1. 업데이트

sudo apt-get update

sudo apt-get upgrade (안하셔도 됩니다.)

sudo apt-get install open-vm-tools

만약 apt-get update 가 에러뜨신다면,

https://ksy3241blog.wordpress.com/2016/06/17/sudo-apt-get-update-%EC%97%90%EB%9F%AC/

```
asu@asu-cuckoo:~$ sudo apt-get update
[sudo] asu의 암호:
기존:1 http://kr.archive.ubuntu.com/ubuntu bionic InRelease
기존:2 http://kr.archive.ubuntu.com/ubuntu bionic-updates InRelease
기존:3 http://kr.archive.ubuntu.com/ubuntu bionic-backports InRelease
기존:4 http://security.ubuntu.com/ubuntu bionic-security InRelease
패키지 목록을 읽는 중입니다... 완료
asu@asu-cuckoo:~$
```

```
asu@asu-cuckoo:~$ sudo apt-get install open-vm-tools
패키지 목록을 읽는 중입니다... 완료
의존성 트리를 만드는 중입니다
상태 정보를 읽는 중입니다... 완료
다음의 추가 패키지가 설치될 것입니다 :
  ethtool libdumbnet1 libmspack0 libxmlsec1-openssl zerofree
제안하는 패키지:
  open-vm-tools-desktop cloud-init
다음 새 패키지를 설치할 것입니다:
  ethtool libdumbnet1 libmspack0 libxmlsec1-openssl open-vm-tools zerofree
0개 업그레이드, 6개 새로 설치, 0개 제거 및 101개 업그레이드 안 함.
800 kB바이트 아카이브를 받아야 합니다.
이 작업 후 3,048 kB바이트의 디스크 공간을 더 사용하게 됩니다.
계속 하시겠습니까? [Y/n]
```

2. python 설치

sudo apt-get install python python-pip python-dev libffi-dev libssl-dev
sudo apt-get install python-virtualenv python-setuptools
sudo apt-get install libjpeg-dev zlib1g-dev swig

```
asu@asu-cuckoo:~$ sudo apt-get install python python-pip python-dev libffi-dev
libssl-dev
패키지 목록을 읽는 중입니다... 완료
의존성 트리를 만드는 중입니다
상태 정보를 읽는 중입니다... 완료
다음의 추가 패키지가 설치될 것입니다 :
  build-essential dpkg-dev fakeroot g++ g++-7 gcc gcc-7
  libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl
  libasan4 libatomic1 libc-dev-bin libc6-dev libcilkrts5 libexpat1-dev
  libfakeroot libgcc-7-dev libitm1 liblsan0 libmpx2 libpython-all-dev
  libpython-dev libpython-stdlib libpython2.7-dev libquadmath0 libssl-doc
  libstdc++-7-dev libtsan0 libubsan0 linux-libc-dev make manpages-dev
  python-all python-all-dev python-asn1crypto python-cffi-backend
  python-crypto python-cryptography python-dbus python-enum34 python-gi
  python-idna python-ipaddress python-keyring python-keyrings.alt
  python-minimal python-pip-whl python-pkg-resources python-secretstorage
  python-setuptools python-six python-wheel python-xdg python2.7
  python2.7-dev python2.7-minimal
제안하는 패키지:
  debian-keyring g++-multilib g++-7-multilib gcc-7-doc libstdc++6-7-dbg
  gcc-multilib autoconf automake libtool flex bison gcc-doc gcc-7-multilib
  gcc-7-locales libgcc1-dbg libgomp1-dbg libitm1-dbg libatomic1-dbg
asu@asu-cuckoo:~$ sudo apt-get install python-virtualenv python-setuptools
패키지 목록을 읽는 중입니다... 완료
의존성 트리를 만드는 중입니다
상태 정보를 읽는 중입니다... 완료
패키지 python-setuptools는 이미 최신 버전입니다 (39.0.1-2).
python-setuptools 패키지는 수동설치로 지정합니다.
다음의 추가 패키지가 설치될 것입니다 :
  python3-distutils python3-lib2to3 python3-virtualenv virtualenv
다음 새 패키지를 설치할 것입니다:
  python-virtualenv python3-distutils python3-lib2to3 python3-virtualenv
  virtualenv
0개 업그레이드, 5개 새로 설치, 0개 제거 및 101개 업그레이드 안 함.
312 kB바이트 아카이브를 받아야 합니다.
이 작업 후 2,434 kB바이트의 디스크 공간을 더 사용하게 됩니다.
계속 하시겠습니까? [Y/n]
asu@asu-cuckoo:~$ sudo apt-get install libjpeg-dev zlib1g-dev swig
패키지 목록을 읽는 중입니다... 완료
의존성 트리를 만드는 중입니다
상태 정보를 읽는 중입니다... 완료
다음의 추가 패키지가 설치될 것입니다 :
  libjpeg-turbo8-dev libjpeg8-dev swig3.0
제안하는 패키지:
  swig-doc swig-examples swig3.0-examples swig3.0-doc
다음 새 패키지를 설치할 것입니다:
  libjpeg-dev libjpeg-turbo8-dev libjpeg8-dev swig swig3.0 zlib1g-dev
0개 업그레이드, 6개 새로 설치, 0개 제거 및 101개 업그레이드 안 함.
1,504 kB바이트 아카이브를 받아야 합니다.
이 작업 후 7,137 kB바이트의 디스크 공간을 더 사용하게 됩니다.
계속 하시겠습니까? [Y/n]
```

3. 몽고 DB 설치

sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv 2930ADAE8CAF5059EE73BB4B58712A2291FA4AD5

echo "deb [arch=amd64,arm64] https://repo.mongodb.org/apt/ubuntu xenial/mongodb-org/3.6 multiverse" | sudo tee /etc/apt/sources.list.d/mongodb-org-3.6.list

