

Office of the District Attorney Crime Laboratory
Digital and Multimedia Evidence Unit (DMEU) Software and Hardware

Annual Surveillance Report for July 1, 2022 – June 30, 2023

Section 1: Description of How the Technology Was Used

The technology was used to extract, process, analyze, or enhance data from various types of digital devices (including, but not limited to, computers, cellular phones, tablets, thumb drives, and audio and video equipment) associated with the investigation of a criminal case or activity. The data retrieved included computer files, e-mails, text messages, contacts, digital images, audio and video files, and other multimedia files. All examinations were performed according to limited-scope search warrants, or by consent of the owner. In the reporting period, a total of 11 examiners were authorized to use the technology, and a total of 230 cases were completed.

Section 2: Data Sharing with Outside Entities

Consistent with the Surveillance Use Policy, copies of forensic images and electronic reports were transferred to discs, thumb drives, external hard drives, digital tape, or similar digital medium, for secure dissemination to only the law enforcement customer and/or prosecuting attorney, and the data was also subject to discovery in criminal proceedings.

Section 3: Community Complaints or Concerns about the Technology

The Crime Lab has a procedure for receiving and dispositioning complaints from any source. No complaints or concerns about the Crime Lab's DMEU software and hardware were received in the reporting period.

Section 4: Audits/Policy Violations

The DMEU Supervisor, Crime Lab Director, Assistant Crime Lab Director, and the Crime Lab's Quality Manager are all responsible for compliance with the Surveillance Use Policy, and the policy is shared with all members of the DMEU. The DMEU Supervisor maintains a record that all authorized users have read and understand the Policy. Compliance is monitored, in part, through the routine administrative review of all casework and annual internal audits. There were no identified policy violations in the reporting period.

Section 5: Effectiveness of Achieving Identified Purpose

The Crime Lab does not keep records regarding the outcome of criminal investigations in which the DMEU software and hardware tools are utilized. But from a forensic perspective, in the reporting period, the tools were generally effective for their intended purpose. However, some of the tools are not capable of extracting some data from some high-end, passcode-protected digital devices without using the passcode.

Section 6: Public Records Act Requests

All Public Record Act Requests received by the District Attorney's Office, including the Crime Lab, are handled by members of the District Attorney's Office. No Public Record Act Requests pertaining to the Crime Lab's DMEU software and hardware tools were submitted in the reporting period.

Section 7: Costs Incurred from July 1, 2022 – June 30, 2023

In the reporting period, the DMEU incurred approximately \$1,597,676 in examiner salaries and benefits, and approximately \$118,689 in purchases and software license upgrades. Of this total, two of the examiner positions are funded by the Workers' Compensation Grant (WCG), and approximately 55% of other costs are billed to city Law Enforcement Agencies through Memoranda of Understanding. In the coming year, future costs will be funded by the Crime Lab's FY2024 budget, ongoing WCG, and Law Enforcement Agency revenue, mentioned above. In addition, six software licenses, specifically Magnet Axiom licenses, will be purchased using Paul Coverdell Forensic Science Improvement Program grant funds.