JOAQUIM ANGUAS

Serving Search Warrants in Spain

The expert witness's perspective

janguas

31/12/2009

Contents

Abstract

This article describes the most common schema and basic procedure in which search warrants related to computer evidences are served in Spain from the expert witness perspective, and presents a guide, concrete tools, commands and recommendations oriented to maximize the effectiveness and validity of the action.

Glossary

Expert Witness

Procedural law in Spain allows the introduction of facts into a conflict in the form of “expert witnesses proof” (prueba de peritos). In the Spanish Legal System an expert witness is someone that has expert knowledge on a matter related to the case. They can be appointed by court or by the parties in conflict. They issue their results in writing and use to be questioned during the trial act.

Search Warrant

In Spain a search warrant is a court commission to search for evidence related to a case. They use to be produced in criminal procedures, but Spanish law also allows them as precautionary measures in intellectual property, patents or unfair competition cases.

“Comisión Judicial”

A group of persons leaded by the court clerk to serve a court commission is called a “Comisión Judicial”. In the case of search warrants it is constituted by the court clerk together with law enforcement personnel and/or the expert witness(es) if needed. The court clerk attests the action because he/she can act as a legal authority and takes detailed minutes of the whole procedure.

Introduction

Description

In Spain expert witnesses can be appointed by court to serve search warrants. In civil litigation these actions use to be precautionary measures derived from unfair competition actions. In penal prosecution they use to act in less serious crimes, as secrets' discovery and revelation.

When law enforcement specialized units (terrorism, drugs, economic crime, etc) are investigating more serious crimes, they don't rely on expert witnesses but usually get coverage from their own units (scientific police).

Depending on how the judge envisions the action, constrained on how the part or the attorney requests it, expert witnesses receive an assignment to act as assistants for law enforcement or instead they get the required coverage from them to guarantee the action effectiveness. In the first case it would correspond to a case in which there is a current investigation in place and the second could correspond to precautionary measures requested by the plaintiff. In any case it is advisable to let law enforcement do their job as long as it does not interfere with the court assignment.

Expert witnesses have to be and keep independent and impartial during the case. They must disclose any detail that may compromise its independency and/or impartiality and restrain to act in any action they may have any kind of interest in.

The court commission must specify in detail what is being searched and what are the means that can be used to serve it. It may include file names, examples of file contents, file hashes (MD5, SHA), if it allows the search and/or seizure of computers, optical media, etc.

An expert witness appointed to serve a search warrant will have to respond of the outcome of the action and needs to plan it well because these kinds of duties don't forgive errors easily.

In non computer related actions, serving a search warrant is a one step activity. But in this case of study, computer evidence oriented search warrants, the action has to be performed in multiple steps:

1. Material acquisition in the place where the search warrant is served.
2. In-court storage media imaging.
3. Expert witness analysis and result presentation.

The reason why it is split in different steps is that media imaging and analysis are time intensive tasks and tactical and practical issues recommend agility in the service of search warrant.

Steps 1 and 2 are performed under the court clerk legal authority and control. After reviewing the results presentation, the court may require further iteration of step 3.

Structure

This article is structured as follows:

- Basic procedure. It explains how the action is performed.
- Recommendations. Some recommendations regarding how to serve the commission.
- Tools and commands. Review of some effective tools and commands. There are different good approaches to this, but it will focus on the use of a computer forensic distribution to boot the target computer and perform the cloning. The directory and file names in the proposed examples have been redacted but results come from real data.

Basic procedure

Search warrants use to be served in what is called a “commission judicial”. In the proposed scenario it consists of:

- A judicial clerk. He/she will inform those receiving the warrant and take detailed minutes of every action performed to serve it. S/he acts as legal authority and can attest the action.
- Law enforcement agents. Some of them are agents who have prepared the tactics of the action (identification of persons of interest and places, the best time to conduct the action, etc) and some are from specialized units conducting the investigation of the acts being prosecuted.
- One or more expert witnesses. At least one of the expert witnesses is appointed directly from court. The plaintiff may be allowed to appoint an expert witness himself/herself, but s/he has to be properly empowered to be allowed to attend the action. In any case s/he may raise concerns or questions that can get transcript to the minutes but will NOT be allowed to intervene directly in the action.

Action

The “commission judicial” gets constituted when all those appointed by the court are present and the judicial clerk starts taking the minutes.

Once in the place where the warrant is to be served, law enforcement gets access to the place and identifies the person of interest to receive it. The judicial clerk informs him/her about the circumstances that trigger the action, his/her rights, what is going to be searched and how the action is going to be deployed.

The person of interest is asked for computers, storage media or devices that may contain what is being searched. If s/he provides this information, in front of him/her and the judicial clerk, this fact is verified by the expert witness and all gets documented in the minutes. In any case all suspicious media, devices or computers are seized by the expert witness and documented in the minutes, always being proportional, observing the rights of the person receiving the action and obeying what the judge allowed in the search warrant.

