Module-2 Assignment: Analysis of NC220 Firmware

Nawaraj Khatiwada
ECE-531 Intro to the Internet of Things
Prof. Dr. Lamb
Summer 2024

Introduction

The purpose of this report is to analyze the firmware images of the NC220 device to understand their structure, components, and functionalities. This report has been developed on the foundation of all the concepts and tools discussed in the course, especially firmware extraction and reverse engineering. The tools used here is tools include but are not limited to; binwalk, binutils, qemu and other necessary Linux libraries. Three given files were used in this assignment:

- NC220_1.1.12_Build_160321_Rel.27531.bin
- NC220_1.1.12_Build_160321_Rel.27531_upgrade.bin
- NC220_1.2.0_Build_170516_Rel.B4AC0D_2017-05-16_16.00.32.bin

Methodology

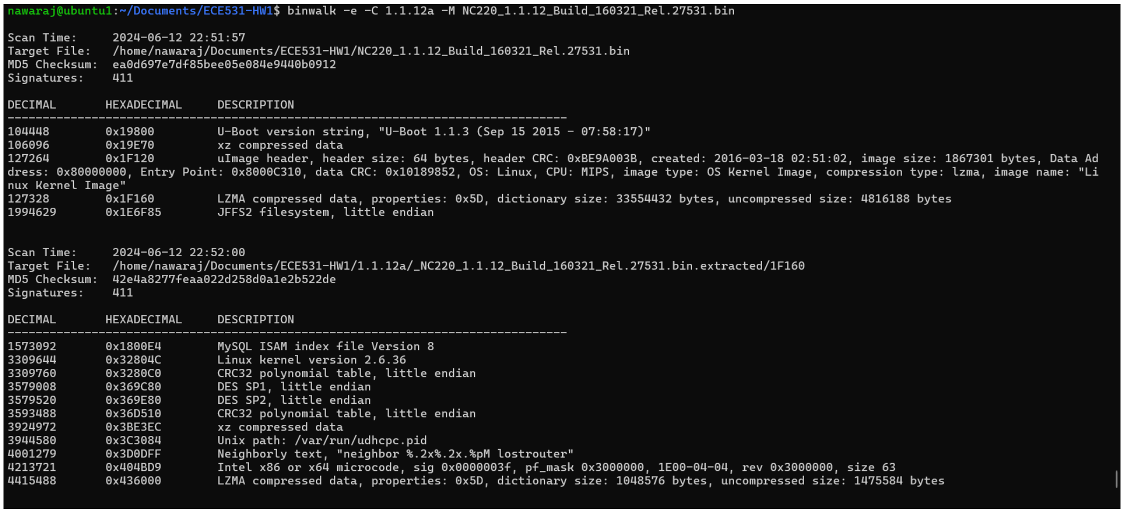
This report is based on a process which begins with the installation of necessary libraries on virtual Ubuntu Linux machine and then moves to the extraction of firmware images. The following steps were taken to set up and carry out the analysis:

- sudo apt install binwalk
- sudo apt install binutils
- sudo apt install tree
- sudo apt install qemu-user-static

Extraction of Firmware Images:

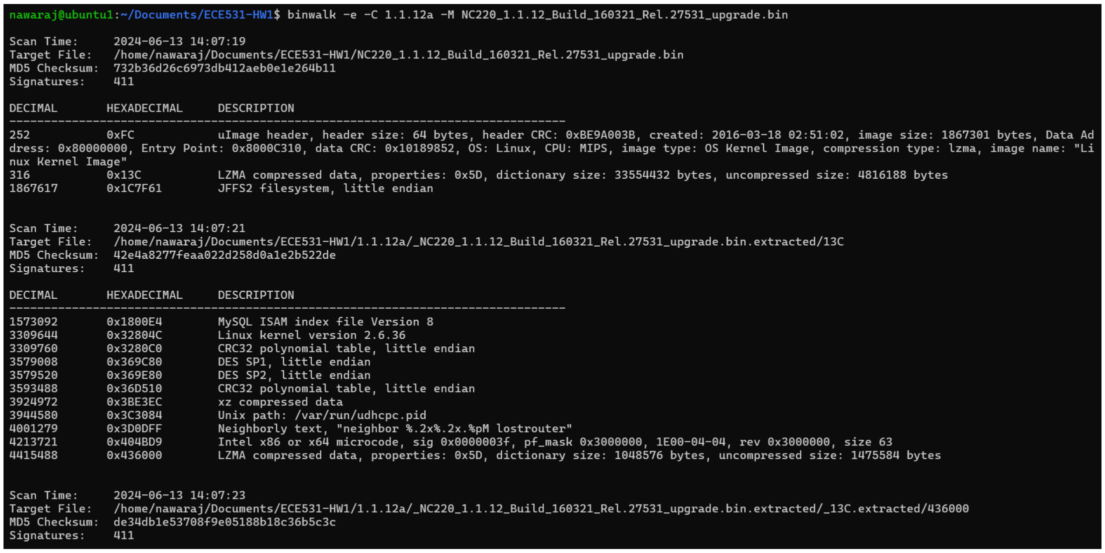
Binwalk is used for analyzing binary files and packages files for the presence of files and codes such as firmware images.

1) binwalk -e -C 1.1.12a -M NC220_1.1.12_Build_160321_Rel.27531.bin
2) binwalk -e -C 1.1.12a -M NC220_1.1.12_Build_160321_Rel.27531_upgrade.bin
3) binwalk -e -C 1.1.12a -M NC220_1.2.0_Build_170516_Rel.B4AC0D_2017-05-16_16.00.32.bin



