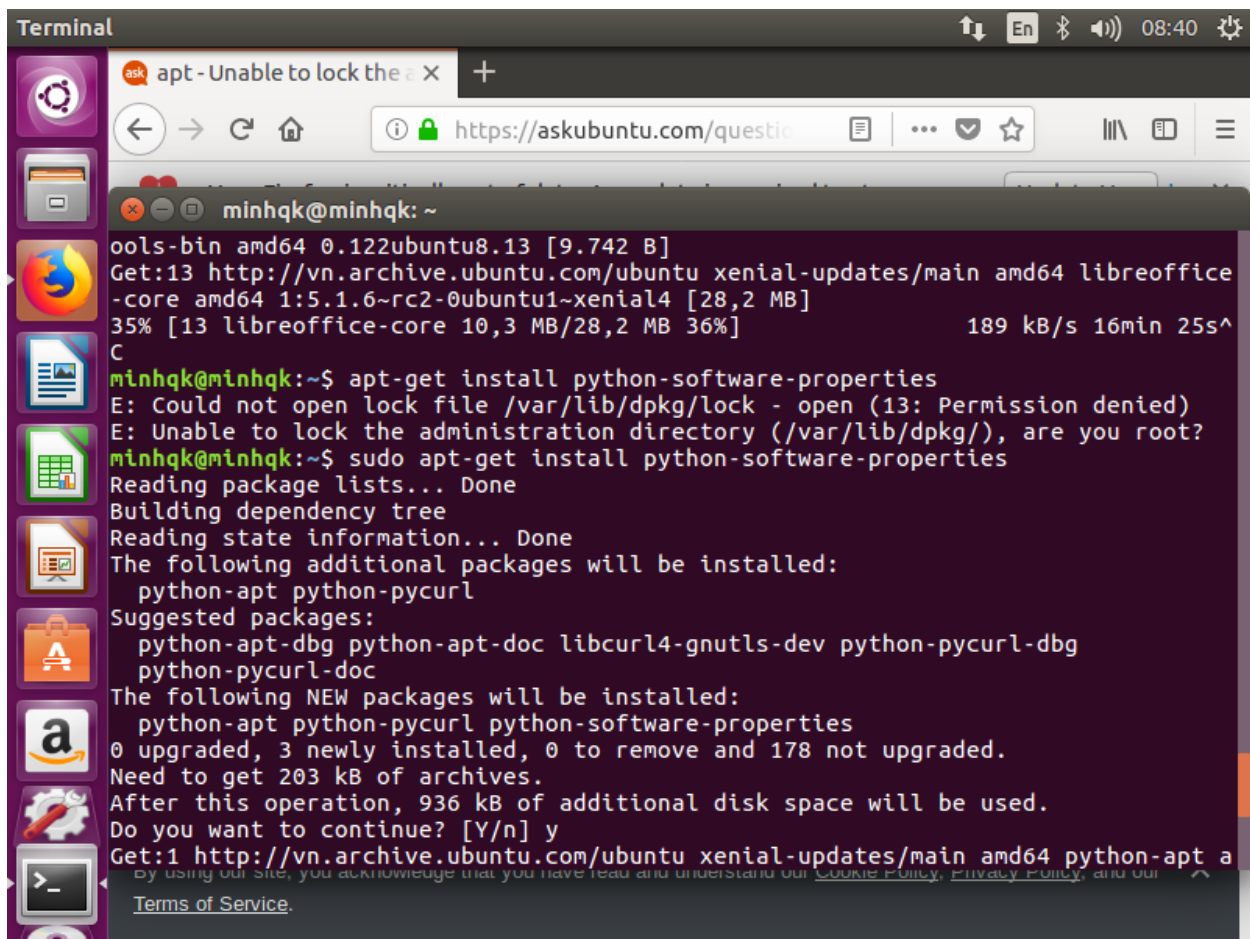
Terminal

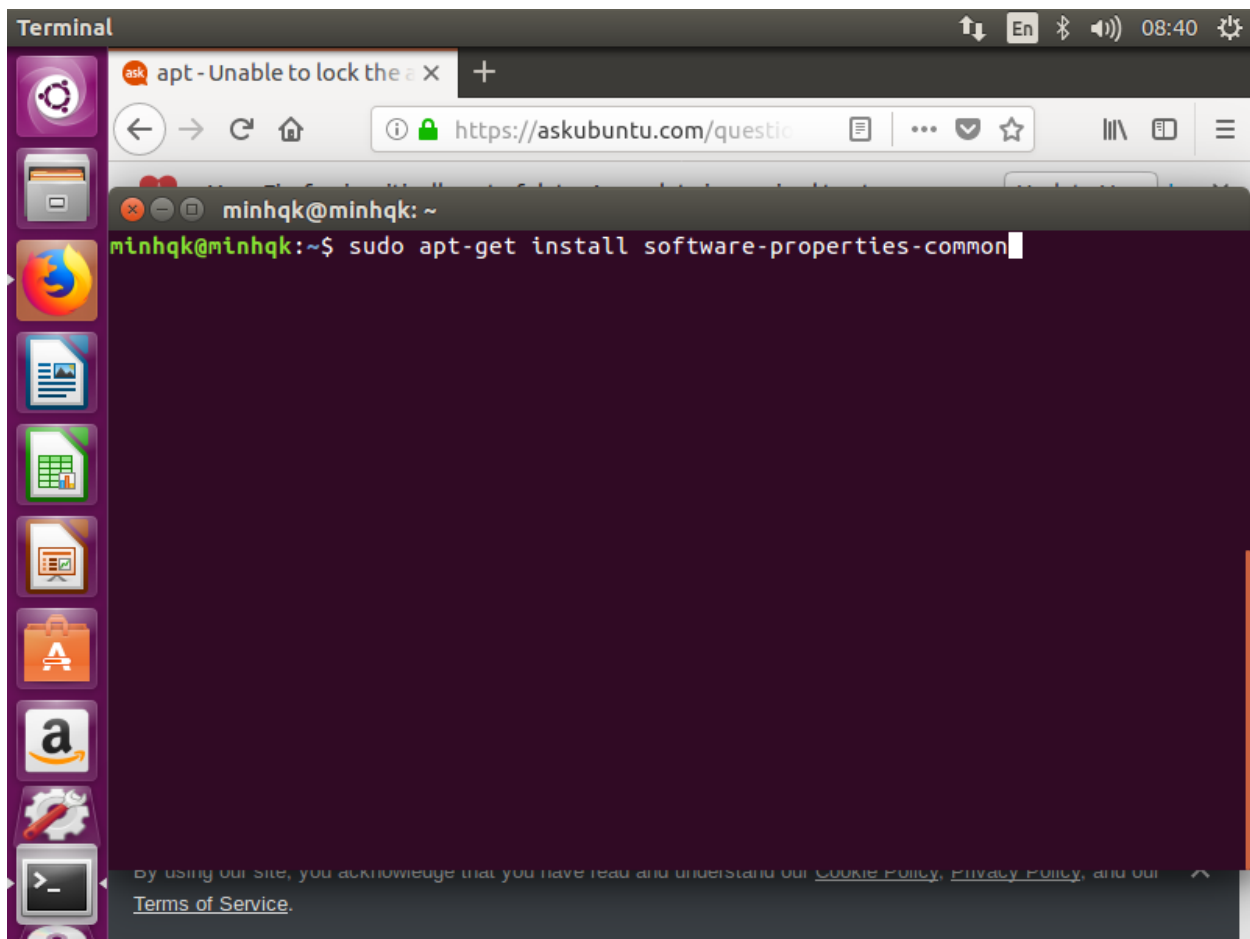
minhqk@minhqk: ~

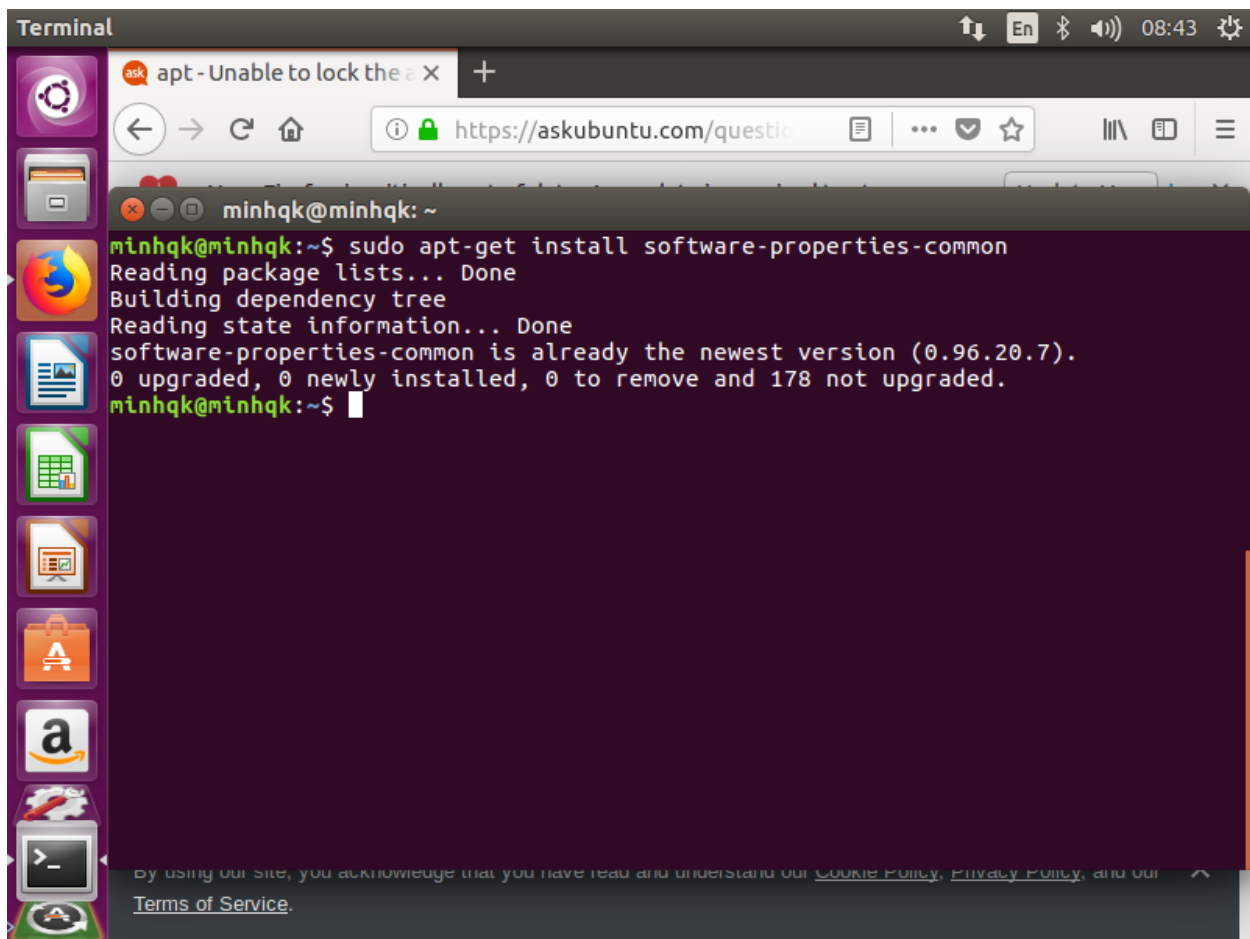
```
minhqk@minhqk:~$ sudo apt-get update
[sudo] password for minhqk:
Get:1 http://security.ubuntu.com/ubuntu xenial-security InRelease [107 kB]
Hit:2 http://vn.archive.ubuntu.com/ubuntu xenial InRelease
Get:3 http://vn.archive.ubuntu.com/ubuntu xenial-updates InRelease [109 kB]
Get:4 http://vn.archive.ubuntu.com/ubuntu xenial-backports InRelease [107 kB]
Get:5 http://security.ubuntu.com/ubuntu xenial-security/main amd64 Packages [568 kB]
Get:6 http://vn.archive.ubuntu.com/ubuntu xenial-updates/main amd64 Packages [860 kB]
Get:7 http://security.ubuntu.com/ubuntu xenial-security/main i386 Packages [490 kB]
Get:8 http://vn.archive.ubuntu.com/ubuntu xenial-updates/main i386 Packages [771 kB]
Get:9 http://security.ubuntu.com/ubuntu xenial-security/main Translation-en [238 kB]
Get:10 http://security.ubuntu.com/ubuntu xenial-security/main amd64 DEP-11 Metadata [67,7 kB]
Get:11 http://security.ubuntu.com/ubuntu xenial-security/main DEP-11 64x64 Icons [68,0 kB]
Get:12 http://security.ubuntu.com/ubuntu xenial-security/universe amd64 Packages [388 kB]
Get:13 http://vn.archive.ubuntu.com/ubuntu xenial-updates/main Translation-en [351 kB]
package
```