All seized material is left in an in-court deposit.

In-court disk clone

Later, the expert witness makes an image copy of the seized material for analysis. The respondent is informed when the copy is being performed and allowed to get a copy at his/her own expense. The image copy is performed in front of the judicial clerk, who takes minutes of the actions performed.

Once the copy is finished all seized material returns to the in-court deposit.

Analysis and result presentation

The expert witness performs the required analysis of the imaged material and presents a report to the court that documents all the process, from the commission constitution to the final result, including all the details that may allow someone else to reproduce all his findings.

It is very important that no information unrelated to the search warrant is disclosed in the result presentation, as this may affect the rights of the person suffering the action. It is better to make indications regarding the possible outcome of further analysis and get confirmation from the court before conducting it than releasing information that may affect the rights of the person suffering the measure.

Recommendations

General

It is very important to always keep in mind what the assignment says and what doesn't. It has to be clear and complete, and if it is not, it is better to seek clarification or raise any concerns to the court in writing.

Also, during the action and the results' presentation, the rights of the person that receives the action have to be kept and the means, actions performed and possible consequences have to be proportional.

Preparation

Preparation is the key to success because while in the action there is not much room for improvisation.

1. You have to get all the information you can regarding the systems you are going to search and/or seize and plan the tools, devices and commands you are going to need to serve the commission. Law enforcement agents or the documentation included in the court proceedings may help you get the case background.
2. Ask the plaintiff (if it is the case) how to identify the object of the search. It is advised that you only get access to the minimum amount of information that identifies the object of the search. If you are searching for a PDF document, the document's name and the file hash is enough.
3. If you are not familiar with the tools, devices or commands you may need to use, you should not be serving the court commission. If you don't feel confident, you'd better find someone else to act in your place. You'd better talk to the judge and let someone else with the needed skills do the job.
4. If you do feel confident, practice, practice, practice: set up a test environment and perform the planed actions on them until you feel you can perform them without risks in a hostile environment. Take into account all possible variations that may appear and be prepared for the unexpected.
5. Prepare checklists in advance for the material and actions.
6. Try to get contact with law enforcement personnel serving the action with you. Tell them what your plan is. Listen to them and raise any concern you may have in advance. Don't leave anything for you that may result in a surprise during the action.
7. Get good rest the night before the action. You'll need to be alert and agile to respond to the problems you will encounter.

Material

Law enforcement uses to bring thin rubber gloves and anti-tampering labels and bags, but you are advised to bring yours just in case.

It is advisable to bring material to have some security that you will be able to respond to some eventualities, but not too much: a heavy load will tire you and reduce your mobility and agility.

You are not supposed to use these, but just in case:

- Mobile access to the internet in case you have to search/download something.
- Some forensics distributions in CD and USB format.
- A cloning device or an IDE/SATA to USB adapter.
- One or more computers (they don't need a hard drive because you'll boot them from the forensics distribution if needed).
- A power strip.
- An Ethernet cable.
- A multitool.
- Some storage media.
- A camera, replacement batteries and its connection cable.
- A crossover Ethernet cable.
- A flashlight.
- A cloth and/or paper tissues.

There's different opinions relating this, but I prefer acting wearing my usual work wear: a suit. Of course you need to feel comfortable working in a suit and expect that you may have to deal with dusty computers and devices, but if you are get to it, in my humble opinion, wearing a suit may help.

Social issues

You are going to get into a place and/or a system the user may not want you in. Getting you access to the place or system and let serve the warrant is law enforcement mission. Let them do their job.

Fortunately in countries that are ruled by law the citizen's rights are preserved. The person suffering the action will have a way to defend his/her point in front of a court.

Your presence and attitude has an influence on how the person receiving the action behaves and, what is more important, the way s/he reacts to it and cooperates or otherwise tries to block the action.

My advice is that it is better to be straight faced (poker face, not angry), be polite and respectful but firm, show a self-confidence calmed attitude but go straight to work and keep in general a neutral professional attitude.

In my experience you use to get what you want if you ask politely.

The person receiving the action may get under arrest so s/he can get questioned in law enforcement offices. Some (the less and the more used to it) take it easy, but others don't. Keep in mind that it is not your fault, your only goal is to serve your assignment while keeping the rights of the parties. If you see any irregularity, you can address the issue in the minutes or in your report to the court.

Passwords and encryption keys

There might be password protected computers or devices and you may need encryption keys to be able to read the content to perform the commissioned analysis of the seized media. If

the computers are turned on, review them for encrypted disks or directories and requests the encryption keys or passwords. Take a dump of the RAM.

Tools and commands

While there are multiple valid approaches to this, I will focus on booting from a computer forensics distribution for the actions of cloning and analyzing the media seized and using an IDE/SATA to USB adapter. In my experience this is a flexible, solid and convenient approach. Performance is about 80GB/hour. If you serve search warrants frequently you may consider getting a disk cloner. Performance for a cloner is about 250GB/hour.

