C50 Forensic Examination of Video- Information Extracted From Digital CCTV-Systems and Phones

Zeno J. Geradts, PhD, and Rikert Zoun, MS, Netherlands Forensic Institute, Laan van Ypenburg 6, Den Haag, SH 2288 GD, Netherlands*

After attending this presentation, attendees will understand what kind of examinations can be done with digital CCTV-systems and for video extracted from other devices such as phones, and what the limitations are.

The issue in examination of CCTV systems is that there exist many different formats and it is not standardized. With the examination of a new system, this presentation will impact the forensic community and/or humanity by demonstrating how new methods should be tested and validated.

Most new CCTV-systems have been changed from analogue video to digital format. The information from these systems is often used as evidence in court or to visualize what happened at a given time. Since more CCTV systems are placed on streets, shopping centers and many other places, often these systems will have information that is of interest as what actually happened during a particular event. The CCTV-systems can be from government or from private companies; however, digital video is also presented as evidence from other sources, as mobile phones or CCTV-systems that are installed by individuals.

Sometimes the commercial systems have standards such as MPEG- 2 or JPEG streams implemented on them. However, if the systems are proprietary, they might have implemented other methods for storing the information on digital media. By analyzing the raw data, more information on the method of storage is available. Nowadays many of these systems are hard disk recorders, which store information for a given time on the hard disk and then overwrite the hard disk with new information.

An issue compared to the analogue systems is the digital compression that is used. Often the digital compression causes the introduction of artifacts into the video streams. This should be taken into account when making a comparison with a person or doing measurements in the image.

It is important that the evidence is extracted in a proper forensic manner. There exist guidelines from different organizations such as ENFSI, SWGDE, IOCE, and ACPO for analyzing digital evidence, which are also appropriate to the hard disk recorder. One should also take into account the time and date stamps that are used in these system to make a time line analysis. If a severe crime takes place, it is important that all CCTV-information is extracted from this system as soon as possible, since the information might be overwritten. Also the education of the persons that collect this evidence should be taken care of, since due to the many different systems that exist, it is with some of these systems easy to erase the evidence by accident.

The use of biometric software for face comparison, or any other biometric feature is not feasible at the moment in most cases, since images from these systems are typical not under standard conditions. In most cases the examination of the video streams is manual, or with some help of software that will help the examiner to look faster through the video.

Examinations of these systems often require the proprietary player from the manufacturer from which the information is extracted. It is important that all information recorded is really shown during the display of the evidence. Different CCTV-system software is examined and a database in developed for law enforcement.

Sometimes other sources are also used as evidence such as a crime recorded with the camera available on a cell phone. In these cases it is important to examine the integrity of the recordings. It is also possible that erased parts of the memory stick should be examined. When the file is not complete, and headers are missing, efforts should be made to repair the video file. In this presentation cases and methods will be presented for repairing video streams and conducting further analysis.

CCTV, Cameras, Video Streams

 ** Presenting Author*