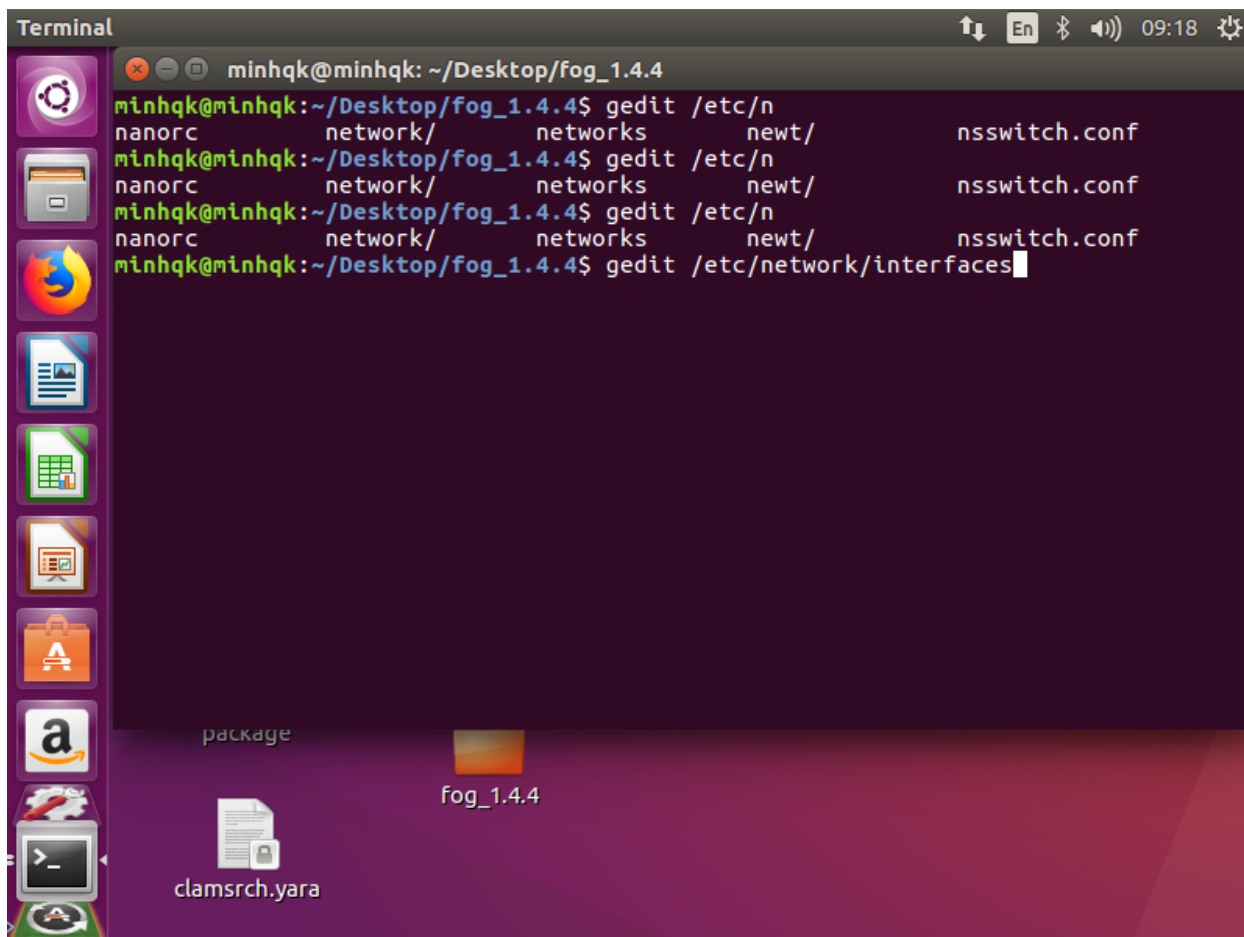
burpsuite_free_linux_v1_7_26.sh

clamsrch.yara









*interfaces [Read-Only] (/etc/network) - gedit












↑↓

En


🔊

09:21

⚙️



Open ▾



Save

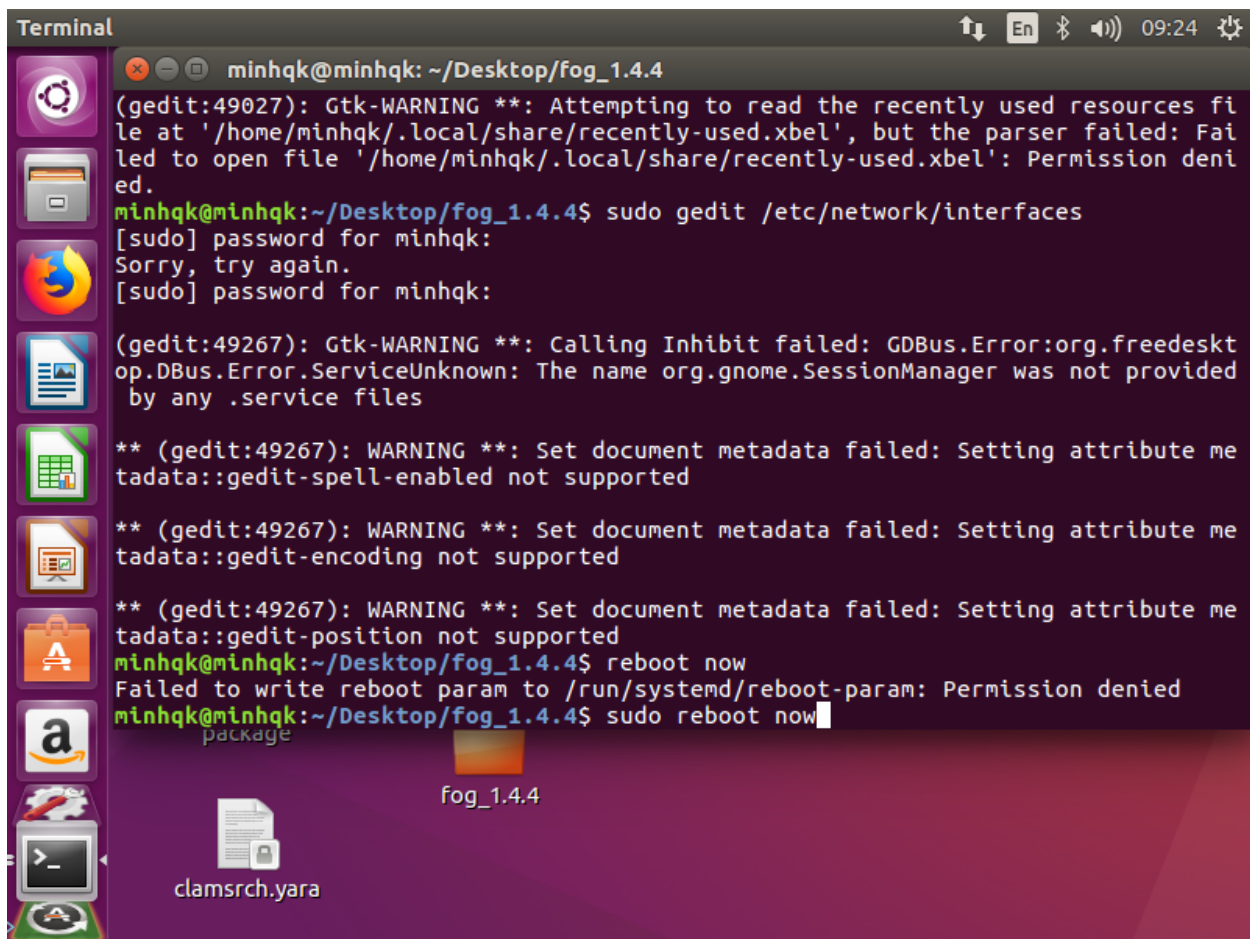
```
# interfaces(5) file used by ifup(8) and ifdown(8)
auto ens33
iface ens33 inet static
address 192.168.2.200
netmask 255.255.255.0
gateway 192.168.2.1
dns-nameserver 8.8.8.8
iface lo inet loopback
```