sudo apt update
sudo apt install -y mongodb-org

sudo service mongod start
sudo systemctl enable mongod.service

```
asu@asu-cuckoo:~$ sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --
recv 2930ADAE8CAF5059EE73BB4B58712A2291FA4AD5
Executing: /tmp/apt-key-gpghome.cqWWsGt0Ir/gpg.1.sh --keyserver hkp://keyserver
.ubuntu.com:80 --recv 2930ADAE8CAF5059EE73BB4B58712A2291FA4AD5
gpg: key 58712A2291FA4AD5: public key "MongoDB 3.6 Release Signing Key <packagi
ng@mongodb.com>" imported
gpg: Total number processed: 1
gpg:               imported: 1
asu@asu-cuckoo:~$
```

```
asu@asu-cuckoo:~$ echo "deb [ arch=amd64,arm64 ] https://repo.mongodb.org/apt/u
buntu xenial/mongodb-org/3.6 multiverse" | sudo tee /etc/apt/sources.list.d/mon
godb-org-3.6.list
deb [ arch=amd64,arm64 ] https://repo.mongodb.org/apt/ubuntu xenial/mongodb-org
/3.6 multiverse
asu@asu-cuckoo:~$
```

```
asu@asu-cuckoo:~$ sudo apt update
기존:1 http://kr.archive.ubuntu.com/ubuntu bionic InRelease
기존:2 http://kr.archive.ubuntu.com/ubuntu bionic-updates InRelease
기존:3 http://kr.archive.ubuntu.com/ubuntu bionic-backports InRelease
무시:4 https://repo.mongodb.org/apt/ubuntu xenial/mongodb-org/3.6 InRelease
기존:5 http://security.ubuntu.com/ubuntu bionic-security InRelease
받기:6 https://repo.mongodb.org/apt/ubuntu xenial/mongodb-org/3.6 Release [3,45
7 B]
받기:7 https://repo.mongodb.org/apt/ubuntu xenial/mongodb-org/3.6 Release.gpg [
801 B]
받기:8 https://repo.mongodb.org/apt/ubuntu xenial/mongodb-org/3.6/multiverse am
d64 Packages [6,495 B]
받기:9 https://repo.mongodb.org/apt/ubuntu xenial/mongodb-org/3.6/multiverse ar
m64 Packages [6,483 B]
내려받기 17.2 kB바이트, 소요시간 2초 (7,292 바이트/초)
패키지 목록을 읽는 중입니다... 완료
의존성 트리를 만드는 중입니다
상태 정보를 읽는 중입니다... 완료
101 packages can be upgraded. Run 'apt list --upgradable' to see them.
asu@asu-cuckoo:~$
```

```
asu@asu-cuckoo:~$ sudo apt install -y mongodb-org
패키지 목록을 읽는 중입니다... 완료
의존성 트리를 만드는 중입니다
상태 정보를 읽는 중입니다... 완료
다음의 추가 패키지가 설치될 것입니다 :
  mongodb-org-mongos mongodb-org-server mongodb-org-shell mongodb-org-tools
다음 새 패키지를 설치할 것입니다:
  mongodb-org mongodb-org-mongos mongodb-org-server mongodb-org-shell
  mongodb-org-tools
0개 업그레이드, 5개 새로 설치, 0개 제거 및 101개 업그레이드 안 함.
67.9 MB바이트 아카이브를 받아야 합니다.
이 작업 후 278 MB바이트의 디스크 공간을 더 사용하게 됩니다.
```

```
asu@asu-cuckoo:~$ sudo service mongod start
asu@asu-cuckoo:~$ sudo systemctl enable mongod.service
Created symlink /etc/systemd/system/multi-user.target.wants/mongod.service →/l
ib/systemd/system/mongod.service.
asu@asu-cuckoo:~$
```

4. tcpdump 설치

sudo apt-get install tcpdump apparmor-utils
sudo aa-disable /usr/sbin/tcpdump
sudo apt-get install tcpdump
sudo setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump
sudo getcap /usr/sbin/tcpdump

```
asu@asu-cuckoo:~$ sudo apt-get install tcpdump apparmor-utils
패키지 목록을 읽는 중입니다... 완료
의존성 트리를 만드는 중입니다
상태 정보를 읽는 중입니다... 완료
패키지 tcpdump는 이미 최신 버전입니다 (4.9.2-3).
다음의 추가 패키지가 설치될 것입니다 :
  python3-apparmor python3-libapparmor
제안하는 패키지:
  vim-addon-manager
다음 새 패키지를 설치할 것입니다:
  apparmor-utils python3-apparmor python3-libapparmor
0개 업그레이드, 3개 새로 설치, 0개 제거 및 101개 업그레이드 안 함.
157 k바이트 아카이브를 받아야 합니다.
이 작업 후 961 k바이트의 디스크 공간을 더 사용하게 됩니다.
계속 하시겠습니까? [Y/n]
```

```
asu@asu-cuckoo:~$ sudo aa-disable /usr/sbin/tcpdump
Disabling /usr/sbin/tcpdump.
asu@asu-cuckoo:~$ sudo apt-get install tcpdump
패키지 목록을 읽는 중입니다... 완료
의존성 트리를 만드는 중입니다
상태 정보를 읽는 중입니다... 완료
패키지 tcpdump는 이미 최신 버전입니다 (4.9.2-3).
0개 업그레이드, 0개 새로 설치, 0개 제거 및 101개 업그레이드 안 함.
asu@asu-cuckoo:~$ sudo setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump
asu@asu-cuckoo:~$ sudo getcap /usr/sbin/tcpdump
/usr/sbin/tcpdump = cap_net_admin,cap_net_raw+eip
asu@asu-cuckoo:~$
```

5. volatility 설치

sudo apt-get install volatility

```
asu@asu-cuckoo:~$ sudo apt-get install volatility
패키지 목록을 읽는 중입니다... 완료
의존성 트리를 만드는 중입니다
상태 정보를 읽는 중입니다... 완료
다음의 추가 패키지가 설치될 것입니다 :
  dwarfdump libdistorm3-3 libyara3 python-attr python-bs4 python-chardet
  python-distorm3 python-et-xmlfile python-funcsigs python-html5lib
  python-jdcal python-lxml python-olefile python-openpyxl python-pil
  python-pluggy python-py python-pytest python-tz python-webencodings
  python-yara volatility-tools
제안하는 패키지:
  python-attr-doc python-funcsigs-doc python-genshi python-lxml-dbg
  python-lxml-doc python-pil-doc python-pil-dbg subversion
  python-pytest-xdist python-mock lime-forensics-dkms
다음 새 패키지를 설치할 것입니다:
  dwarfdump libdistorm3-3 libyara3 python-attr python-bs4 python-chardet
  python-distorm3 python-et-xmlfile python-funcsigs python-html5lib
  python-jdcal python-lxml python-olefile python-openpyxl python-pil
  python-pluggy python-py python-pytest python-tz python-webencodings
  python-yara volatility volatility-tools
0개 업그레이드, 23개 새로 설치, 0개 제거 및 101개 업그레이드 안 함.
3,520 kB바이트 아카이브를 받아야 합니다.
이 작업 후 33.6 MB바이트의 디스크 공간을 더 사용하게 됩니다.
계속 하시겠습니까? [Y/n]
```

6. m2crypto 설치

sudo pip install m2crypto

```
asu@asu-cuckoo:~$ sudo pip install m2crypto
The directory '/home/asu/.cache/pip/http' or its parent directory is not owned
by the current user and the cache has been disabled. Please check the permissio
ns and owner of that directory. If executing pip with sudo, you may want sudo's
 -H flag.
The directory '/home/asu/.cache/pip' or its parent directory is not owned by th
e current user and caching wheels has been disabled. check the permissions and
owner of that directory. If executing pip with sudo, you may want sudo's -H fla
g.
Collecting m2crypto
  Downloading https://files.pythonhosted.org/packages/41/50/7d85dc99b1c4f29eca8
3873d851ec29a8e484a66b31351e62e30be9db7d1/M2Crypto-0.30.1.tar.gz (1.3MB)
    100% |████████████████████████████████| 1.3MB 867kB/s
Collecting typing (from m2crypto)
  Downloading https://files.pythonhosted.org/packages/cc/3e/29f92b7aeda5b078c86
d14f550bf85cff809042e3429ace7af6193c3bc9f/typing-3.6.6-py2-none-any.whl
Installing collected packages: typing, m2crypto
  Running setup.py install for m2crypto ... done
Successfully installed m2crypto-0.30.1 typing-3.6.6
asu@asu-cuckoo:~$
```