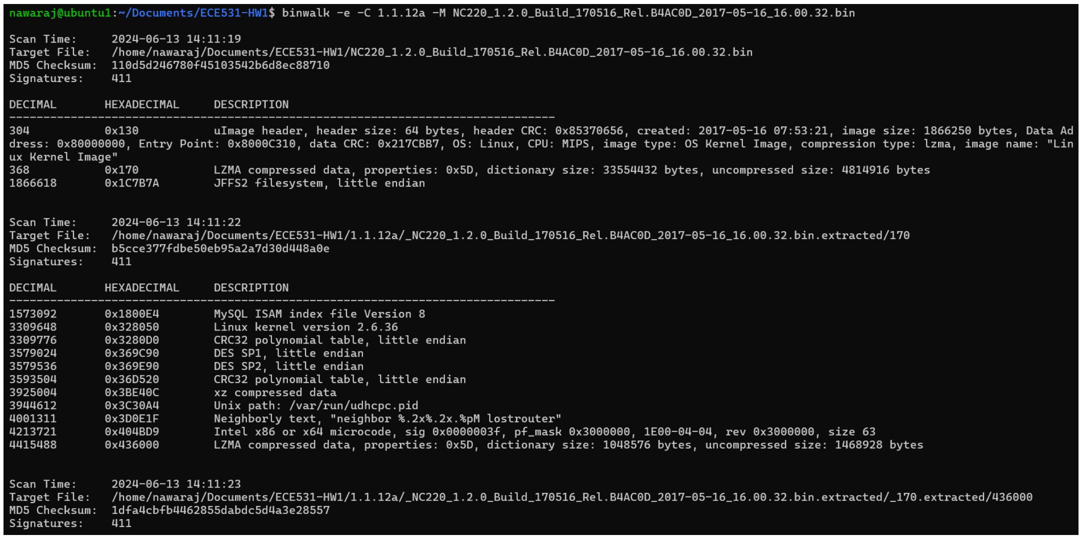
```
nawaraj@ubuntu1:~/Documents/ECE531-HW1$ binwalk -e -C 1.1.12a -M NC220_1.1.12_Build_160321_Rel.27531.bin

Scan Time:     2024-06-12 22:51:57
Target File:   /home/nawaraj/Documents/ECE531-HW1/NC220_1.1.12_Build_160321_Rel.27531.bin
MD5 Checksum:  ea0d697e7df85bee05e084e9440b0912
Signatures:    411

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
104448        0x19800         U-Boot version string, "U-Boot 1.1.3 (Sep 15 2015 - 07:58:17)"
106096        0x19E70         xz compressed data
127264        0x1F120         uImage header, header size: 64 bytes, header CRC: 0xBE9A003B, created: 2016-03-18 02:51:02, image size: 1867301 bytes, Data Ad
dress: 0x80000000, Entry Point: 0x8000C310, data CRC: 0x10189852, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "Li
nux Kernel Image"
127328        0x1F160         LZMA compressed data, properties: 0x5D, dictionary size: 33554432 bytes, uncompressed size: 4816188 bytes
1994629       0x1E6F85        JFFS2 filesystem, little endian


Scan Time:     2024-06-12 22:52:00
Target File:   /home/nawaraj/Documents/ECE531-HW1/1.1.12a/_NC220_1.1.12_Build_160321_Rel.27531.bin.extracted/1F160
MD5 Checksum:  42e4a8277feaa022d258d0a1e2b522de
Signatures:    411

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
1573092       0x1800E4        MySQL ISAM index file Version 8
3309644       0x32804C        Linux kernel version 2.6.36
3309760       0x3280C0        CRC32 polynomial table, little endian
3579008       0x369C80        DES SP1, little endian
3579520       0x369E80        DES SP2, little endian
3593488       0x36D510        CRC32 polynomial table, little endian
3924972       0x3BE3EC        xz compressed data
3944580       0x3C3084        Unix path: /var/run/udhcpc.pid
4001279       0x3D0DFF        Neighborly text, "neighbor %.2x%.2x.%pM lostrouter"
4213721       0x404BD9        Intel x86 or x64 microcode, sig 0x0000003f, pf_mask 0x3000000, 1E00-04-04, rev 0x3000000, size 63
4415488       0x436000        LZMA compressed data, properties: 0x5D, dictionary size: 1048576 bytes, uncompressed size: 1475584 bytes
```