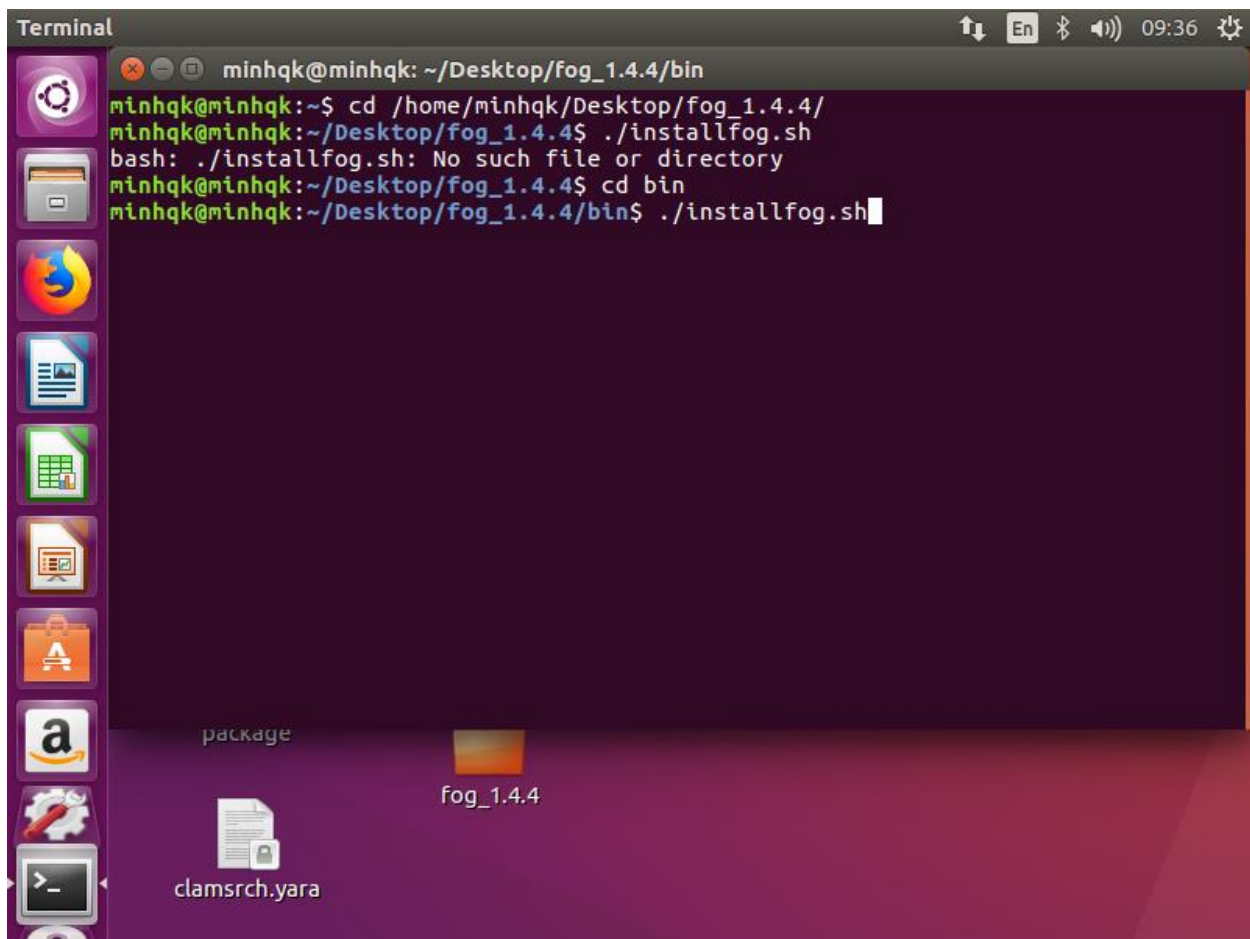
Plain Text ▾

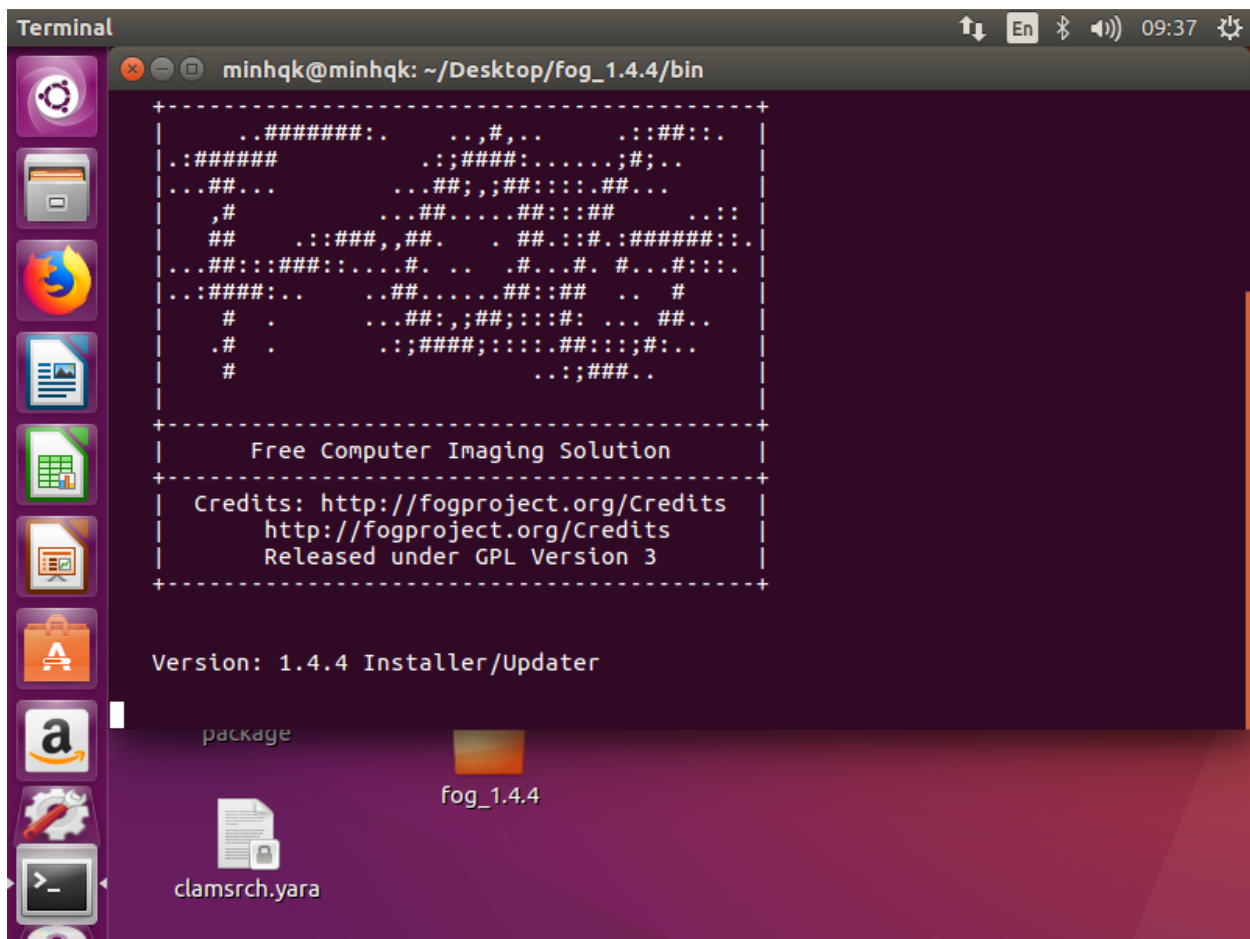
Tab Width: 8 ▾

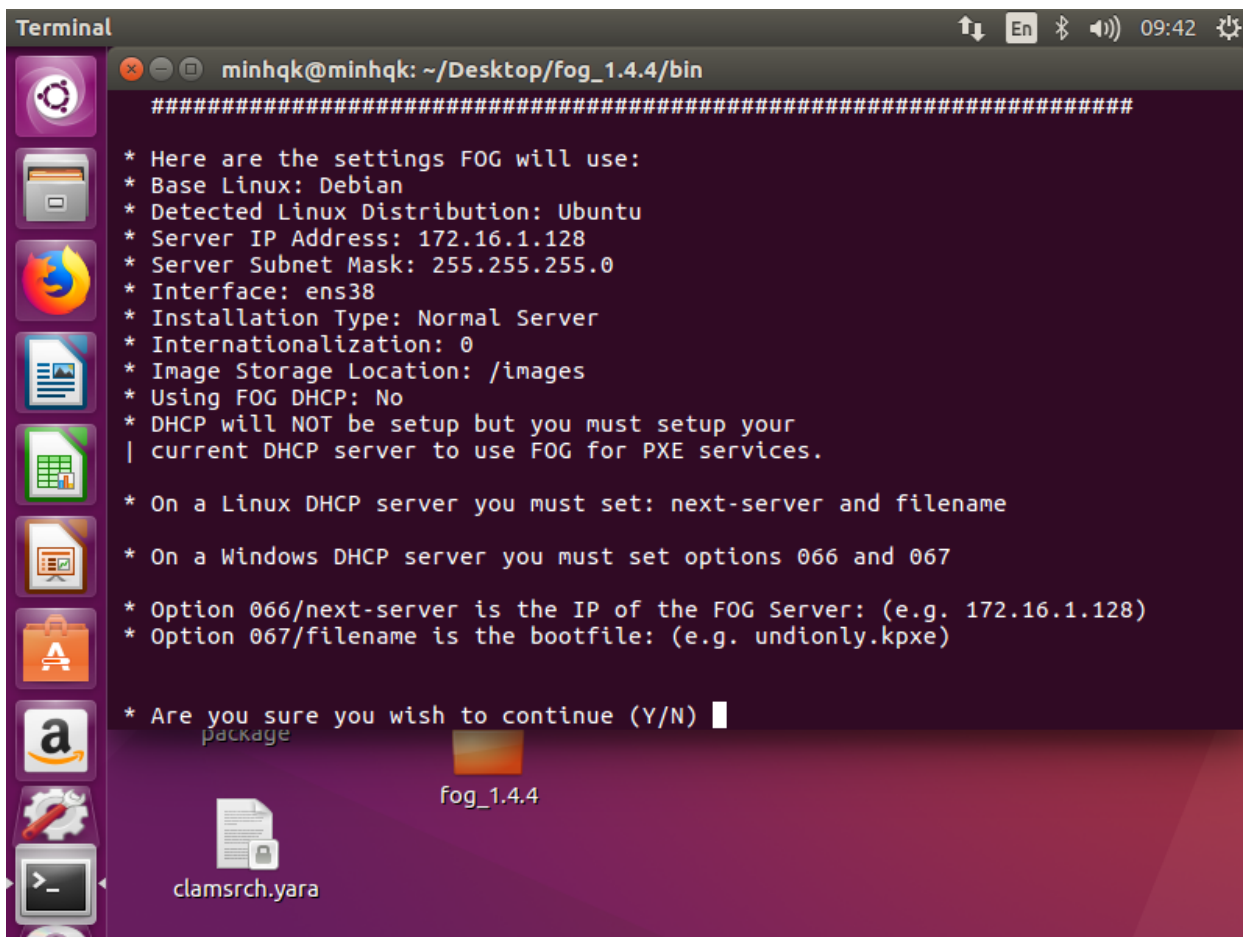
Ln 7, Col 23 ▾

INS









```
Terminal
minhqk@minhqk: ~/Desktop/fog_1.4.4/bin
#####
* Here are the settings FOG will use:
* Base Linux: Debian
* Detected Linux Distribution: Ubuntu
* Server IP Address: 192.168.198.136
* Server Subnet Mask: 255.255.255.0
* Interface: ens33
* Installation Type: Normal Server
* Internationalization: 0
* Image Storage Location: /images
* Using FOG DHCP: No
* DHCP will NOT be setup but you must setup your
| current DHCP server to use FOG for PXE services.
* On a Linux DHCP server you must set: next-server and filename
* On a Windows DHCP server you must set options 066 and 067
* Option 066/next-server is the IP of the FOG Server: (e.g. 192.168.198.136)
* Option 067/filename is the bootfile: (e.g. undionly.kpxe)
* Are you sure you wish to continue (Y/N) y
package
fog_1.4.4
clamsrch.yara
```