7. cuckoo 샌드박스 설치

sudo pip install cuckoo
sudo pip install -U cuckoo
cuckoo -d

```
asu@asu-cuckoo:~$ sudo pip install cuckoo
The directory '/home/asu/.cache/pip/http' or its parent directory is not owned
by the current user and the cache has been disabled. Please check the permissio
ns and owner of that directory. If executing pip with sudo, you may want sudo's
 -H flag.
The directory '/home/asu/.cache/pip' or its parent directory is not owned by th
e current user and caching wheels has been disabled. check the permissions and
owner of that directory. If executing pip with sudo, you may want sudo's -H fla
g.
Collecting cuckoo
  Downloading https://files.pythonhosted.org/packages/ae/cc/2ee841d414a7274455b
b0d969567ba9a4cd72594e3ad34dbdee98f999c7b/Cuckoo-2.0.6.2.tar.gz (5.3MB)
    3% |                                | 184kB 1.7MB/s eta 0:00:03
```

```
asu@asu-cuckoo:~$ sudo pip install -U cuckoo
The directory '/home/asu/.cache/pip/http' or its parent directory is not owned
by the current user and the cache has been disabled. Please check the permissio
ns and owner of that directory. If executing pip with sudo, you may want sudo's
 -H flag.
The directory '/home/asu/.cache/pip' or its parent directory is not owned by th
e current user and caching wheels has been disabled. check the permissions and
owner of that directory. If executing pip with sudo, you may want sudo's -H fla
g.
Requirement already up-to-date: cuckoo in /usr/local/lib/python2.7/dist-package
s
Requirement already up-to-date: alembic==0.8.8 in /usr/local/lib/python2.7/dist
-packages (from cuckoo)
```

```
asu@asu-cuckoo:~$ cuckoo -d

  .-----------------.
  | Cuckoo Sandbox? |
  |     OH NOES!    |\  '-.__.-'
  '-----------------' \  /oo |--.--,--,--.
                      \_.-'._i__i__i_.'
                         """""""""


 Cuckoo Sandbox 2.0.6
 www.cuckoosandbox.org
 Copyright (c) 2010-2018

================================================================================
    Welcome to Cuckoo Sandbox, this appears to be your first run!
    We will now set you up with our default configuration.
    You will be able to see and modify the Cuckoo configuration,
    Yara rules, Cuckoo Signatures, and much more to your likings
    by exploring the /home/asu/.cuckoo directory.

    Among other configurable items of most interest is the
    new location for your Cuckoo configuration:
              /home/asu/.cuckoo/conf
================================================================================

Cuckoo has finished setting up the default configuration.
Please modify the default settings where required and
start Cuckoo again (by running `cuckoo` or `cuckoo -d`).
```

cuckoo -d 를 하셨을때 이렇게 나오시면 성공하신겁니다. 여기서 에러가 나신다면, 밑에 설명의 ip 설정까지 다하시고 이후에 cuckoo -d 와 cuckoo community 를 해보시길 바랍니다. 그래도 안된다면, home 디렉토리에 .cuckoo 폴터가 생성되지 않은 겁니다. 정상적으로 설치될때 생성되는 .cuckoo 폴터들 보내드릴 테니 댓글남겨주시면 보내드리겠습니다. 10MB 보다 크면 안올려진다고 하네요. 받으시고 home 디렉토리에 옮겨주시고 진행하시면 정상적으로 됩니다.

```
asu@asu-cuckoo:~$ cuckoo community
2018-09-07 15:23:19,319 [cuckoo.apps.apps] INFO: Downloading.. https://github.com/cuckoosandbox/community/archive/master.tar.gz
2018-09-07 15:23:26,109 [cuckoo] INFO: Finished fetching & extracting the community files!
```

8. VirtualBox 설치

wget -q https://www.virtualbox.org/download/oracle_vbox_2016.asc -O- | sudo apt-key add -
wget -q https://www.virtualbox.org/download/oracle_vbox.asc -O- | sudo apt-key add -

sudo sh -c 'echo "deb http://download.virtualbox.org/virtualbox/debian $(lsb_release -sc) contrib" >> /etc/apt/sources.list.d/virtualbox.list'

