

# MCSD

## MICROSOFT CERTIFIED SOLUTION DEVELOPER

# DIGITAL EVIDENCE LOCKER®

## MCSD ANALYSIS

### From a Law Enforcement Perspective

More of the information that serves as currency in the judicial process is being stored, transmitted, or processed in digital form.

We have all witnessed an explosive growth in the quantity of digital files collected for evidentiary purposes. This has exacerbated the problem of securely processing, storing and managing photographs, documents, audio and video, and their attendant metadata. CD storage and other WORM media solutions are cumbersome, with Chain of Custody issues for the media itself, and these do not leverage the promise of inter-agency data interoperability. Off-the-shelf 'Multi-Media' solutions and network storage security do not properly account for evidence processing policy enforcement, auditing and verification of evidence file management.

The Justice Data Group (JUDG) offers a comprehensive solution for managing your agency's digital evidence growth pain.

Authenticating the user to the Digital Evidence Locker and RMS, all requests for evidence processing are made to the Locker, which is the master-controller and auditor for the system. A user's access to a particular case is based on RMS permissions; no rights management of the evidence system is required. The system tracks a user's current cases, allowing efficient processing, management and viewing of evidence and case information.

Cryptographic 'DNA' is computed for files as they are processed, and securely stored for verification of authenticity against the original file. Documents, images, audio and video files are processed when the user 'browses' to any local device or network location and selects files for processing. Integration with the department's in-car video data allows users to browse, filter and preview video before adding an event to a case. The associated file metadata is submitted to the database for processing, and the Storage Server processes incoming files for secured network access.

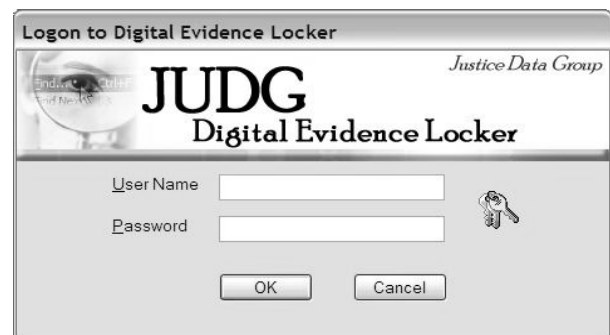
Processing a digital camera captures all photographs on the device, confirming picture sequence, and logging the model and serial number of the camera. Photographs from one camera may be assigned to separate cases; however, the original 'Processed Camera' can be reconstructed for review. All photographic information (f-stop, focal length, etc.) is preserved, and available for review within the client program.

Audited users can submit selected evidence, or entire cases, for processing by Media Robot Servers. The robot burns selected evidence files to optical media generating a web page 'Evidence Log' with active links to the files included on the disc. If the evidence includes specialized video formats, the required viewer program can be burned to disc, also. The disc is labeled with the case number, date and contact information of the intended recipient.

### What is Digital Evidence?

Digital evidence is any information of probative value that is either stored or transmitted in a binary form. This field includes not only computers in the traditional sense but also includes digital audio and video. It includes all facets of crime where evidence may be found in a digital or binary form.

*Scientific Working Group on Digital Evidence (www.fbi.gov)*



### Ease of Deployment and Maintenance

are paramount for a successful IT project in a networked environment. Centrally managed support, alleviating the need for your staff to 'touch' desktop computers, must be envisioned at design-time. The Digital Evidence Locker® client software is easily deployed to workstations from a Windows server. Software updates are verified and automatically applied when a user launches the program. Errors encountered within the system are forwarded to a central repository, which allows our support team to provide proactive support for your users.

### Turn-Around Time and Personnel-Hours Required

for evidence processing and discovery requests are significantly reduced for your agency and your Justice partners. The Courts and District Attorneys are the ultimate consumers of any agency's evidence, and they are delighted to receive access to all digital files for a case, organized as a web page on a secured network or on CD/DVD media.

**Justice Data Group**  
Digital Evidence Locker

2101 N Jordan Ave  
Juneau, AK 99801  
(888) 834-5834  
www.judg.net