

# The CCTV File Format Minefield

Dr Mark Sugrue

## What you should know:

With 3000+ video file formats in the CCTV industry, viewing footage can be a challenge.

## Learn how to:

Identify formats and the best places to get 3rd party player applications.

The first and often most difficult issue faced by CCTV investigators is simply getting the video evidence to play, but tips and technology can help...

CCTV footage is a rapidly growing source of evidence for Law enforcement agencies. It has surpassed fingerprints and other common evidence sources. The growth in CCTV as a source of evidence has primarily arisen due to a fundamental shift in technology— the move from Analog to Digital surveillance systems. Whilst the technology shift has provided a rich source of evidence, there are some technical issues which can give Law enforcement agencies a headache.

Digital Video Recorders began to replace older Analog CCTV recorders about 15 years ago, and they promised a lot: better quality, ease of use and reliability. One important feature was lost in the changeover: a standard data format.

With Digital Video Recorders it was left to the manufacturer to decide how to actually encode and store the video data. With no proper industry standard to follow, each manufacturer brewed their own file format, and made players to accommodate the format. The result is near chaos.

We at Kinesense have documented more than 1,500 different CCTV video file formats in circulation. This is by no means all the formats that exist, and DVR manufacturers (mainly Chinese and South Korean companies) are producing new formats

on a weekly basis. Our best estimate is that there are a minimum of 2,500 to 3,000 file formats and codecs in existence.

When an investigating officer is handed a disk or USB key containing case-critical CCTV video, he usually needs to first try to identify the file format and spend hours trawling the internet and specialist forums trying to locate the right player software. It is a very time consuming, inefficient process and has huge knock on costs through the whole law enforcement system.

## History: How did we end up with this mess?

The first widely adopted digital video file format was Microsoft's 'AVI' format, released with Windows 3.1 in 1992. AVI is a versatile, and therein lies the problem for CCTV. AVI is a container format; meaning it has a standard file header, but the actual data can be encoded in any way desired. All that's needed is a codec – a small piece of software installed and hidden away on your PC that does the work of decoding the file. The AVI file header contains a four letter code which describes which codec is used, so then Media Player runs off to the Registry, finds the codec software, and plays the file. Great, in theory...

The problem is that 1992 was long before the modern internet. The four character identifier in the AVI header isn't enough to tell the computer where to get the codec if it doesn't happen to be installed already. A four character code (formally called 'FourCC') could be unique – there are over 16 million possible combinations – however, Microsoft never thought to include any way of issuing unique codes or of preventing companies from using a few popular codes. (Actually, this isn't quite fair. Microsoft does ask that manufacturers email them to register new FourCC codes, but there doesn't seem to be any place to look up the full official list; neither does there seem to be any enforcement) There are 835 different AVI codecs in our format database with many companies using the same four characters to represent different codecs.

AVI is only the beginning of this story. There are at least 20 different 'open' video file formats – meaning the layout of the file is publicly available. A few of these are used by DVRs. Flash (flv) and mpg (and its evil twin, VOB) are used by a few manufacturers. Of the open formats, AVI is the most common in CCTV, and within AVI, most manufactures use their own, non-standard, codecs.

That brings us to the nest of vipers that are closed video file formats. Most DVR manufacturers don't even adhere to the loose and flexible AVI standard. They branch out all on their own and make something completely new – and completely incompatible with everyone's format or player. This isn't just a minor irritation – there are now thousands of incompatible and undocumented video formats in circulation, and it is increasingly difficult to simply identify the brand or origin of a video file.

## The Cost of CCTV

CCTV is a powerful tool and, when a crime is caught on camera (and the video quality is good) few other types of evidence are as convincing to a judge or jury. The cost of gathering CCTV evidence is monumental. The UK has one of the highest densities of CCTV cameras of any major country, with an estimated 5 million CCTV cameras – the vast majority of which are privately owned and operated. Other countries may have fewer cameras, but are catching up quickly. A Study by Tayside Police in Scotland has shown that at least 65% of criminal investigations gather CCTV evidence, and a similar study by Cheshire police showed that 75% of that is from 3rd party sources. This means that half of all criminal cases involve video evidence captured from private DVRs (which equates to approximately 900,000 cases in the UK each year).