sudo apt update
sudo apt-get install virtualbox-5.2
sudo apt-get install net-tools

```
asu@asu-cuckoo:~$ wget -q https://www.virtualbox.org/download/oracle_vbox_2016.asc -O- | sudo apt-key add -
OK
asu@asu-cuckoo:~$ wget -q https://www.virtualbox.org/download/oracle_vbox.asc -O- | sudo apt-key add -
OK
asu@asu-cuckoo:~$ sudo sh -c 'echo "deb http://download.virtualbox.org/virtualbox/debian $(lsb_release -sc) contrib" >> /etc/apt/sources.list.d/virtualbox.list'
asu@asu-cuckoo:~$
```

```
asu@asu-cuckoo:~$ sudo apt update
기존:1 http://kr.archive.ubuntu.com/ubuntu bionic InRelease
기존:2 http://kr.archive.ubuntu.com/ubuntu bionic-updates InRelease
기존:3 http://kr.archive.ubuntu.com/ubuntu bionic-backports InRelease
받기:4 http://download.virtualbox.org/virtualbox/debian bionic InRelease [4,429
 B]
기존:5 http://security.ubuntu.com/ubuntu bionic-security InRelease
무시:6 https://repo.mongodb.org/apt/ubuntu xenial/mongodb-org/3.6 InRelease
기존:7 https://repo.mongodb.org/apt/ubuntu xenial/mongodb-org/3.6 Release
받기:9 http://download.virtualbox.org/virtualbox/debian bionic/contrib amd64 Pa
ckages [1,453 B]
내려받기 5,882 바이트, 소요시간 1초 (4,927 바이트/초)
패키지 목록을 읽는 중입니다... 완료
의존성 트리를 만드는 중입니다
상태 정보를 읽는 중입니다... 완료
101 packages can be upgraded. Run 'apt list --upgradable' to see them.
N: Skipping acquire of configured file 'contrib/binary-i386/Packages' as reposi
tory 'http://download.virtualbox.org/virtualbox/debian bionic InRelease' doesn'
t support architecture 'i386'
asu@asu-cuckoo:~$
```

```
asu@asu-cuckoo:~$ sudo apt-get install virtualbox-5.2
패키지 목록을 읽는 중입니다... 완료
의존성 트리를 만드는 중입니다
상태 정보를 읽는 중입니다... 완료
다음의 추가 패키지가 설치될 것입니다 :
  libcurl4 libdouble-conversion1 libqt5core5a libqt5dbus5 libqt5gui5
  libqt5network5 libqt5opengl5 libqt5printsupport5 libqt5svg5 libqt5widgets5
  libqt5x11extras5 libsdl-ttf2.0-0 libsdl1.2debian libxcb-xinerama0
  qt5-gtk-platformtheme qttranslations5-l10n
제안하는 패키지:
  qt5-image-formats-plugins qtwayland5
다음 새 패키지를 설치할 것입니다:
  libcurl4 libdouble-conversion1 libqt5core5a libqt5dbus5 libqt5gui5
  libqt5network5 libqt5opengl5 libqt5printsupport5 libqt5svg5 libqt5widgets5
  libqt5x11extras5 libsdl-ttf2.0-0 libsdl1.2debian libxcb-xinerama0
  qt5-gtk-platformtheme qttranslations5-l10n virtualbox-5.2
0개 업그레이드, 17개 새로 설치, 0개 제거 및 101개 업그레이드 안 함.
78.2 M바이트 아카이브를 받아야 합니다.
이 작업 후 210 M바이트의 디스크 공간을 더 사용하게 됩니다.
계속 하시겠습니까? [Y/n]
```

```
asu@asu-cuckoo:~$ sudo apt-get install net-tools
패키지 목록을 읽는 중입니다... 완료
의존성 트리를 만드는 중입니다
상태 정보를 읽는 중입니다... 완료
다음 새 패키지를 설치할 것입니다:
  net-tools
0개 업그레이드, 1개 새로 설치, 0개 제거 및 101개 업그레이드 안 함.
194 k바이트 아카이브를 받아야 합니다.
이 작업 후 803 k바이트의 디스크 공간을 더 사용하게 됩니다.
받기:1 http://kr.archive.ubuntu.com/ubuntu bionic/main amd64 net-tools amd64 1.
60+git20161116.90da8a0-1ubuntu1 [194 kB]
내려받기 194 k바이트, 소요시간 0초 (898 k바이트/초)
Selecting previously unselected package net-tools.
(데이터베이스 읽는중 ...현재 140337개의 파일과 디렉터리가 설치되어 있습니다.)
Preparing to unpack .../net-tools_1.60+git20161116.90da8a0-1ubuntu1_amd64.deb .
..
Unpacking net-tools (1.60+git20161116.90da8a0-1ubuntu1) ...
Processing triggers for man-db (2.8.3-2) ...
net-tools (1.60+git20161116.90da8a0-1ubuntu1) 설정하는 중입니다 ...
asu@asu-cuckoo:~$
```

윈도우 7 32bit iso 설치

https://heidoc.net/joomla/technology-science/microsoft/67-microsoft-windows-and-office-iso-download-tool

Microsoft Windows and Office ISO Download Tool

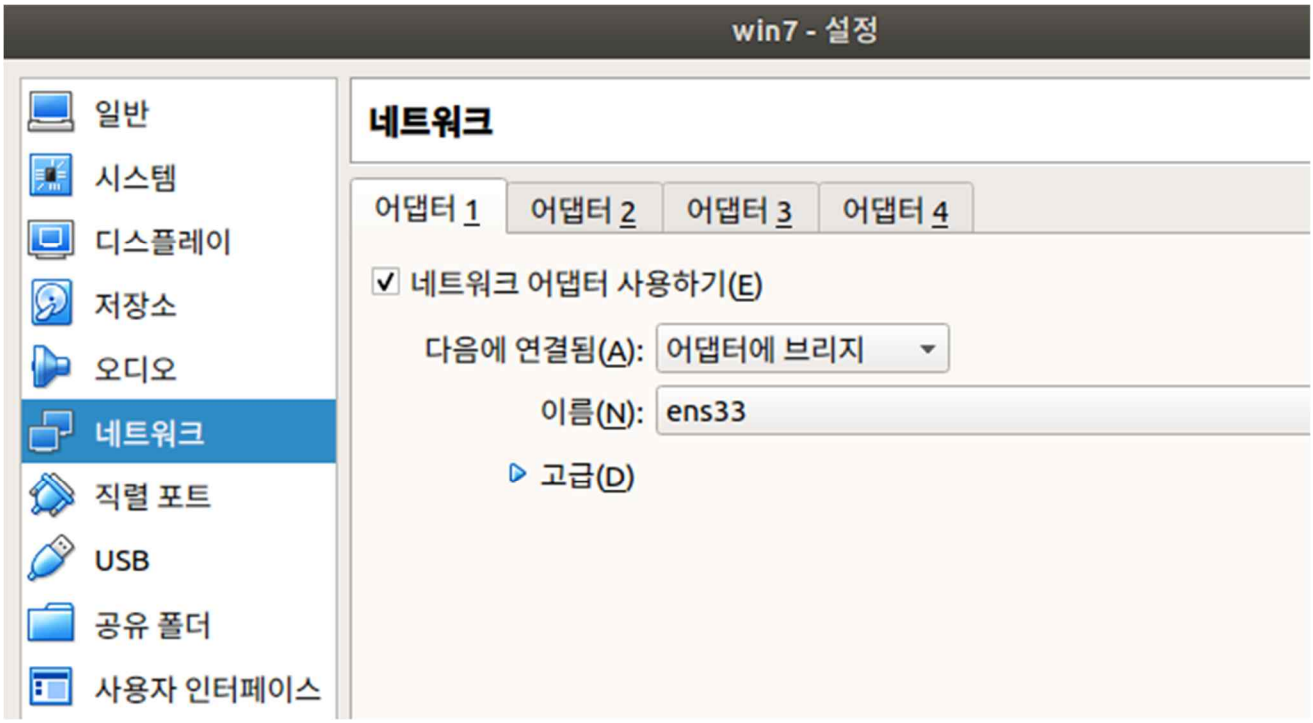
Microsoft Windows and Office ISO Download Tool Details Written by Jan Krohn Category: Microsoft Published: 20 May 2016 Hits: 16185775 Microsoft Windows Office User Rating: 4 / 5 Please Rate Microsoft Windows and Office ISO Download Tool Release History Contributors Purchase a Wind

