Mission Name

ReconCar

Background

Claire and Ethan are inside a cave trying to search the Recon CAR for the bug left by Dr. Pinche.

Technical High-Level Overview

A Raspberry pi forensic image is provided to the player. The goal of this challenge is to identify which bug was left by Dr.Pinche inside the Reconcar. In this scenario player will be investigating filesystem to locate any clue to a backdoor. Finally, considering filesystem dates and forensic artifacts related to persistence, the challenge could be solved.

Short Description

You´re going to analyse ReconCar system. This time ReconCar has a Raspberry Pi connected to infotainment system. Your goal will be to locate the IP address which involves Dr.Pinche´s malicious activity.

Mission Description

The goal of this challenge is to identify which bug was left by Dr.Pinche inside the Reconcar. In this scenario you will be investigating a filesystem to locate any clue to a backdoor or other method which involves Dr.Pinche´s malicious activity. Your goal will be to locate the IP address which which leads that Dr.Pinche tampered ReconCar.

Location

RECON CAR - AIR / ALTAI MOUNTAINS

Tools

- Imount
- floss

Questions

Which port was used by Dr.Pinche to access ReconCar?

- 22

Which command was used to hide their steps in terms of time?

- Touch

Which is the real date (year) of the backdoor left by Dr.Pinche?

- 2021

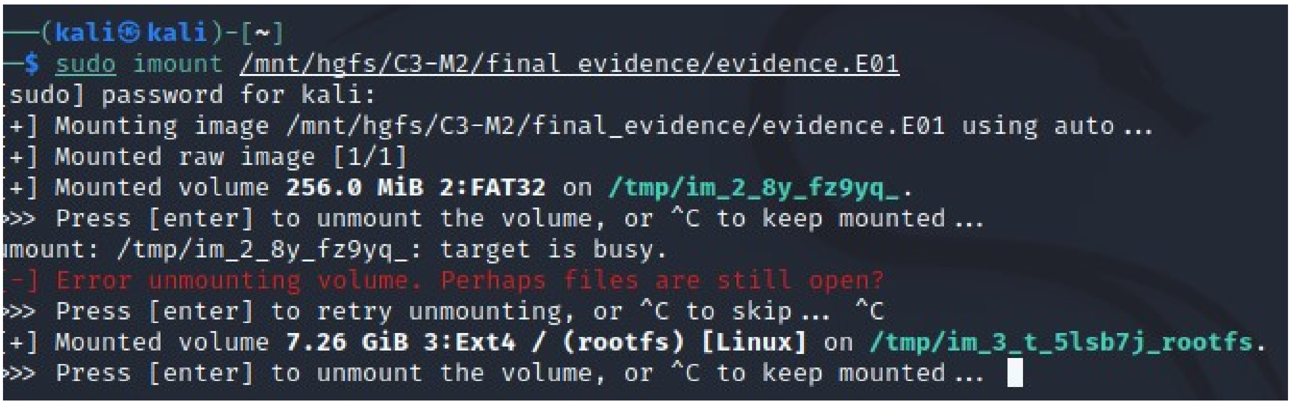
Hints

1. Use imount to mount the evidence
2. Identify all persistence Linux artifacts, including binaries with root privileges.
3. Identify binaries with timestamps tampered and analyse them to get ip addresses.

Write Up

First of all player must mount encase evidence provided.

