THE NIMROD PROJECT

Shaikh Mamun Hoque
IIT Jammu

With the increasing number of IoT devices around us, the need for them to be secure is something that cannot be taken lightly. A lot of tools are available to help security researchers in this pursuit. Even though every firmware is a different game in itself there are some steps in the process that are similar. This project aims to abstract as much of the work as possible to aid the researchers in accelerating their analysis of a firmware. It provides a Graphical User Interface for easy access to common tasks like reading file signatures, slicing out parts, extracting files, spawning cross architectural shells, creating virtual machines, etc.

Eel

Eel is a lightweight python library used for creating desktop applications using web technologies. This project has been built using Eel. All of the logic is contained in the *main.py* file. However it will be separated based on functionality.

https://github.com/samuelhwilliams/Eel

Binwalk

Binwalk is an open source firmware extraction tool that extracts embedded file systems from firmware images. Binwalk is used in this project for identifying file signatures and also for its various utilities like viewing entropy etc.

https://github.com/ReFirmLabs/binwalk

QEMU

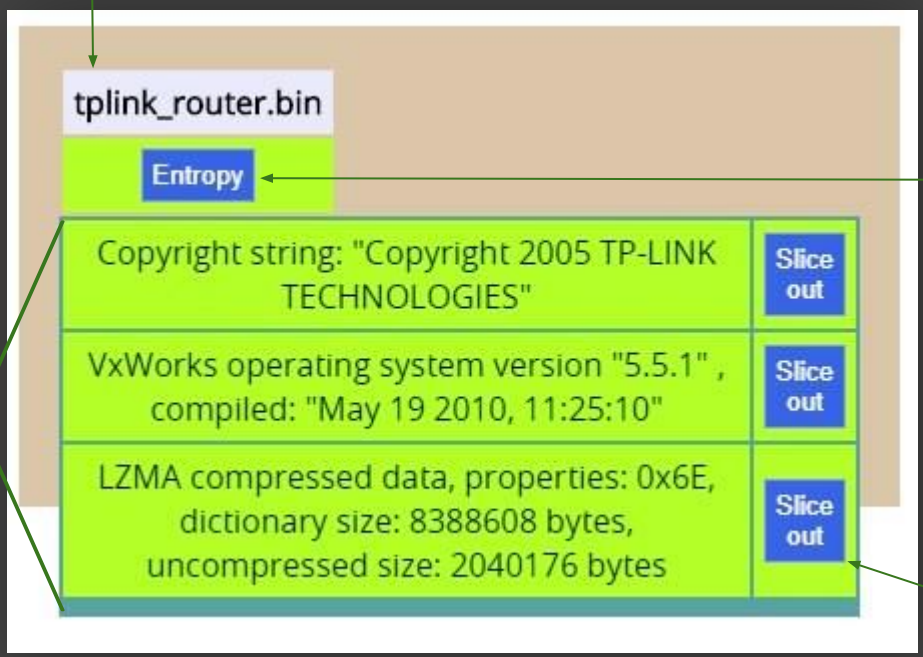
QEMU is a generic and open source machine emulator and virtualizer. It is able to perform both User-mode emulation and Full-system emulation.

https://www.qemu.org/

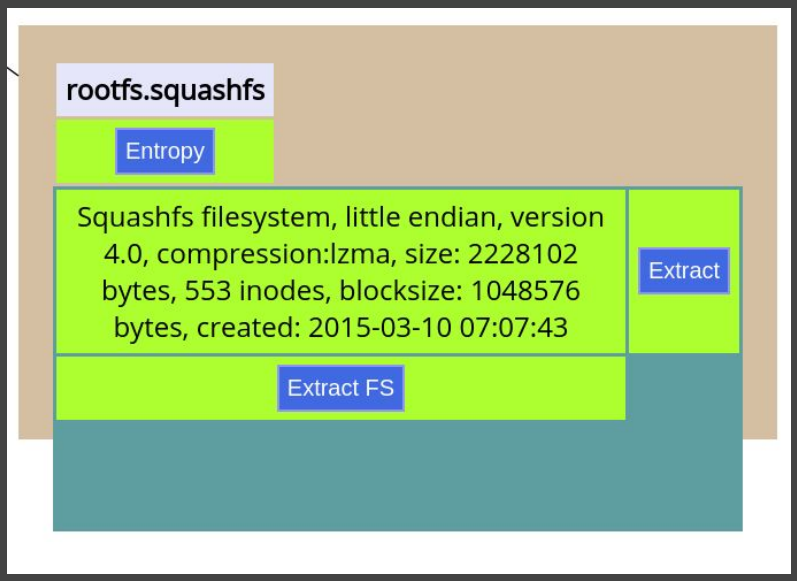
Along with these, many utilities are used for visualisation, extraction etc

GUI

The GUI is rendered using HTML and JS. All the analysis tasks are done by the python scripts. Currently everything in it is just at the prototype stage and there is just once case handled for each task; extractor for only squashfs file system, vm for only debian-mips etc.



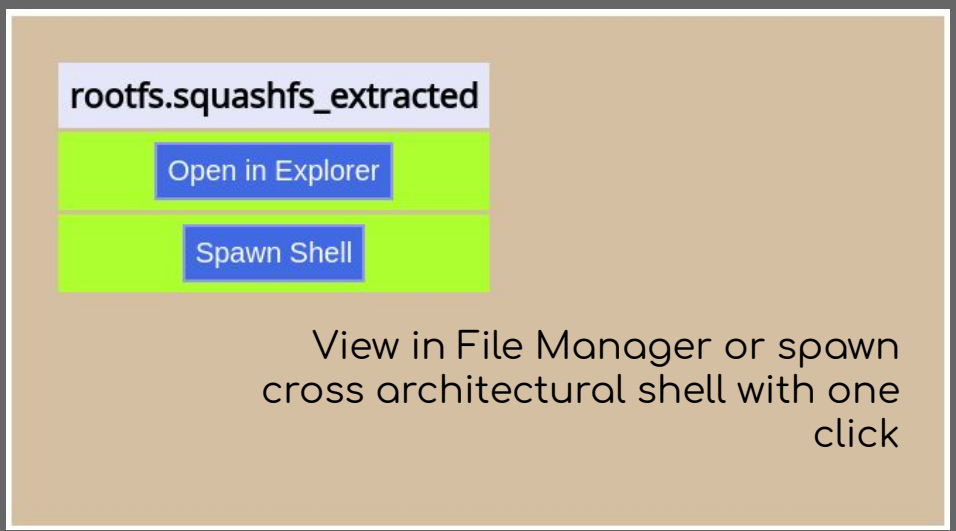
A sample card



Extract File Systems

QEMU performs the emulation. However the detecting of architecture type and few configurations are done in the background which enables the user to spawn shells for the required architecture with one click. Full System emulation is a bit tricky. We can setup a vm and copy the files for starter but every firmware has quirks of its own. Nevertheless the process is a bit less cumbersome now.

EMULATION



View in File Manager or spawn cross architectural shell with one click

Immediate Objectives

- Add support for multiple File System formats
- Automate the common ways for user-mode emulation
- Automate common ways for Full-System Emulation
- Fix bugs in GUI renders

GitHub Repo : https://github.com/PositronPiercer/tereBinWalk