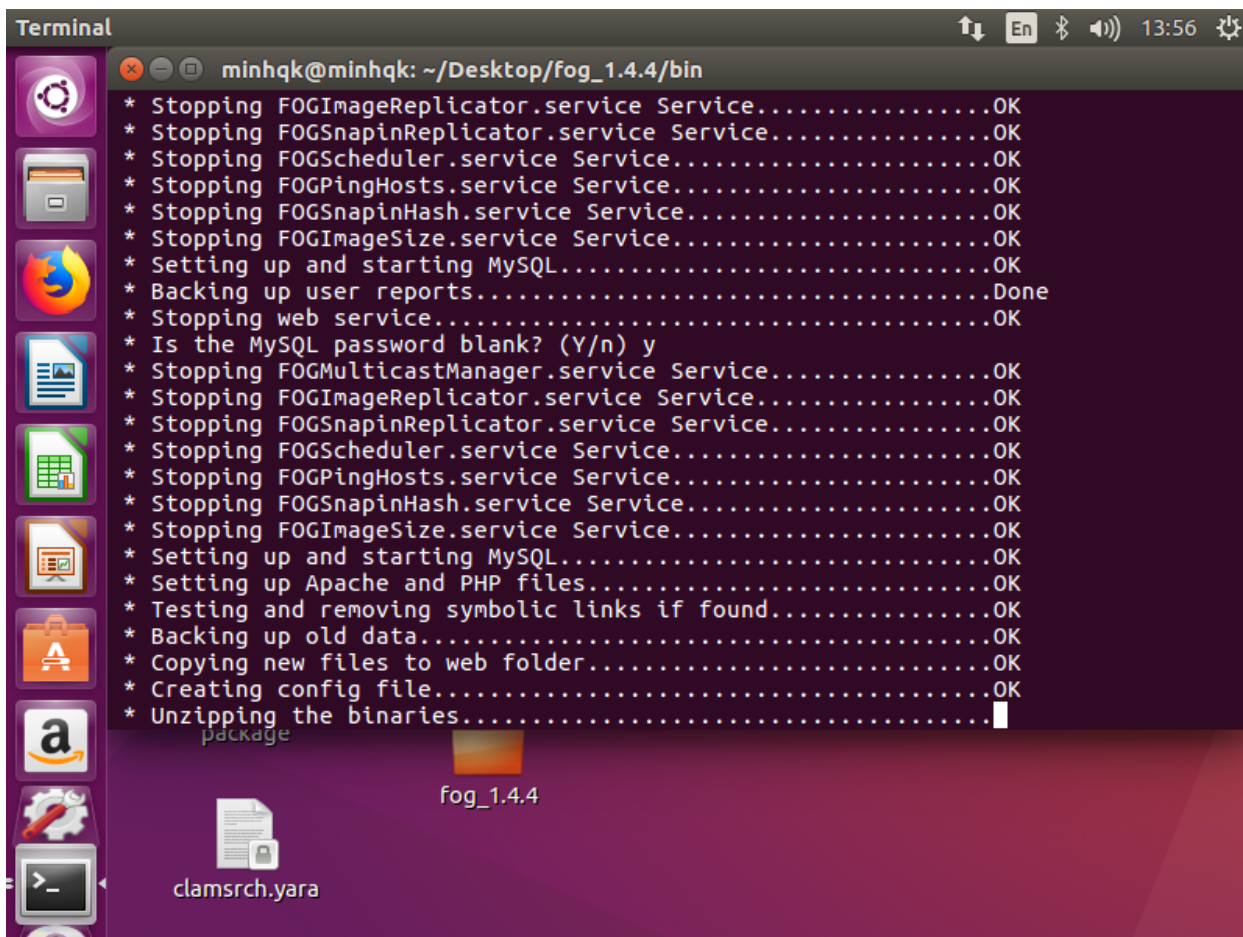
Terminal

13:11

```
minhqk@minhqk: ~/Desktop/fog_1.4.4/bin
l-server openssh-server php7.1 php7.1-bcmath php7.1-cli php7.1-curl php7.1-fpm p
hp7.1-gd php7.1-json php7.1-ldap php7.1-mbstring php7.1-mcrypt php7.1-mysql php7
.1-mysqld php-gettext sysv-rc-conf tar tftpd-hpa tftp-hpa unzip vsftpd wget xin
etd zlib1g

* Installing package: apache2.....OK
* Skipping package: bc.....(Already Installed)
* Skipping package: build-essential.....(Already Installed)
* Skipping package: cpp.....(Already Installed)
* Installing package: curl.....OK
* Skipping package: g++.....(Already Installed)
* Installing package: gawk.....OK
* Skipping package: gcc.....(Already Installed)
* Skipping package: gzip.....(Already Installed)
* Installing package: htmldoc.....OK
* Installing package: lftp.....OK
* Installing package: libapache2-mod-php7.1.....OK
```

clamsrch.yara fog_1.4.4



Terminal

13:56

minhqb@minhqb: ~/Desktop/fog_1.4.4/bin

```
* Stopping FOGImageReplicator.service Service.....OK
* Stopping FOGSnapinReplicator.service Service.....OK
* Stopping FOGScheduler.service Service.....OK
* Stopping FOGPingHosts.service Service.....OK
* Stopping FOGSnapinHash.service Service.....OK
* Stopping FOGImageSize.service Service.....OK
* Setting up and starting MySQL.....OK
* Backing up user reports.....Done
* Stopping web service.....OK
* Is the MySQL password blank? (Y/n) y
* Stopping FOGMulticastManager.service Service.....OK
* Stopping FOGImageReplicator.service Service.....OK
* Stopping FOGSnapinReplicator.service Service.....OK
* Stopping FOGScheduler.service Service.....OK
* Stopping FOGPingHosts.service Service.....OK
* Stopping FOGSnapinHash.service Service.....OK
* Stopping FOGImageSize.service Service.....OK
* Setting up and starting MySQL.....OK
* Setting up Apache and PHP files.....OK
* Testing and removing symbolic links if found.....OK
* Backing up old data.....OK
* Copying new files to web folder.....OK
* Creating config file.....OK
* Unzipping the binaries.....
```