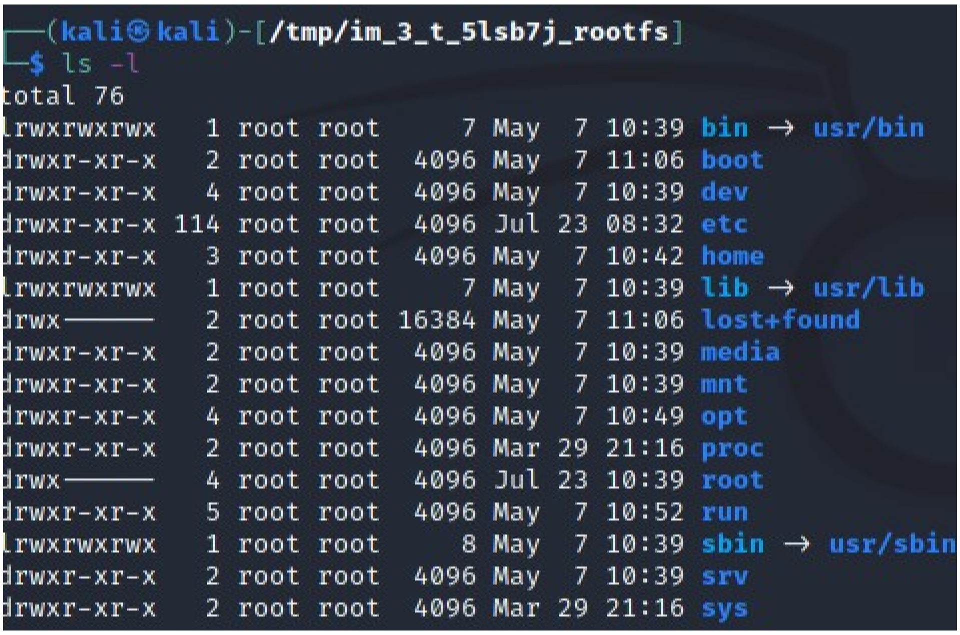
sudo apt-get install python-setuptools
sudo apt-get install xmount
sudo apt-get install ewf-tools
sudo apt-get install afflib-tools
sudo apt-get install sleuthkit
sudo apt-get install lvm2
sudo apt-get install mdadm
sudo apt-get install cryptsetup
sudo pip3 install imagemounter
sudo imount /evidence.E01



```
──(kali㉿kali)-[~]
─$ sudo imount /mnt/hgfs/C3-M2/final_evidence/evidence.E01
[sudo] password for kali:
[+] Mounting image /mnt/hgfs/C3-M2/final_evidence/evidence.E01 using auto...
[+] Mounted raw image [1/1]
[+] Mounted volume 256.0 MiB 2:FAT32 on /tmp/im_2_8y_fz9yq_.
>>> Press [enter] to unmount the volume, or ^C to keep mounted...
umount: /tmp/im_2_8y_fz9yq_: target is busy.
[-] Error unmounting volume. Perhaps files are still open?
>>> Press [enter] to retry unmounting, or ^C to skip...  ^C
[+] Mounted volume 7.26 GiB 3:Ext4 / (rootfs) [Linux] on /tmp/im_3_t_5lsb7j_rootfs.
>>> Press [enter] to unmount the volume, or ^C to keep mounted...
```

Figure 1

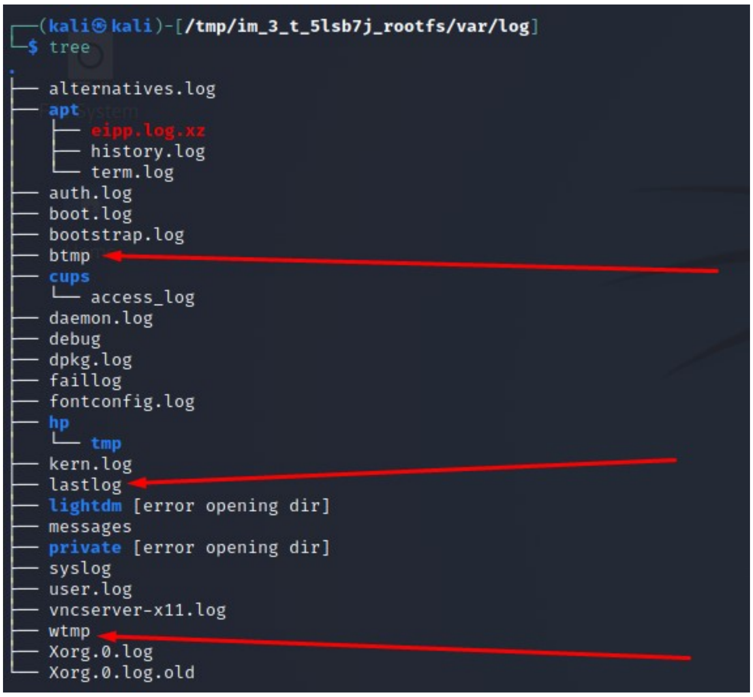
Once evidence is mounted, don´t close the window, leave it and move to other shell prompt. **Access to the file system on /tmp/xxxxx_rootFS**



```
┌──(kali㉿kali)-[/tmp/im_3_t_5lsb7j_rootfs]
└─$ ls -l
total 76
lrwxrwxrwx   1 root root     7 May  7 10:39 bin → usr/bin
drwxr-xr-x   2 root root  4096 May  7 11:06 boot
drwxr-xr-x   4 root root  4096 May  7 10:39 dev
drwxr-xr-x 114 root root  4096 Jul 23 08:32 etc
drwxr-xr-x   3 root root  4096 May  7 10:42 home
lrwxrwxrwx   1 root root     7 May  7 10:39 lib → usr/lib
drwx──────   2 root root 16384 May  7 11:06 lost+found
drwxr-xr-x   2 root root  4096 May  7 10:39 media
drwxr-xr-x   2 root root  4096 May  7 10:39 mnt
drwxr-xr-x   4 root root  4096 May  7 10:49 opt
drwxr-xr-x   2 root root  4096 Mar 29 21:16 proc
drwx──────   4 root root  4096 Jul 23 10:39 root
drwxr-xr-x   5 root root  4096 May  7 10:52 run
lrwxrwxrwx   1 root root     8 May  7 10:39 sbin → usr/sbin
drwxr-xr-x   2 root root  4096 May  7 10:39 srv
drwxr-xr-x   2 root root  4096 Mar 29 21:16 sys
```

