

detect[®] Incident Library



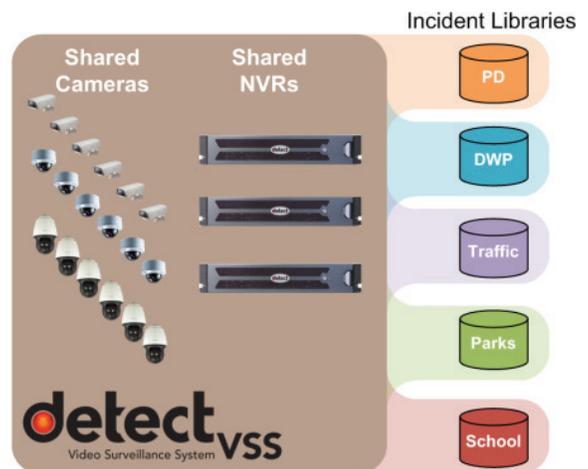
A proactive and collaborative Municipal Video Surveillance System

keeps Public Safety and Communities safe. Protection of video evidence in any small or large-scaled Municipal Video Surveillance System is critical. DETECT[®] Incident Library captures and protects digital evidence and is a feature included with DETECT VMS.

ACCESS to secure surveillance video is made possible within DETECT VMS through user privileges and watermarking of video to ensure authenticity when transitioned to digital evidence. **EXPORTING** Digital Evidence is commonplace in Public Safety agencies and requires authenticity verification when provided to 3rd parties. The DETECT VMS export process includes a Thin Client incident viewer that authenticates digital evidence for 3rd Party use.

The DETECT Incident Library is a collection of events (Incidents) consisting of one or more video clips each with notes, bookmarks, or audio. An Incident is created from surveillance video recorded to a DETECT Network Video Recorder. In some cases an incident is automatically created; as in the DETECT Interview Room feature, or upon a violation generated by video analytics or other stimulus. The DETECT Incident Library is a network share location reachable by the Video Surveillance System and access is controlled by VMS group and user privileges.

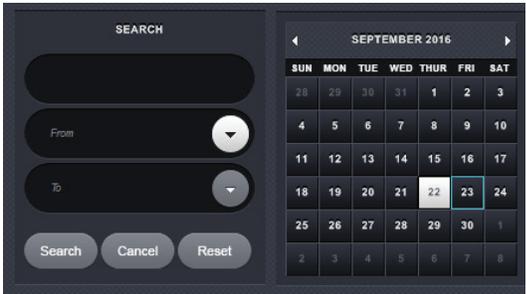
Municipal surveillance systems can be effective and efficient through the sharing of assets. The need for Incident Libraries within a Municipal Wide Surveillance system becomes apparent when considering security and confidentiality needs of individual departments. All departments benefit from shared resources such as network infrastructure, surveillance cameras, Network Video Recorders, and more.



DETECT Network Video Recorders collect surveillance video including associated notes and alarms. Surveillance video becomes digital evidence as a DETECT Incident is created. During this process a meticulous watermarking process that can detect a single bit change is created.

Viewing of Incident Library video is more commonplace than live or recorded video viewing, and extends to those who do not necessarily have access to the Video Surveillance System. Digital evidence can be exported from the Video Surveillance System with watermark validation, or without watermarking or for general consumption.

Finding an incident is made simple with the full text and/or date range search capabilities. Look for incidents related to a date, street, individual, or even notes. The search feature will repopulate the incident library window with any incidents that meet the search criteria. Once found, an incident may be reviewed or exported to removable media.



DETECT VMS ensures the integrity of Incident Library Video from the time of incident creation to viewing, either within the VMS application or through the DETECT Thin Client viewer, which validates incident information. The DETECT Thin Client Incident Viewer possesses the same functionality as the Incident Viewer within the DETECT VMS application, as well as watermark validation. Group and user permissions control access to and export of Incidents. DETECT Incidents are easily exported to removable media or even a network share location. End-user audit logs ensure accountability, while export options address a wide variety of needs. A stenographer may require an MP3 audio file. One or more camera's video within an incident may be exported for publication in a standard media format.



From Human Resource interviews to capturing nuisance and criminal behavior, the DETECT Incident Library is an effective tool to capture, preserve, and protect digital information.

