COMP 5970: Firmware Homework

Alex Lewin

11/13/14

1 Define Each of the following extensions:

* **.img**: This is a disc image file, which contains image data for a system. This includes
* **.bin**: This is a firmware file for some models of routers.
* **.trx**: This is a firmware image file for some embedded systems and routers.

What is the difference between firmware extensions?:

At their core, firmware files hold basically the same information. The different file extensions just distinguish different organizational structures or header information.
What is the model number that correlates with each of the files?

- **.img**: R6950

```
root@kali:~/Firmware# binwalk R6950.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             uImage header, header size: 64 bytes, header CRC: 0xADA6C902, created: 2018-11-29 19:46
:01, image size: 207800 bytes, Data Address: 0xA0200000, Entry Point: 0xA0200000, data CRC: 0xD58A6B6F, OS: Linux, CP
U: MIPS, image type: Standalone Program, compression type: none, image name: "NAND Flash I"
170624        0x29A80         U-Boot version string, "U-Boot 1.1.3 (Nov 29 2018 - 14:45:51)"
982970        0xEFFBA         Sercomm firmware signature, version control: 256, download control: 0, hardware ID: "BZ
V", hardware version: 0x4100, firmware version: 0x42, starting code segment: 0x0, code size: 0x7300
2097152       0x200000        uImage header, header size: 64 bytes, header CRC: 0xA6A44421, created: 2019-01-21 08:12
:38, image size: 3351268 bytes, Data Address: 0x81001000, Entry Point: 0x8100D1D0, data CRC: 0xB743A7B0, OS: Linux, C
PU: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "Linux Kernel Image"
2097216       0x200040        LZMA compressed data, properties: 0x5D, dictionary size: 33554432 bytes, uncompressed s
ize: 8456576 bytes
5291456       0x600000        Squashfs filesystem, little endian, version 4.0, compression:xz, size: 28037611 bytes,
2406 inodes, blocksize: 131072 bytes, created: 2019-01-21 08:12:29
```

- **.bin**: dir300

```
root@kali:~/Firmware# binwalk dir300-firmware.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             TRX firmware header, little endian, image size: 3801116 bytes, CRC32: 0xF4D6C223, flags
: 0x1, version: 1, header size: 28 bytes, loader offset: 0x1C, linux kernel offset: 0x0, rootfs offset: 0x0
28            0x1C            LZMA compressed data, properties: 0x6D, dictionary size: 8388608 bytes, uncompressed si
ze: 2480040 bytes
851996        0xD001C         Squashfs filesystem, little endian, version 4.0, compression:xz, size: 2945894 bytes, 6
08 inodes, blocksize: 131072 bytes, created: 2019-08-06 03:16:06
```

- **.trx**: RT-N56U found in etc_ro/xml folder

```
root@kali:~/Firmware/trx_squashfs/etc_ro/xml# cat WFADeviceDesc.xml
<?xml version="1.0" encoding="utf-8"?>
<root xmlns="urn:schemas-upnp-org:device-1-0">
  <specVersion>
    <major>1</major>
    <minor>0</minor>
  </specVersion>
  <device>
    <deviceType>urn:schemas-wifialliance-org:device:WFADevice:1</deviceType>
    <friendlyName>ASUS Wireless Router</friendlyName>
    <manufacturer>ASUSTeK Computer Inc.</manufacturer>
    <manufacturerURL>http://www.asus.com</manufacturerURL>
    <modelDescription>ASUS Wireless WPS Router</modelDescription>
    <modelName>RT-N56U</modelName>
    <modelNumber>RT-N56U</modelNumber>
    <modelURL>http://www.asus.com</modelURL>
    <serialNumber>00000000</serialNumber>
    <UDN>uuid:Upnp-WSC-1_0-1234567890001</UDN>
    <serviceList>
      <service>
        <serviceType>urn:schemas-wifialliance-org:service:WFAWLANConfig:1</serviceType>
        <serviceId>urn:wifialliance-org:serviceId:WFAWLANConfig1</serviceId>
        <SCPDURL>WFAWLANConfigSCPD.xml</SCPDURL>
        <controlURL>control</controlURL>
        <eventSubURL>event</eventSubURL>
      </service>
    </serviceList>
  </device>
</root>
```

  # What file system is being used by the file system?

- **.img**: This uses a squash file system, found by using dd to pull out a zip file, then using binwalk after unzipping the file:

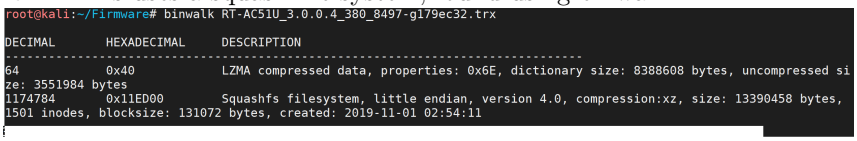
```
root@kali:~/Firmware# binwalk AC2100-V1.2.0.42_1.0.1.img

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Sercomm firmware signature, version control: 256, download control: 0, hardware ID: "BZ
V", hardware version: 0x4100, firmware version: 0x42, starting code segment: 0x0, code size: 0x7300
512           0x200           Zip archive data, at least v2.0 to extract, compressed size: 32712621, uncompressed siz
e: 83886080, name: R6950.bin
32713261      0x1F32A2D       End of Zip archive, footer length: 22
```

```
root@kali:~/Firmware# binwalk R6950.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             uImage header, header size: 64 bytes, header CRC: 0xADA6C902, created: 2018-11-29 19:46
:01, image size: 207800 bytes, Data Address: 0xA0200000, Entry Point: 0xA0200000, data CRC: 0xD58A6B6F, OS: Linux, CP
U: MIPS, image type: Standalone Program, compression type: none, image name: "NAND Flash I"
170624        0x29A80         U-Boot version string, "U-Boot 1.1.3 (Nov 29 2018 - 14:45:51)"
982970        0xEFFBA         Sercomm firmware signature, version control: 256, download control: 0, hardware ID: "BZ
V", hardware version: 0x4100, firmware version: 0x42, starting code segment: 0x0, code size: 0x7300
2097152       0x200000        uImage header, header size: 64 bytes, header CRC: 0xA6A44421, created: 2019-01-21 08:12
:38, image size: 3351268 bytes, Data Address: 0x81001000, Entry Point: 0x8100D1D0, data CRC: 0xB743A7B0, OS: Linux, C
PU: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "Linux Kernel Image"
2097216       0x200040        LZMA compressed data, properties: 0x5D, dictionary size: 33554432 bytes, uncompressed s
ize: 8456576 bytes
5291456       0x600000        Squashfs filesystem, little endian, version 4.0, compression:xz, size: 28037611 bytes,
2406 inodes, blocksize: 131072 bytes, created: 2019-01-21 08:12:29
```

- **.bin**: This uses a squash file system, found using binwalk:

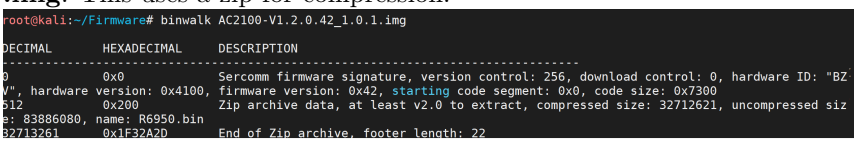
```
root@kali:~/Firmware# binwalk dir300-firmware.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             TRX firmware header, little endian, image size: 3801116 bytes, CRC32: 0xF4D6C223, flags
: 0x1, version: 1, header size: 28 bytes, loader offset: 0x1C, linux kernel offset: 0x0, rootfs offset: 0x0
28            0x1C            LZMA compressed data, properties: 0x6D, dictionary size: 8388608 bytes, uncompressed si
ze: 2480040 bytes
851996        0xD001C         Squashfs filesystem, little endian, version 4.0, compression:xz, size: 2945894 bytes, 6
98 inodes, blocksize: 131072 bytes, created: 2019-08-06 03:16:06
```

- **.trx**: This uses a squash file system, found using binwalk:



  # What compression scheme is being used by the firmware?

- **.img**: This uses a zip for compression:



- **.bin**: This uses a zip for compression:

```
root@kali:~/Firmware# binwalk AC2100-V1.2.0.42_1.0.1.img

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Sercomm firmware signature, version control: 256, download control: 0, hardware ID: "BZ
V", hardware version: 0x4100, firmware version: 0x42, starting code segment: 0x0, code size: 0x7300
512           0x200           Zip archive data, at least v2.0 to extract, compressed size: 32712621, uncompressed siz
e: 83886080, name: R6950.bin
32713261      0x1F32A2D       End of Zip archive, footer length: 22
```

- **.trx**: This uses LZMA for compression:

```
root@kali:~/Firmware# binwalk RT-AC51U_3.0.0.4_380_8497-g179ec32.trx

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
64            0x40            LZMA compressed data, properties: 0x6E, dictionary size: 8388608 bytes, uncompressed si
ze: 3551984 bytes
1174784       0x11ED00        Squashfs filesystem, little endian, version 4.0, compression:xz, size: 13390458 bytes,
1501 inodes, blocksize: 131072 bytes, created: 2019-11-01 02:54:11
```

What information in a file system can be used during a penetration test?

From the file system, attackers can gather a litany of information including firewall information, hashed passwords, private keys, and network configurations.