Figure 2

The following logs were cleaned:

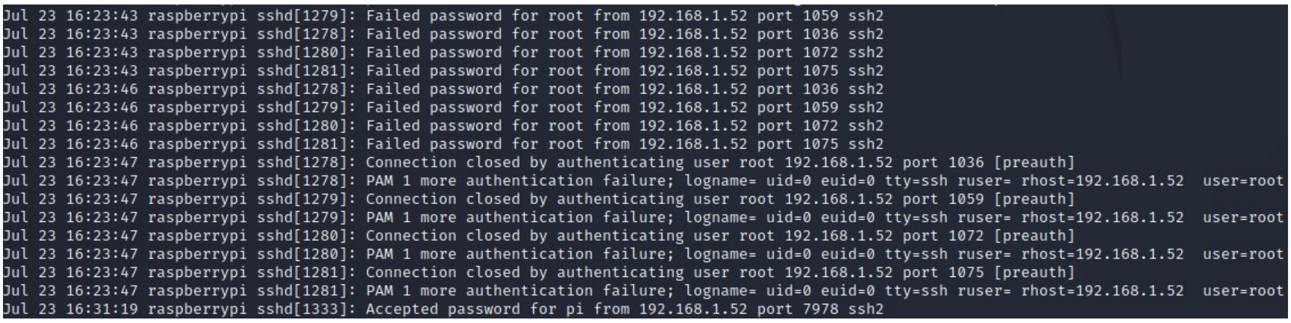


```
┌──(kali㉿kali)-[/tmp/im_3_t_5lsb7j_rootfs/var/log]
└─$ tree
.
├── alternatives.log
├── apt
│   ├── eipp.log.xz
│   ├── history.log
│   └── term.log
├── auth.log
├── boot.log
├── bootstrap.log
├── btmp
├── cups
│   └── access_log
├── daemon.log
├── debug
├── dpkg.log
├── faillog
├── fontconfig.log
├── hp
│   └── tmp
├── kern.log
├── lastlog
├── lightdm [error opening dir]
├── messages
├── private [error opening dir]
├── syslog
├── user.log
├── vncserver-x11.log
├── wtmp
├── Xorg.0.log
└── Xorg.0.log.old
```

Figure 3

At least, auth.log and messages are fully completed.

