ECE 531: Introduction to Internet of Things

Homework #1: Binary File Analysis

Joseph Hilland – 101104172 –
jhilland@unm.edu

Summer 2022

Contents

List of Figures

2 Abstract

The purpose of this assignment is to understand the contents of firmware binary files¡as well as test the knowledge and setup of tools within the Linux host environment that has been created. These tools include but are not limited to binwalk, binutils, radare and qemu. Three files were utilized during this assignment which included:

- NC220_1.1.12_Build_160321_Rel.27531.bin (Version A)
- NC220_1.1.12_Build_160321_Rel_upgrade.27531.bin (Version B)
- NC220_1.2.0_Build_170516_Rel.B4AC0D_2017-05-16_.00.32.bin (Version 2)

3 Binwalk

Binwalk is a tool for searching and identifying files and code embedded within binary files, specifically within firmware images.

To begin, binwalk was used to analyze the Version A, Version B and Version 2 binary files.

```
$ binwalk -e -C 1.1.12a -M NC220_1.1.12_Build_160321_Rel.27531.bin
$ binwalk -e -C 1.1.12a -M NC220_1.1.12_Build_160321_Rel_upgrade.27531.bin
$ binwalk -e -C 1.1.12a -M \
NC220_1.2.0_Build_170516_Rel.B4AC0D_2017-05-16.00.32.bin
```

The figure from the binwalk output below shows that the firmware images were running MIPS architecture. The firmware images also use JFFS2 filesystem. JFFS2 is a filesystem designed for use on flash drives in embedded systems.

There is a U-Boot version and date listed as well as the Linux kernel version. These components could be further investigated as needed to identify any risks or vulnerabilities within the system.

By changing directories into the jffs2-root directory, other directories can be seen that contain different information about the firmware images.

By investigating the bin/ directory, there are several commands that can be seen which are utilized within this firmware image.

There are several other directories including lib, etc and www. These directories appear to contain a web interface, password files, certificates and libraries used. Further investigation can be done on these files and commands to broaden the understanding of their uses in this firmware image.

When analyzing the version 2 image, there were some extra files and commands found. One of those commands used in the bin directory was logCtrl.

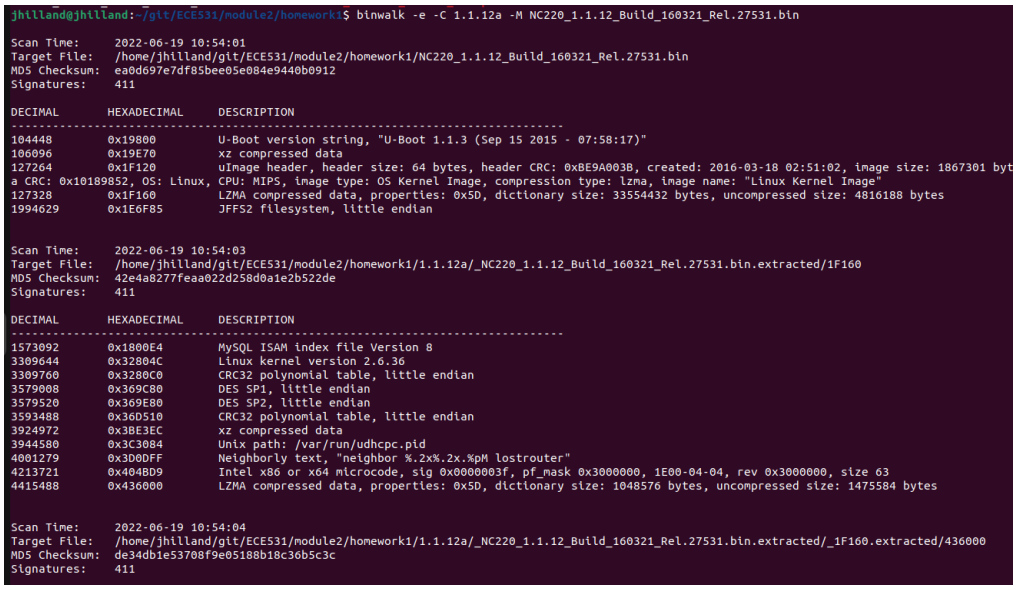

Figure 1: Binwalk Command Output

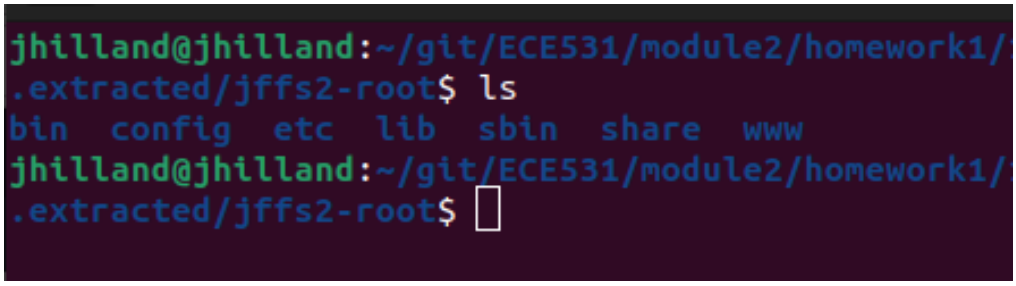

Figure 2: JFFS2 Filesystem Contents

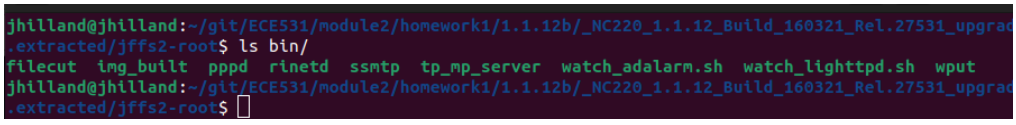

Figure 3: Bin Directory Contents

4 Analyzing Tools

Tools used for further analysis included but were not limited to:

- qemu-mips-static - QEMU emulator static version
- binutils - collection of binary tools

Some of the binutil commands used during analysis are listed below. Many of the commands and files in these images were not able to be analyzed by readelf or objdump tools. However the strings command worked well in searching the files. A lot of the files within the config directory were viewable in plain text. These configuration files may contain important information pertaining to how the system is configured. Radare2 was also installed which comes with other tools for analyzing binary elements.