Binwalk Command Output _v1.1.12_160321_a



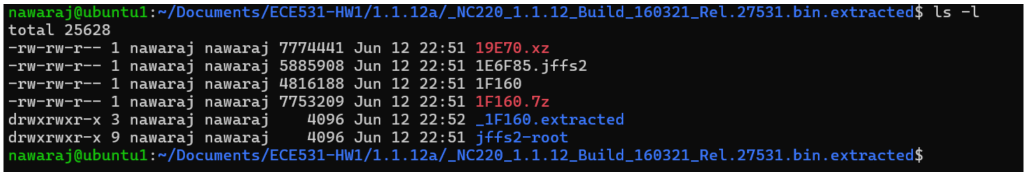
```
nawaraj@ubuntu1:~/Documents/ECE531-HW1$ binwalk -e -C 1.1.12a -M NC220_1.1.12_Build_160321_Rel.27531_upgrade.bin

Scan Time:     2024-06-13 14:07:19
Target File:   /home/nawaraj/Documents/ECE531-HW1/NC220_1.1.12_Build_160321_Rel.27531_upgrade.bin
MD5 Checksum:  732b36d26c6973db412aeb0e1e264b11
Signatures:    411

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
252           0xFC            uImage header, header size: 64 bytes, header CRC: 0xBE9A003B, created: 2016-03-18 02:51:02, image size: 1867301 bytes, Data Ad
dress: 0x80000000, Entry Point: 0x8000C310, data CRC: 0x10189852, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "Li
nux Kernel Image"
316           0x13C           LZMA compressed data, properties: 0x5D, dictionary size: 33554432 bytes, uncompressed size: 4816188 bytes
1867617       0x1C7F61        JFFS2 filesystem, little endian


Scan Time:     2024-06-13 14:07:21
Target File:   /home/nawaraj/Documents/ECE531-HW1/1.1.12a/_NC220_1.1.12_Build_160321_Rel.27531_upgrade.bin.extracted/13C
MD5 Checksum:  42e4a8277feaa022d258d0a1e2b522de
Signatures:    411

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
1573092       0x1800E4        MySQL ISAM index file Version 8
3309644       0x32804C        Linux kernel version 2.6.36
3309760       0x3280C0        CRC32 polynomial table, little endian
3579008       0x369C80        DES SP1, little endian
3579520       0x369E80        DES SP2, little endian
3593488       0x36D510        CRC32 polynomial table, little endian
3924972       0x3BE3EC        xz compressed data
3944580       0x3C3084        Unix path: /var/run/udhcpc.pid
4001279       0x3D0DFF        Neighborly text, "neighbor %.2x%.2x.%pM lostrouter"
4213721       0x404BD9        Intel x86 or x64 microcode, sig 0x0000003f, pf_mask 0x3000000, 1E00-04-04, rev 0x3000000, size 63
4415488       0x436000        LZMA compressed data, properties: 0x5D, dictionary size: 1048576 bytes, uncompressed size: 1475584 bytes


Scan Time:     2024-06-13 14:07:23
Target File:   /home/nawaraj/Documents/ECE531-HW1/1.1.12a/_NC220_1.1.12_Build_160321_Rel.27531_upgrade.bin.extracted/_13C.extracted/436000
MD5 Checksum:  de34db1e53708f9e05188b18c36b5c3c
Signatures:    411
```

Binwalk Command Output_ v1.1.12_160321_b



```
nawaraj@ubuntu1:~/Documents/ECE531-HW1$ binwalk -e -C 1.1.12a -M NC220_1.2.0_Build_170516_Rel.B4AC0D_2017-05-16_16.00.32.bin

Scan Time:     2024-06-13 14:11:19
Target File:   /home/nawaraj/Documents/ECE531-HW1/NC220_1.2.0_Build_170516_Rel.B4AC0D_2017-05-16_16.00.32.bin
MD5 Checksum:  110d5d246780f45103542b6d8ec88710
Signatures:    411

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
304           0x130           uImage header, header size: 64 bytes, header CRC: 0x85370656, created: 2017-05-16 07:53:21, image size: 1866250 bytes, Data Ad
dress: 0x80000000, Entry Point: 0x8000C310, data CRC: 0x217CBB7, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "Lin
ux Kernel Image"
368           0x170           LZMA compressed data, properties: 0x5D, dictionary size: 33554432 bytes, uncompressed size: 4814916 bytes
1866618       0x1C7B7A        JFFS2 filesystem, little endian


Scan Time:     2024-06-13 14:11:22
Target File:   /home/nawaraj/Documents/ECE531-HW1/1.1.12a/_NC220_1.2.0_Build_170516_Rel.B4AC0D_2017-05-16_16.00.32.bin.extracted/170
MD5 Checksum:  b5cce377fdbe50eb95a2a7d30d448a0e
Signatures:    411

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
1573092       0x1800E4        MySQL ISAM index file Version 8
3309648       0x328050        Linux kernel version 2.6.36
3309776       0x3280D0        CRC32 polynomial table, little endian
3579024       0x369C90        DES SP1, little endian
3579536       0x369E90        DES SP2, little endian
3593504       0x36D520        CRC32 polynomial table, little endian
3925004       0x3BE40C        xz compressed data
3944612       0x3C30A4        Unix path: /var/run/udhcpc.pid
4001311       0x3D0E1F        Neighborly text, "neighbor %.2x%.2x.%pM lostrouter"
4213721       0x404BD9        Intel x86 or x64 microcode, sig 0x0000003f, pf_mask 0x3000000, 1E00-04-04, rev 0x3000000, size 63
4415488       0x436000        LZMA compressed data, properties: 0x5D, dictionary size: 1048576 bytes, uncompressed size: 1468928 bytes


Scan Time:     2024-06-13 14:11:23
Target File:   /home/nawaraj/Documents/ECE531-HW1/1.1.12a/_NC220_1.2.0_Build_170516_Rel.B4AC0D_2017-05-16_16.00.32.bin.extracted/_170.extracted/436000
MD5 Checksum:  1dfa4cbfb4462855dabdc5d4a3e28557
Signatures:    411
```

