[Case Study] Detailed Steps for Extracting Data from Burned & Watered Hard Drive of DVR System

Editor's note: At about 8:00 A.M., September 10th, 2017, explosion occurred in the liquefaction gas station at a certain place in Shandong Province. Local units concerned rushed to the scene for the first time and made a save, and the fire was controlled. During the investigation of cause of the fire, it needs to find the cause of fire by taking the surveillance video of the station, but the DVR and its hard drive were soaked due to firefighting, they could not be powered on directly, local law enforcement submitted this DVR to SalvationDATA for forensic inspection overnight and hoped that we can repair the hard drive and retrieve the evidentiary data therein, so as to provide clues for the explosion case.

After receiving the notice of assisting the case, our forensic experts concentrated on the work immediately, and successfully get video data for the desired period and provide valuable information to the law enforcement for detecting the explosion case.

Details of inspection materials involved in the case:

DVR Brand – Jovision

Hard Drive – West Digital (3T Memory)

Video data needed for the case:

Videos from 6:00 A.M., September 10th, 2017 to the time of the crime

Steps to DVR Forensics for the case:

As the case of surveillance video is involved at this time, attention shall be paid to the following matters for data extraction of the surveillance video case:

First it needs to make the accurate analysis of the state of surveillance video in the needed time period of crime, and several points are mainly included below:

(1) Calibration of standard time, clarifying the difference between surveillance system time and actual standard time.

(2) Analysis on surveillance log, eliminating some uncertain factors, e.g. according to the log analysis, the monitoring host in the time period of crime is powered off so it can confirm that the DVR does not record in the time period of crime.

(3) Confirmation of surveillance channels involved in the case.

(4) Confirmation of surveillance recording cycle.

(5) Confirmation of storage mode: hard drive, RAID, SD card, etc.

(6) Other surrounding circumstances.

Note: the above operations need to be judged under the condition that the DVR can normally be powered on.

2. For the DVR at the fire and explosion scene, its internal hard drive may be damaged by high temperature, soaking, and vibration, so attention shall be paid to several points below during handling:

(1) Take the hard drive, but do not power it on (impurities will be generated in the disk cavity after being fired and soaked, if powered on, the hard drive will be damaged worse, and success rate of its data recovery will be affected).

(2) If water enters the hard drive, for preventing the circuit structure of the hard drive from being rusted, the PCB may be disassembled first and dried at room temperature.

(3) Seek professional engineer to undertake omnidirectional detection in a certain environment.

(4) Deal with the water spots or impurities after opening the drive, and carry out physical repair and firmware recovery according to the corresponding faults.

(5) Select professional forensic tools (For example VIP, DRS, and HPE Pro) for data extraction.

Specific operating process of DVR forensics

DVR processing

By looking at the state of the DVR, it is found that the DVR is in a serious state of damage and fails to be powered on directly for viewing the videos, system log, and other information. Know by system administrators, there is no obvious difference between the surveillance time and the Beijing time, so the decision is to directly disassemble the DVR hard drive for analysis.

TIPS：

Generally, the system log is stored in the DVR. based on that we can know the video data in the needed period of time are normal, lost or overwritten.

Make no mistake: do not connect the original DVR hard drive on the DVR to prevent data rewritten.

External processing of DVR hard drive

The hard drive of the DVR shall be disassembled to find out that the drive is not damaged seriously through appearance inspection, and the status of the most important PCB outside thereof is as follows.

PCB processing of DVR hard drive

The PCB is disassembled and there is water found; trough simple processing, connecting with DRS, showing there is no abnormal, so the PCB is in good condition.

TIPS:

The PCB of the hard drive with water is disassembled to check whether there is water stain if so, this shall be handled by using air blower (pay attention to controlling the temperature) and sponge mat and placing it at the ventilated place for air drying;

If there is a problem on the PCB, the system will give an alarm after DRS is connecting.

Internal processing of DVR hard drive

Opening up the hard drive for processing in the standard clean room through professional tool: HPE Pro, to find out that there is no water stain in the drive cavity, the physical state of the head is good, the platter has no damage and other structures have no obvious damage.