- grep -iRn 'SEARCH_TEXT'
- strings -n 10 'filename'
- mips-linux-gnu-readelf -d COMMAND
- sudo chroot . ./qemu-mips-static COMMAND -option
- rabin2 -I file

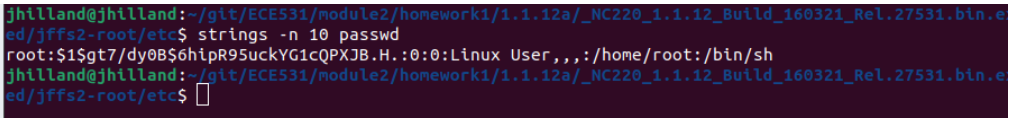

Figure 4: Strings on passwd

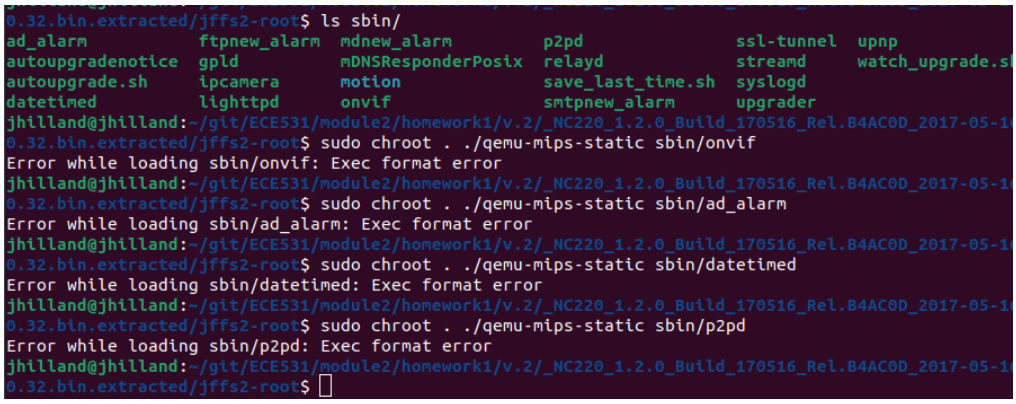

Figure 5: Qemu Commands

Radare2's rabin2 command was used to analyze multiple files. This tool can tell us information about the file, such as the programming language and operating system supported.

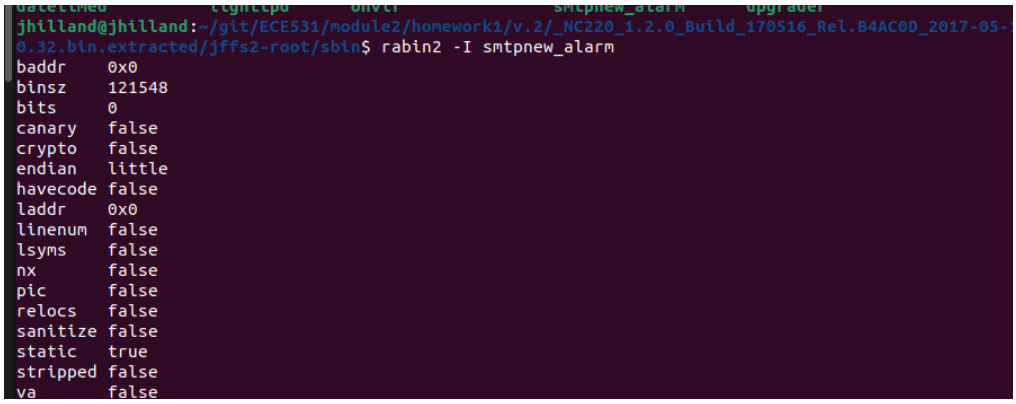

Figure 6: Radare2 Commands

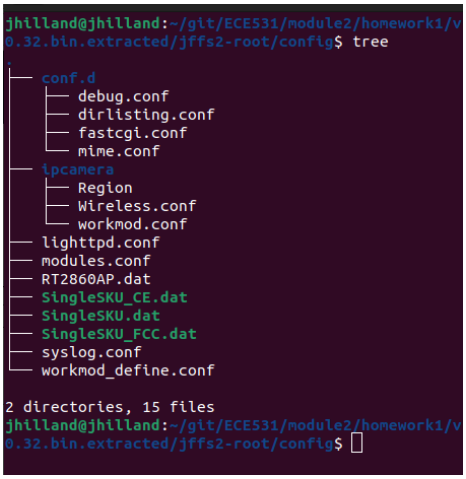

Figure 7: Config Directory Contents

5 Conclusion

The file structure is fairly similar to that of the HS110 image that was explored during lecture slides. However there is no usr/bin directory for analysis. All three NC220 binary files have similar filesystem setups. They are all running off of the JFFS2 filesystem. All three have the same Linux kernel version number. There are a few files extra within the version 2 binary file. Based on commands found in the bin and sbin directories, further research and analysis could be done. There were attempts at running some commands via qemu-mips-static, however results were unsuccessful.