What is the cost of this to the police? There is no systematic study which quantifies the cost in time or resources of finding and recording or copying CCTV, bringing back to the station or delivering it to the audio-visual department, or even the cost in time and manpower of simply watching it – but that cost must be vast. I have spoken with quite a number of UK bobbies who find that their routine police work is frequently sidetracked by hours spent fiddling with DVRs and attempting to play or retrieve the footage, or simply driving the possibly-important but unplayable video recording in a squad car to the Audio-visual department. The number I have heard anecdotally is an average of two hours per week, per officer. That equates to 5% of each police officer's time, or about 13 million man-hours per year across all 43 UK police forces. This calculation does not include the knock on costs and delays to the back office and technical staff or to case preparation or to the courts.

CCTV need not be this inefficient. DVRs could be designed

with standard formats and user interfaces. Technology does exist to speed up the process of accessing video, of sending it securely (without having to use a squad car!) to a server and for speedily reviewing it. In many forces, audio-visual or computer crime departments end up doing too much of the work that should be done by investigative officers and there are tools available to enable front line officers to do this work.

## CCTV video files: How to view them?

So what can be done when faced with a new and unknown video file from a CCTV DVR? There are a number of tools and clues that can help identify it.

- **Which file is the video file?**

An investigator is typically presented with a CD/DVD or USB key with video evidence. Determining which file on the device is the video file should be straightforward but often it is not. When video is retrieved from the DVR, lots of random log files can also be exported along with the important video files. Sometimes the data arrives in a complex folder tree with the important video files squirreled away up in the high branches of the folder structure. Generally, the video files will be the largest files on the disk. The tool TreeSize Free is handy for quickly scanning the size of folders and subfolders and detecting where the big files are.

- **Can the DVR supply the player software?**

Sometimes, kind and considerate DVR manufactures configure their machines to save a copy of the CCTV player to the disk or USB key when you hit 'export'. Sometimes, this is an option hidden away in a menu. If the DVR can give you the player or codec, perfect. More often than not, the DVR doesn't do this.

- **What is the file extension of the video file?**

The letters or numbers after the final '.' in the video file name are key to identifying it. If the file ends in 'AVI' the next step is to determine what codec the file requires. If it is 'mpeg', 'mpg', 'flv' or one of the other open formats, the file will likely play in a standard movie player such as VLC or Windows Media Player. If it is none of these, the file format is most likely closed and will only play in the manufacturers own software.

- **Identify the AVI Codec?**

For AVI files, the codec is written into the file header. It is possible to look yourself by opening the file in HxD (look at byte position 188) but two fine tools exist to make this easier: MediaInfo and GSpot. Either tool will give you useful information, such as width, height and duration; but the key information is the codec. Maybe 850 different AVI codecs exist. If you find the right one, download it from the manufacturer, and install it correctly, then Windows Media Player should play the file.

Useful sites for finding information on codecs are fourcc.org, Vid-ID.com and media-geek.com (more about these below).

- **Identify a proprietary CCTV file format?**

This one is tough. There are at least 1,500 to 2,000 different proprietary (closed) video file formats in use. If MediaInfo can't open it, and VLC or Windows Media Player can't play it, most likely the file is simply a closed format that can only play in the player software supplied by the DVR manufacturer. There are a few websites that can help identify the format and suggest players to download.

Kinesense's own Vid-ID tool is a good place to start. Just open the website [www.Vid-ID.com](http://www.Vid-ID.com) and select the file you wish to identify. Vid-ID checks its internal database of file formats and emails a list of possible matches to you. For AVI files, you should use the Media-Info application to access the codec name, and then enter that into Vid-ID.

Kinesense also make a handy desktop application called Player Manager which includes an off-line copy of the Vid-ID database and can automatically detect the codec name in AVI files and tell you which codecs are already installed on your PC. It does more than this – it also searches your hard disk to find CCTV players and tells you which one to use for a given file. Player Manager keeps notes on each player, can record tips on how to use it and keep screenshots. When you encounter a new file, and download a new player, it becomes part of the Player Manager database. Player Manager can back up your library of players and let you synchronise the library across different PCs. You can download a free 30 day trial of Player Manager from the Kinesense website.

Alternatively, there are a number of websites which offer long lists of file formats where you can manually look up a file type. Most of these sites are members only, or restricted to police in particular countries.