Binwalk Command Output_v1.2.0_170516



```
nawaraj@ubuntu1:~/Documents/ECE531-HW1/1.1.12a/_NC220_1.1.12_Build_160321_Rel.27531.bin.extracted$ ls -l
total 25628
-rw-rw-r-- 1 nawaraj nawaraj 7774441 Jun 12 22:51 19E70.xz
-rw-rw-r-- 1 nawaraj nawaraj 5885908 Jun 12 22:51 1E6F85.jffs2
-rw-rw-r-- 1 nawaraj nawaraj 4816188 Jun 12 22:51 1F160
-rw-rw-r-- 1 nawaraj nawaraj 7753209 Jun 12 22:51 1F160.7z
drwxrwxr-x 3 nawaraj nawaraj    4096 Jun 12 22:52 _1F160.extracted
drwxrwxr-x 9 nawaraj nawaraj    4096 Jun 12 22:51 jffs2-root
nawaraj@ubuntu1:~/Documents/ECE531-HW1/1.1.12a/_NC220_1.1.12_Build_160321_Rel.27531.bin.extracted$
```

Files content

Analysis and Findings

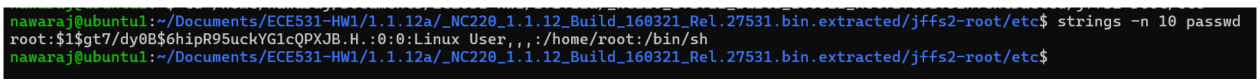
From the analysis, it was discovered that the firmware employed MIPS architecture and incorporated JFFS2 filesystem, appropriate for use in the flash drives of embedded systems. The most interesting components in the firmware identified in the paper are the U-Boot bootloader and the Linux kernel, which can be examined for new vulnerabilities.

By exploring the jffs2-root directory, various subdirectories were found, including bin/: Holds several command strings involved in the firmware, lib/, etc/, and www/: Holds libraries, password files, certificates, and web interface components besides the configuration files.

Looking at the contents of the directory /etc, there were password files; passwd and shadow. Plaintext passwords or weak password hashes may be present which could prove insecure.

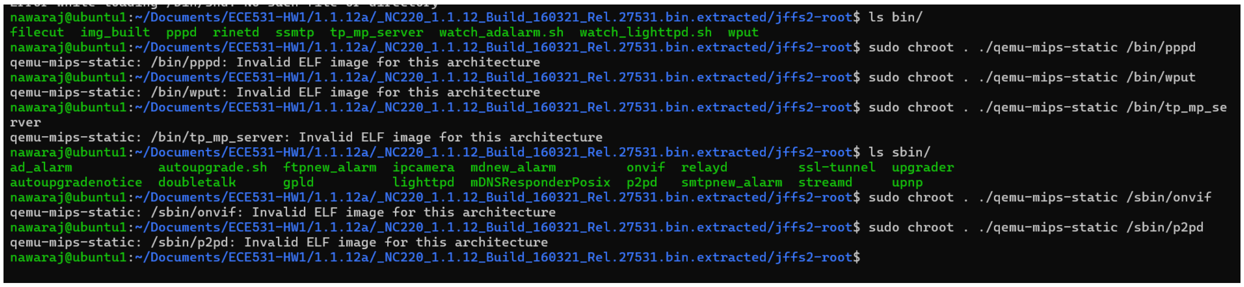
For the further analysis tools used are:

- qemu-mips-static
- binutils
- sudo chroot . ./qemu-mips-static COMMAND -option
- strings -n 10 ’filename’



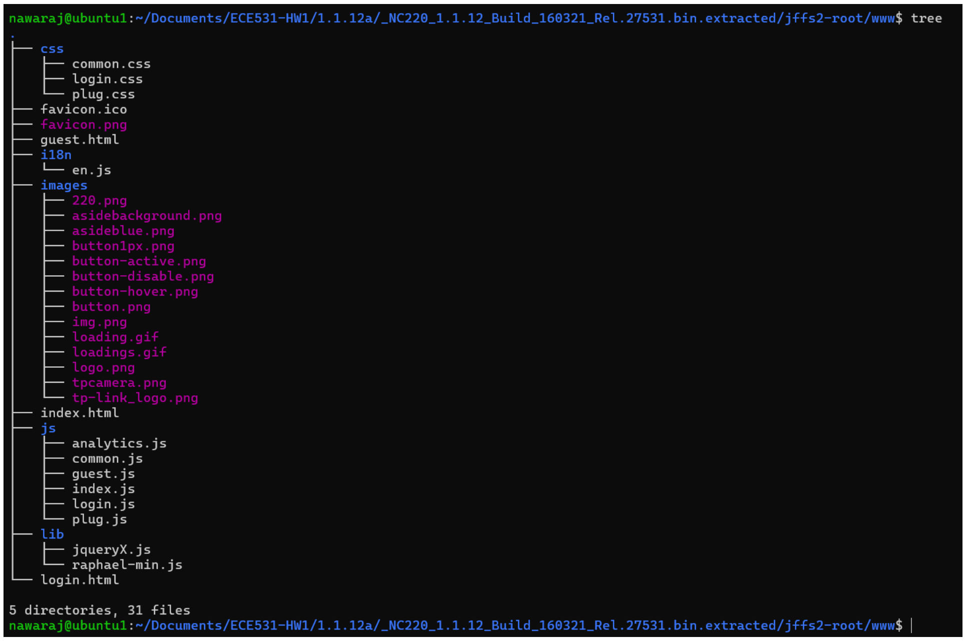
```
nawaraj@ubuntu1:~/Documents/ECE531-HW1/1.1.12a/_NC220_1.1.12_Build_160321_Rel.27531.bin.extracted/jffs2-root/etc$ strings -n 10 passwd
root:$1$gt7/dy0B$6hipR95uckYG1cQPXJB.H.:0:0:Linux User,,,:/home/root:/bin/sh
nawaraj@ubuntu1:~/Documents/ECE531-HW1/1.1.12a/_NC220_1.1.12_Build_160321_Rel.27531.bin.extracted/jffs2-root/etc$
```

