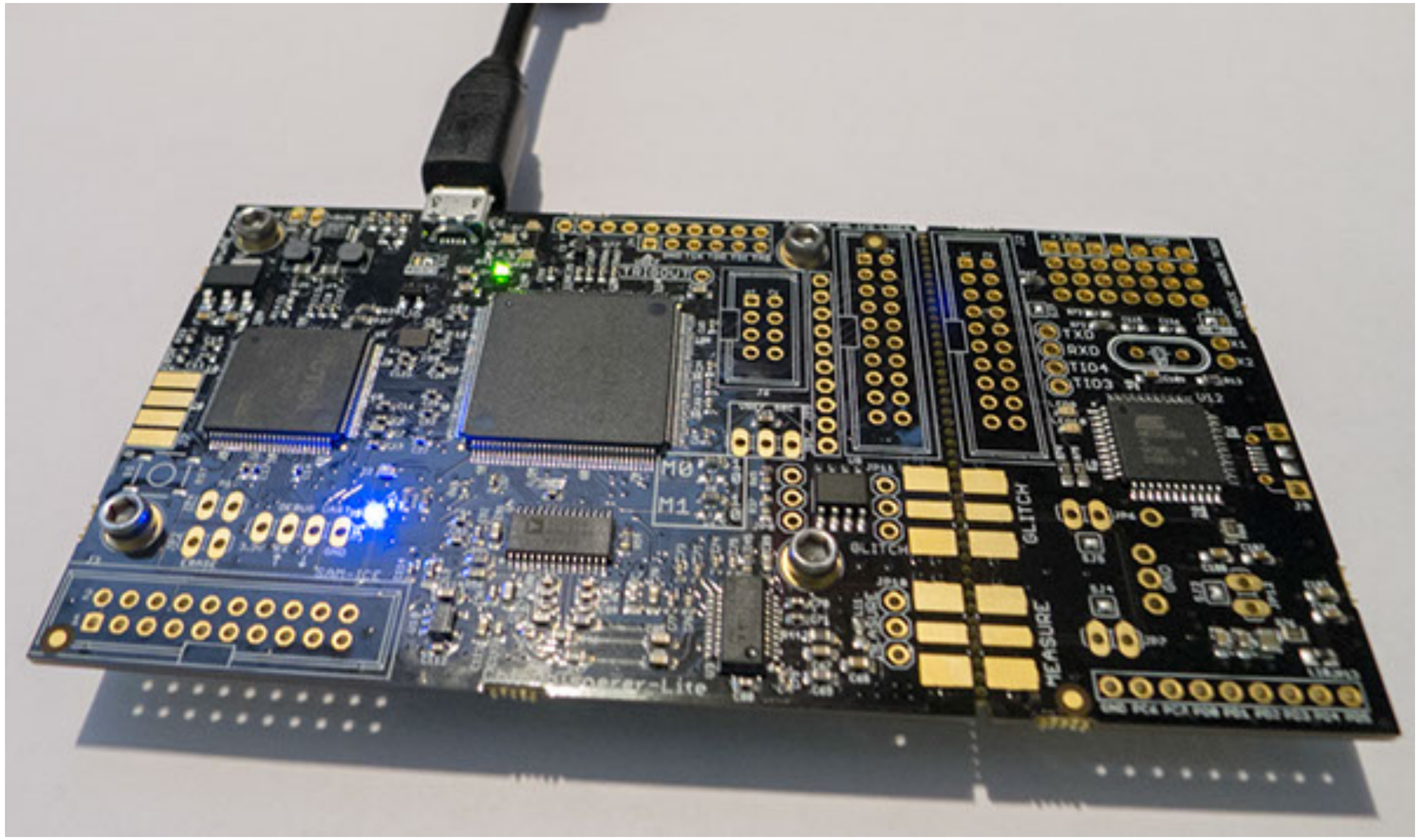
부채널 분석

전력 분석 공격 2

실습

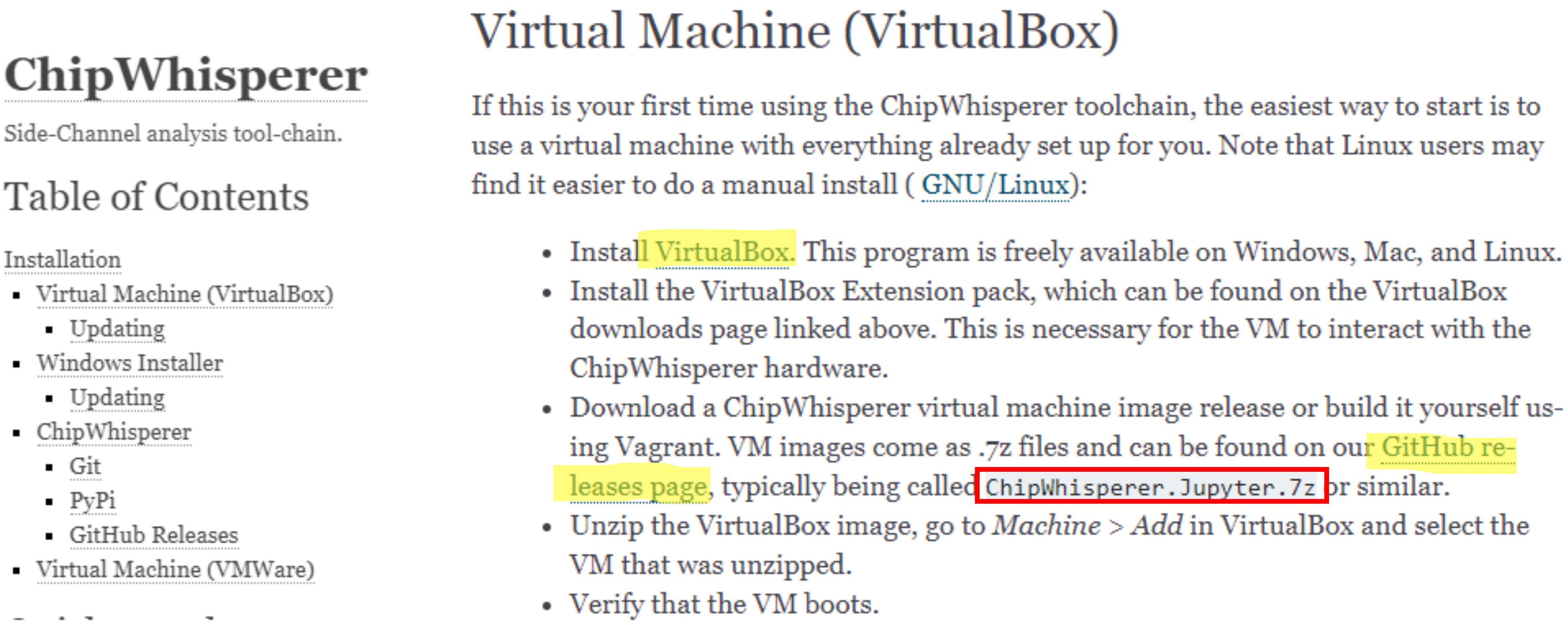
ChipWhisperer : 부채널 전력 분석 오픈 소스 도구

ChipWhisperer V5
ChipWhisperer-Lite Xmega



설치

- https://chipwhisperer.readthedocs.io/en/latest/installing.html#install-virtual-machine
- GitHub : https://github.com/newaetech/chipwhisperer/releases
- VirtualBox : https://www.virtualbox.org/wiki/Downloads



ChipWhisperer

Side-Channel analysis tool-chain.