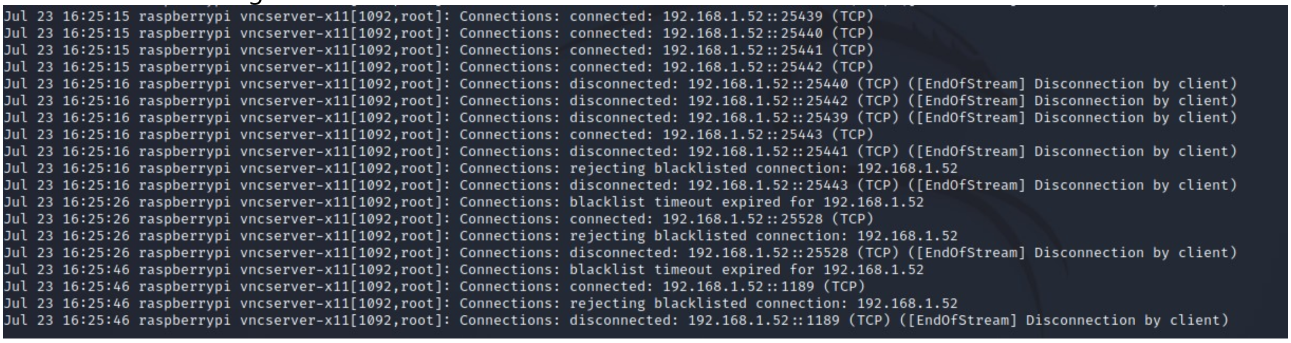
- tail auth.log



```
Jul 23 16:23:43 raspberrypi sshd[1279]: Failed password for root from 192.168.1.52 port 1059 ssh2
Jul 23 16:23:43 raspberrypi sshd[1278]: Failed password for root from 192.168.1.52 port 1036 ssh2
Jul 23 16:23:43 raspberrypi sshd[1280]: Failed password for root from 192.168.1.52 port 1072 ssh2
Jul 23 16:23:43 raspberrypi sshd[1281]: Failed password for root from 192.168.1.52 port 1075 ssh2
Jul 23 16:23:46 raspberrypi sshd[1278]: Failed password for root from 192.168.1.52 port 1036 ssh2
Jul 23 16:23:46 raspberrypi sshd[1279]: Failed password for root from 192.168.1.52 port 1059 ssh2
Jul 23 16:23:46 raspberrypi sshd[1280]: Failed password for root from 192.168.1.52 port 1072 ssh2
Jul 23 16:23:46 raspberrypi sshd[1281]: Failed password for root from 192.168.1.52 port 1075 ssh2
Jul 23 16:23:47 raspberrypi sshd[1278]: Connection closed by authenticating user root 192.168.1.52 port 1036 [preauth]
Jul 23 16:23:47 raspberrypi sshd[1278]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.52  user=root
Jul 23 16:23:47 raspberrypi sshd[1279]: Connection closed by authenticating user root 192.168.1.52 port 1059 [preauth]
Jul 23 16:23:47 raspberrypi sshd[1279]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.52  user=root
Jul 23 16:23:47 raspberrypi sshd[1280]: Connection closed by authenticating user root 192.168.1.52 port 1072 [preauth]
Jul 23 16:23:47 raspberrypi sshd[1280]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.52  user=root
Jul 23 16:23:47 raspberrypi sshd[1281]: Connection closed by authenticating user root 192.168.1.52 port 1075 [preauth]
Jul 23 16:23:47 raspberrypi sshd[1281]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.52  user=root
Jul 23 16:31:19 raspberrypi sshd[1333]: Accepted password for pi from 192.168.1.52 port 7978 ssh2
```