Media clone in court

Procedure

There are two approaches to the cloning: if you only seized the disks but not the complete computer you'll have to connect them to a cloner or an adapter. If you got the whole computer you may boot it to a forensic distribution and perform the cloning.

Most storage media needs disassembly. In the days from the action to the disk clone in court, get all the service manuals of the devices or computers you may have to disassemble.

The action is planned in advance and parties can attend and get their own copy. Get to the court on time. The court clerk receives you in court and starts the cloning minutes. S/he gets or requests the computers, devices or storage media from the in-court deposit.

Depending on the cloning option you prepared, boot the cloning computer or cloner. If needed, in front of the court clerk, extract the disks from the computer, device or enclosure for cloning and process them one by one taking careful minutes of your actions.

Make the court clerk check the computer time and copy the hashes to the minutes.

Once finished, sign the minutes. The court clerk takes the devices back to the in-court deposit.

Command and options

It is recommended to issue a "date" command before and after the cloning command for reference.

The command "dcfldd" is an improvement of command "dd" and is used to clone devices. It copies the contents of the whole device, not only the data on in, but also free space.

"conv=sync,noerror"

This option indicates not to stop at errors, and if there are errors, add zeros to the result so there are no "holes" left in the resulting image.

"hashwindow=0 hashlog=file.txt hash=sha256"

This calculates a hash on the fly for the whole operation to file.txt.

Example

```
ubuntu@ubuntu:~$ date; sudo dcfldd if=/dev/sdc of=/media/disk/CASE_ID/LOCATION_ID/DEVICE_ID.dd
conv=sync,noerror hashwindow=0 hashlog=DEVICE_ID_md5.txt; date

Thu Nov 16 13:18:22 UTC 2009

4883968 blocks (152624Mb) written.
4884090+1 records in
4884091+0 records out

Thu Nov 16 15:26:34 UTC 2009
```

Where CASE_ID is the case identification, LOCATION_ID is the identification for the location where the media was seized and DEVICE_ID is the device identification.

Analysis

Get partition information

The result of a “dcfldd” command can be mounted as a loop device. Disk images may contain more than one partition each. In order to mount loopback, you need to know the starting byte for every partition. You can use command parted to list the starting bytes for every partition in a “dcfldd” image file.

Start command “parted”, set unit to bytes and print the partition table.

Example

```
ubuntu@ubuntu:/media/disk/CASE_ID/DEVICE_ID$ parted DEVICE_ID.dd

WARNING: You are not superuser.  Watch out for permissions.
Warning: Unable to open /media/disk/CASE_ID/DEVICE_ID/DEVICE_ID.dd read-write
(Permission denied).  /media/disk/CASE_ID/DEVICE_ID/DEVICE_ID.dd has been
opened read-only.

GNU Parted 1.7.1
Using /media/disk/CASE_ID/DEVICE_ID/DEVICE_ID.dd
Welcome to GNU Parted! Type 'help' to view a list of commands.

(parted) unit

Unit?  [compact]? B

(parted) print


Disk /media/disk/CASE_ID/DEVICE_ID/DEVICE_ID.dd: 30005821439B

Sector size (logical/physical): 512B/512B

Partition Table: msdos


Number  Start         End           Size          Type      File system  Flags

 1      8225280B      10487231999B  10479006720B  extended               lba

 5      8257536B      10487231999B  10478974464B  logical   ntfs

 2      10487232000B  29997596159B  19510364160B  primary   ntfs         boot


(parted) q
```

Numbers under the “Start” column are the input for the “mount” command when mounting every partition.

Mount

As said, in order to mount the result of “dcfldd” you need to provide the starting byte of the partition you got from the “parted” execution.

Example

```
ubuntu@ubuntu:/media/disk/CASE_ID/DEVICE_ID$ sudo mount -r -o loop,offset=10487232000 -t ntfs DEVICE_ID.dd /media/DEVICE_ID
```

This mounts the partition that starts at byte 10487232000 with type NTFS.

Hash calculation

It is better not to be unnecessary exposed to the contents of the seized media.

It is normally useful to create a list of all the disk contents with the MD5 hash calculated so you can search this file without having to see the rest of the disk.

Example

```
ubuntu@ubuntu:/media/DEVICE_ID$ find $@ ! -type d -print0 | xargs -0 md5sum | tee /media/disk/CASE_ID/LOCATION_ID/DEVICE_ID-PARTITION_ID.md5
```

This calculates the MD5 hash of every file in the partition.

Clean-up

After finishing the case, all data has to be effectively erased.

A case ends when:

- All charges are drop.
- There’s a settlement.
- There’s a final judgment (res judicata).

After the report is presented and while the case is not closed, it is advised to move all data to secondary encrypted storage.

Example

```
ubuntu@ubuntu:/$ sudo dcfldd if=/dev/urandom of=/dev/sda statusinterval=10 bs=10M conv=notrunc
```

This fills the device /dev/sda (the device you want to erase) with random data.