Table of Contents

Installation

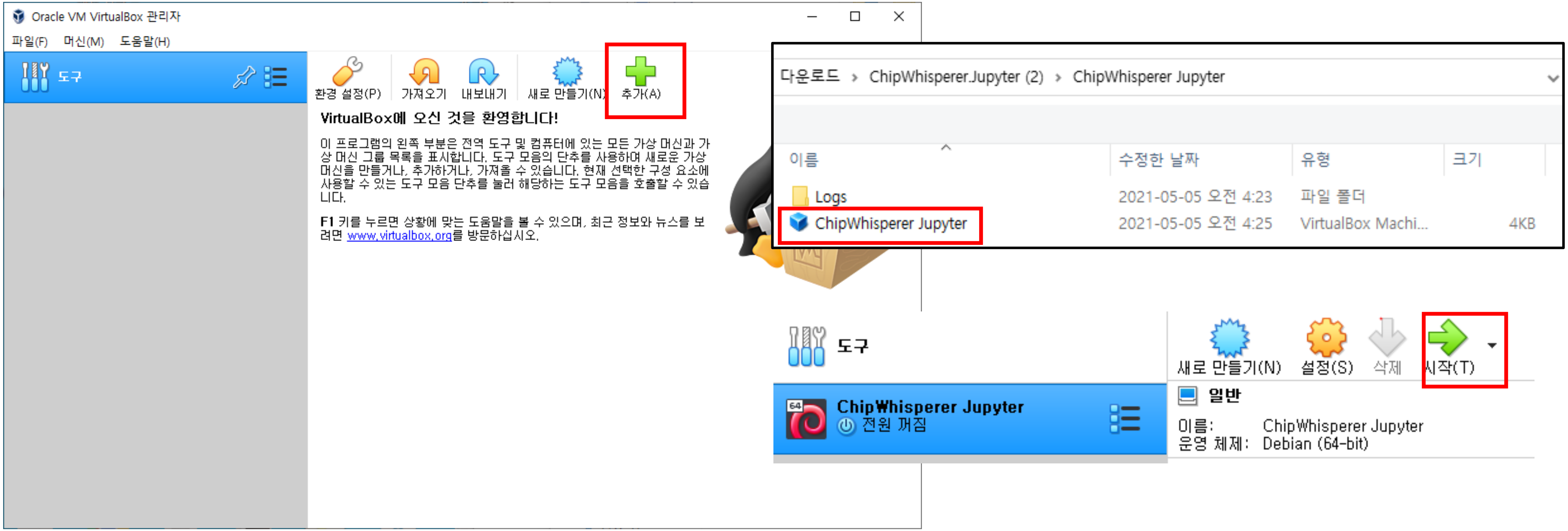
- Virtual Machine (VirtualBox)
  - Updating
- Windows Installer
  - Updating
- ChipWhisperer
  - Git
  - PyPi
  - GitHub Releases
- Virtual Machine (VMWare)

Virtual Machine (VirtualBox)

If this is your first time using the ChipWhisperer toolchain, the easiest way to start is to use a virtual machine with everything already set up for you. Note that Linux users may find it easier to do a manual install (GNU/Linux):

- Install VirtualBox. This program is freely available on Windows, Mac, and Linux.
- Install the VirtualBox Extension pack, which can be found on the VirtualBox downloads page linked above. This is necessary for the VM to interact with the ChipWhisperer hardware.
- Download a ChipWhisperer virtual machine image release or build it yourself using Vagrant. VM images come as .7z files and can be found on our GitHub releases page, typically being called `ChipWhisperer.Jupyter.7z` or similar.
- Unzip the VirtualBox image, go to *Machine* > *Add* in VirtualBox and select the VM that was unzipped.
- Verify that the VM boots.

설치



VirtualBox에 오신 것을 환영합니다!

이 프로그램의 왼쪽 부분은 전역 도구 및 컴퓨터에 있는 모든 가상 머신과 가상 머신 그룹 목록을 표시합니다. 도구 모음의 단추를 사용하여 새로운 가상 머신을 만들거나, 추가하거나, 가져올 수 있습니다. 현재 선택한 구성 요소에 사용할 수 있는 도구 모음 단추를 눌러 해당하는 도구 모음을 호출할 수 있습니다.

F1 키를 누르면 상황에 맞는 도움말을 볼 수 있으며, 최근 정보와 뉴스를 보려면 www.virtualbox.org를 방문하십시오.

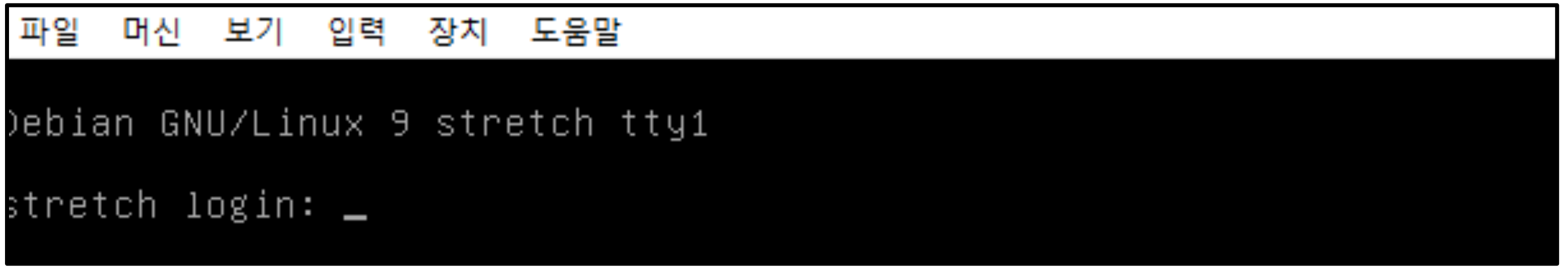
다운로드 › ChipWhisperer.Jupyter (2) › ChipWhisperer Jupyter