Strings on passwd



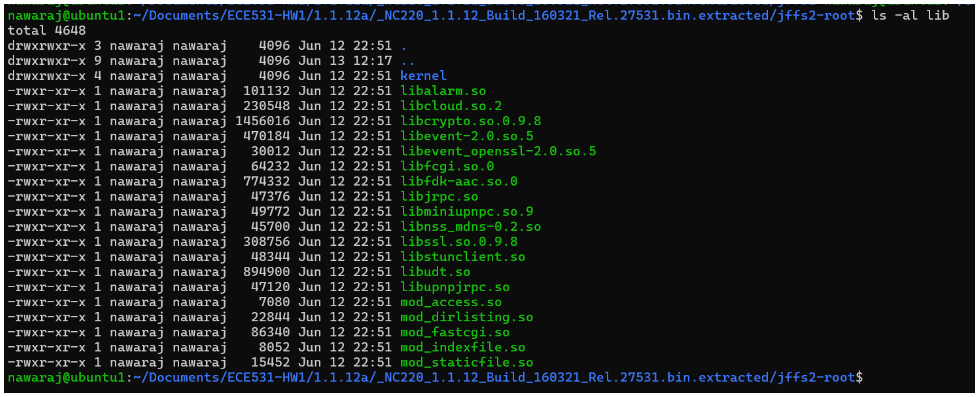
```
nawaraj@ubuntu1:~/Documents/ECE531-HW1/1.1.12a/_NC220_1.1.12_Build_160321_Rel.27531.bin.extracted/jffs2-root$ ls bin/
filecut  img_built  pppd  rinetd  ssmtp  tp_mp_server  watch_adalarm.sh  watch_lighttpd.sh  wput
nawaraj@ubuntu1:~/Documents/ECE531-HW1/1.1.12a/_NC220_1.1.12_Build_160321_Rel.27531.bin.extracted/jffs2-root$ sudo chroot . ./qemu-mips-static /bin/pppd
qemu-mips-static: /bin/pppd: Invalid ELF image for this architecture
nawaraj@ubuntu1:~/Documents/ECE531-HW1/1.1.12a/_NC220_1.1.12_Build_160321_Rel.27531.bin.extracted/jffs2-root$ sudo chroot . ./qemu-mips-static /bin/wput
qemu-mips-static: /bin/wput: Invalid ELF image for this architecture
nawaraj@ubuntu1:~/Documents/ECE531-HW1/1.1.12a/_NC220_1.1.12_Build_160321_Rel.27531.bin.extracted/jffs2-root$ sudo chroot . ./qemu-mips-static /bin/tp_mp_se
rver
qemu-mips-static: /bin/tp_mp_server: Invalid ELF image for this architecture
nawaraj@ubuntu1:~/Documents/ECE531-HW1/1.1.12a/_NC220_1.1.12_Build_160321_Rel.27531.bin.extracted/jffs2-root$ ls sbin/
ad_alarm           autoupgrade.sh  ftpnew_alarm  ipcamera  mdnew_alarm         onvif  relayd         ssl-tunnel  upgrader
autoupgradenotice  doubletalk      gpld          lighttpd  mDNSResponderPosix  p2pd   smtpnew_alarm  streamd     upnp
nawaraj@ubuntu1:~/Documents/ECE531-HW1/1.1.12a/_NC220_1.1.12_Build_160321_Rel.27531.bin.extracted/jffs2-root$ sudo chroot . ./qemu-mips-static /sbin/onvif
qemu-mips-static: /sbin/onvif: Invalid ELF image for this architecture
nawaraj@ubuntu1:~/Documents/ECE531-HW1/1.1.12a/_NC220_1.1.12_Build_160321_Rel.27531.bin.extracted/jffs2-root$ sudo chroot . ./qemu-mips-static /sbin/p2pd
qemu-mips-static: /sbin/p2pd: Invalid ELF image for this architecture
nawaraj@ubuntu1:~/Documents/ECE531-HW1/1.1.12a/_NC220_1.1.12_Build_160321_Rel.27531.bin.extracted/jffs2-root$
```

Qemu Commands



```
nawaraj@ubuntu1:~/Documents/ECE531-HW1/1.1.12a/_NC220_1.1.12_Build_160321_Rel.27531.bin.extracted/jffs2-root/www$ tree
.
├── css
│   ├── common.css
│   ├── login.css
│   └── plug.css
├── favicon.ico
├── favicon.png
├── guest.html
├── i18n
│   └── en.js
├── images
│   ├── 220.png
│   ├── asidebackground.png
│   ├── asideblue.png
│   ├── button1px.png
│   ├── button-active.png
│   ├── button-disable.png
│   ├── button-hover.png
│   ├── button.png
│   ├── img.png
│   ├── loading.gif
│   ├── loadings.gif
│   ├── logo.png
│   ├── tpcamera.png
│   └── tp-link_logo.png
├── index.html
├── js
│   ├── analytics.js
│   ├── common.js
│   ├── guest.js
│   ├── index.js
│   ├── login.js
│   └── plug.js
├── lib
│   ├── jqueryX.js
│   └── raphael-min.js
└── login.html

5 directories, 31 files
nawaraj@ubuntu1:~/Documents/ECE531-HW1/1.1.12a/_NC220_1.1.12_Build_160321_Rel.27531.bin.extracted/jffs2-root/www$ |
```