Figure 4

- tail messages



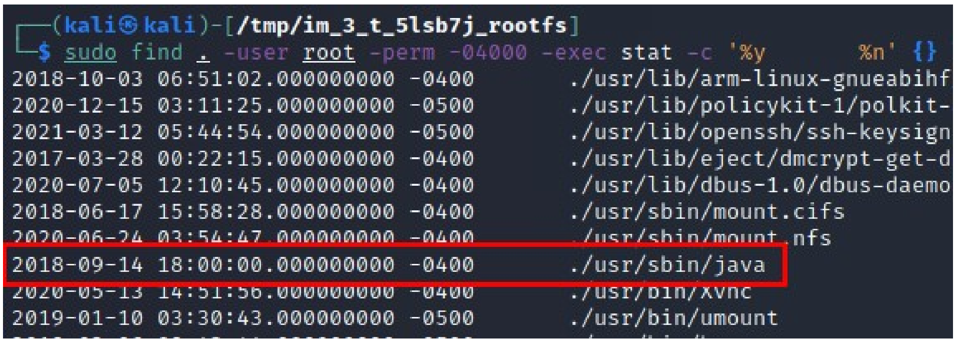
```
Jul 23 16:25:15 raspberrypi vncserver-x11[1092,root]: Connections: connected: 192.168.1.52::25439 (TCP)
Jul 23 16:25:15 raspberrypi vncserver-x11[1092,root]: Connections: connected: 192.168.1.52::25440 (TCP)
Jul 23 16:25:15 raspberrypi vncserver-x11[1092,root]: Connections: connected: 192.168.1.52::25441 (TCP)
Jul 23 16:25:15 raspberrypi vncserver-x11[1092,root]: Connections: connected: 192.168.1.52::25442 (TCP)
Jul 23 16:25:16 raspberrypi vncserver-x11[1092,root]: Connections: disconnected: 192.168.1.52::25440 (TCP) ([EndOfStream] Disconnection by client)
Jul 23 16:25:16 raspberrypi vncserver-x11[1092,root]: Connections: disconnected: 192.168.1.52::25442 (TCP) ([EndOfStream] Disconnection by client)
Jul 23 16:25:16 raspberrypi vncserver-x11[1092,root]: Connections: disconnected: 192.168.1.52::25439 (TCP) ([EndOfStream] Disconnection by client)
Jul 23 16:25:16 raspberrypi vncserver-x11[1092,root]: Connections: connected: 192.168.1.52::25443 (TCP)
Jul 23 16:25:16 raspberrypi vncserver-x11[1092,root]: Connections: disconnected: 192.168.1.52::25441 (TCP) ([EndOfStream] Disconnection by client)
Jul 23 16:25:16 raspberrypi vncserver-x11[1092,root]: Connections: rejecting blacklisted connection: 192.168.1.52
Jul 23 16:25:16 raspberrypi vncserver-x11[1092,root]: Connections: disconnected: 192.168.1.52::25443 (TCP) ([EndOfStream] Disconnection by client)
Jul 23 16:25:26 raspberrypi vncserver-x11[1092,root]: Connections: blacklist timeout expired for 192.168.1.52
Jul 23 16:25:26 raspberrypi vncserver-x11[1092,root]: Connections: connected: 192.168.1.52::25528 (TCP)
Jul 23 16:25:26 raspberrypi vncserver-x11[1092,root]: Connections: rejecting blacklisted connection: 192.168.1.52
Jul 23 16:25:26 raspberrypi vncserver-x11[1092,root]: Connections: disconnected: 192.168.1.52::25528 (TCP) ([EndOfStream] Disconnection by client)
Jul 23 16:25:46 raspberrypi vncserver-x11[1092,root]: Connections: blacklist timeout expired for 192.168.1.52
Jul 23 16:25:46 raspberrypi vncserver-x11[1092,root]: Connections: connected: 192.168.1.52::1189 (TCP)
Jul 23 16:25:46 raspberrypi vncserver-x11[1092,root]: Connections: rejecting blacklisted connection: 192.168.1.52
Jul 23 16:25:46 raspberrypi vncserver-x11[1092,root]: Connections: disconnected: 192.168.1.52::1189 (TCP) ([EndOfStream] Disconnection by client)
```

Figure 5

Above images show that one ip addres on July 23th were trying to access an finally they accessed. This evidence was tampered to hide the real timestamp of the files. So player must to put into practique their knowledge about backdoors. To find out where the bug is deployed by Dr.Pinche, would be necessary to launch the following command, based on root rights.

Timstamps based on last modification and setuid =1

- sudo find . -user root -perm -04000 -exec stat -c '%y   %n' {} \;