이름	수정한 날짜	유형	크기
Logs	2021-05-05 오전 4:23	파일 폴더	
ChipWhisperer Jupyter	2021-05-05 오전 4:25	VirtualBox Machi...	4KB

일반

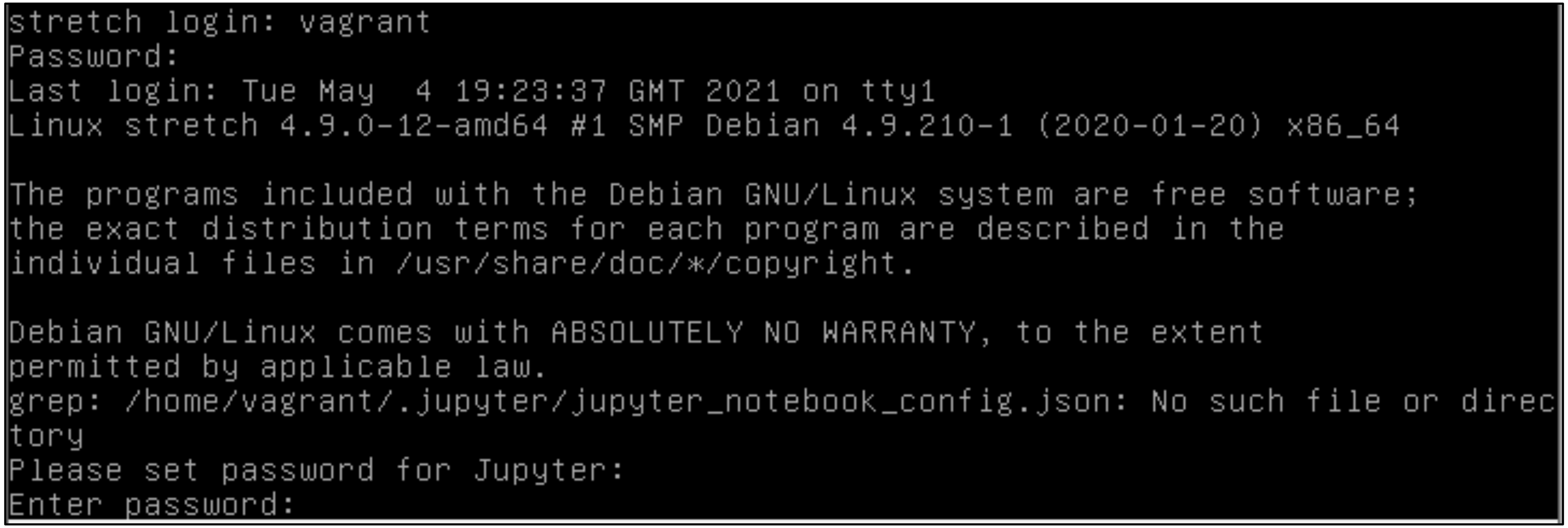
이름: ChipWhisperer Jupyter
운영 체제: Debian (64-bit)

jupyter notebook 실행



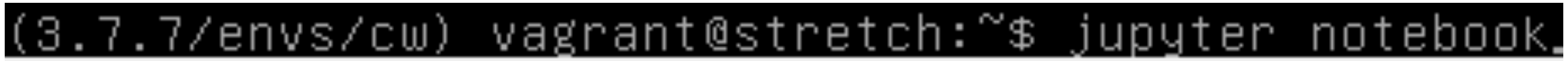
```
)ebian GNU/Linux 9 stretch tty1

stretch login: _
```