When looking through the bin's squash file system, I came across the etc configurations directory that contains some useful information:

```
root@kali:~/Firmware/bin_squash/etc/config# ls
1sputnik.webhotspot       http-redirect.webhotspot          pptpd_client.options        schedulerb.webalive
3hotss.webhotspot         language.nvramconfig              pptpd_client.sh             smtp-redirect.firewall
5wifidog.webhotspot       language.startup                  pptpd_client.startup        smtp-redirect.nvramconfig
base.nvramconfig          language.webconfig                pptpd_client.vpn            smtp-redirect.webhotspot
base.webconfig            networksettings.brcm.nvramconfig  proxywatchdog.nvramconfig   sputnik.nvramconfig
chillispot.nvramconfig    networksettings.brcm.webconfig    proxywatchdog.sh            sshd.webservices
chillispot.webhotspot     nocat.nvramconfig                 proxywatchdog.startup       syslog.webservices
dhcpd.startup             nocat.startup                     proxywatchdog.webalive      telnet.webservices
dhcpd.webservices         nocat.webhotspot                  radiooff.nvramconfig        ttraff.nvramconfig
eop-tunnel.firewall       notifier.nvramconfig              radiooff.webservices        ttraff.webservices
eop-tunnel.prewall        notifier.websecurity              routerstyle.nvramconfig     wdswatchdog.nvramconfig
fon.nvramconfig           olsrd.nvramconfig                 routerstyle.webconfig       wdswatchdog.sh
fon.webhotspot            overclocking.webconfig            routerstyle.webconfig.orig  wdswatchdog.startup
hotss.nvramconfig         pptpd_client.ip-down              schedulerb.nvramconfig      wdswatchdog.webalive
http-redirect.firewall    pptpd_client.ip-up                schedulerb.sh               wifidog.nvramconfig
http-redirect.nvramconfig pptpd_client.nvramconfig          schedulerb.startup
```

I also found a private key:

```
root@kali:~/Firmware/bin_squash/etc# cat key.pem
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA2G52fNEtkKlRFXhaYJD5inLmTuJiqrqFnW5Fj1j6XgGz1DIV
42J2VgmvvQfL16nBRqXOt8b5IwEsFE9+If7KoKu1D73N7ek9OFSV78z2wznrVlGD
kszIxDjSbjb/IuOLh5Ic+g/ws/P15eHevWEOjb8n5Mq0h5SsazzX7ALsJAfbTE9v
RkR8J59OoUsiDgf1FSpgibNcbhUCmj5Qlat6PlkWzEBIqLHi2ZSqhrcgYb+DGdI0
gjVnI3bUl5dTQYUinOlMNeaXABkGndZwiSceloyEcRCIl2w9HcDTUgFur8AE2Nfa
h16Yps5Yf2E40TZURIiufkd/6YzIpN/XmHuZ9QIDAQABAoIBADisTDiI6b6Mp5/Q
oRHSRJW9WpNjcmS0bNJ5kptjuEOvfHBfIR4mpUgIR01fYkA5wlOGjWfQIWLKJsm2
uxeZyWNjMwlJMUhQH+jFNXHSoPckDnzO4X4qQ5QmMOwNWKfBH8NDPnU4gVYN1uD4
UUQTy6riWEbv0XADPVbjWsMBTOZt8Pcxh1cqGxE6SBZtacp+mBDq5TwsKq4RE8ur
bJnB7xSHvJAyoiOn5AefFCz04zJk1gWb8AEb9T/SbwXordsXpzLCXiW17g7FvqUS
CHmqeJJ38irg4PmvxizW5Kc9g9+OMLo1isnTlqKoah9X0n8OIPv6rLGV7IU/S/1d
85XAvU0CgYEA7Gsm3vFtqRAPHJHWiUPu8k/B+Nsg+9YVmi3jAnqumrcIw00cXvEf
lkFF7OhhV0ccQTByRynbPZ3GEmb3St8IEMiJqNZFyDC77O6/ZUTs71CD2O6h3PA7
QegGWYDqPlVYrxL5LzNRVKsJxgfhzdllmEURfU/KDNm5cWni+h3o+38CgYEA6luF
C2uvqZ3FbnsT/NAeX25oxpJIOXJVoiSdama7Ke4sSLKDbMsRedjefTvdCmirwReL
jUKxRnr/0uhLXUEJK8AMU8HnXw1dKy9bGskGKiOlGcwrRnV9ZBnU4zE7THTKtiY0
CtrTg0o0HSioyV4623FG0cPdeNy4g/VPC++69IsCgYEAoYHV7Snbc0pgOHE8sUsy
WmC4L2xrTP+EhG5ijZgH3fO6TclI32cz3+65eU2K6hfPKo2RFCJ4/s/gt0OWHpTc
qrKEsE2pIEiCqSq0n9cFUbucRr9G3mtS4ARFCjHyVM/WJMv+ZQtWvVOW+qz5yimA
qRRODWBLtJmsgNkIUTvLpLsCgYA38iMfp9RmfGhuSGlsF864X2YZyT/+nsG8lFsT
1HRnvRjLPfpL1WpVmST75neNDZG65cEFtt8VATXjBls/ZtAmppEKyaZPNaSBM6vf
CBA1rQ6zyt6l0lRduiDtH4qVZOgjdZlE4hpOJD+umk84ywrn6fHLD6PmP2K49a2q
Hs+VowKBgQDowNXAPTop1Y4QRDluHCfbWPSs2lXg05SKna+kqnARave4rRwAj2QP
9FRNLJhpWXZXIn8Z8ZsxJQ9nxwhOdKwSkuYpkov4uGy2TiUkuZ4uZyuI1wEYwaa5
N5MqjqzzMj/eAKX2uqTi0IzS88S8GhLrFrdTg+7EajHoRyomsv/f4A==
-----END RSA PRIVATE KEY-----
```