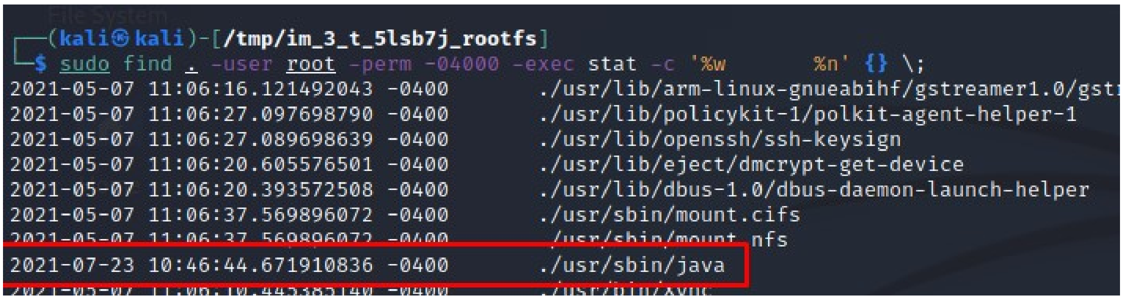


```
┌──(kali㉿kali)-[/tmp/im_3_t_5lsb7j_rootfs]
└─$ sudo find . -user root -perm -04000 -exec stat -c '%y        %n' {}
2018-10-03 06:51:02.000000000 -0400        ./usr/lib/arm-linux-gnueabihf
2020-12-15 03:11:25.000000000 -0500        ./usr/lib/policykit-1/polkit-
2021-03-12 05:44:54.000000000 -0500        ./usr/lib/openssh/ssh-keysign
2017-03-28 00:22:15.000000000 -0400        ./usr/lib/eject/dmcrypt-get-d
2020-07-05 12:10:45.000000000 -0400        ./usr/lib/dbus-1.0/dbus-daemo
2018-06-17 15:58:28.000000000 -0400        ./usr/sbin/mount.cifs
2020-06-24 03:54:47.000000000 -0400        ./usr/sbin/mount.nfs
2018-09-14 18:00:00.000000000 -0400        ./usr/sbin/java
2020-05-13 14:51:56.000000000 -0400        ./usr/bin/Xvnc
2019-01-10 03:30:43.000000000 -0500        ./usr/bin/umount
```

Figure 6

Timstamps based on birthday and setuid =1

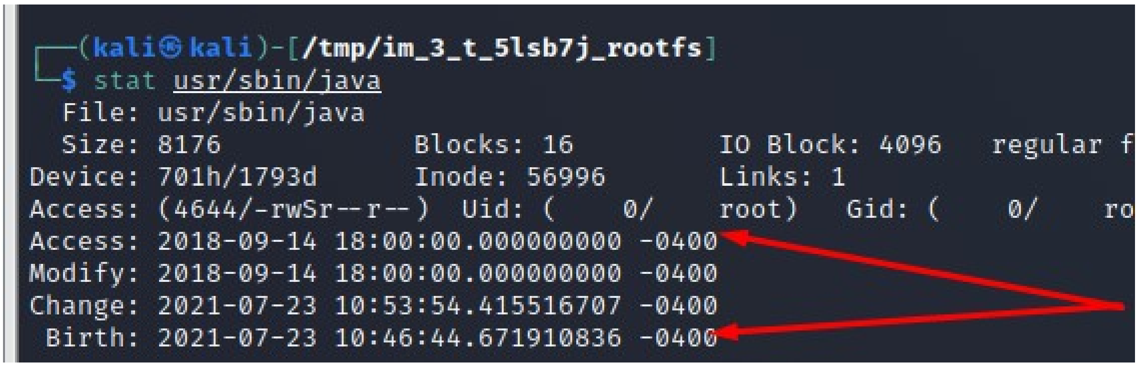
- sudo find . -user root -perm -04000 -exec stat -c '%w   %n' {} \;



```
┌──(kali㉿kali)-[/tmp/im_3_t_5lsb7j_rootfs]
└─$ sudo find . -user root -perm -04000 -exec stat -c '%w      %n' {} \;
2021-05-07 11:06:16.121492043 -0400      ./usr/lib/arm-linux-gnueabihf/gstr
2021-05-07 11:06:27.097698790 -0400      ./usr/lib/policykit-1/polkit-agent-helper-1
2021-05-07 11:06:27.089698639 -0400      ./usr/lib/openssh/ssh-keysign
2021-05-07 11:06:20.605576501 -0400      ./usr/lib/eject/dmcrypt-get-device
2021-05-07 11:06:20.393572508 -0400      ./usr/lib/dbus-1.0/dbus-daemon-launch-helper
2021-05-07 11:06:37.569896072 -0400      ./usr/sbin/mount.cifs
2021-05-07 11:06:37.569896072 -0400      ./usr/sbin/mount.nfs
2021-07-23 10:46:44.671910836 -0400      ./usr/sbin/java
```