- user: vagrant pass: vagrant



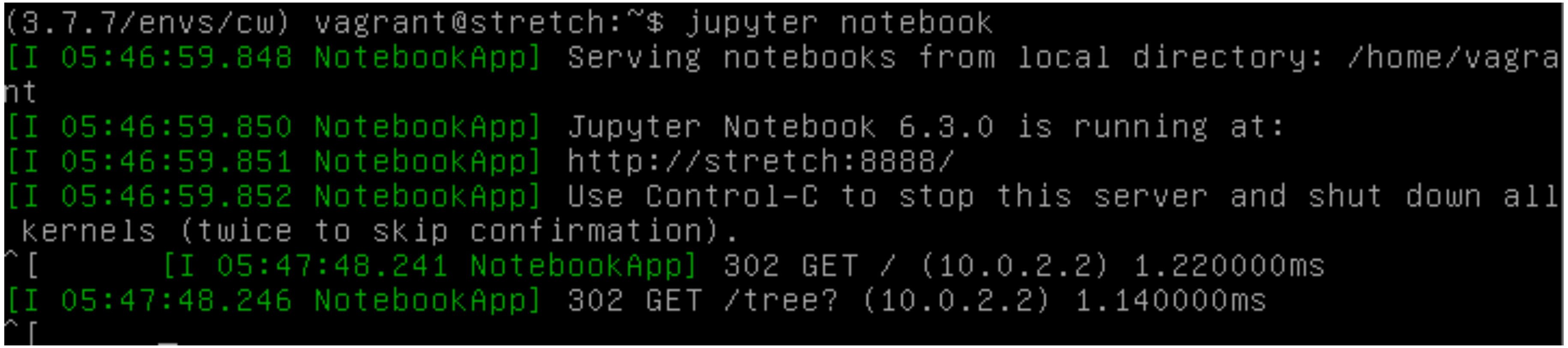
```
stretch login: vagrant
Password:
Last login: Tue May  4 19:23:37 GMT 2021 on tty1
Linux stretch 4.9.0-12-amd64 #1 SMP Debian 4.9.210-1 (2020-01-20) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
grep: /home/vagrant/.jupyter/jupyter_notebook_config.json: No such file or direc
tory
Please set password for Jupyter:
Enter password:
```

jupyter notebook 실행

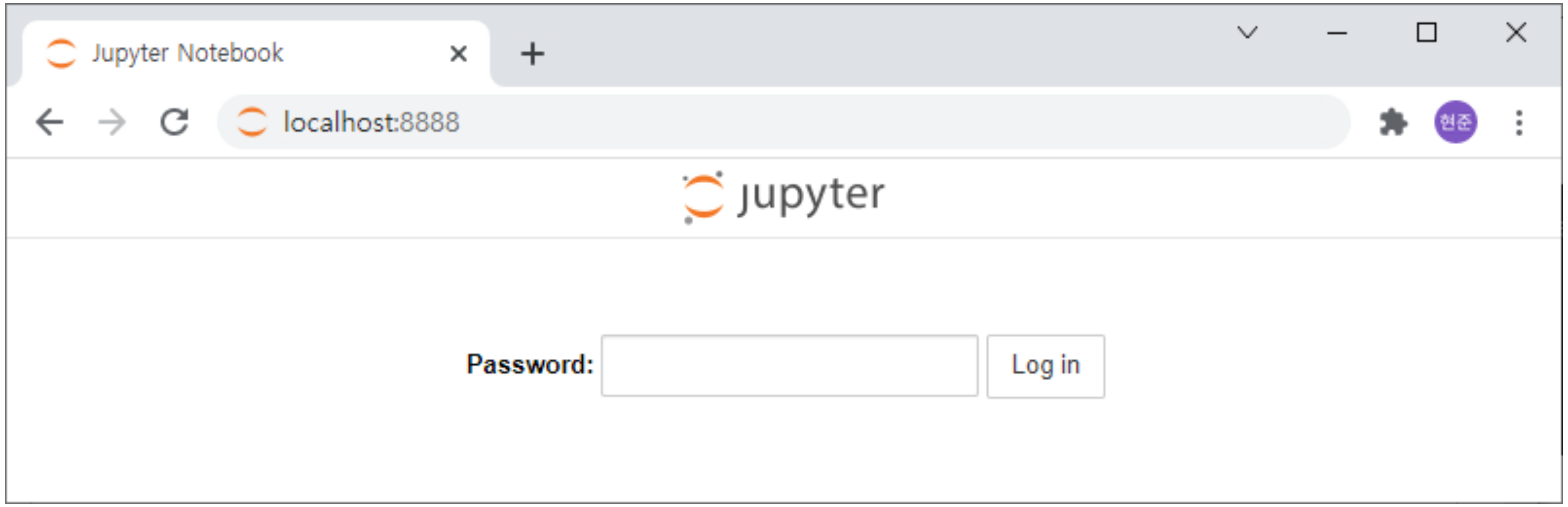


```
(3.7.7/envs/cw) vagrant@stretch:~$ jupyter notebook
```

