Mission Name

ReconCar

History Context

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 Smart Fridge 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 or other method to intercept traffic. Finally, considering filesystem dates, player must see one file modified resolv.conf

Short Description

You´re going to analyse ReconCar system partition. Your goal is to locate Dr.Pinche´s IP address to send information from ReconCar to its command a control server in Maputo.

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 to intercept traffic. Your goal is to locate Dr.Pinche´s IP address to send information from ReconCar to its command a control server in Maputo.

Location

- RECON CAR - AIR / ALTAI MOUNTAINS

Tools

- Access Data FTK Imager

Questions

Which is the Ethan´s Bluetooth MAC Address?

- 48:4B:AA:AB:B8:7B

ReconCar has a WiFi Access Point, could you identify the last IP Address provided by the DHCP server?

- 192.168.7.61

Which is the ReconCar MAC Address?

- 71:2c:1f:41:e2:42

Hints

1. Use Access Data FTK Imager to mount the evidence.
2. Identify stranger dates, specially modified dates.
3. Analyse resolv.conf located at /etc/ folder

Write Up

Linux Method

1. mount -o loop /home/challenges/12_ReconCar.dd /home/tools/rawimages
2. cat /home/tools/rawimages/etc/resolv.conf

```
┌──(recon㉿kali)-[/home/tools/rawimage/etc]
└─$ cat resolv.conf
# Generated by Connection Manager
server 197.235.132.11
```

Figure 1

Windows Methods

First of all player must mount ReconCar system partition using Access Data FTK Imager, as usual, it´s neccesary to select the evidence provided "Adding image

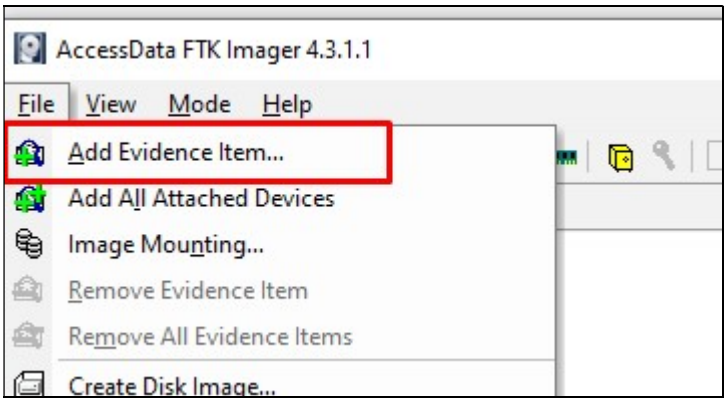


Figure 2

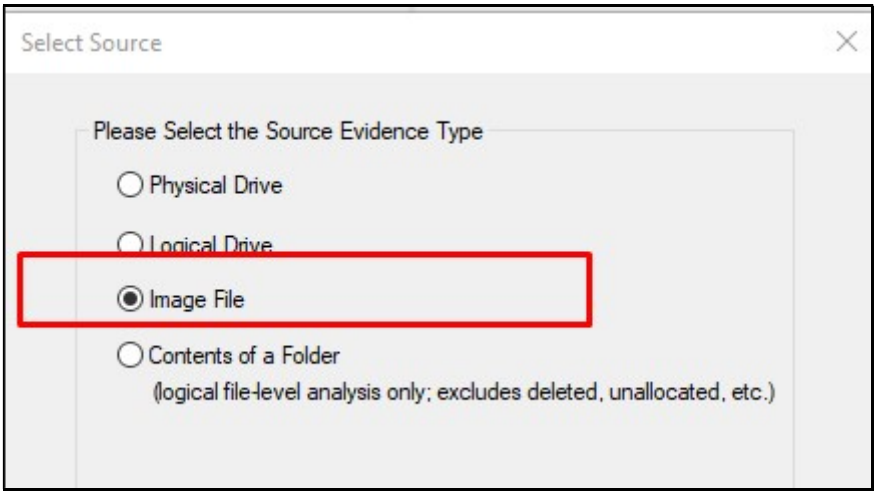


Figure 3

Once mounted, the clue would be to identify any wrong date:

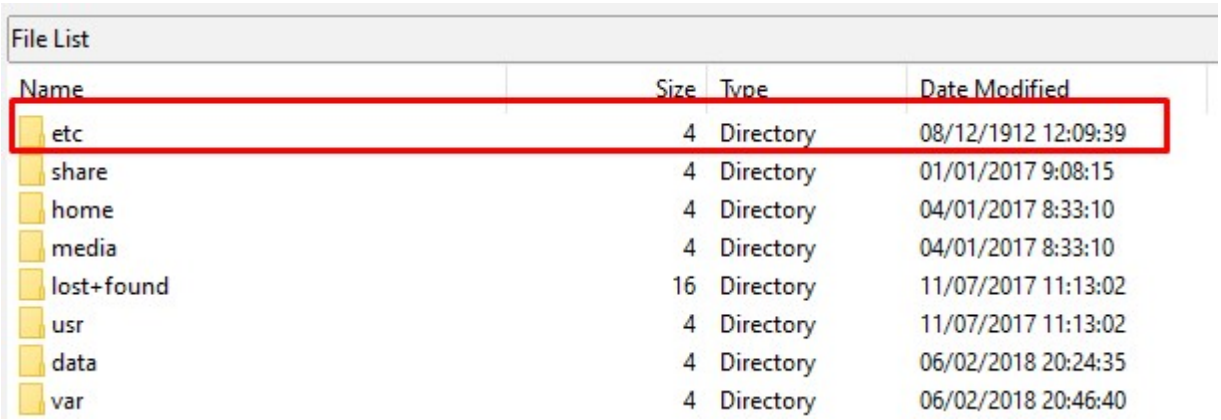
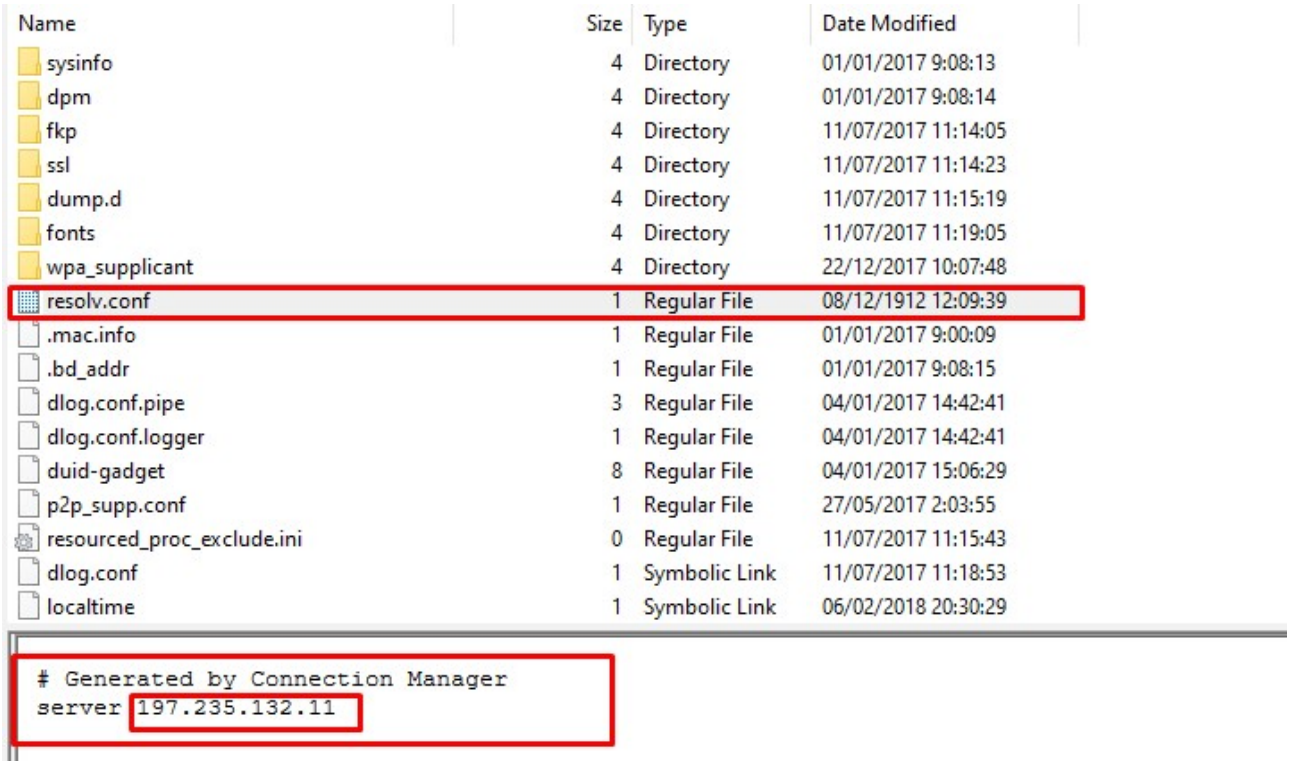


Figure 4

ETC folder contains:



Name	Size	Type	Date Modified
sysinfo	4	Directory	01/01/2017 9:08:13
dpm	4	Directory	01/01/2017 9:08:14
fkp	4	Directory	11/07/2017 11:14:05
ssl	4	Directory	11/07/2017 11:14:23
dump.d	4	Directory	11/07/2017 11:15:19
fonts	4	Directory	11/07/2017 11:19:05
wpa_supplicant	4	Directory	22/12/2017 10:07:48
resolv.conf	1	Regular File	08/12/1912 12:09:39
.mac.info	1	Regular File	01/01/2017 9:00:09
.bd_addr	1	Regular File	01/01/2017 9:08:15
dlog.conf.pipe	3	Regular File	04/01/2017 14:42:41
dlog.conf.logger	1	Regular File	04/01/2017 14:42:41
duid-gadget	8	Regular File	04/01/2017 15:06:29
p2p_supp.conf	1	Regular File	27/05/2017 2:03:55
resourced_proc_exclude.ini	0	Regular File	11/07/2017 11:15:43
dlog.conf	1	Symbolic Link	11/07/2017 11:18:53
localtime	1	Symbolic Link	06/02/2018 20:30:29

```
# Generated by Connection Manager
server 197.235.132.11
```

Figure 5

And finally resolv.conf file was modified to get dns requests. Finally player will able to IP Address: 197.235.132.11

Flag Information

flag{197.235.132.11}