[Case Study] Computer Forensics: Data Extraction From a Raspberry Pi

Editor's note: In this article, SalvationDATA forensic experts will explain the process of forensic data extraction from a Raspberry Pi.

What is Raspberry Pi?

The Raspberry Pi is a small single-board computer in the size of a credit card. It is installed with an operating system based on Linux and designed to promote the teaching of basic computer science in schools. Do not be fooled by its tiny size because it is capable of complicated computing tasks like document processing, video games or playing HD videos.

Because Raspberry Pis are tiny and portable, they are often used by criminals as WiFi base stations. Illegal web links can be pushed to any devices connected to the WiFi network, spreading illegal information to the public.

Analysis

Although it is yet new and rare to use Raspberry Pis as criminal tools, forensic data extraction from a Raspberry Pi is not a very difficult operation.

Most Raspberry Pis' systems are Linux-based and use SD card for data storage, some use memory chips too. We must first check what kind of storage media is installed when faced with a Raspberry Pi investigation. If an SD card is found, we can directly remove the SD card, connect it to a write-blocker and create an image copy. Then use professional equipment to extract and analyze the digital data.

Now let's see how to extract data from a Raspberry Pi by using our DRS(Data Recovery System). You can download DRS Preview from our resources page of the website and have a free trial.

Case Study

Introduction: A criminal case of illegal civil information collection and the spread of illegal information with Raspberry Pis.

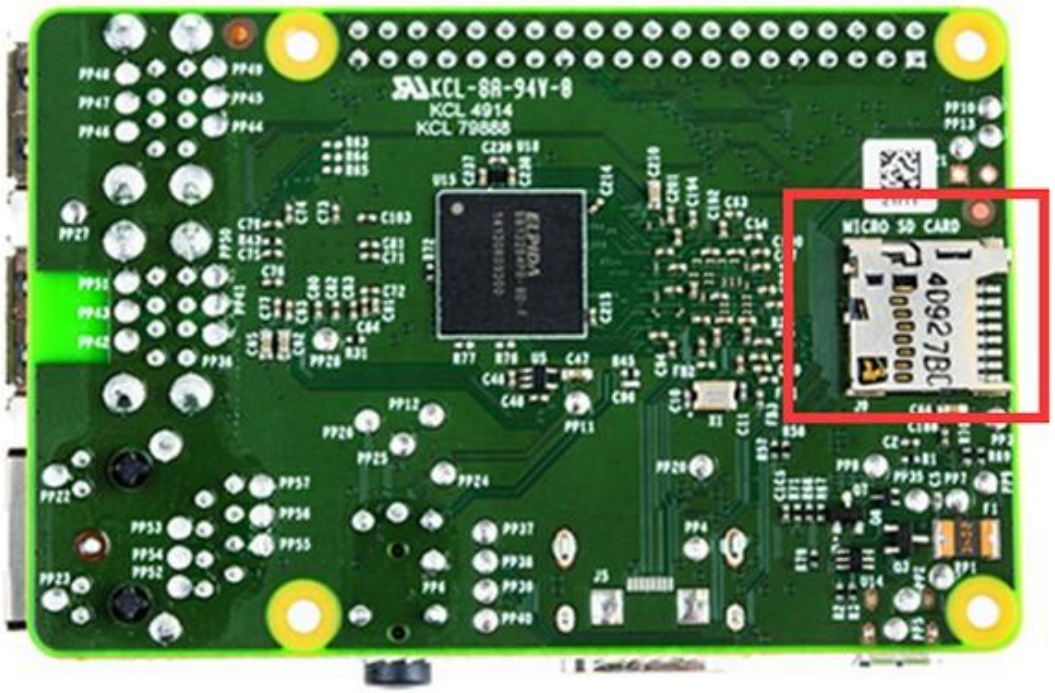
Material: 1 Raspberry Pi

Requirements: Extract and preserve the evidentiary digital data stored in the Raspberry Pi for analysis.