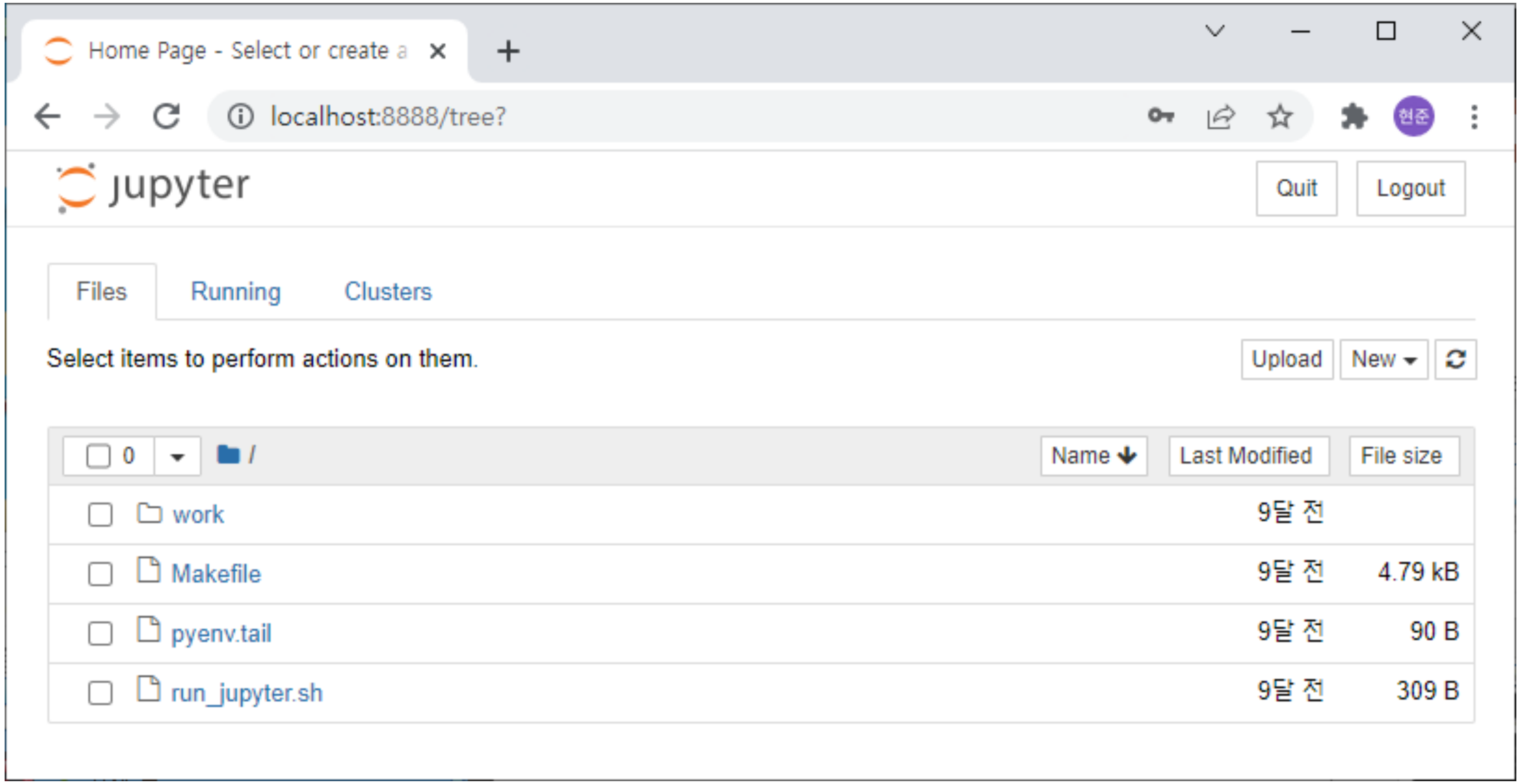
$ Jupyter notebook



```
(3.7.7/envs/cw) vagrant@stretch:~$ jupyter notebook
[I 05:46:59.848 NotebookApp] Serving notebooks from local directory: /home/vagra
nt
[I 05:46:59.850 NotebookApp] Jupyter Notebook 6.3.0 is running at:
[I 05:46:59.851 NotebookApp] http://stretch:8888/
[I 05:46:59.852 NotebookApp] Use Control-C to stop this server and shut down all
 kernels (twice to skip confirmation).
^[      [I 05:47:48.241 NotebookApp] 302 GET / (10.0.2.2) 1.220000ms
[I 05:47:48.246 NotebookApp] 302 GET /tree? (10.0.2.2) 1.140000ms
^[
```