heidoc.net

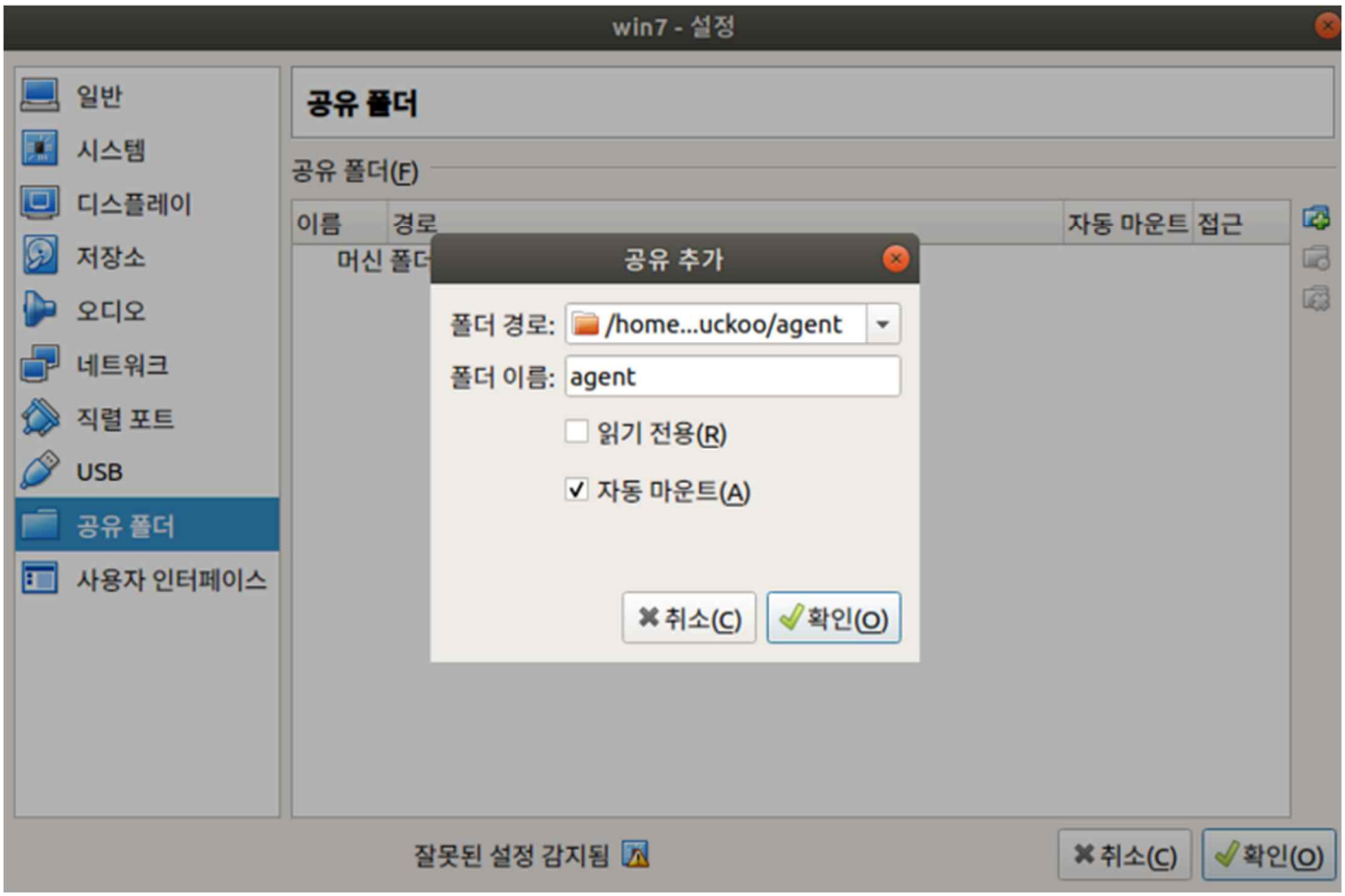
마이크로 소프트 공식홈페이지에서 무료로 ISO 를 다운로드 할 수 있게 합니다. 30 정도 무료로 사용 가능합니다. 이 툴로 다운받고, 네이버 클라우드를 이용하여 우분투로 옮겼습니다.

9. VirtualBox 설정

새 가상머신을 만드시고 모든 설정은 디폴트로 했습니다. 그리고 실행하시기 전에 설정에서,

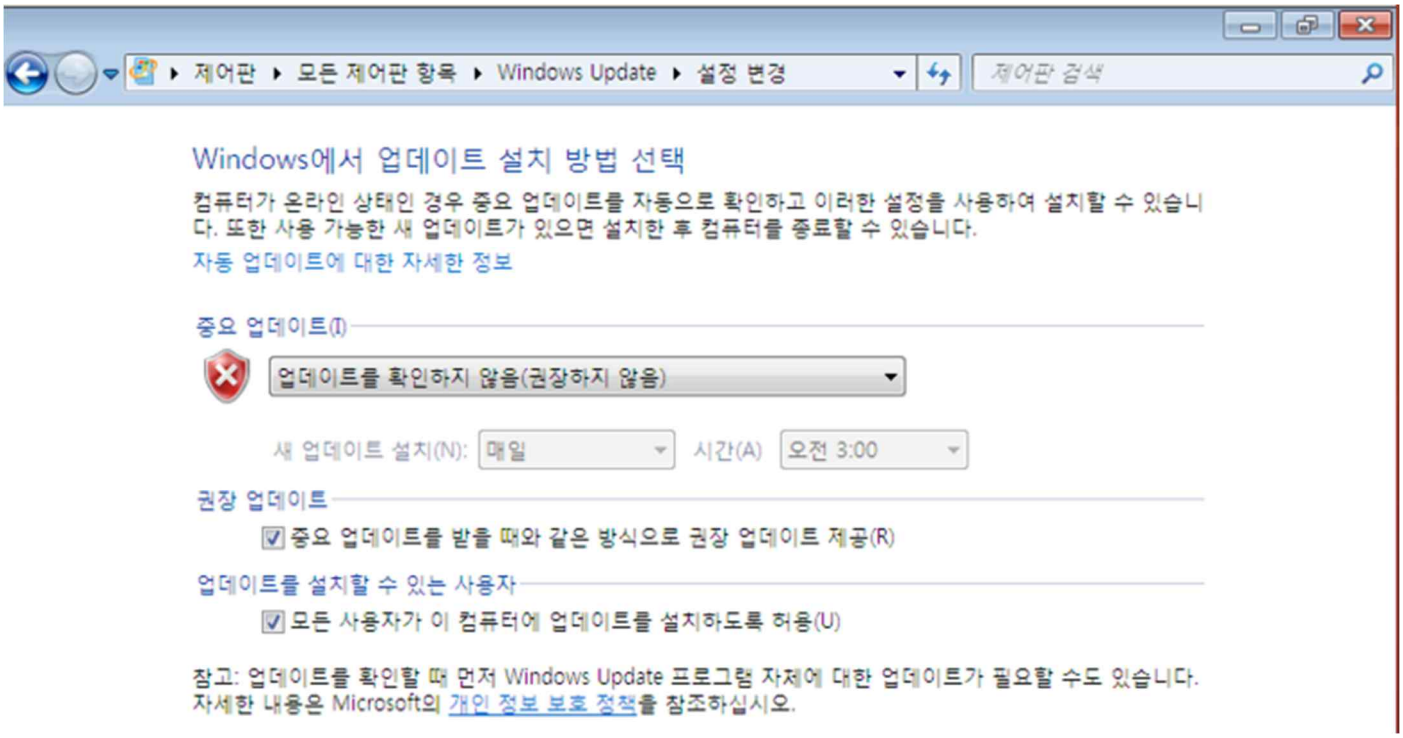


네트워크 어댑터를 브릿지로 해줍니다.