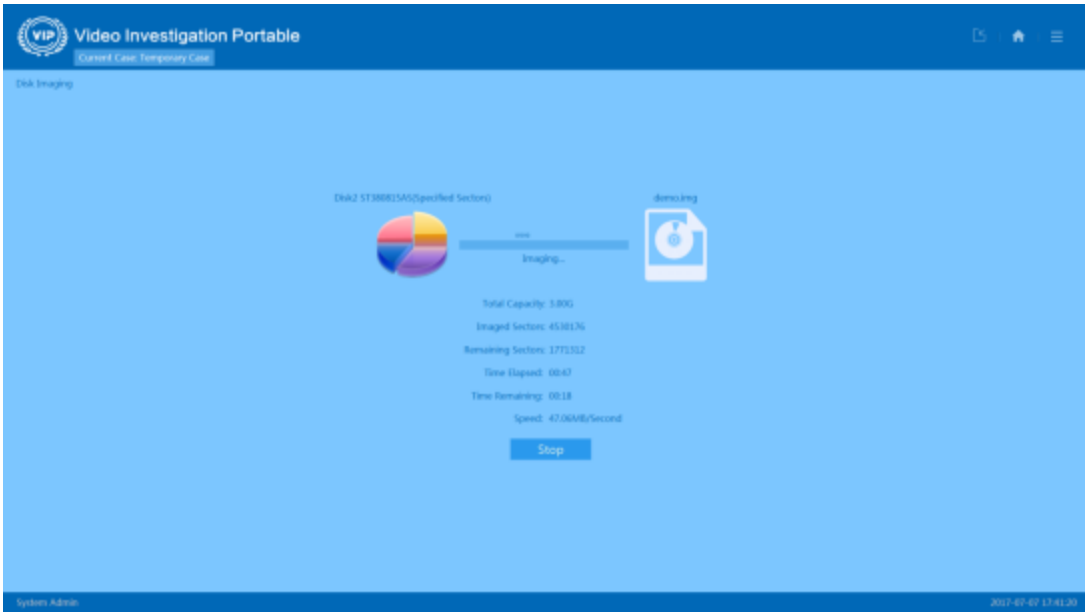
TIPS:

If the head damaged and needs to be replaced with new one, and the platter is badly damaged, the possibility of forensic data recovery will be very low.

Finding the evidentiary video data

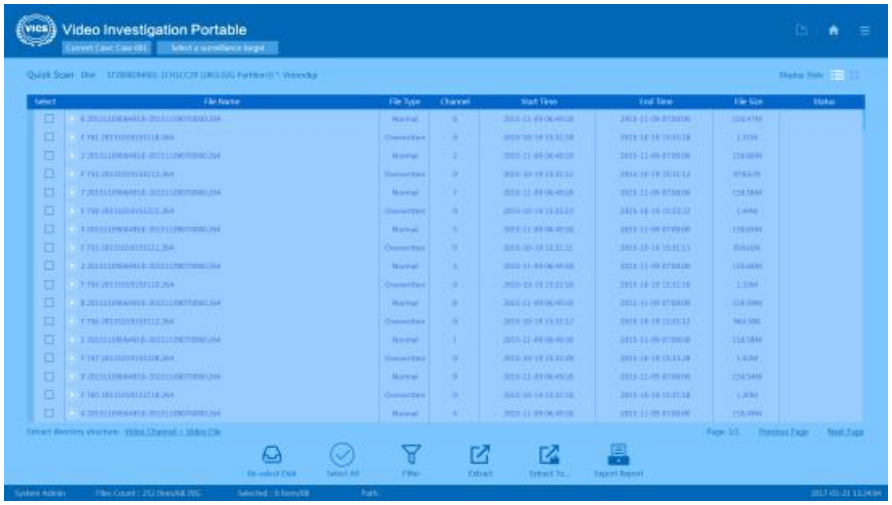
After no problem is found, the hard drive shall be powered on for detection by using DRS. If the hard drive can be identified normally, with the influence of some bad sectors, but there is no problem on data access of the hard drive.

Then we can use VIP for data extraction. Scanning the video data from the hard drive by using VIP, we found that the video data on September 10th exists in one partition thereof. For extracting complete data or avoiding the influence on the bad sectors better, we need use the disk imaging function of VIP to image the whole data and make a hash calculation.