jupyter notebook



Select items to perform actions on them.

Name	Last Modified	File size
□ work	9달 전	
□ Makefile	9달 전	4.79 kB
□ pyenv.tail	9달 전	90 B
□ run_jupyter.sh	9달 전	309 B

파형 수집

RSA attack : SPA

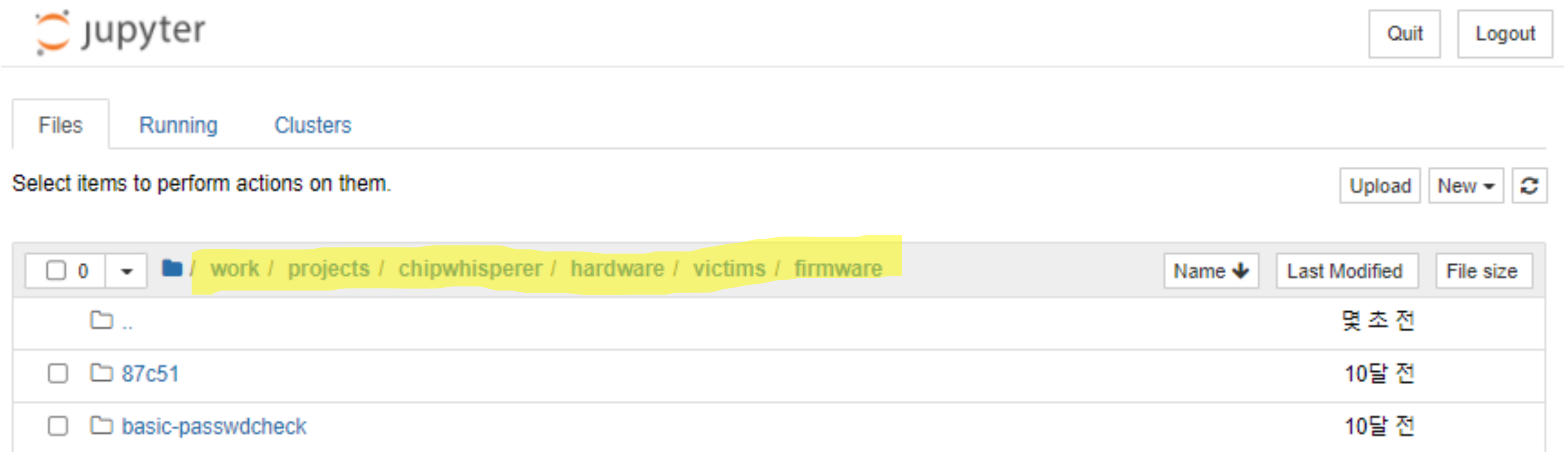
https://wiki.newae.com/V3:Tutorial_B11_Breaking_RSA

AES attack : DPA, CPA

https://chipwhisperer.readthedocs.io/en/latest/tutorials/courses_sca101_soln_lab%203_3%20-openadc-cwlitearm.html#conclusions-next-steps

https://chipwhisperer.readthedocs.io/en/latest/tutorials/courses_sca101_soln_lab%204_2%20-openadc-cwlitexmega.html#aes-trace-capture

scope 연결 → target 연결 → target 보드에 코드 업로드 → 설정 → 수집 → 공격



Select items to perform actions on them.

□ 0 / work / projects / chipwhisperer / hardware / victims / firmware

	..	몇 초 전
□	87c51	10달 전
□	basic-passwdcheck	10달 전

simpleserial-aes, simpleserial-rsa