www directory contents



```
nawaraj@ubuntu1:~/Documents/ECE531-HW1/1.1.12a/_NC220_1.1.12_Build_160321_Rel.27531.bin.extracted/jffs2-root$ ls -al lib
total 4648
drwxrwxr-x 3 nawaraj nawaraj    4096 Jun 12 22:51 .
drwxrwxr-x 9 nawaraj nawaraj    4096 Jun 13 12:17 ..
drwxrwxr-x 4 nawaraj nawaraj    4096 Jun 12 22:51 kernel
-rwxr-xr-x 1 nawaraj nawaraj  101132 Jun 12 22:51 libalarm.so
-rwxr-xr-x 1 nawaraj nawaraj  230548 Jun 12 22:51 libcloud.so.2
-rwxr-xr-x 1 nawaraj nawaraj 1456016 Jun 12 22:51 libcrypto.so.0.9.8
-rwxr-xr-x 1 nawaraj nawaraj  470184 Jun 12 22:51 libevent-2.0.so.5
-rwxr-xr-x 1 nawaraj nawaraj   30012 Jun 12 22:51 libevent_openssl-2.0.so.5
-rwxr-xr-x 1 nawaraj nawaraj   64232 Jun 12 22:51 libfcgi.so.0
-rwxr-xr-x 1 nawaraj nawaraj  774332 Jun 12 22:51 libfdk-aac.so.0
-rwxr-xr-x 1 nawaraj nawaraj   47376 Jun 12 22:51 libjrpc.so
-rwxr-xr-x 1 nawaraj nawaraj   49772 Jun 12 22:51 libminiupnpc.so.9
-rwxr-xr-x 1 nawaraj nawaraj   45700 Jun 12 22:51 libnss_mdns-0.2.so
-rwxr-xr-x 1 nawaraj nawaraj  308756 Jun 12 22:51 libssl.so.0.9.8
-rwxr-xr-x 1 nawaraj nawaraj   48344 Jun 12 22:51 libstunclient.so
-rwxr-xr-x 1 nawaraj nawaraj  894900 Jun 12 22:51 libudt.so
-rwxr-xr-x 1 nawaraj nawaraj   47120 Jun 12 22:51 libupnpjrpc.so
-rwxr-xr-x 1 nawaraj nawaraj    7080 Jun 12 22:51 mod_access.so
-rwxr-xr-x 1 nawaraj nawaraj   22844 Jun 12 22:51 mod_dirlisting.so
-rwxr-xr-x 1 nawaraj nawaraj   86340 Jun 12 22:51 mod_fastcgi.so
-rwxr-xr-x 1 nawaraj nawaraj    8052 Jun 12 22:51 mod_indexfile.so
-rwxr-xr-x 1 nawaraj nawaraj   15452 Jun 12 22:51 mod_staticfile.so
nawaraj@ubuntu1:~/Documents/ECE531-HW1/1.1.12a/_NC220_1.1.12_Build_160321_Rel.27531.bin.extracted/jffs2-root$
```

list all files and directories

Conclusion

The firmware images of the NC220 offered a clear and detailed insight of the workings of the device. With the help of Binwalk, QEMU, and GNU Binutils, the firmware was successfully analyzed, and the main features and purpose of the firmware was revealed. It has been noticed that three NC220 binary files share the same filesystem configurations. They are all using the JFFS2 filesystem as their base. All three have the same Linux kernel version number.