Disassembly and observation

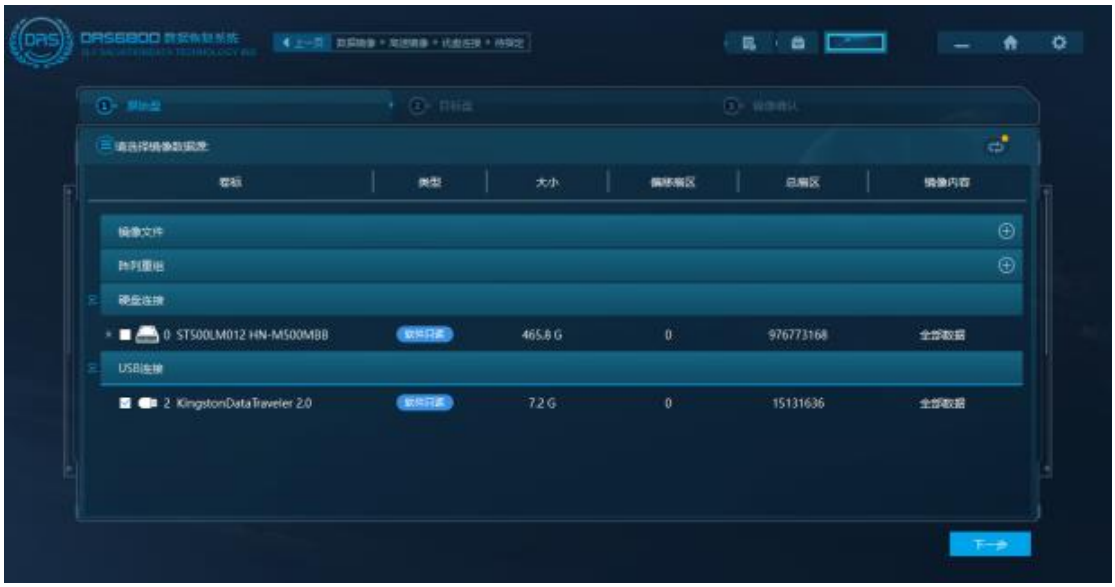
We disassembled the Raspberry Pi, it is equipped with abundant interfaces. And an SD card was identified in a socket on the board, which is used for system and data storage. So the next

step is to extract and preserve the digital data from this SD card.