clamsrch.yara

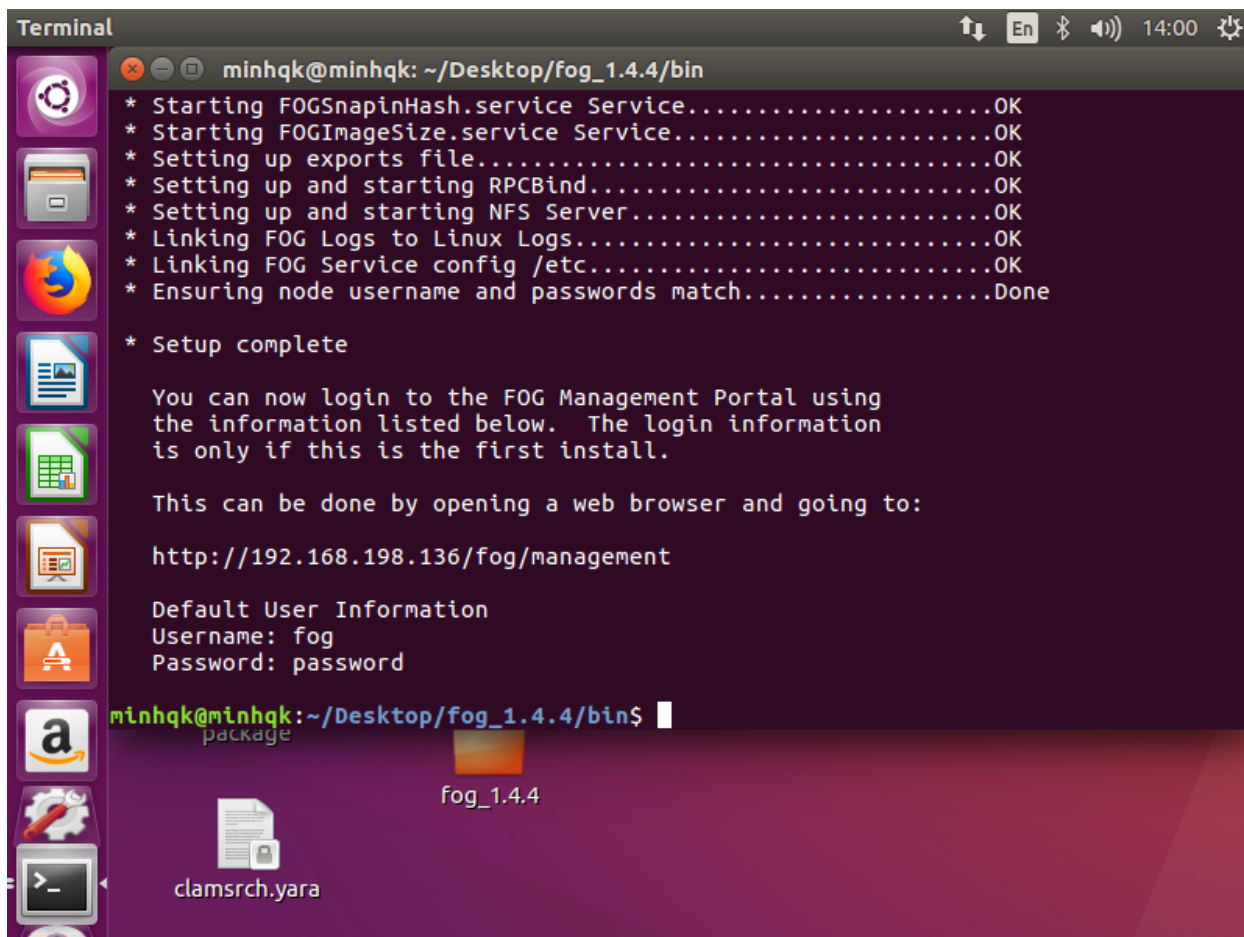
fog_1.4.4

```
minhqk@minhqk: ~/Desktop/fog_1.4.4/bin
* Setting up Apache and PHP files.....OK
* Testing and removing symbolic links if found.....OK
* Backing up old data.....OK
* Copying new files to web folder.....OK
* Creating config file.....OK
* Unzipping the binaries.....Done
* Copying binaries where needed.....Done
* Enabling apache and fpm services on boot.....OK
* Creating SSL CA.....OK
* Creating SSL Private Key.....OK
* Creating SSL Certificate.....OK
* Creating auth pub key and cert.....OK
* Resetting SSL Permissions.....OK
* Setting up SSL FOG Server.....OK
* Starting and checking status of web services.....OK
* Changing permissions on apache log files.....OK
* Backing up database.....OK

* You still need to install/update your database schema.
* This can be done by opening a web browser and going to:

http://192.168.198.136/fog/management

* Press [Enter] key when database is updated/installed.
package
fog_1.4.4
clamsrch.yara
```

Database Schema Installer / Updater > FOG > Open Source Computer Cloning Solu

Database Schema Install x

192.168.198.136/fog/management/index

Tue Oct 16, 2018 7:02 am
Running Version 1.4.4
SVN Revision: 6077

Open Source Computer Cloning Solution

Database Schema Installer / Updater

Your FOG database schema is not up to date, either because you have updated or this is a new FOG installati
upgrade, there will be a database backup stored on your FOG server defaulting under the folder /home/fogDBba
anything go wrong, this backup will enable you to return to the previous install if needed.
Are you sure you wish to install or update the FOG database?

INSTALL/UPGRADE NOW

If you would like to backup your FOG database you can do so using MySQL Administrator or by running the follow
terminal window (Applications->System Tools->Terminal), this will save the backup in your home direc


cd
mysqldump --allow-keywords -x -v fog > fogbackup.sql

Credits FOG Client Donate to FOG

Login > Management Login > FOG > Open Source Computer Cloning Solution - Moz

192.168.198.136/fog/management/in

14:04



Tue Oct 16, 2018 7:04 am

Running Version 1.4.4

SVN Revision: 6077

Open Source Computer Cloning Solution

Management Login

Username

fog

Password

.....

Language

English

LOGIN

Estimated FOG Sites: **3948**

Latest Version: **1.5.4**

Latest Development Version: **1.5.4**

Latest SVN Version: **6078**

Credits

FOG Client

Donate to FOG