공유폴더를 home/.cuckoo/agent 로 해줍니다. 이제 윈도우를 설치합니다. 설치를 마치시고 윈도우를 실행하고 바로 설정해야 되는 것들이 몇개 있습니다.

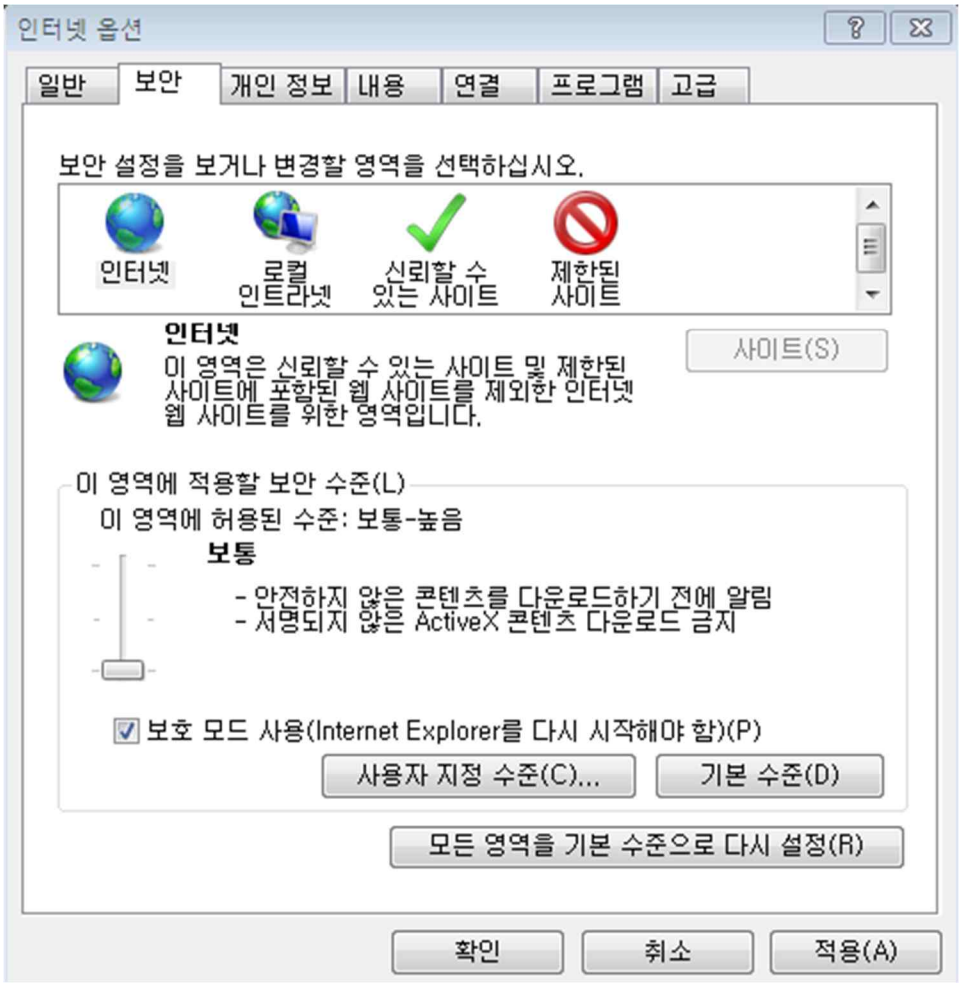
a) 업데이트 설정 - 안함으로 설정



b) 방화벽 설정 - 사용 안함으로 설정

c) 브라우저 설정

도구 - 인터넷 옵션 - 보안 에서 안전을 최하로 낮춥니다.



그리고 VirtualBox 툴을 설치해줍니다.