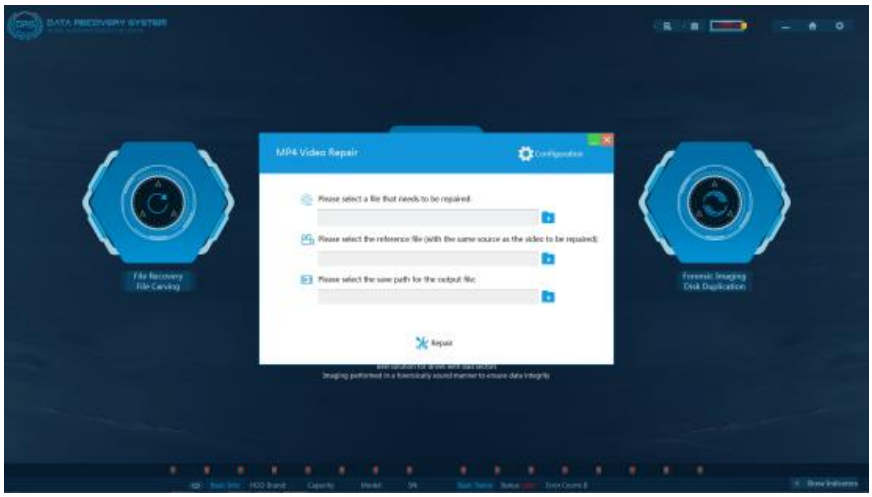
Data extraction

Data extraction shall be carried out through the function of loading image in the VIP, and then the video data in the needed period of time is stored (for finding relevant evidence better, the videos two days before shall also be extracted).



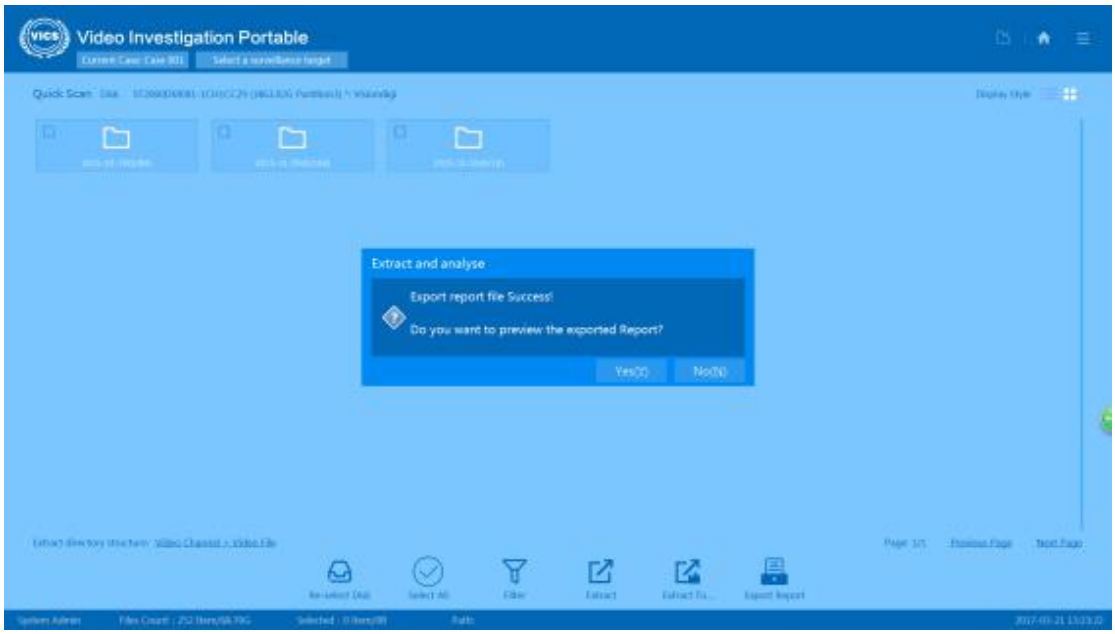
Viewing whether relevant video data can be played normally

Using Ultra-player of VIP to check the video data can be played or not, one video clip cannot be played. We can use MP4 Video Repair tool of DRS to repair, then the video can be viewed normally.



Finding the evidentiary video data successfully and make forensic report

Find out the explosion cause successfully by viewing the relevant videos, generate forensic report through report module of VIP, and combine with the analysis and processing status to make a full inspection report.



Warm tips for dealing with watered hard drive:

1. For this kind of watered hard drive, do not power it on directly.

2. Make a physical inspection of the hard drive first to check whether there is a problem on the hard drive if so, fix it.

3. In case of the operation of replacing the head of hard drive, it is best to image the source drive first to prevent the hard drive from being damaged again during the operation.