Media-geek.com is certainly one of the best collections of format and player information available, and includes a wiki with reams of useful information. It is members only, but membership is free of charge and open to forensic investigators in any country.

The London Metropolitan Police have an online DVR and codec database but it is restricted to UK Police only. CCTV-codec.com is a similar site based in Denmark. In the next few months, the FBI is planning to launch their own codec database. This one will be freely accessible to everyone I am told, and will be found at: [www.fbivipr.org](http://www.fbivipr.org).

## Most Difficult Formats

The player applications themselves can be quite a pain, even after you have found a match for that troublesome format. Some players have not been updated in years and only work in XP, Windows 2000 or even earlier incarnations. This is where keeping detailed notes on how to use each player, and sharing this information across the police force reaps rewards. Kinesense's own Vid-ID.com tool gives us a unique insight into which video formats investigators find the most troubling. The online tool is used by thousands of investigators around the world. For all those overworked forensic investigators facing the latest frustrating DVR or video format, rest assured you are not alone – this is a problem shared by police in at least 112 different countries. Google Analytics provides a breakdown of country of origin for (anonymised) website visitors. Visitors from the UK top the poll for using Vid-ID, followed by the US, India, Canada, Japan and, somewhat surprisingly, Tri-

nidad and Tobago! The most searched for formats are .box (used by i3DVR and SAY Security), .bix, .dat, .264 – I interpret these as being the most perplexing formats, rather than the most common.

## The Future

The chief driver of CCTV installations is not government or police, but insurance companies, who offer sizable discounts to clients with CCTV cameras. Strangely, insurance companies don't specify a minimum level of quality – meaning the only pressure on the CCTV owner is cost, and they will almost always buy the cheapest DVR which allows them to claim the insurance discount. The owner buys, installs the system, and then forgets about it until some incident occurs. The true end user is the police who are faced with badly maintained cameras, old DVRs, lost manuals and forgotten passwords. CCTV can often be of such poor quality as to be useless as evidence. Even so, police must spend the time to collect and view this video before they can determine if it is usable.

What is needed is a proper industry standard which specifies a common file format and a minimum level of quality. There is work being done both in the US and EU to write such standards, but they are years away and actual enforcement seems unlikely to be stringent. Even when such a standard is in place, it will be many years, if not decades, before all the older non-standard DVRs are replaced. Again, only the insurance companies truly have the clout to set and enforce such a standard – but while the true end user – the police – continue to shoulder the cost of the current system, neither the insurance companies nor their customers are likely to change.

Despite all this, CCTV can be an excellent source of evidence and it will continue to be used. During this time of tightening police budgets, some modest changes to work practices and adoption of new technology with regards to the collection and reviewing of CCTV presents considerable opportunity for savings.

## Useful Links

- [www.media-geek.com](http://www.media-geek.com) website by LEVA member Larry A. Compton for the Forensic Multimedia Community.
- [www.Vid-ID.com](http://www.Vid-ID.com) A free tool for finding codec and format information
- <http://www.headbands.com/gspot/> G-Spot Codec Information Appliance software
- <http://mediainfo.sourceforge.net/en> MediaInfo tool for identifying codecs
- <http://www.kinesense-vca.com/product/kinesense-player-manager/> Kinesense Player Manager
- [http://www.jam-software.com/treesize\\_free/](http://www.jam-software.com/treesize_free/) TreeSize Free – for scanning folder sizes
- <http://mh-nexus.de/en/hxd/> HxD – for looking at file bytes
- <http://fbivipr.org/> A FBI DVR database (in development).
- <http://cctvcodec.com/> A members only codec database based in Denmark

- <http://www.videolan.org/vlc/index.html> VLC player by VideoLan
- <http://www.fourcc.org/> More information on FourCC codes
- <http://www.doktorjon.co.uk/> CCTV News site



### Author bio

**Dr Mark Sugrue** is Chief Technology Officer of the Video Analytics company Kinesense Ltd and is responsible for new product development. He holds a BSc in Applied Physics from the University of Limerick and a PhD in Video Analytics from the Royal Holloway, University of London. Kinesense has worked with law enforcement and security agencies in Europe and North America for many years and is focused on making CCTV more efficient and easier to use for the police. Kinesense products and services include the video search and reporting products “Kinesense Law Enforcement” and “Covert-Suite”, the free Vid-ID.com tool and Player Manager.