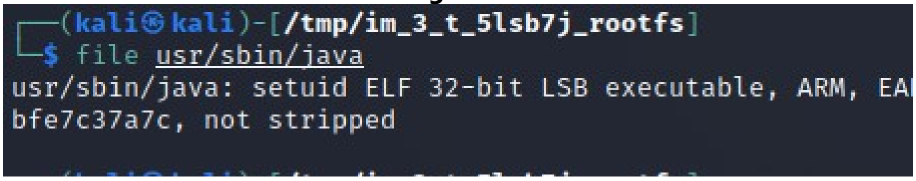
Figure 7

Dr.Piche tampered timestamps on /usr/bin/java



```
┌──(kali㉿kali)-[/tmp/im_3_t_5lsb7j_rootfs]
└─$ stat usr/sbin/java
  File: usr/sbin/java
  Size: 8176            Blocks: 16         IO Block: 4096   regular f
Device: 701h/1793d      Inode: 56996       Links: 1
Access: (4644/-rwSr--r--)  Uid: (    0/    root)   Gid: (    0/    ro
Access: 2018-09-14 18:00:00.000000000 -0400
Modify: 2018-09-14 18:00:00.000000000 -0400
Change: 2021-07-23 10:53:54.415516707 -0400
 Birth: 2021-07-23 10:46:44.671910836 -0400
```

Figure 8



```
┌──(kali㉿kali)-[/tmp/im_3_t_5lsb7j_rootfs]
└─$ file usr/sbin/java
usr/sbin/java: setuid ELF 32-bit LSB executable, ARM, EA
bfe7c37a7c, not stripped
```