참고자료,

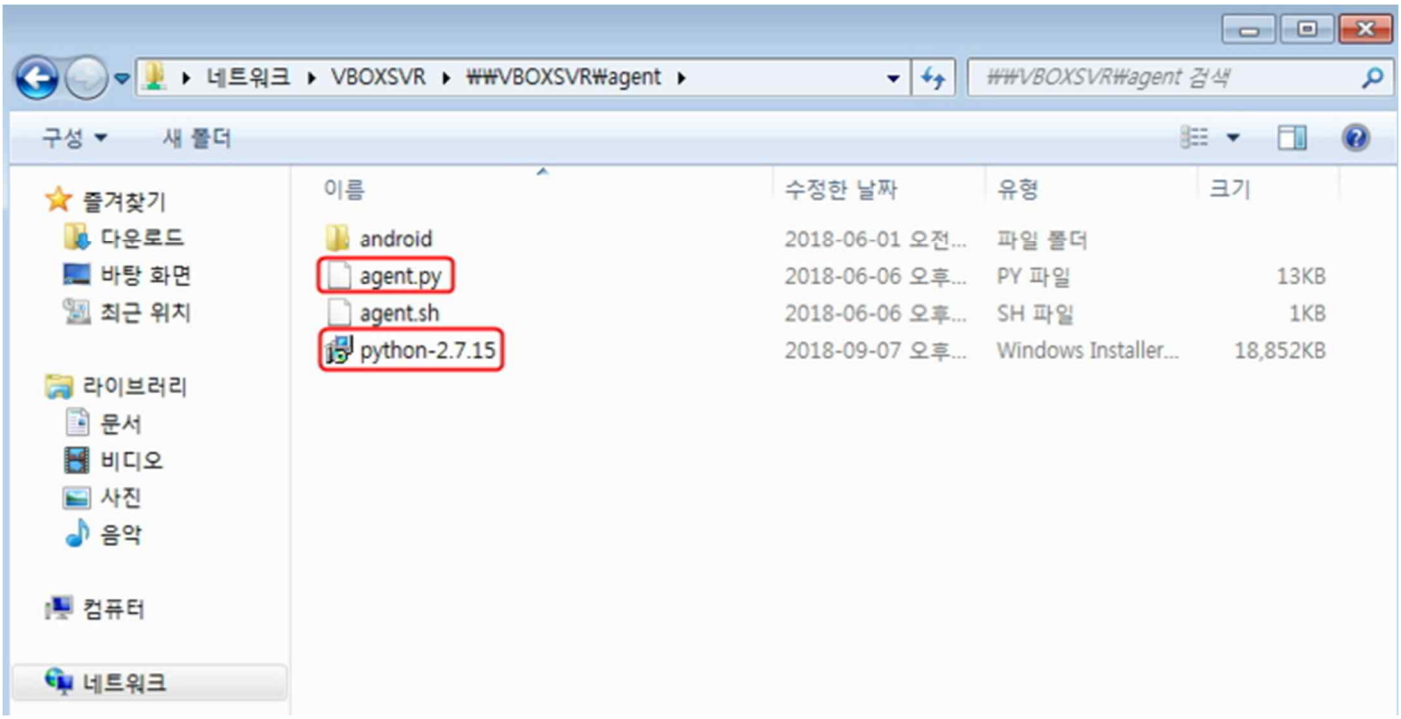
http://ccm3.net/archives/23976

[VirtualBox] 버추얼박스 윈도우 10 게스트 확장 설치하기

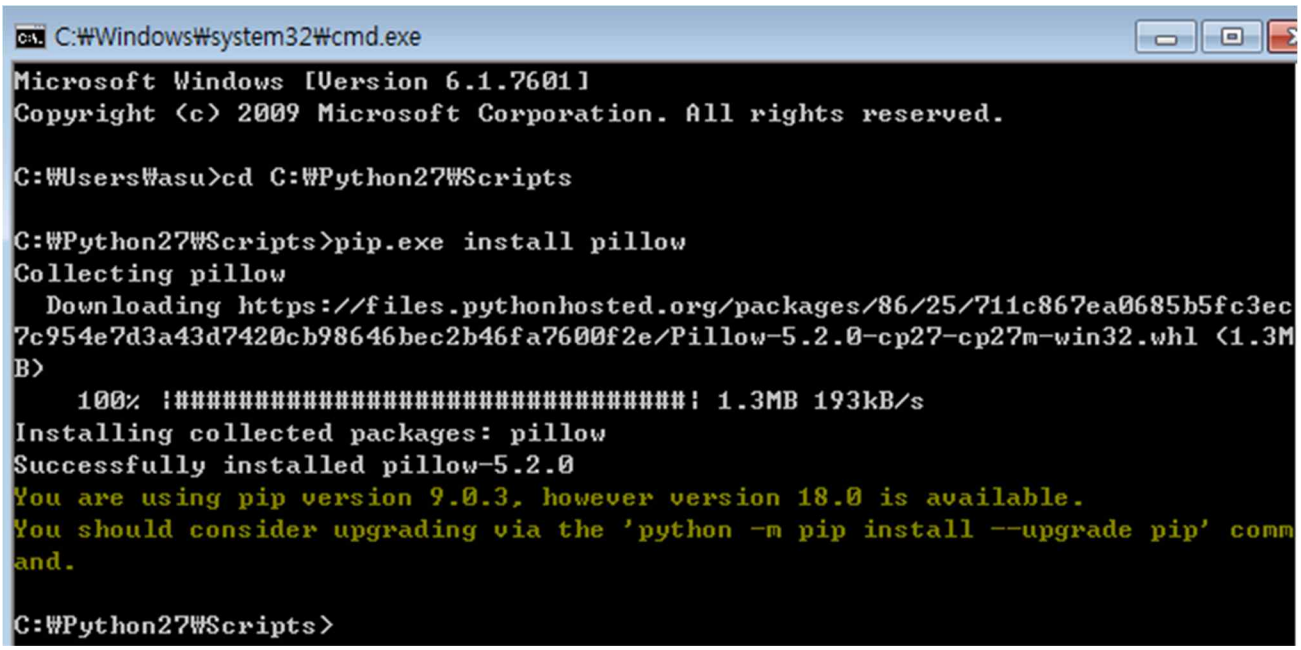
게스트 확장을 설치하면 해상도를 자유롭게 조절하거나 공유 폴더를 설정하는 등 게스트 운영체제를 좀 더 편리하게 사용할 수 있습니다.

ccm3.net

게스트 확장을 하시면, 공유폴더에 접근이 가능해집니다. 리눅스 agent 폴더에서 윈도우로 옮기기 전에 python2.7 버전을 설치 후에 agent 폴더로 옮겨 두시길 바랍니다. 무슨 이유인지 모르겠지만, 윈도우에서 파이썬 홈페이지가 접속이 안됩니다. 그 후에



표시된 위 두파일을 바탕화면에 옮깁니다. 그리고 파이썬 2.7 을 설치합니다. 그 후

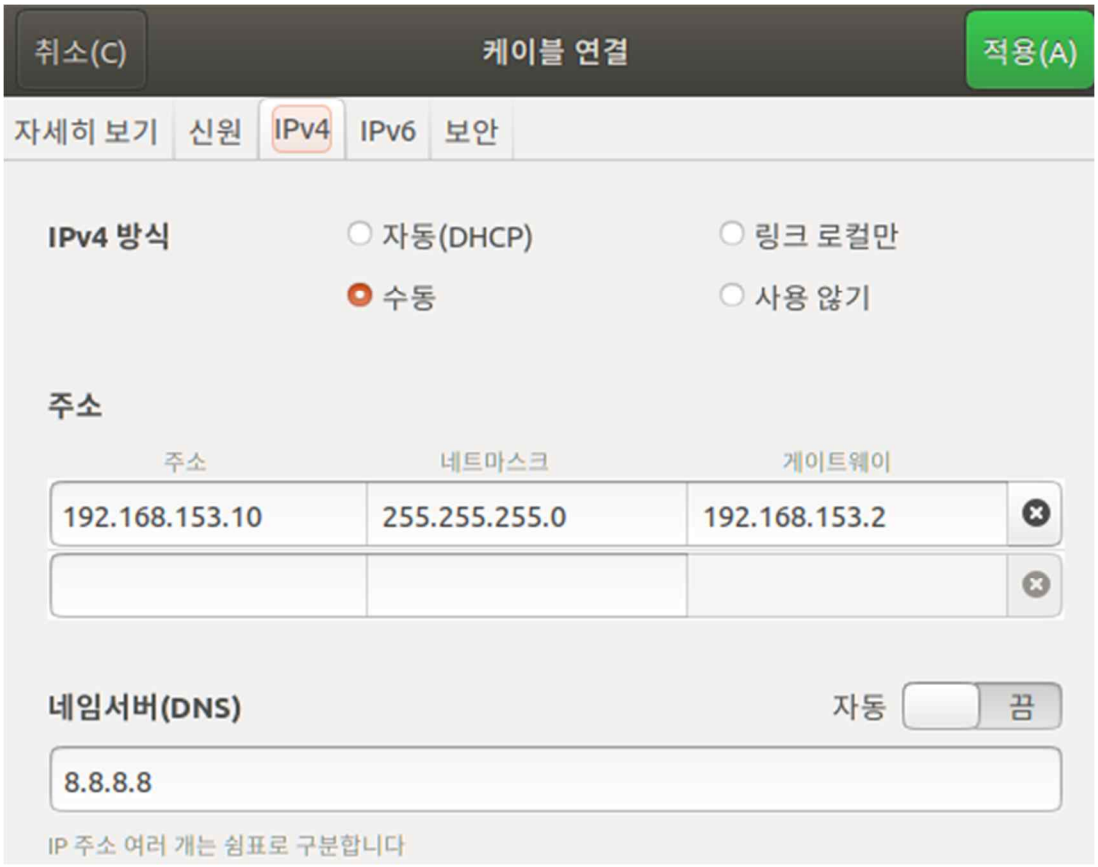


pip 명령을 이용해서 pillow 를 설치해줍니다.