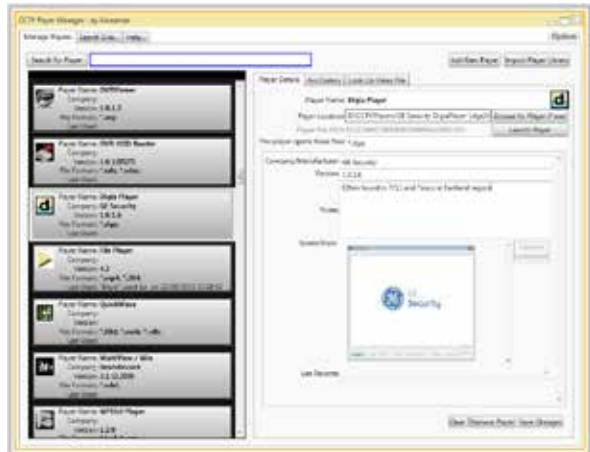
### Figures



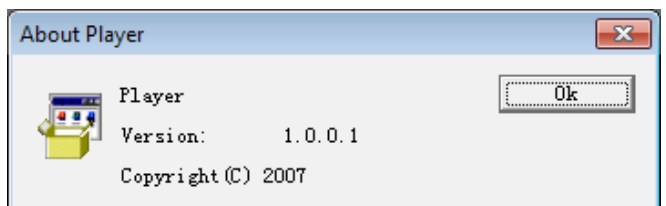
**Figure 1.** Privately operated CCTV can be quite poorly maintained.



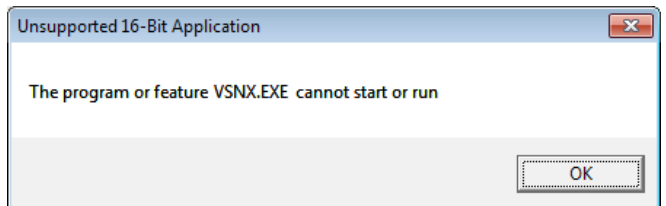
**Figure 2.** “Have you seen this man?” Badly installed CCTV can be next to useless, as in this image released by Blackpool Police in August 2012. <http://www.blackpoolgazette.co.uk/news/cctv-plea-over-attack-at-club-1-4818286>



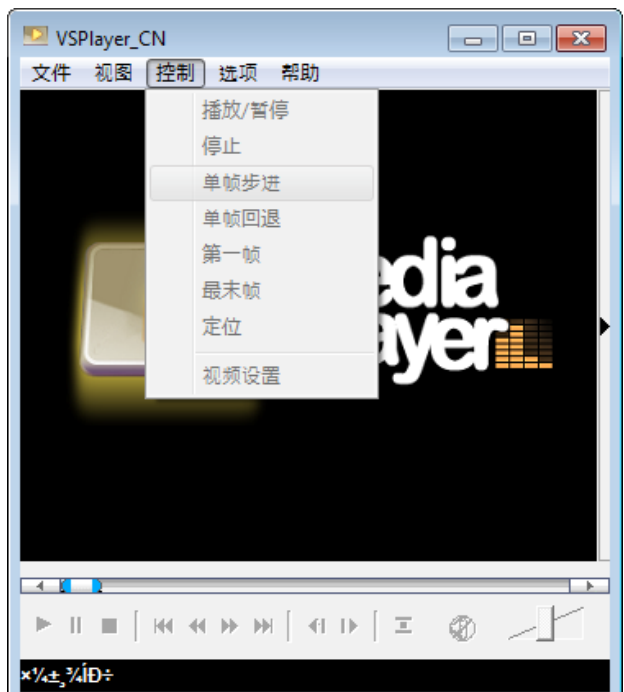
**Figure 3.** Player Manager with a list of players, screenshots and searchable notes on each one.



**Figure 4.** An ‘About Box’ from a player called ‘Player’, providing very little useful information.



**Figure 5.** This error message suggests this CCTV player was designed for Windows 3.1, pre-1995. The DVR is still in use.



**Figure 6.** Many player applications are difficult to use so keeping good notes on how to use players is essential.