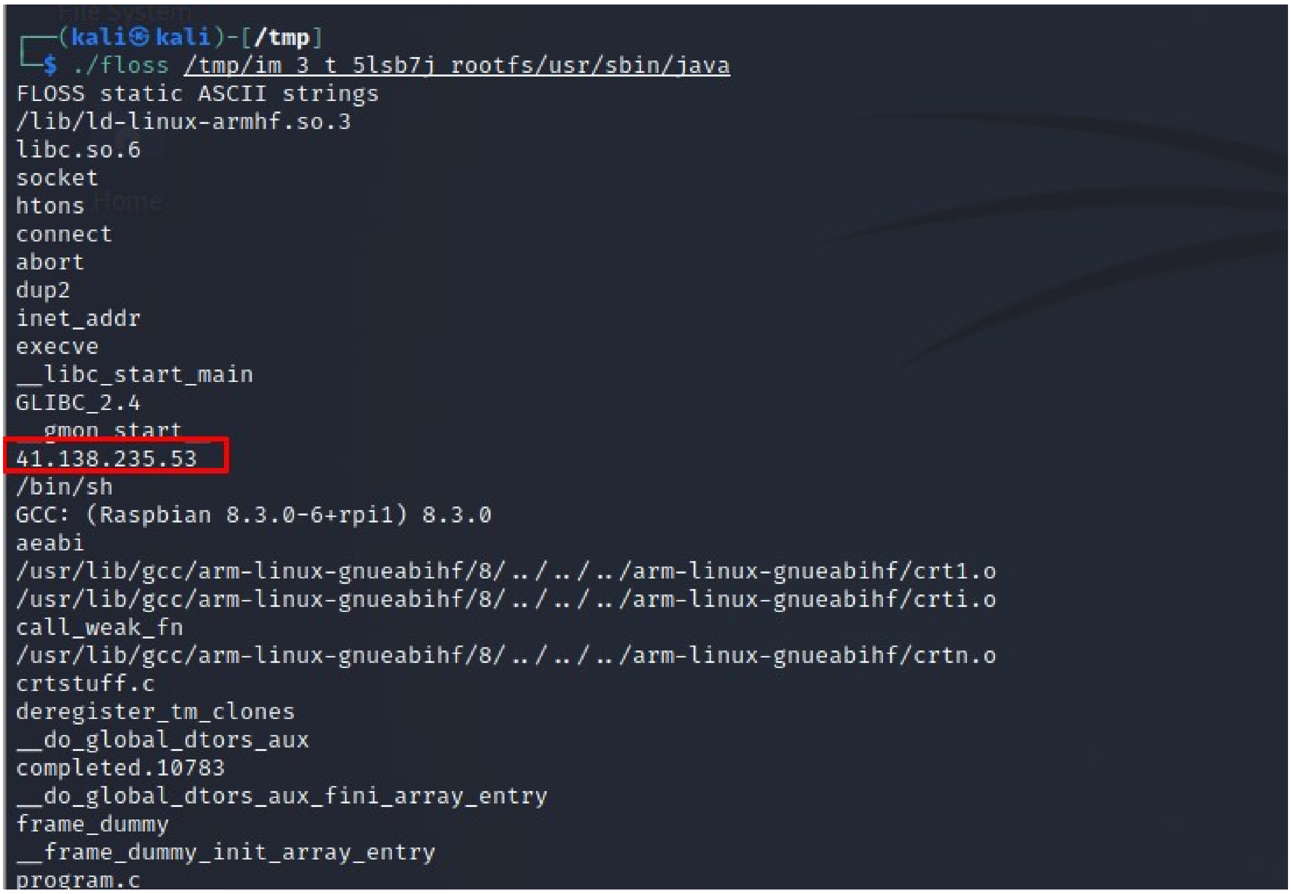
Figure 9

Finally player could reverse the binary or launching floss tool to discover Dr.Pinche´s ip address.

- wget https://github.com/fireeye/flare-floss/releases/download/v1.7.0/floss-v1.7.0-linux.zip

- unzip floss-v1.7.0-linux.zip

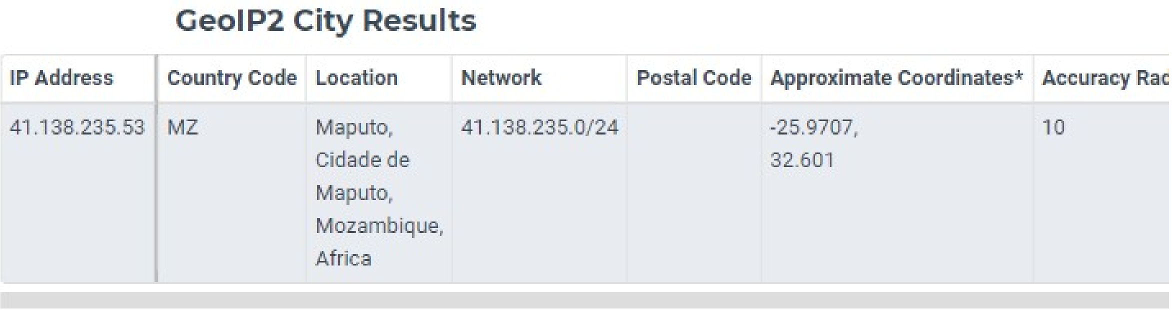
- ./floss /tmp/im_3_t_5lsb7j_rootfs/usr/sbin/java



```
┌──(kali㉿kali)-[/tmp]
└─$ ./floss /tmp/im_3_t_5lsb7j_rootfs/usr/sbin/java
FLOSS static ASCII strings
/lib/ld-linux-armhf.so.3
libc.so.6
socket
htons
connect
abort
dup2
inet_addr
execve
__libc_start_main
GLIBC_2.4
__gmon_start__
41.138.235.53
/bin/sh
GCC: (Raspbian 8.3.0-6+rpi1) 8.3.0
aeabi
/usr/lib/gcc/arm-linux-gnueabihf/8/../../../arm-linux-gnueabihf/crt1.o
/usr/lib/gcc/arm-linux-gnueabihf/8/../../../arm-linux-gnueabihf/crti.o
call_weak_fn
/usr/lib/gcc/arm-linux-gnueabihf/8/../../../arm-linux-gnueabihf/crtn.o
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.10783
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
program.c
```

Figure 10

The IP address has been located, the final clue will be to locate in the world to check if it´s in MAPUTO:



GeoIP2 City Results

IP Address	Country Code	Location	Network	Postal Code	Approximate Coordinates*	Accuracy Rad
41.138.235.53	MZ	Maputo, Cidade de Maputo, Mozambique, Africa	41.138.235.0/24		-25.9707, 32.601	10

Figure 11

Flag Information

flag{41.138.235.53}