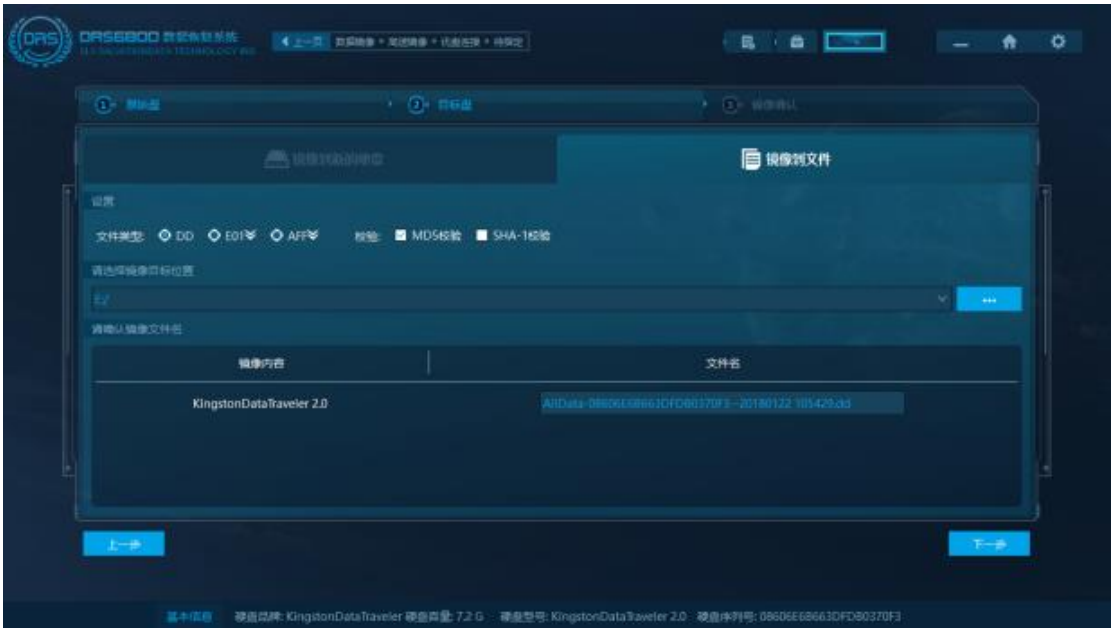


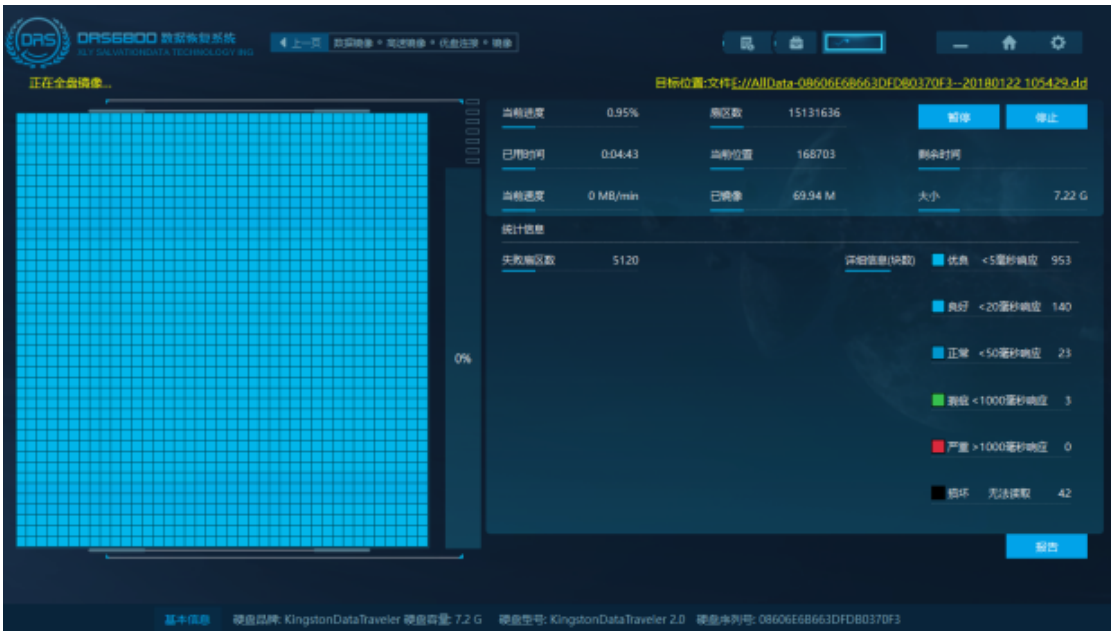
Extraction and preservation

1. First, connect the SD card with a write-blocker, use DRS(Data Recovery System) to create a physical image copy.

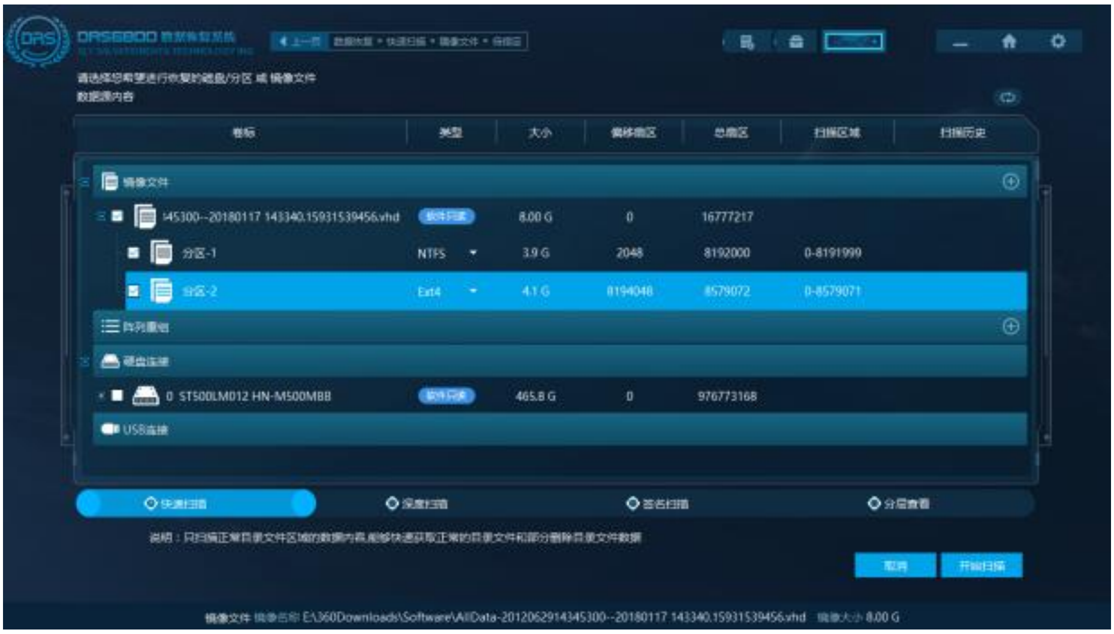


2. Select the SD card as imaging data source, continue to the next step, and check the box of MD5 for HASH calculation.

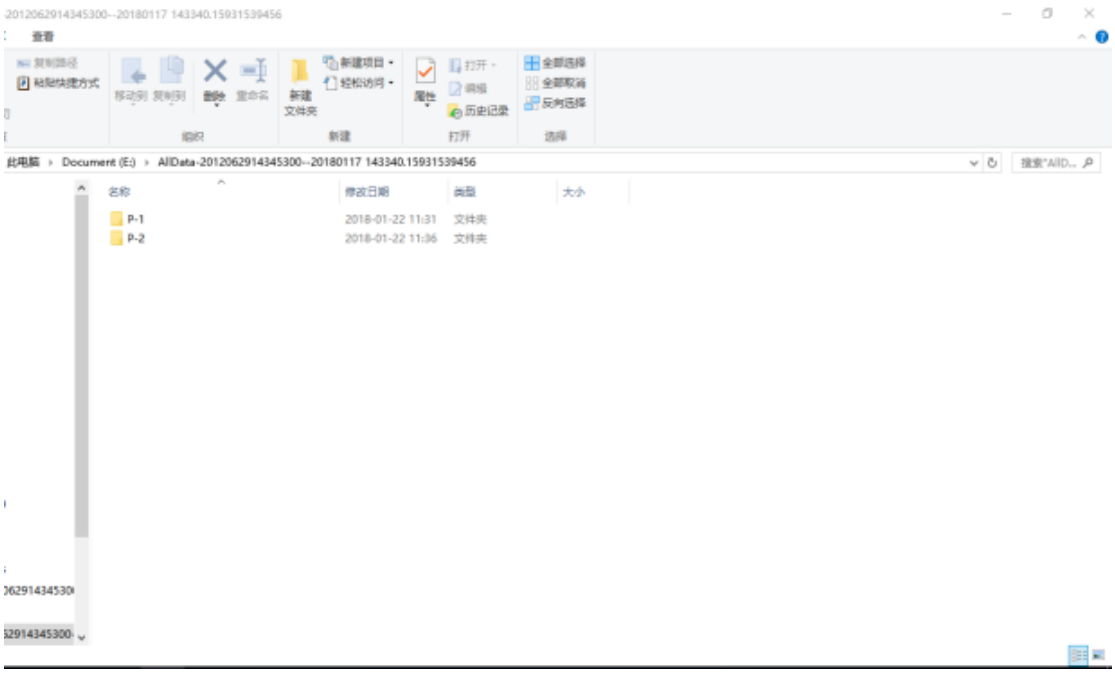




3. After the imaging process is complete, use DRS to scan and analyze the image file for deleted and lost data recovery then exports the data.


分区-1
NTFS
3.9 G
2048
8192000
0-8191999
分区-2
Ext4
4.1 G
8194048
8579072
0-8579071
0 ST500LM012 HN-M500MBB
465.8 G
976773168
E:\360Downloads\Software\AllData-2012062914345300--20180117 143340.15931539456.vhd
8.00 G


Root
$Extend
System Volume Information
lib
lost
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
bin
boot
dev
etc
home
$RECYCLE.BIN
E:\360Downloads\Software\AllData-2012062914345300--20180117 143340.15931539456.vhd
8.00 G



4. After analysis of the exported files, case-relevant data was found in partition 2, home folder.

Conclusion

1. **Most Raspberry Pi operating systems are Linux-based, which uses ext 4 file system to store and manage the data. However, this files system cannot be identified by a Windows operating system. Therefore, a professional forensic tool is required in order to access and analyze the digital data stored in it.**

2. **When creating an image copy of the SD card, make sure not to use a normal card reader to connect it to your PC. Because you may corrupt the important evidentiary digital data, and it's against the digital forensic protocols. Please use a write-blocker.**

3. When conducting a digital forensic investigation with a special device like Raspberry Pi, make sure to learn its structures and how it works before making your moves. Or you may risk losing crucial evidentiary digital data.