10. ip 설정

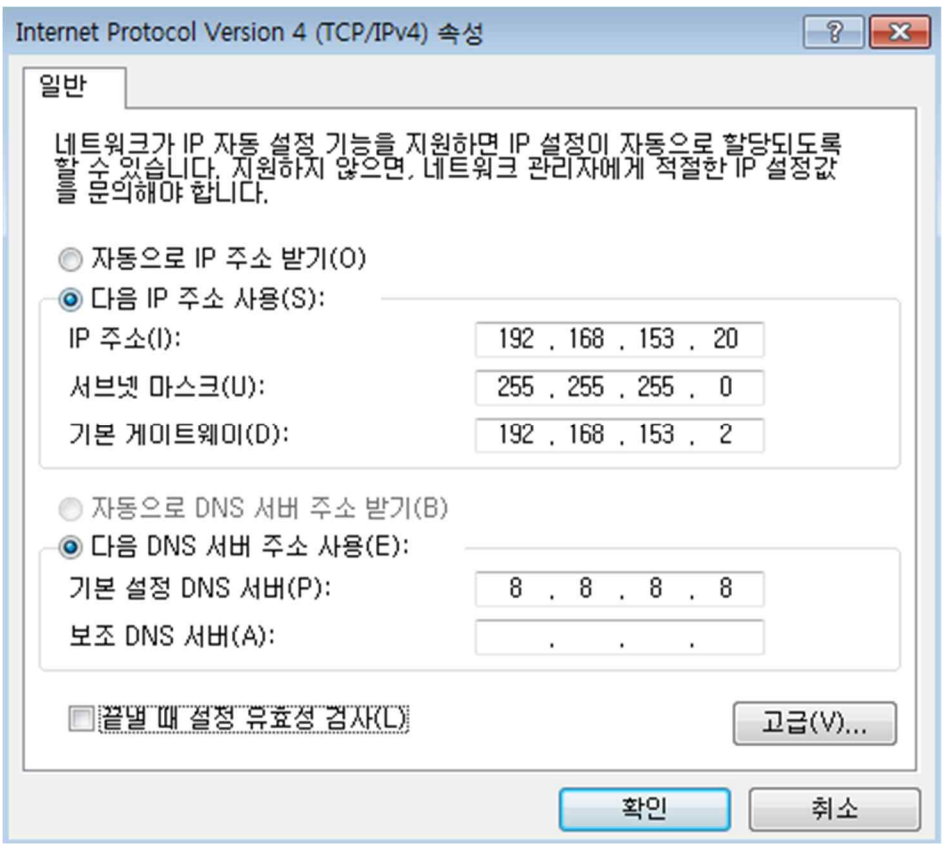
a) 우분투

설정 - 네트워크 - ipv4 에서 설정하시면 됩니다. 저는 원래 주소 192.168.153.133 에서 뒷자리만 바꾸어 192.168.153.10 으로 했습니다. 네임서버도 저렇게 설정해주시길 바랍니다.



b) 윈도우 ip 설정

제어판 - 네트워크 및 공유센터 - 로컬 영역 연결 - 속성 - ipv4



윈도우는 끝자리만 20 으로 설정했습니다. 인터넷이 되는지 반드시 확인하시구요.

윈도우 에서 agent.py 를 실행시키고 스냅샷 한 번 찍어줍니다. 그리고 종료시켜줍니다.

```
asu@asu-cuckoo:~$ VBoxManage snapshot "win7" take "Snapshot" --pause
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
Snapshot taken. UUID: a66b5d47-9784-4cf5-9181-1d37473dbc5a
asu@asu-cuckoo:~$ VBoxManage controlvm "win7" poweroff
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
asu@asu-cuckoo:~$
```

11. cuckoo 샌드박스 설정

home - .cuckoo - conf 로 가시면,

a) reportin.conf

```
[mongodb]
enabled = yes
host = 127.0.0.1
port = 27017
db = cuckoo
store_memdump = yes
paginate = 100
# MongoDB authentication (optional).
username =
password =
```

표시된 부분만 바꾸어 줍니다.

b) cuckoo.conf

```
[resultserver]
# The Result Server is used to receive in real time the behavioral logs
# produced by the analyzer.
# Specify the IP address of the host. The analysis machines should be able
# to contact the host through such address, so make sure it's valid.
# NOTE: if you set resultserver IP to 0.0.0.0 you have to set the option
# `resultserver_ip` for all your virtual machines in machinery configuration.
ip = 192.168.153.10
```

우분투 ip 주소로 설정해 줍니다.

c) virtualbox.conf

```
[virtualbox]
# Specify which VirtualBox mode you want to run your machines on.
# Can be "gui" or "headless". Please refer to VirtualBox's official
# documentation to understand the differences.
mode = gui

# Path to the local installation of the VBoxManage utility.
path = /usr/bin/VBoxManage
# If you are running Cuckoo on Mac OS X you have to change the path as follows:
# path = /Applications/VirtualBox.app/Contents/MacOS/VBoxManage

# Default network interface.
interface = ens33

# Specify a comma-separated list of available machines to be used. For each
# specified ID you have to define a dedicated section containing the details
# on the respective machine. (E.g. cuckoo1,cuckoo2,cuckoo3)
machines = cuckoo1
[cuckoo1]
# Specify the label name of the current machine as specified in your
# VirtualBox configuration.
label = win7

# Specify the operating system platform used by current machine
# [windows/darwin/linux].
platform = windows

# Specify the IP address of the current virtual machine. Make sure that the
# IP address is valid and that the host machine is able to reach it. If not,
# the analysis will fail.
ip = 192.168.153.20
```

label 은 벌추얼 머신 이름, ip 주소는 윈도우 ip 주소

12. cuckoo 박스 실행

터미널 두 개가 필요합니다.

하나의 터미널 - cuckoo

다른 하나의 터미널 - cuckoo web runserver

```
asu@asu-cuckoo:~$ cuckoo

                              ),-.      /
  Cuckoo Sandbox             <(a  `---','
     no chance for malwares!  ( `-, ._> )
                               ) _>.___/
                                 _/


 Cuckoo Sandbox 2.0.6
 www.cuckoosandbox.org
 Copyright (c) 2010-2018

 Checking for updates...
 You're good to go!

 Our latest blogposts:
 * Cuckoo Sandbox 2.0.6, June 07, 2018.
   Interim release awaiting the big release.
   More at https://cuckoosandbox.org/blog/206-interim-release

 * Cuckoo Sandbox 2.0.5: Office DDE, December 03, 2017.
   Brand new release based on a DDE case study.
   More at https://cuckoosandbox.org/blog/205-office-dde
```

```
asu@asu-cuckoo:~$ cuckoo web runserver
Performing system checks...

System check identified no issues (0 silenced).
September 07, 2018 - 16:31:24
Django version 1.8.4, using settings 'cuckoo.web.web.settings'
Starting development server at http://127.0.0.1:8000/
Quit the server with CONTROL-C.
```

이 상태에서 웹 브라우저를 키고, 127.0.0.1:8000 을 입력하면,